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

JAN 3 9 1989

MEMORANDUM FOR: Edward Jordan, Chairman
Committee to Review Generic Requirements

FROM: James H. Sniezek, Deputy Director
Office of Nuclear Reactor Regulation

SUBJECT: WAIVER OF CRGR REVIEW OF TOPICAL REPORTS WCAP-10271 SUPPLEMENT 2 AND WCAP-10271 SUPPLEMENT 2, REVISION 1 "EVALUATION OF SURVEILLANCE FREQUENCIES AND OUT OF SERVICE TIMES FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM"

Enclosed is a Safety Evaluation Report prepared by NRR which finds that WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1 provide acceptable bases for extending surveillance test intervals (STIs) and allowed outage times (AOTs) for the Westinghouse PWR Engineered Safety Features Actuation System (ESFAS). The Reactor Protection System (RPS) had similar Technical Specification (TS) changes approved in a staff SER dated January 11, 1985.

Based on the CRGR charter, all staff approvals of topical reports should be reviewed by the CRGR. However, since WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1 do not present new methodology beyond that presented in WCAP-10271 or require a new staff position, we believe that CRGR review is not necessary.

If you find that a CRGR review is necessary, please inform us and an appropriate CRGR package will be prepared.

James H. Sniezek

James H. Sniezek, Deputy Director
Office of Nuclear Reactor Regulation

Enclosure:
As stated

CONTACT: Millard Wohl, OTSB
x21181

8901310279 31pp.

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

Mr. Roger A. Newton
Westinghouse Owners Group
Wisconsin Electric Power Company
212 W. Michigan Avenue
Milwaukee, Wisconsin 53201-2909

SUBJECT: WESTINGHOUSE TOPICAL REPORTS WCAP-10271 SUPPLEMENT 2 AND WCAP-10271 SUPPLEMENT 2, REVISION 1, "EVALUATION OF SURVEILLANCE FREQUENCIES AND OUT OF SERVICE TIMES FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM"

Dear Mr. Newton:

We have completed our review of the subject topical reports submitted by the Westinghouse Owners Group by letters dated March 20, 1986 and May 12, 1987. Enclosure 1 provides our Safety Evaluation Report (SER), which was prepared after reviewing the Technical Evaluation Report (TER attached to the SER) developed under contract by Brookhaven National Laboratory. We concur with the findings contained in the TER.

Note: to be provided by NRR staff

As noted in the enclosed SER, applicants for proposed Technical Specification changes for individual plants must:

1. Confirm the applicability of the generic analyses of WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1.

2. Confirm that any increase in instrument drift due to the extended STIs is properly accounted for in the setpoint calculation methodology. (For additional information on this issue, see letter from C. E. Rossi to R. F. Janecek, dated April 27, 1988.)

Enclosure 2 provides an acceptable format for proposed TS Changes based on WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1. Our review of plant-specific changes will consider the applicabilities of the topical reports to the specific plant.

Licensees and applicants are encouraged to propose changes to TS that are consistent with the guidance provided in the enclosures. Proposed license amendments conforming to this guidance will be expeditiously reviewed by the NRC Project Manager for the facility. Proposed amendments that deviate from this guidance will require a longer, more detailed review. Please contact the Project Manager if you have questions on this matter.

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

In accordance with procedures established in NUREG-0390, "Topical Reports Review Status," we request that the Westinghouse Owners Group publish accepted revisions of WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1, both proprietary and non-proprietary, within three months of receipt of this letter. The accepted versions should (1) incorporate this letter and the enclosed Safety Evaluation Report including the Technical Evaluation Report, between the title page and the abstract and (2) include an - A (designated accepted) following the report identification symbols.

Should our acceptance criteria or regulations change so that our conclusions as to the acceptability of the reports are no longer valid, the Westinghouse Owners Group and/or the applicants referencing these topical reports will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the topical reports without revision of their documentation.

Sincerely,

Charles E. Rossi, Director
Division of Operational Events
Assessment
Office of Nuclear Reactor Regulation

Enclosures:
As stated

ENCLOSURE 1

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION REVIEW OF WESTINGHOUSE REPORT WCAP-10271 SUPPLEMENT 2 AND WCAP-10271 SUPPLEMENT 2, REVISION 1 ON EVALUATION OF SURVEILLANCE FREQUENCIES AND OUT OF SERVICE TIMES FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

1.0 SUMMARY

The staff has reviewed the Westinghouse Topical Reports WCAP-10271, Supplement 2 and WCAP-10271 Supplement 2, Revision 1 "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System", supported by the Westinghouse Owners Group (WOG) for purposes of proposing extensions of surveillance test intervals (STIs) and test and maintenance allowed outage times (AOTs) for the Engineered Safety Features Actuation System (ESFAS).

Specifically, bases were provided for increasing the STI for the analog channels from 1 month to 3 months; no STI changes were requested for the combinational logic, or the master or slave relays.

It was also proposed that 1) the AOTs for test for the analog channels be increased from 2 hours to 4 hours for both solid state and relay systems, 2) the AOTs for test for all components be increased to 4 hours in solid state systems, and 3) in relay systems, the AOTs for test for the logic trains and master relays be increased to 8 hours and for the slave relays to 12 hours.

Additionally, it was requested that the AOT for maintenance for all components be extended to 12 hours for both relay and solid state systems. All components except the analog channels would be in bypass during the maintenance AOT, with an analog channel tripped after spending 6 hours in bypass.

Finally, it was requested that a staggered test requirement not be implemented for analog channels in the ESFAS and that this requirement be removed for analog channels in the Reactor Protection System (RPS) (Ref. 1), many of which are common with ESFAS channels.

The staff has concluded that the analyses presented in WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1, augmented by a Brookhaven National Laboratory (BNL) technical evaluation report (TER) are acceptable for resolving the STI and AOT extension issues, subject to any limitations and conditions presented herein.

Additionally the staff concludes that a staggered test strategy is no longer required for RPS analog channel testing, as originally stipulated in Ref. 1.

2.0 BACKGROUND

Item 4.5.3 of Generic Letter 83-28 (Ref. 2) requested that all licensees and applicants review the existing RPS on-line functional test intervals required by Technical Specifications (TS). They are to ensure that current and proposed intervals (Ref. 1) for such testing are consistent with a goal of achieving high RPS availability. Extensions to RPS STIs have been granted for Westinghouse PWR plants.

The ESFAS shares some common instrumentation with the RPS. On the average, the number of ESFAS analog channels sensing either process or nuclear parameters is 58, with 20 channels dedicated to the ESFAS and 38 channels common between ESFAS and RPS. It is therefore worthwhile from an operational viewpoint to consider extensions of STIs for all ESFAS analog channels. Additionally, plant operational effectiveness is enhanced by considering STI extensions for the ESFAS logic cabinets and master and slave relays. At the same time, consideration of extension of test and maintenance AOTs will allow more effective test and maintenance operations. This will reduce human error rates in these activities and the number of inadvertent actuations of engineered safety features.

3.0 APPROACH

The Westinghouse Owners Group (WOG) approached resolution of this issue generically. The unavailabilities of the ESFAS signals were calculated by Westinghouse/WOG (Ref.'s 3 and 4) for both relay and solid state systems. The analyses show that the unavailabilities of the relay and solid state ESFAS signals are of similar magnitude.

The WOG originally evaluated the impact of the proposed STI and AOT changes on core damage frequency (CDF) and public health risk on the Millstone Unit 3 plant. This plant has a solid state ESFAS with 2-out-of-4 (2/4) logic. The staff and its contractor, Brookhaven National Laboratory (BNL), had a concern that Millstone Unit 3 might not fully bound the change in CDF due to the proposed STI and AOT changes for all Westinghouse plants. Some plants have either a 2-out-of-3 (2/3) logic or a combination which may have higher unavailability than that associated with a 2/4 logic such as at Millstone Unit 3. In response to this concern, Westinghouse performed an analysis, documented as WCAP-10271 Supplement 2, Revision 1, Addendum 2 to determine the effect on the change in the Millstone 3 CDF of an assumed change of the ESFAS logic from 2/4 to 2/3. This resulted in a CDF increase for the 2/3 logic over the 2/4 logic of less than 1 percent of the base case CDF for the solid state system. The staff concludes that the relay plants would exhibit similar relative CDF changes with respect to the impact of 2/3 vs. 2/4 logic.

4.0 NRC ACTION

The staff engaged the services of Brookhaven National Laboratory (BNL) to review the approach used and the analyses performed in the Westinghouse reports. This

review was performed to determine the adequacy of the methods used to establish the technical bases for the proposed modifications of STIs and AOTs for the Westinghouse PWR ESFAS instrumentation and actuation relays.

The BNL review calculations yielded, for the proposed ESFAS STI/AOT changes, a CDF increase of 2.8% for solid state plants, which is in good agreement with the 2.4% increase calculated by the WOG.

BNL performed a variety of parametric CDF increase calculations. Among the results was a relay plant CDF increase of 4% assuming concurrent slave relay testing. Another BNL sensitivity study yielded a CDF increase of 5.7%, assuming a very conservative sequential testing scheme which is not used in practice.

BNL also determined that use of Millstone Unit 3 as a reference plant may not fully bound the change in CDF due to the proposed STI/AOT changes because of its 2/4 ESFAS logic, which yielded the 2.4% CDF increase. The 2/3 ESFAS logic WOG analysis, discussed earlier, yielded a 3.3% CDF increase.

The staff concludes, therefore that an overall upper bound for the CDF increase due to the proposed STI/AOT changes is less than 6% for Westinghouse PWR plants. The staff also concludes that actual CDF increases for individual plants are expected to be substantially less than 6%. The staff considers this CDF increase to be small compared to the range of uncertainty in the CDF analyses and therefore acceptable.

Based on the Westinghouse/WOG analyses and the BNL audit and sensitivity analyses, the staff concludes that the proposed STI and AOT changes for the ESFAS would have only a small and therefore acceptable impact on plant risk. BNL issued a technical evaluation report (Enclosure to this Safety Evaluation) presenting the details and results of its reviews.

Additionally the staff concludes that a staggered test strategy need not be implemented for ESFAS analog channel testing and is no longer required for RPS analog channel testing, as originally stipulated in Ref. 1. This is based on the small relative contribution of the analog channels to RPS/ESFAS unavailability, process parameter signal diversity, and normal operational test spacing.

5.0 CONCLUSIONS

Based on a review of the BNL technical evaluation report (TER), the staff concludes that a 6% CDF increase due to the proposed STI/AOT extensions represents an upper bound. For realistic testing strategies, the CDF increase will be substantially less than this. The staff therefore concludes that the analyses presented in WCAP-10271 Supplement 2 and WCAP-10271 Supplement 2, Revision 1, augmented by the TER, form an acceptable basis for increasing the STI for ESFAS analog channels from 1 month to 3 months.

Additionally, the staff finds that 1) AOTs for test for the analog channels may be increased from 2 hours to 4 hours for both solid state and relay systems, 2) the AOTs for test for all components may be increased to 4 hours

in solid state systems, 3) The AOTs for test for the logic trains and master relays may be increased to 8 hours and the AOT for the slave relays to 12 hours in relay systems, and 4) the AOT for maintenance for all components may be extended to 12 hours for both relay and solid state systems. Additionally, all components except the analog channels are to be in bypass during the maintenance AOT, with an analog channel tripped after spending 6 hours in bypass.

Further, the staff will not require a staggered test strategy for ESFAS analog channel testing, and will no longer require a staggered test strategy for RPS analog channel testing, as stipulated in the staff SER of February 21, 1985 (Ref. 1). The removal of the staggered test requirement is based on the small relative contribution of the analog channels to RPS/ESFAS unavailability, process parameter signal diversity, and normal operational test spacing, which is neither staggered nor sequential, but yields some of the benefits of staggered testing.

Table 1 lists plant-specific conditions that each licensee or applicant must meet to make any proposed STI or AOT changes fully acceptable. Table 2 summarizes the approved changes.

6.0 REFERENCES

1. Safety Evaluation by the Office of Nuclear Reactor Regulation WCAP-10271, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," February 21, 1985.

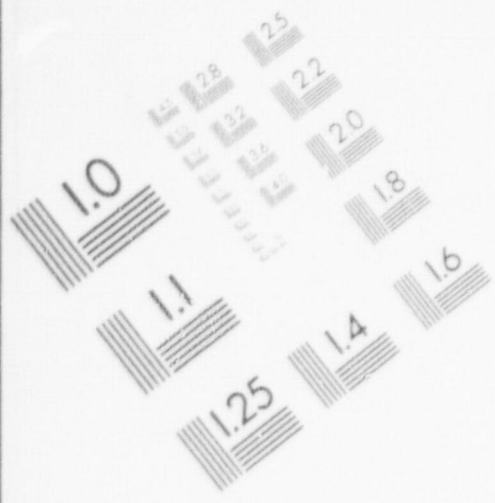
2. Eisenhut, D. G., NRC Letter to All Licensees of Operating Reactors, Applicants for Operating License, and Holders of Construction Permits, "Requested Actions Based on Generic Implications of Salem ATWS Events," July 8, 1983.

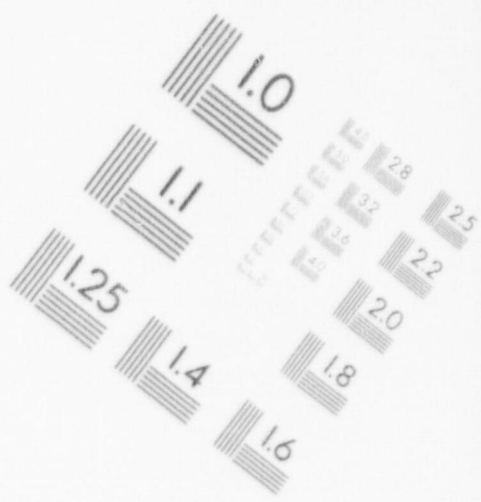
3. Andre, G. R., Howard, R. C., Jansen, R. L., and Leonelli, K., "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271, Supplement 2, February 1986.

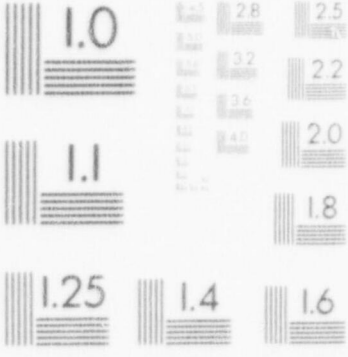
4. Andre, G. R., Howard, R. C., Jansen, R. L., and Leonelli, K., "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271, Supplement 2, Revision 1, March 1987.

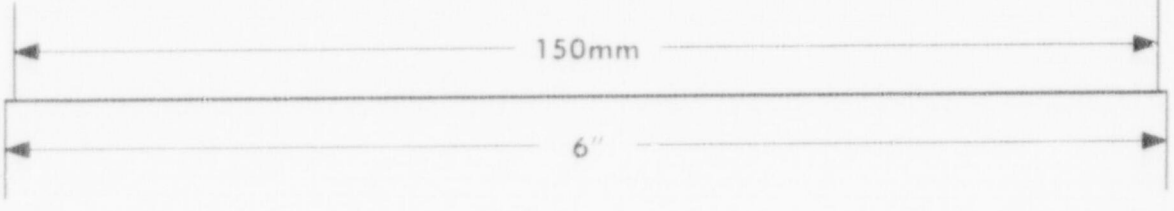
1

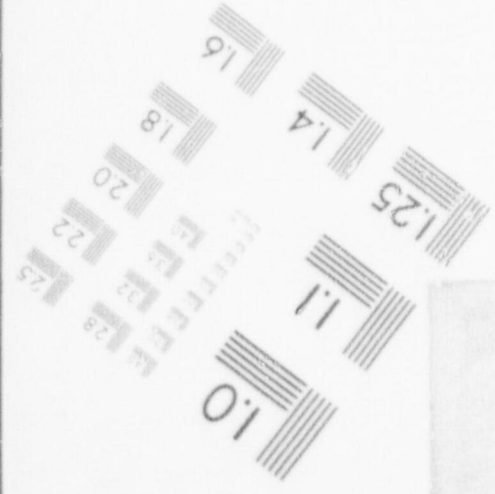
IMAGE EVALUATION TEST TARGET (MT-3)

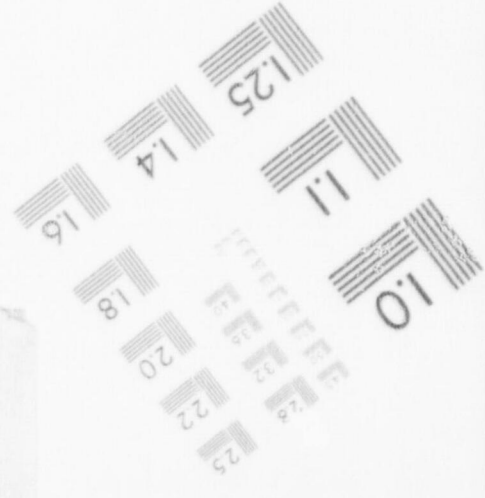


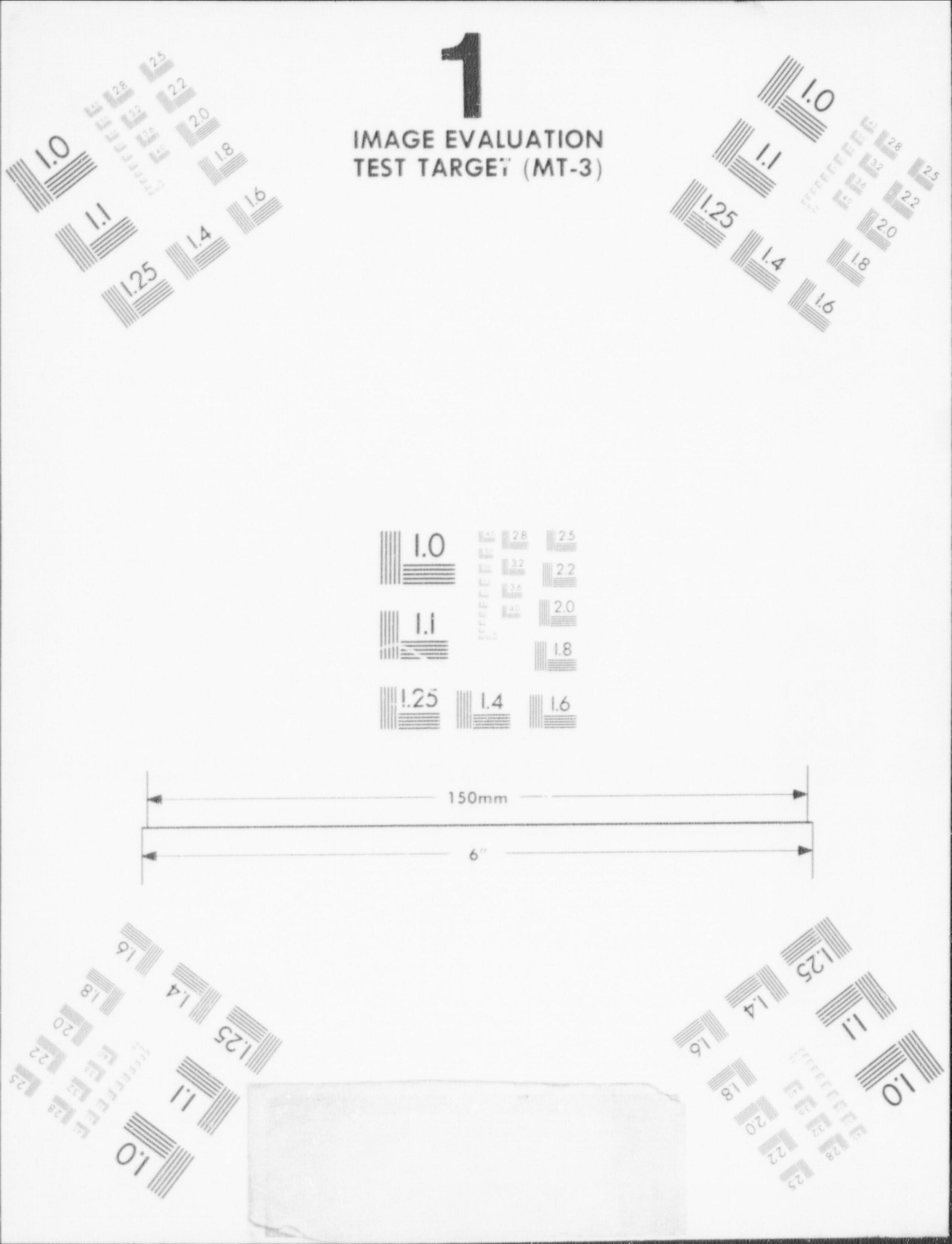











1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

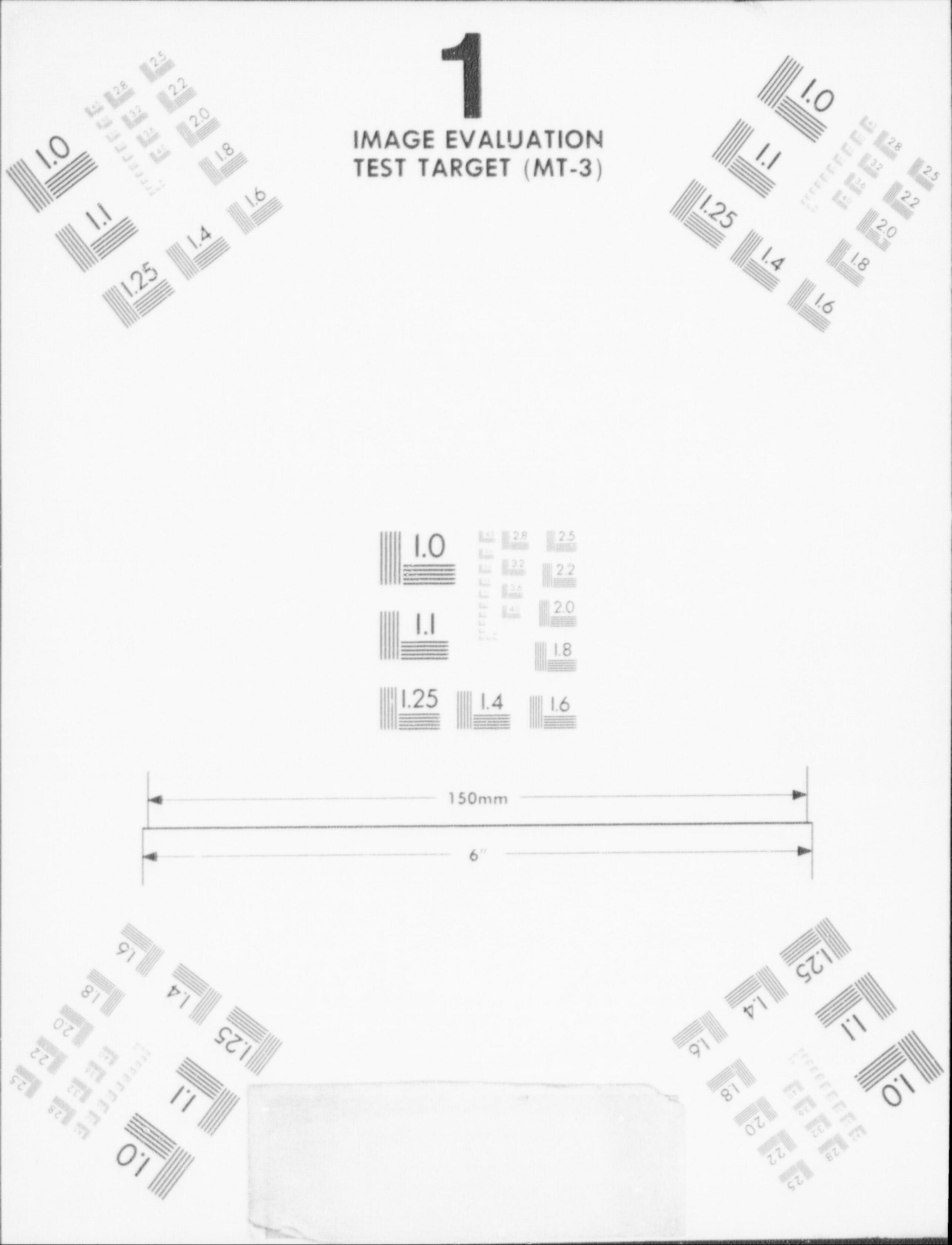

1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

TABLE 1

CONDITIONS TO CLOSE OUT PLANTS

For plant-specific application of the TS changes for the Engineered Safety Features Actuation System (ESFAS) that are proposed, the licensee must:

(1) Confirm the applicability of the generic analyses to the plant.

(2) Confirm that any increase in instrument drift due to the extended STIs is properly accounted for in the setpoint calculation methodology. (For additional information on this issue, see letter from C. E. Rossi to R. F. Janecek, dated April 27, 1988.)

TABLE 2

APPROVED SURVEILLANCE TEST INTERVAL (STI) AND ALLLOWED OUTAGE TIME (AOT) CHANGES

	RELAY SYSTEM	SOLID STATE SYSTEM
LOGIC CABINETS		
STI	1 mo → 1 mo	2 mo → 2 mo
TEST AOT	3 hr → 8 hr	1.5 hr → 4 hr
MAINTENANCE AOT	2 hr → 12 hr	2 hr → 12 hr
MASTER RELAYS		
STI	1 mo → 1 mo	2 mo → 2 mo
TEST AOT	3 hr → 8 hr	1.5 hr → 4 hr
MAINTENANCE AOT	6 hr → 12 hr	2 hr → 12 hr
SLAVE RELAYS		
STI	3 mo → 3 mo	3 mo → 3 mo
TEST AOT	6 hr → 12 hr	4 hr → 4 hr
MAINTENANCE AOT	6 hr → 12 hr	2 hr → 12 hr
ANALOG CHANNELS		
STI	1 mo → 3 mo	1 mo → 3 mo
TEST AOT	2 hr → 4 hr	2 hr → 4 hr
MAINTENANCE AOT	1 hr → 12 hr	1 hr → 12 hr

WESTINGHOUSE CLASS 3

ENCLOSURE 2

APPENDIX A1
PROPOSED CHANGES TO STANDARD TECHNICAL SPECIFICATIONS†

INSTRUMENTATION

3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

LIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels and interlocks shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

a. With an ESFAS instrumentation channel or interlock trip setpoint less conservative than the value shown in the Allowable values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint value.

b. With an ESFAS instrumentation channel or interlock inoperable, take the ACTION shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel and interlock and the automatic actuation logic and relays shall be demomstrated OPERABLE by the performance of the engineered safety feature actuation system instrumentation surveillance requirements specified in Table 4.3-2.

4.3.2.2 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one train such that both trains are tested at least once per 36 months and one channel per function such that all channels are tested at least once per N times 18 months where N is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

† Changes underlined

TABLE 3.3-3

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
1. SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER.					
a. Manual Initiation	2	1	2	1, 2, 3, 4	19
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
c. Containment Pressure-High	3	2	2	1, 2, 3	20*
d. Pressurizer Pressure-Low	4	2	3	1, 2, 3#	20*
e. Differential Pressure Between Steam Lines - High				1, 2, 3##	
1) Four Loop Plant					
Four Loops Operating	3/steam line	2/steam line any steam line	2/steam line		20*
Three Loops Operating	3/operating steam line	1###/steam line any operating steam line	2/operating steam line		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
11) Three Loop Plant					
Three Loops Operating	3/steam line	2/steam line twice and 1/3 steam lines	2/steam line		20*
Two Loops Operating	3/operating steam line	2### /steam line twice in either operating steam line	2/operating steam line		16
f. Steam Flow in Two Steam Lines-High				1, 2, 3##	
1) Four Loop Plant					
Four Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Three Loops Operating	2/operating steam line	1### /any operating steam line	1/operating steam line		16

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
ii) Three Loop Plant					
Three Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Two Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16
Coincident With Either T_{avg}--Low-Low				1, 2, 3##	
1) Four Loop Plant					
Four Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 3 loops		20*
Three Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any two operating loops		16

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
ii) Three Loop Plant					
Three Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops		20*
Two Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in operating loop		16
Or, Coincident With Steam Line Pressure-Low				1, 2, 3##	
1) Four Loop Plant					
Four Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 3 loops		20*
Three Loops Operating	1 pressure operating loop	1### pressure in any operating loop	1 pressure in any 2 operating loops		16

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER (Continued)					
11) Three Loop Plant					
Three Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 2 loops		20*
Two Loops Operating	1 pressure/ loop	1### pressure in any operating loop	1 pressure any operating loop		16
2. CONTAINMENT SPRAY					
a. Manual	2	1 with 2 coincident switches	2	1, 2, 3, 4	19
b. Automatic Actuation Logic and actuation Relays	2	1	2	1, 2, 3, 4	14
c. Containment Pressure-- High-High	4	2	3	1, 2, 3	17
3. CONTAINMENT ISOLATION					
a. Phase "A" Isolation					
1) Manual	2	1	2	1, 2, 3, 4	19
2) Safety Injection	See 1 for above for all Safety Injection initiating functions and requirements.				

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
CONTAINMENT ISOLATION (continued)					
3) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
b. Phase "B" Isolation					
1) Manual	2	1 with 2 coincident switches	2	1, 2, 3, 4	19
2) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
3) Containment Pressure--High-High	4	2	3	1, 2, 3	17
c. Purge and Exhaust Isolation					
1) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	18
2) Containment Radioactivity-High	4	2	3	1, 2, 3, 4	18
3) Safety Injection	See 1 above for all Safety Injection initiating functions and requirements.				

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION					
a. Manual	1/steam line	1/steam line	1/operating steam line	1, 2, 3	24
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3	22
c. Containment Pressure--High-High	4	2	3	1, 2, 3	17
d. Steam Flow in Two Steam Lines--High				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Three Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16
ii) Three Loop Plant					
Three Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Two Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION (continued)					
Coincident With Either T_{avg}--Low-Low				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 3 loops		20*
Three Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any two operating loops		16
ii) Three Loop Plant					
Three Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops		20*
Two loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any operating loop		16

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION (continued)					
Or, Coincident With					
Steam Line Pressure-Low				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 3 loops		20*
Three Loops Operating	1 pressure/ operating loop	1### pressure in any operating loop	1 pressure in any 2 operating loops		16
ii) Three Loop Plant					
Three Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 2 loops		20*
Two Loops Operating	1 pressure/ operating loop	1### pressure in any operating loop	1 pressure any operating loop		16
5. TURBINE TRIP & FEEDWATER ISOLATION					
a. Steam Generator Water Level-- High-High	3/stm. gen.	2/stm. gen. in any operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2	20*
b. Automatic Actuation Logic and Actuation Relay	2	1	2	1, 2	22

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
6. AUXILIARY FEEDWATER					
a. Manual Initiation	2	1	2	1, 2, 3	23
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3	22
c. Stm. Gen. Water Level-Low-Low					
i. Start Motor-Driven Pumps	3/stm. gen.	2/stm. gen. in any operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
ii. Start Turbine-Driven Pump	3/stm. gen.	2/stm. gen. in any 2 operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
d. Undervoltage-RCP Start Turbine-Driven Pump	4-1/bus	2	3	1, 2	20*
e. Safety Injection Start Motor-Driven Pumps and Turbine-Driven Pump	See 1 above for all Safety Injection initiating functions and requirements				
f. Station Blackout Start Motor-Driven Pumps and Turbine-Driven Pump	2	1	2	1, 2, 3	19

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
AUXILIARY FEEDWATER (Continued)					
g. Trip of Main Feedwater Pumps Start Motor-Driven Pumps and Turbine-Driven Pump	2/pump	1/pump	1/pump	1, 2	19
7. AUTOMATIC SWITCHOVER TO CONTAINMENT SUMP					
a. RWST Level - Low	4	2	3	1, 2, 3, 4	17
Coincident With					
Containment Sump Level - High	4	2	3	1, 2, 3, 4	17
And					
Safety Injection	See 1 above for Safety Injection initiating functions and requirements				
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
8. LOSS OF POWER					
a. 4 kv Bus Loss of Voltage	4/Bus	2/Bus	3/Bus	1, 2, 3, 4	20*
b. Grid Degraded Voltage	4/Bus	2/Bus	3/Bus	1, 2, 3, 4	20*

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INTERLOCKS					
a. Pressurizer Pressure, P-11	3	2	2	1, 2, 3	21
b. Low-Low T_{avg}, P-12	4	2	3	1, 2, 3	21
c. Reactor Trip, P-4	2	2	2	1, 2, 3	23

WESTINGHOUSE CLASS 3

TABLE 3.3-3 (Continued)

TABLE NOTATION

Trip function may be blocked in this MODE below the P-11 (Pressurizer Pressure Interlock) setpoint.

Trip function may be blocked in this MODE below the P-12 (Low-Low T_{avg} Interlock) setpoint.

The channel(s) associated with the protective functions derived from the out of service Reactor Coolant Loop shall be placed in the tripped mode.

* The provisions of Specification 3.0.4 are not applicable.

ACTION STATEMENTS

ACTION 14 With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in COLD SHUTDOWN within the following 30 hours; however, one channel may be bypassed for up to 4 (8)* hours for surveillance testing per Specification 4.3.2.1, provided the other channel is OPERABLE.

ACTION 15 Deleted

ACTION 16 With a channel associated with an operating loop inoperable, restore the inoperable channel to OPERABLE status within 6 hours or be in at least HOT STANDBY within the next 6 hours and in at least HOT SHUTDOWN within the following 6 hours. One channel associated with an operating loop may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 17 With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed provided the inoperable channel is placed in the bypassed condition and the Minimum Channels OPERABLE requirement is met. One additional channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 18 With less than the Minimum Channels OPERABLE requirement, operation may continue provided the containment purge supply and exhaust valves are maintained closed.

*Time outside parentheses is for solid state protection system (SSPS) plant; time inside parentheses is for relay logic plant logic cabinets and master relays. Relay logic plant slave relays may be bypassed for 12 hours. SSPS plant slave relays may be bypassed for 4 hours.

TABLE 3.3-3 (Continued)

ACTION STATEMENTS (Continued)

ACTION 19 With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, restore the inoperable channel to OPERABLE status within 48 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

ACTION 20 With the number of OPERABLE channels one less than the Total Number of Channels, STARTUP and/or POWER OPERATION may proceed provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours.

b. The minimum channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per specification 4.3.2.1.

ACTION 21 With less than the Minimum Number of Channels OPERABLE, within one hour determine by observation of the associated permissive annunciator window(s) that the interlock is in its required state for the existing plant condition, or apply Specification 3.0.3.

ACTION 22 With the number of OPERABLE Channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 6 hours and in at least HOT SHUTDOWN within the following 6 hours; however, one channel may be bypassed for up to 4 (8)* hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

ACTION 23 With the number of OPERABLE channels one less than the Total Number of Channels, restore the inoperable channel to OPERABLE status within 48 hours or be in at least HOT STANDBY within 6 hours and in at least HOT SHUTDOWN within the following 6 hours.

ACTION 24 With the number of OPERABLE channels one less than the Total Number of Channels, restore the inoperable channel to OPERABLE status within 48 hours or declare the associated valve inoperable and take the ACTION required by Specification (3.7.1.5).

TABLE 4.3-2

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
1. SAFETY INJECTION, REACTOR TRIP FEEDWATER ISOLATION, CONTROL ROOM ISOLATION START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4
c. Containment Pressure-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Pressurizer Pressure-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
e. Differential Pressure Between Steam Lines-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
f. Steam Flow in Two Steam Lines-High Coincident With Either	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
1. T_{avg} - Low-Low, or	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
2. Steam Line Pressure-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
2. CONTAINMENT SPRAY								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4
c. Containment Pressure-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
3. CONTAINMENT ISOLATION								
a. Phase "A" Isolation								
1) Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
2) Safety Injection	See 1 above for all Safety Injection Surveillance Requirements							
3) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4
b. Phase "B" Isolation								
1) Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
2) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
CONTAINMENT ISOLATION (Continued)								
3) Containment Pressure-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
c. Purge and Exhaust Isolation								
1) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4
2) Containment Radiological-High	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
3) Safety Injection	See 1 above for all Injection Surveillance Requirements							
4. STEAM LINE ISOLATION								
a. Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3
c. Containment Pressure-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Steam Flow in Two Steam Lines-High Coincident With Either	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
STEAM LINE ISOLATION (Continued)								
1. T_{avg} - Low-Low or	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
2. Steam Line Pressure-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
5. TURBINE TRIP AND FEEDWATER ISOLATION								
a. Steam Generator Water Level-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2
b. Automatic Actuation Logic and Actuation Relay	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2
6. AUXILIARY FEEDWATER								
a. Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3
c. Steam Generator Water Level-Low-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Undervoltage - RCP	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1
e. Safety Injection	See 1 above for all Safety Injection Surveillance Requirements							

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
AUXILIARY FEEDWATER (Continued)								
f. Station Blackout	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
g. Trip of Main Feedwater Pumps	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2
7. AUTOMATIC SWITCHOVER TO CONTAINMENT SUMP								
a. RSWT Level-Low Coincident With Containment Sump Level - High and Safety Injection	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
	See 1 above for all Safety Injection Surveillance Requirements							
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (1)	M (1)	Q	1, 2, 3, 4
8. LOSS OF POWER								
a. 4.16 kV Emergency Bus Undervoltage (Loss of Voltage)	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. 4.16 kV Emergency Bus Undervoltage (Degraded Voltage)	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INTERLOCKS								
a. Pressurizer Pressure, P-11	N.A.	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
b. Low, Low T_{avg}, P-12	N.A.	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
c. Reactor Trip, P-4	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3

WESTINGHOUSE CLASS 3

TABLE 4.3-2 (Continued)

TABLE NOTATION

(1) Each train shall be tested at least every 62 days on a STAGGERED TEST BASIS.

ENCLOSURE

TECHNICAL EVALUATION REPORT

A REVIEW OF THE WESTINGHOUSE OWNERS' GROUP TECHNICAL SPECIFICATION RELAXATION ANALYSIS FOR THE ENGINEERED FEATURES ACTUATION SYSTEM

G. E. Bozoki
K. O. Aliefendioglu
R. G. Fitzpatrick
W. Y. Yoon

September 1988

Risk Evaluation Group
Department of Nuclear Energy
Brookhavan National Laboratory
Upton, NY 11973

Prepared for
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Contract No. DE-AC02-76CH00016
FIN A-3838

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (Continued)

EXECUTIVE SUMMARY

This study was performed by the Risk Evaluation Group, Department of Nuclear Energy, Brookhaven National Laboratory for the Office of Nuclear Reactor Regulation, Technical Specifications Branch, U.S. Nuclear Regulatory Commission. The scope of this project was to support the NRC's effort to respond to a request by the Westinghouse Owners Group (WOG) concerning alternative plant Technical Specifications (TS) for surveillance time intervals (STIs) and allowed outage times (AOTs) for the Engineered Safety Features Actuation System (ESFAS). The WOG request was supported by extensive analysis of the unavailability of ESFAS signals under various LCO (limiting conditions for operation) policies, as well as, an evaluation of the impact of these policies on the core damage frequency and health risk. The documents (WCAP-10271, Supplement 2 and WCAP-10271 Supplement 2, Revision 1) contain the description of the approach and the results of the WOG calculations.

The unavailabilities of ESFAS signals were presented by the WOG for two kinds of system designs: 1) relay and 2) solid state. Relay systems are used at older Westinghouse plants. At newer Westinghouse plants various versions of the solid state systems are installed. The WOG analysis demonstrates that the unavailabilities of the relay and solid state ESFAS signals behave similarly for the most part. It is structured to demonstrate also, that the unavailabilities of solid state ESFAS signals envelope (i.e., are consistently higher than) the unavailabilities of the relay ESFAS signals under the conditions and assumptions applied by the WOG. Based on these results, the WOG decided that it was sufficient to evaluate the impact of the proposed Technical Specification revisions on the core damage and health risk on a relatively new plant having a solid state ESFAS, serving as a "bounding" representative for all the Westinghouse plants.

For such a representative plant, the Millstone Unit 3 plant was selected. The plant has a solid state ESFAS of fairly recent vintage with 2/4 logic. The Millstone 3 Probabilistic Safety Study (PSS) which was reviewed by the NRC, was considered by the WOG to adequately address the importance of the ESFAS. In addition, the relevant results obtained in that PSS concerning the ESFAS were deemed by the WOG to be similar to those obtained in other plants'

PSS. The WOG risk impact analysis involved the evaluation of core damage frequency and changes in person-rem generated by changes in the unavailability of selected ESFAS signals due to modified LCOs. The risk impact analysis was restricted to only internally initiated accident sequences.

The WOG states that while the risk impact analysis was plant specific, because of the application of bounding solid state signal unavailabilities, the results obtained should envelop almost all of the Westinghouse plants. Consequently, the proposed Technical Specificacion modifications were claimed to cover the majority of Westinghouse plants, including those having relay ESFAS designs.

The objectives of this report are:

1. to provide the results of auditing the WOG's calculations on the changes due to the proposed modifications of limiting conditions of operation for the ESFAS,

2. to review the WOG's approach used in the analysis of the impact of these LCO modifications to the core damage frequency (CDF) and to present the results of CDF calculations performed by BNL for its validation, and

3. to analyze the risk analysis methodology applied by the WOG by presenting some independent results obtained through considerations specifically addressing STI and AOT modifications from a risk standpoint.

BNL Findings on ESFAS Signal Unavailabilities

From the depth and extent of the ESFAS signal unavailability analysis, it is clear that the WOG has performed a really thorough study of the ESFAS designs presently used at the plants. In this respect an excellent job was done on the solid state systems as well as on the relay system designs. The following items highlight the BNL findings in this area:

1. BNL concurs with the WOG's finding that the unavailability contributions of the analog channels for the ESFAS logic designs are small and that they become even smaller when one considers process parameter signal diversity. Therefore, whether the analog channels are tested on a staggered or non-staggered basis, there is negligible effect on the ESFAS signal unavailability.

2. Human errors associated with testing and maintenance activities for the logic as well as the master and slave relays were not modelled in the topical report. We note this as a shortcoming of the model. However, although not part of the quantification, it is noted that the requested extended allowed outage times, if granted, would be expected to lower the human error contribution.

BNL Findings on Core Damage Frequency

1. The BNL review calculations provided a CDF frequency increase of 2.8% for solid state plants if the LCO modifications proposed by the WOG are accepted. The value obtained is in acceptable agreement with the value assessed by WOG (i.e., 2.4%) in its Justification Risk Analysis.

2. The increase of the CDF for relay plants calculated by BNL when the same conditions were used for relay ESFAS unavailability as the WOG (i.e., concurrent slave relay testing) is: 4.0%. This value is at variance with the WOG's expectation. The WOG stated that the CDF increases at relay plants would be "bounded" by the CDF increase obtained at a representative solid state plant. The WOG did not do any calculational effort, however, to prove this expectation. As a sensitivity study, BNL also performed a calculation to see the effect that a sequential testing scheme would have on the CDF. The results of the sensitivity study yielded a CDF increase of 5.7%.

3. As part of the review, BNL pointed out that the use of Millstone Unit 3 as a reference plant may not fully bound the change in CDF for Westinghouse plants in general because Millstone has a 2/4 ESFAS logic and other plants have 2/3 logic which produces higher unavailability. In response to BNL's concern, Westinghouse did a separate calculation, which was documented as Supplement 2, Revision 1, Addendum 2 to WCAP-10271. The calculation was performed on Millstone assuming the Millstone logic was simply changed from 2/4 to 2/3. The bottom line result yielded a 3.3% increase in CDF verses the 2.4% for the 2/4 logic designs. BNL accepts this additional calculation as a reasonable estimate for the 2/3 solid state designs. Given that the BNL analysis shows the relay designs as bounding over the solid state, and assuming that the ΔCDF increase in the solid state designs between 2/4 and 2/3 logic would be proportionately equivalent to the relay designs, an overall upper bound for the CDF increase due to the proposed TS changes should be less than 6% for the majority of Westinghouse-design plants.

1. INTRODUCTION AND BACKGROUND

1.1 Scope and Objectives

The scope of this project was to support the NRC's effort to respond to a request by the Westinghouse Owners Group (WOG) concerning alternative plant Technical Specifications for surveillance time intervals (STIs) and allowed outage times (AOTs) for the Engineered Safety Features Actuation System (ESFAS).

The direct objectives of this report are:

1. to provide the results of auditing the WOG's calculations on the changes due to the proposed modifications of limiting conditions of operations (LCOs) for the ESFAS,

2. to review the WOG's approach used in the analysis of the impact of these LCO modifications to the core damage frequency (CDF) and to present the results of CDF calculations performed by BNL for its validation, and

3. to comment on the risk analysis methodology applied by the WOG by presenting some independent results obtained through considerations specifically addressing AOT modifications from a risk standpoint.

1.2 Background

The WOG request is supported by extensive analysis of the unavailability of ESFAS signals under various LCO policies, as well as, an evaluation of the impact of these policies on the core damage frequency and health risk. The documents, WCAP-10271, Supplement 2[1] and WCAP-10271 Supplement 2, Revision 1[2] contain the description of the approach and the results of the calculations. Additional information with regard to various review questions posed by the NRC and BNL was provided by the WOG in three important letters, WOG Memo OG-207,[3] WOG Memo OG-87-15,[4] and NS-NRC-88-3308.[5]

In References 1 and 2 the unavailabilities of ESFAS signals were presented for two kinds of system designs: relay and solid state. Relay systems are used at older Westinghouse plants. At newer Westinghouse plants various versions of the solid state systems are installed. The WOG analysis demonstrates that the unavailabilities of the relay and solid state ESFAS signals behave similarly for the most part. It shows also, that the unavailabilities of solid state ESFAS signals envelope (i.e., are consistently higher than) the unavailabilities of the relay ESFAS signals under the conditions and assumptions applied by the WOG.

Based on these results, the WOG decided that it was sufficient to evaluate the impact of the proposed Technical Specification revisions on the core damage and health risk on a relatively new plant having a solid state ESFAS, serving as a "bounding" representative for all the Westinghouse plants.

For such a representative plant, the Millstone Unit 3 plant was selected. The plant has a solid state ESFAS of fairly recent vintage. Its Probabilistic Safety Study[6] reviewed[7] by the NRC was considered by the WOG to adequately address the importance of the ESFAS. In addition, the relevant results obtained in that PSS[6] concerning the ESFAS were deemed by the WOG to be similar to those obtained in other plants' PSS.

The results of the risk impact analysis based on the Millstone Unit 3 PSS were given in variously detailed and successively modified versions in References 1 through 5. The risk impact analysis involves the evaluations of core damage frequency and man-rem value changes generated by changes in the unavailability of selected ESFAS signals due to modified LCOs. The risk impact analysis was restricted to only internally initiated accident sequences.

The WOG claims that while their risk impact analysis was plant-specific, because of the application of bounding solid state signal unavailabilities, the results obtained are characteristic for almost all of the Westinghouse plants. Consequently, the proposed Technical Specification modifications were claimed to be applicable to the majority of Westinghouse plants, including those having relay ESFAS designs.

The review of the ESFAS unavailability and risk impact analysis by BNL has been a protracted one due to the interactive nature (questions, answers) of the review process. Many questions were posed due to the proprietary aspects of the submitted materials and the abbreviated descriptions of certain methodological or calculational details. The answers resulted in References 3 through 5 and two presentations at the NRC (August 19, 1987 and January 13, 1988).

The present report summarizes the results of the BNL audit calculations on the unavailabilities of actuation signals used in the WOG's risk analysis and the results obtained in reviewing the impact of the signal unavailability changes due to the proposed LCO modifications to the core damage frequency. In order to check the WOG's claim about the general applicability of the proposed Technical Specification modifications, in contrast with the WOG's approach, the BNL review calculations used unavailabilities for both types of signals; signals from solid state and relay ESFAS designs.

1.3 Organization of the Report

The report is organized as follows: Section 2 describes the solid state and relay ESFAS designs and their testing methods. Section 3 presents the proposed relaxation of Technical Specifications and briefly discusses the WOG methodology and the results of the WOG justification analyses. Section 4 presents the results obtained by BNL in auditing the ESFAS signal unavailability analysis of the WOG. Section 5 describes the core damage frequency calculations performed by BNL. Section 6 discusses the comments on the WOG methodology and summarizes the findings and the main conclusions of the BNL review. Appendix A provides formulas to assess relay signal unavailability differences for concurrently or sequentially performed slave relay testing. Appendix B contains some additional results obtained at BNL by using considerations specifically addressing AOT modifications from a risk standpoint.

2. ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

2.1 System Description

The Engineered Safety Features Actuation System (ESFAS) of a nuclear power plant provides actuation signals to safeguard equipment (and for reactor protection) when process and nuclear parameters exceed certain preset limits ensuring that safe operating conditions exist at all times.

The ESFASs presently used at Westinghouse plants belong to two basic designs: solid state and relay.

The main components of both of these designs are:

1. the analog channels,
2. the combinational logic units, and
3. the actuation relays.

2.1.1 Analog Channels

An analog channel involves: an analog sensing device (sensor/transmitter), a loop power supply, a signal conditioning circuit, and a signal comparator. The sensing device monitors a given process or nuclear parameter, such as pressure, level, flow, temperature or flux, etc. At solid state ESFASs the signal is converted to proportional voltage signals by the power supply of the loop (Figure 2.1). At relay plants the sensed signal is transmitted by the current loop (Figure 2.2). The sensed signal is "shaped" by the signal conditioning circuit (signal modifiers). The shaped signal is compared with a preset parameter value by the comparator (bistable). The comparator controls two output relays; one of them provides input signals to the combinational logic train A and the other to combinational logic train B. The output relays may be either ac or dc powered, low voltage (~25V) or high voltage (~120V) depending on the plant-specific application.

2.1.2 Combinational Logic Unit and Master Relays

a. Solid State Design

The combinational logic unit is a dual train electronic system. The trains A and B contain several 2/4, 2/3, and 1/2 logic circuits built on universal logic (UL) cards. The analog channel output relays operate grounding contacts at the inputs of the combinational trains. A trip signal is generated in each of the trains if an appropriate number of card inputs are grounded. Outputs of various logic circuits in each of the trains can be further interconnected by using additional logic circuits to achieve desired reactor trip and safeguard initiator signal combinations. The safeguard initiator signals drive the master relays by creating a current flow which energizes them. The block diagram of a solid state ESFAS is shown in Figure 2.3.

b. Relay Design

The combinational logic unit of relay designs consists of two trains of series-parallel contacts. When an appropriate number of contacts are closed or opened, one or more associated master relays are energized or de-energized, depending on the safety function. The output relays of the analog channels operate the series-parallel contacts of each of the two trains. An appropriate number of contacts may represent a logic of 1/2, 2/3, or 2/4. Thus, if the correct combination of analog channels senses the monitored parameter outside of limits, the master relays are energized. The diagram of a relay logic train is given in Figure 2.4.

2.1.3 Slave Relays

Given an initiator signal, in both of the designs (solid state or relay) the energized master relays close contacts in the slave relay circuits and energize the associated slave relays. The slave relays activate the safety systems by energizing contacts in a sequencer unit or in motor starters, solenoid circuits, etc. Usually each slave relay activates several safety system components. The number of master and slave relays energized is

dependent upon the complexity of a given protective function required by a specific initiating event. The ESFAS trains, independently of the type of design, are train oriented: ESFAS train A energizes train A of a safety system, etc.

Figures 2.5 and 2.6 show the schematics of slave relay arrangements for solid state and relay ESFASs, respectively. Table 2.1 presents the master and slave relay arrangements typically used in generating actuation signals for various safety functions modelled in References 1 and 2.

For the illustration of the ESFAS operation, Table 2.2 shows a list of Design Basis Accidents (DBA), the process or nuclear parameter signals and the associated ESFAS signals which actuate the safety equipment required to mitigate the event.

The average number of analog channels sensing either process or nuclear parameters is 58 (20 channels are dedicated to the ESFAS, 38 channels are common with the Reactor Trip System). For the solid state system, the total number of master relays and slave relays per train (as modelled in the submittal) is 7 and 16, respectively. For the relay system the total number of master and slave relays per train is 6 and 15, respectively.

2.2 Testing of the ESFAS

2.2.1 Testing of the Analog Channels

The functional testing of the analog channels is performed at power. Its purpose is to verify the entire operation of the channel excluding the sensor. Calibration and verification of proper operation of the sensors (the associated electronics included) is usually performed at shutdown. The functional test scheme of the analog channels for solid state and relay designs are shown also in Figures 2.1 and 2.2, respectively. The sensor is disconnected during testing. By using test jacks, test signals are sent through the circuit. A proving lamp is connected to the output of the bistable; usually the bistable is adjusted to ensure that the whole channel performs as required. The input relays of the logic trains are energized from

an outside circuit if the channel is tested in bypass. The input relays are de-energized if the channel is tested in trip.

During normal operation, a failure of a sensor or a loop power supply would cause abnormal indication and/or alarms. The status lights are checked by operators every shift, therefore, an analog channel failure is detectable in eight hours.

The surveillance time interval (STI), test time, and maintenance time of the analog channels currently required in the Technical Specifications for solid state and relay systems are listed in Table 3.1 in the columns; "Base Case." An analog channel is allowed to be bypassed for a duration specified in the Technical Specifications. However, it has to be put in the trip mode if the allowable bypass time is exceeded and surveillance testing or maintenance is made on another channel. The surveillance tests are currently required to be performed on a staggered basis.

2.2.2 Testing of the Combinational Logic Units

a. Solid State Design

While a plant is at power, each of the combinational logic trains located in separate cabinets is allowed to be tested or maintained separately in "bypass" condition. Time sequenced pulses are applied to the logic circuits through switches located on a logic test panel dedicated to each train (semi-automatic tester). The pulses check the logic, but are of such a short duration that slave relay (or trip breaker) actuation is not possible. The semi-automatic tester allows quick and efficient testing of all the possible logic combinations of actuate or non-actuate conditions as well as the effects of the permissives. If one train is in test or in maintenance, the other is charged with providing all the safety function signals. It is not possible to lock out both logic trains without tripping the reactor. The tests of the combinational logic trains are performed on a staggered test basis.

b. Relay Design

There is no semiautomatic tester for relay ESFAS designs. The logic testing method is essentially plant-specific. According to the WOG, the most typical testing method is as follows:

For a given logic combination, an appropriate number of input relay contacts are individually operated by tripping the required number of analog channels, while blocking the operation of the master relay. The verification of actuation signal generation is performed by using a proving lamp or proper voltage indication. Associated with the logic test is the potential for human error in that personnel may omit testing certain logic configurations, induce failures or fail to return components to their operating configuration. Other features of the testing (train unavailability, reactor trip, staggered test bases) are similar to those of the solid state design.

Table 3.1 lists the currently required STI test and maintenance times ("base case") for the logic trains.

2.2.3 Testing of the Actuation Relays

a. Solid State Design

The master relays are "continuity" tested as part of the logic test to demonstrate total circuit operation. The master relays are actuated during master relay testing and proper contact operation is checked. Figure 2.5 shows the test conditions for the actuation relays. Proper contact operation is verified by "continuity" checking of the associated slave relay. This test is performed by applying a voltage to the master relay contact which demonstrates the continuity but which is insufficient to activate the slave relay.

The "actuation" test of a slave relay is performed individually by energizing the relay and demonstrating proper contact operation. Proper contact operation can be demonstrated with or without operating the associated equipment. The slave relay test sometimes requires the reconfiguration of the

equipment to be tested in such a way that the test would not cause adverse effects on the plant operation. After the test, the equipment has to be returned to its normal operating configuration. Therefore, associated with each slave relay test there is also a potential for human error in that the personnel conducting the test could fail to return the equipment to its proper operating configuration.

b. Relay Design

The typical Westinghouse relay plant has a designed-in on-line master relay test capability but no designed-in on-line slave relay capability. The master relay test (see Figure 2.6) requires proper operation of the relay contacts if the relay is energized. Proper contact operation is verified by performing a "continuity" check in the slave relay circuit. The continuity check is performed by observing the operation of a test lamp in series with the coil of the slave relay. The lamp will check the signal continuity, but the resistance of its filament will restrict the slave relay current from operating the contacts of the slave relay.

The actuation test of the slave relays can be performed individually, in a sequential process, similar to that of the solid state design or concurrently. Each slave relay is energized simultaneously and proper contact operation is checked. The verification of proper contact operation can be performed by continuity check, by testing only the operation of the actuation circuit or by effectively operating the associated equipment.

Table 3.1 lists the currently required STI, test and maintenance times ("base cases") for the actuation relays. The master relay tests are usually performed following the associated logic train test on a staggered test basis. Master relay testing or maintenance activities inhibit the entire train. Slave relay testing or maintenance affects only the individual relay being tested. However, when the slave relays are tested concurrently, the entire train is inhibited. During the testing or maintenance of actuation relays belonging to one train the opposite train is kept functional.

Figure 2.7 shows the testing scheme of a complete ESFAS train applied at Millstone Unit 3 power plant. The testing scheme is considered to be typical for solid state Westinghouse plants.

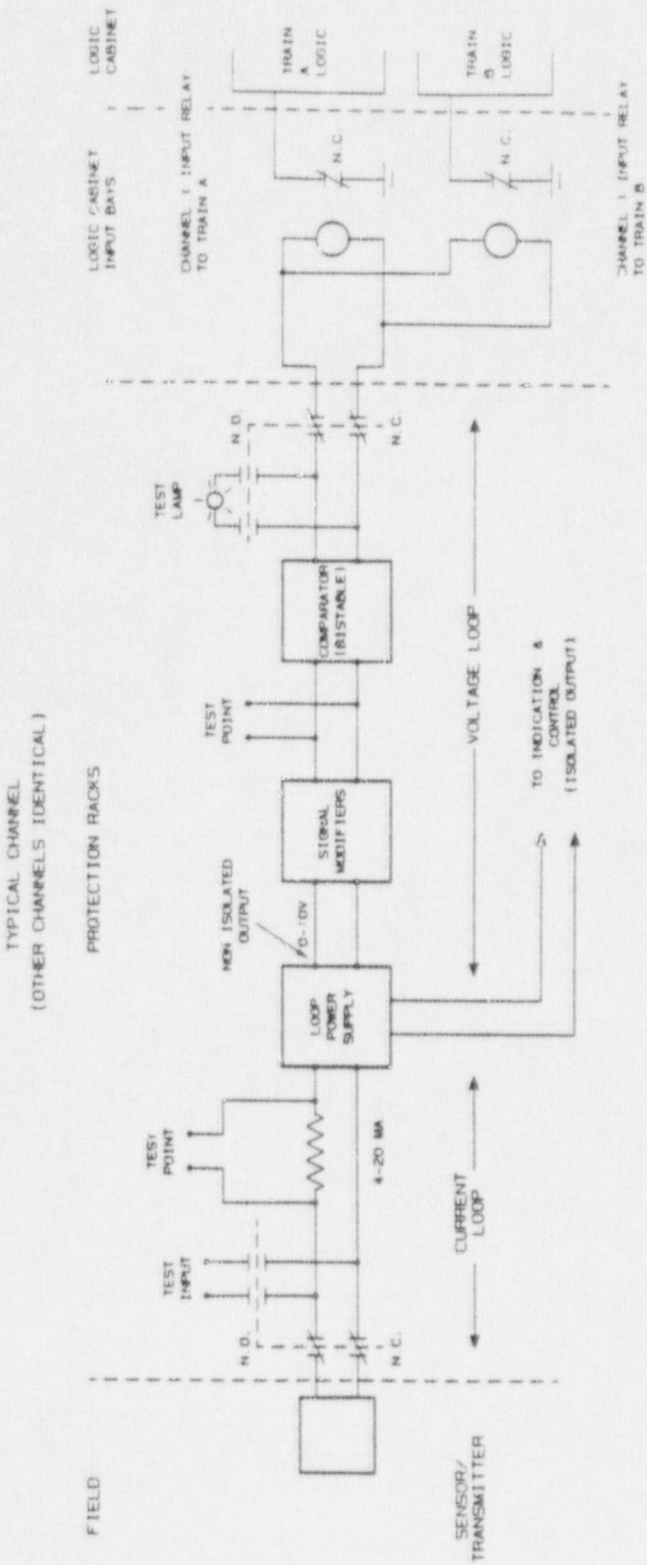


Figure 2.1 Analog channel block diagram (Solid State ESFAS).

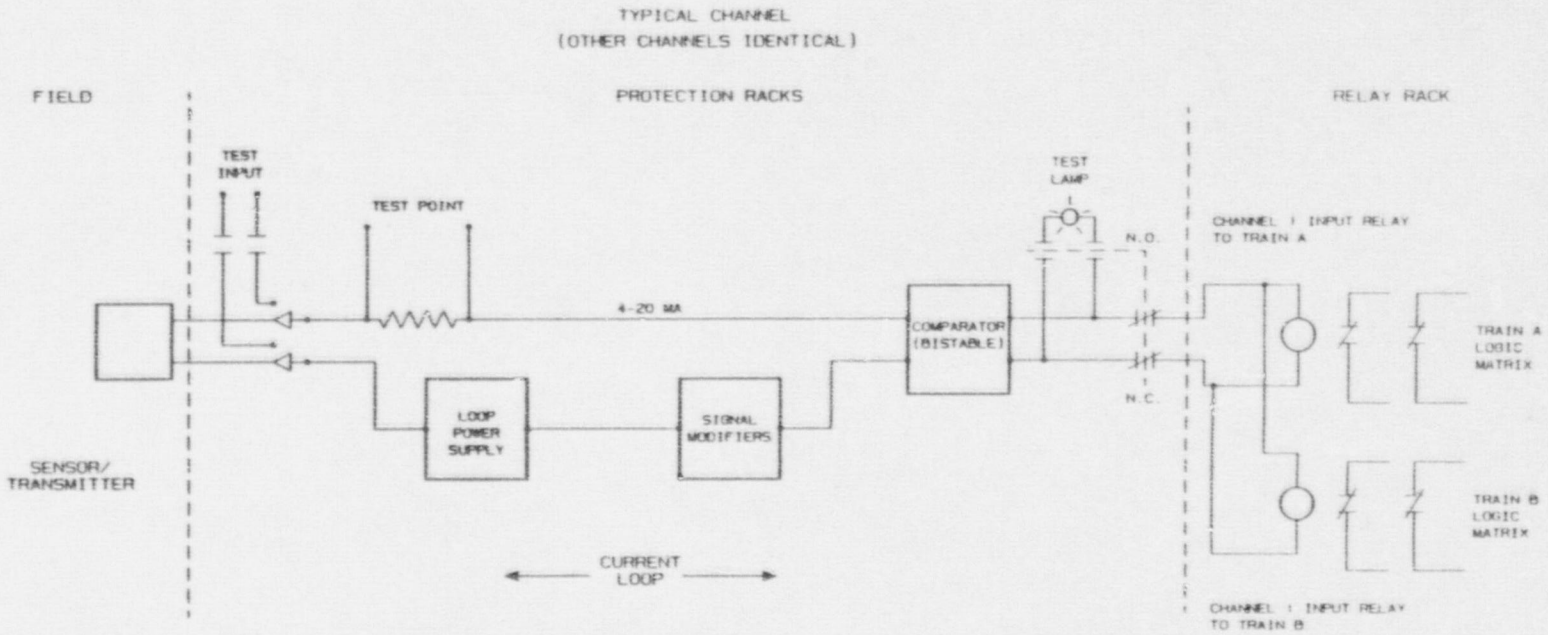


Figure 2.2 Analog channel block diagram (Relay ESFAS).

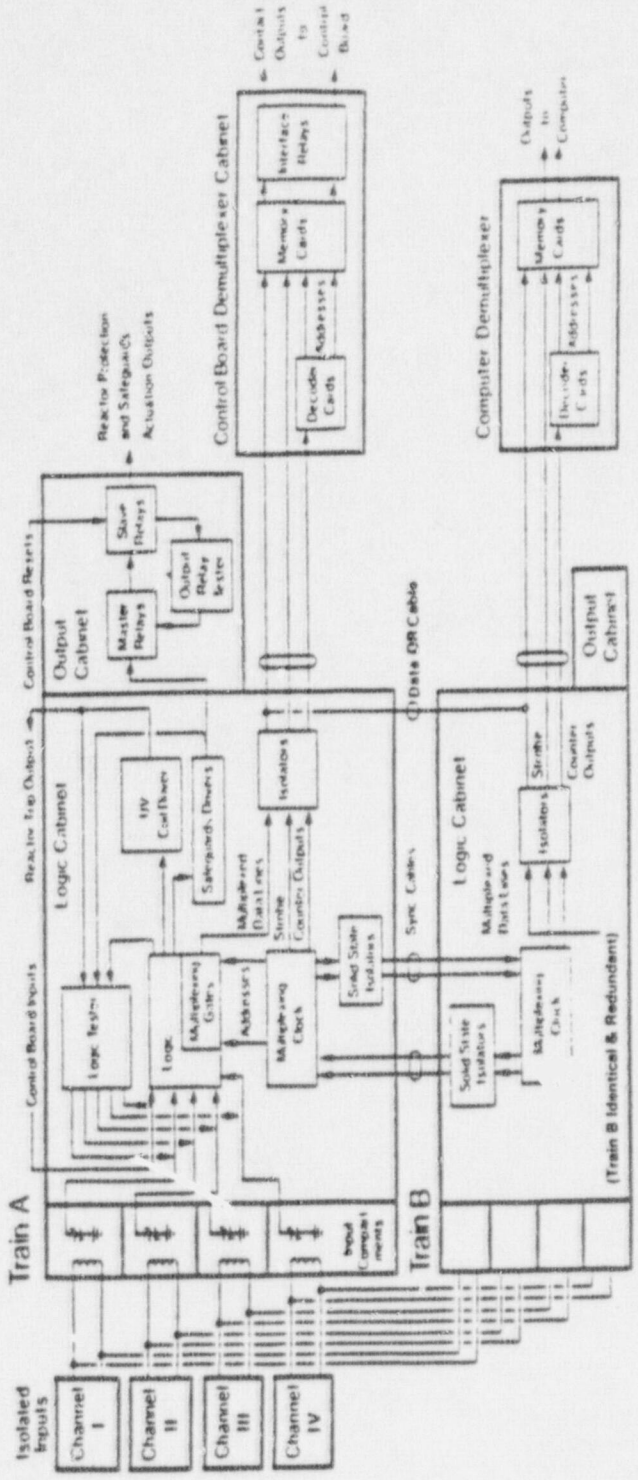


Figure 2.3 Block diagram of solid state ESFAS.

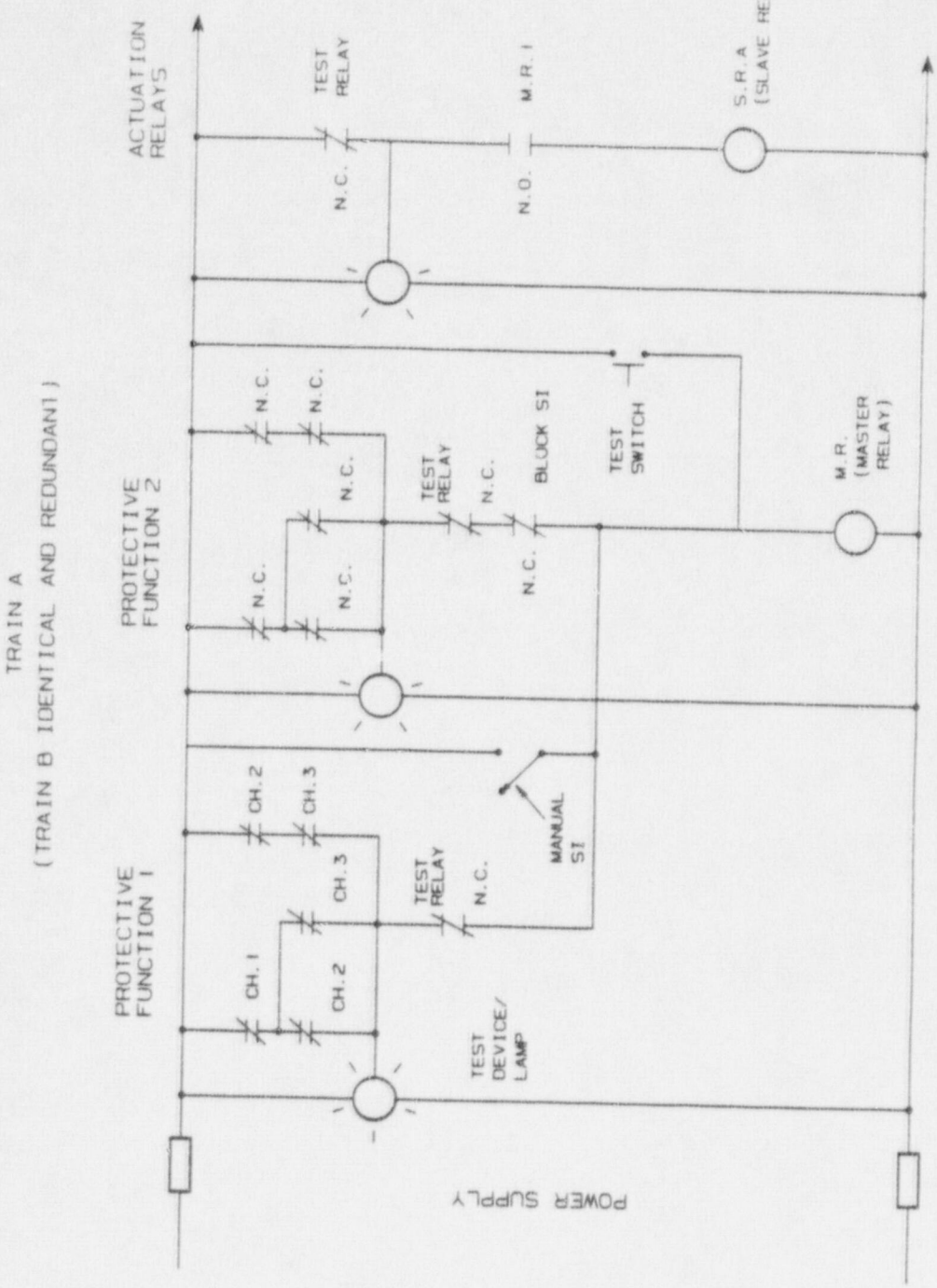


Figure 2.4 Schematic of logic circuit (Relay ESFAS).

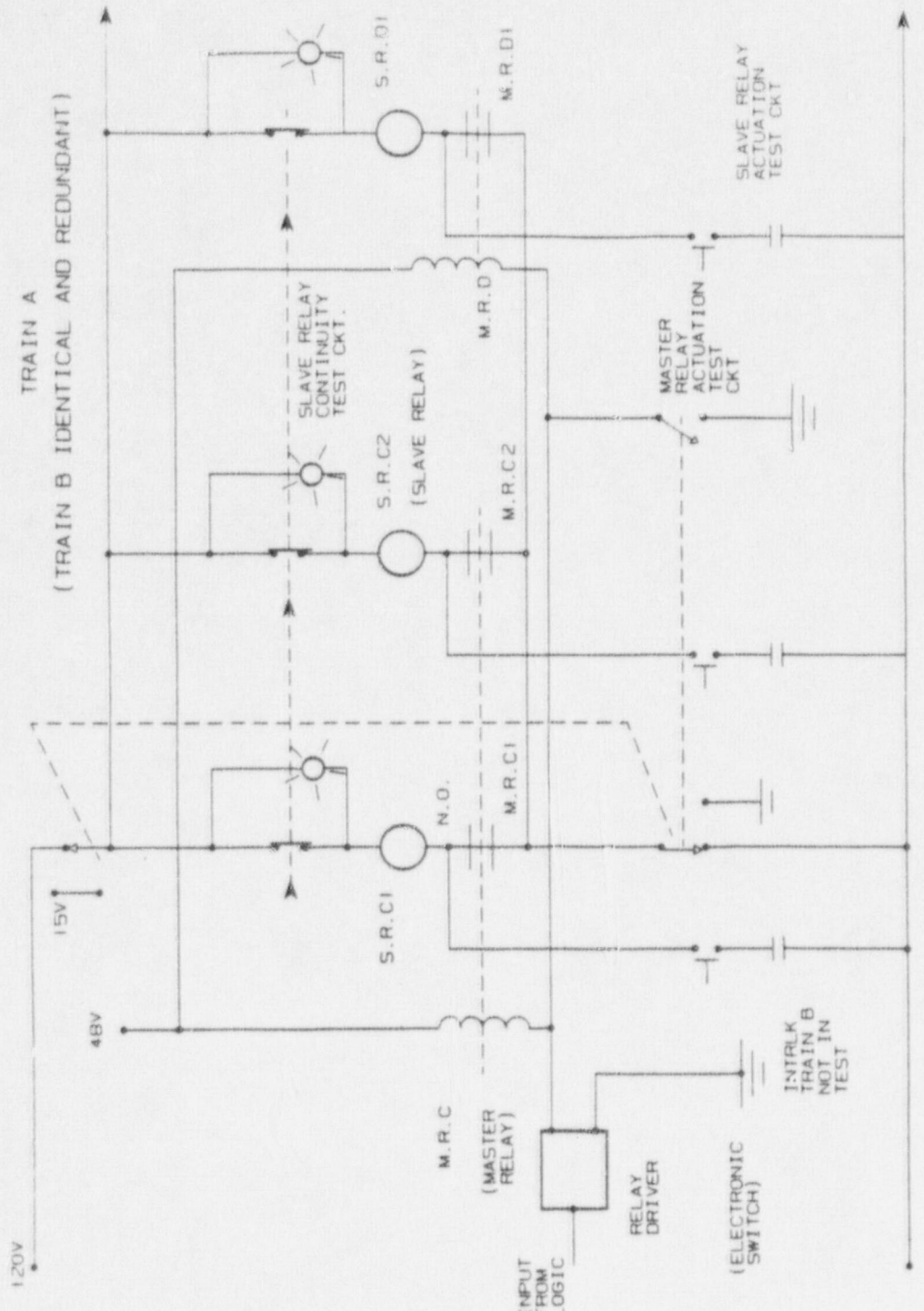


Figure 2.5 Schematic of actuation relays (Solid State ESFAS).

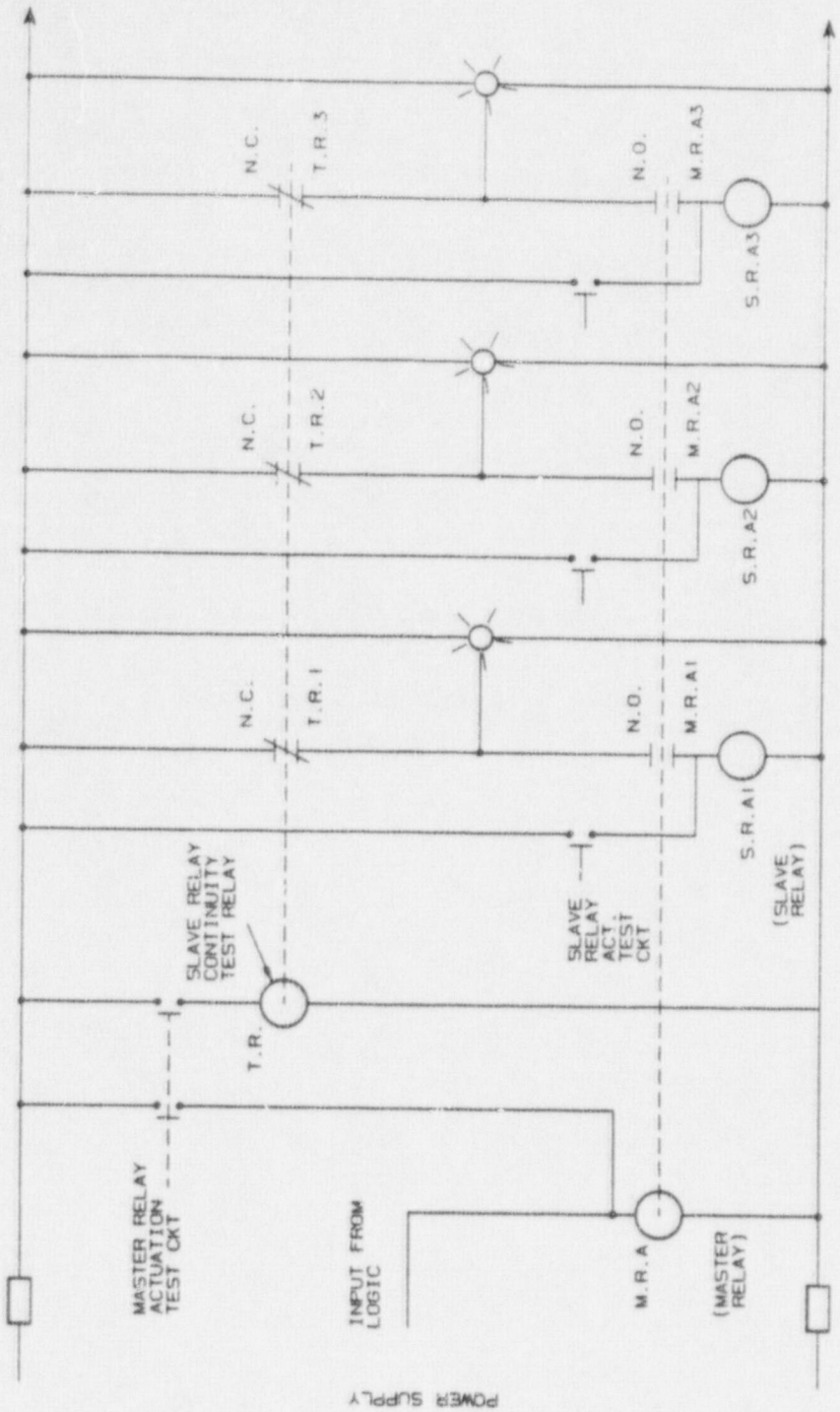


Figure 2.6 Schematic of actuation relays (Relay ESFAS).

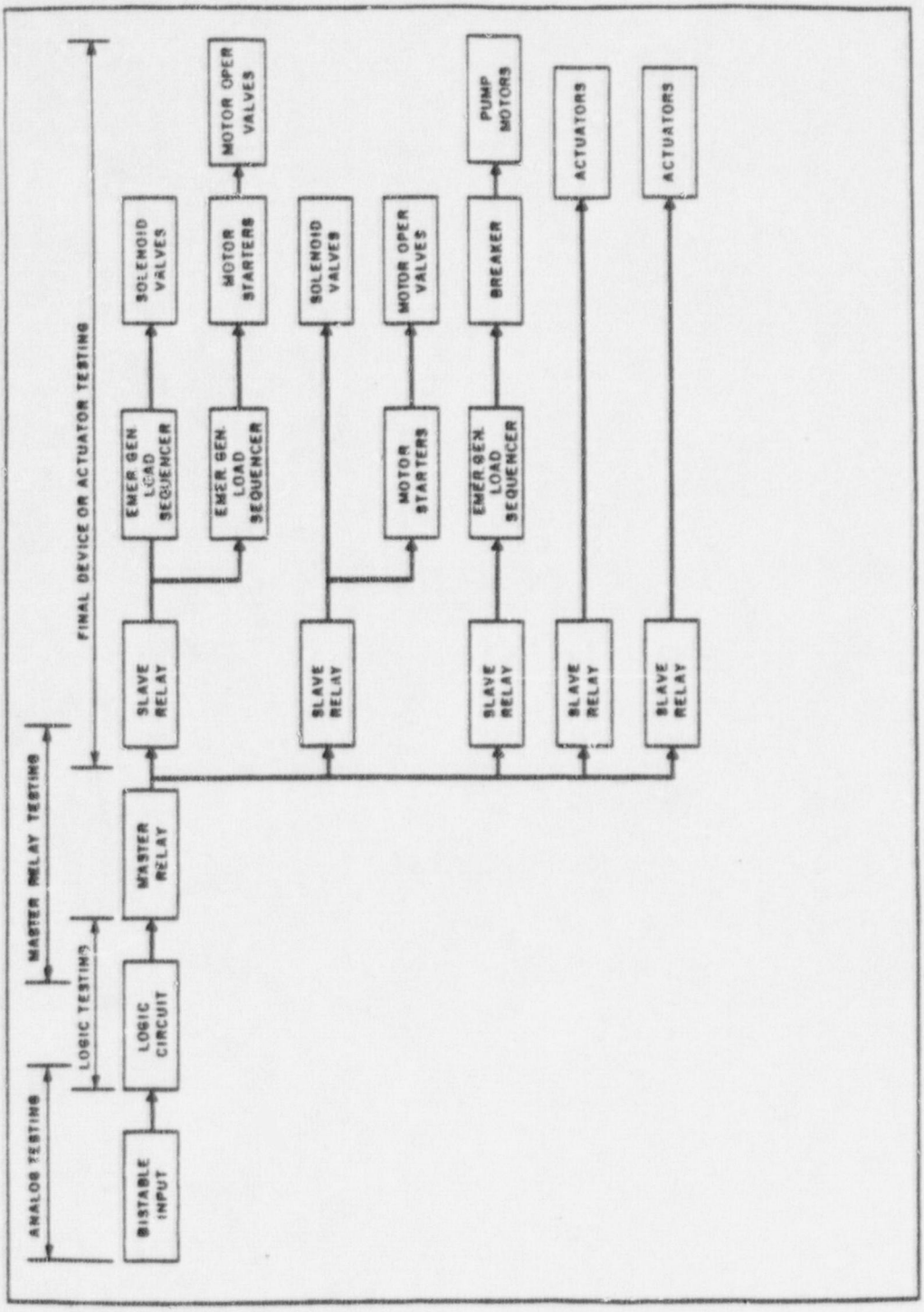


Figure 2.7 Testing scheme of an ESFAS train (Solid State) at Millstone Unit 3 Power Station.

Table 2.1. Master/Slave Relay Arrangements for Various Safety Function Actuation Signals.

Safety Function Actuation Signal	Solid State Design		Relay Design	
	Master Relays[1]	Slave Relays[1]	Master Relays[1]	Slave Relays[1]
1. Safety Injection	A B	A1, A2, A3 B1, B2, B3	A	A1, A2, A3, A4, A5, A6
2. Steam Line Isolation	A	A1, A2	A	A1, A2, A3
3. Main Feedwater Isolation	A	A1, A2	A	None
4. Auxiliary Feedwater Pump Start	A	A1, A2	A	None
5. Containment Spray	A	A1, A2	A	A1, A2, A3
6. Containment Isolation	A	A1, A2	A	A1, A2, A3

[1]Relays per ESFAS train as applied in the unavailability analysis.

Table 2.2. Process Parameter - Engineered Safety Features Actuation Signals for Design Base Accidents

	Process Parameter Signals							ESFA Signals						
Initiators	Pressurizer Pressure-Low	Steamline Pressure-Low	Differential Steam Pressure-High	Containment Pressure-High	Containment Pressure High-High	Containment Pressure High-High-High	Steam Generator Water Level-Low-Low	Safety Injection	Main Steam Isolation	Main Feedwater Isolation	AFW Pump Start	Containment Spray	Containment Isolation	Pressurizer Pressure Relief
Large LOCA	+			+	x	*		+				x	*	
Small LOCA	+			+			0	+			0			
Steam Generator Tube Rupture	+[1]						0	+	M	M	0			M
Steamline Break (New Logic)	+	+•	•	+	•	*	0	+	•		0	x	*	
Feedline Break	+	+•		+			0	+	•		0			

+:For a given initiator similar symbols (+,x,etc.) indicate those process parameter signals from which one is sufficient to generate an associated ESFAS signal.

[1]:With manual action to terminate leak by isolating the steam generator and equalizing pressure.

M:Manual Actions.

3. WOG JUSTIFICATION ANALYSES FOR RELAXED ESFAS TECHNICAL SPECIFICATIONS

For clear understanding and for the sake of convenience this section presents the proposed relaxation of Technical Specifications concerning the ESFAS and a brief summary of the methodology and results of the justification analyses performed by the WOG.

3.1 Proposed Relaxation of ESFAS Technical Specifications

The relaxation of the Technical Specifications proposed by the WOG follows:

a. Surveillance Time Interval. Increase the STI for analog channels from the current one month to three months. No STI relaxation is requested for the logic, master, and slave relays.

b. Test Time. Increase the allowed test time of the analog channels from the current two hours to four hours for both solid state and relay systems. Increase the test time of all components to four hours in solid state systems. Increase the test time of the logic trains and master relays to eight hours and the slave relays to twelve hours in relay systems.

c. Maintenance Time. Increase the allowed maintenance time of all components to 12 hours. During maintenance all the components would be in bypass (except for analog channels); an analog channel would be tripped after having spent six hours in bypass.

d. Staggered Testing. It was requested that the staggered testing requirement for the analog channels be removed.

Table 3.1 details the current and proposed surveillance requirements for ESFAS for both the solid state and relay systems. For comparison, the table also shows the previous and recently granted (NRC SER, 1985)[8] LCO requirements for those analog channels which provide plant parameter signals to the Reactor Protection System.

3.2 Methodology and Results of Justification Analyses

The above proposed set of relaxed Technical Specification requirements was based on WOG experience and by the results of justification analyses. A summary of the WOG justification analyses relevant to this review is given below:

1. A number of safety features actuation signal unavailabilities were calculated for solid state and relay designs by developing and quantifying appropriate "static" fault tree models. The calculation included two-of-three and two-of-four logic requirements and considered the effects of permissives.

   (Figure 3.1 shows the frequency distributions of 24 solid state and 24 relay signal unavailabilities selected in both cases with identical logic requirements and permissives. The distributions were compiled by BNL from WOG data to see the concentrations and spreads of these unavailabilities. The figure shows that the signal unavailabilities of the solid state system are consistently higher than those of the relay system. The distributions relate to the current set of surveillance parameters. Unavailability data given in the submittals shows that other sets of STI and AOT values provide similar distributions, i.e., signal unavailability data for the solid state systems envelope those obtained for the relay systems.)

2. Selected solid state and relay system signal unavailabilities were evaluated by the static fault tree method to study their sensitivities for various combinations of STI and AOT requirements (seven cases). In order to check the results obtained by the static fault trees, "time dependent" (Markovian) unavailability calculations were carried out for several signals of the solid state system. The time dependent unavailabilities provided results in agreement with those of the static fault trees.

3. By using the unavailabilities of two solid state signals (the safety injection signal and the auxiliary feedwater pump start

signal) the impact of the LCO changes on the core damage frequency and man-rem exposure were investigated for the Millstone Unit 3 power plant. From the seven cases studied, Case 3 provided acceptably small increases in core damage frequency (2.4%) and man-rem exposure (4.7%). Since the corresponding surveillance parameters were the closest to the WOG experience, Case 3 parameters (see columns "Proposed" in Table 3.1) were selected to be proposed for NRC acceptance.

Table 3.2 shows the unavailability changes of the selected signals generated by Case 3 parameters. Table 3.3 presents the results of the risk analysis. The risk analysis was based on the Millstone 3 PSS.[6] Some modifications were applied to the Millstone 3 PSS, otherwise the Millstone 3 PSS fault tree/event tree models and data were used.

The WOG results were obtained by the following approach:

- the ESFAS signal unavailabilities corresponding to the seven cases of LCO requirements were propagated through the Millstone support system's state model developed in conjunction with the initiating event frequencies,
- the support system state frequencies were propagated through all event trees (plant matrix),
- the plant damage state frequencies were propagated through the containment matrix, and
- the release category frequencies were propagated through the site analysis matrix to determine man-rem values.

The WOG modifications were:

a. Two kinds of ESFAS signals (defined earlier in this report) were used instead of a single typical safety injection signal representing all types of actuation signals in the original Millstone 3 PSS.

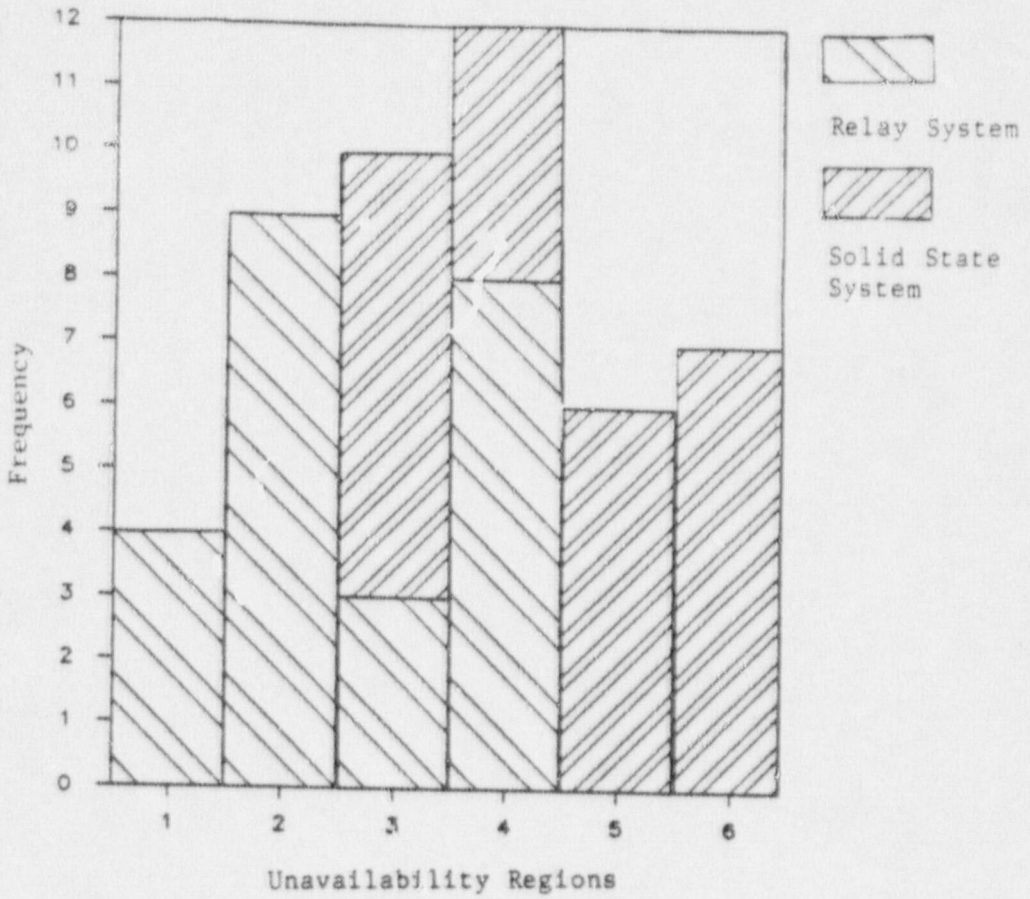
b. Manual recovery actions were added to appropriate transient events to provide credit for manually starting an auxiliary feedwater train.

c. No recovery was considered for large LOCA. The probability of failure of recovery of safety injection for medium LOCA was assumed to be 0.1 instead of 0.01 applied in the PSS.[6] For all other initiators the failure of recovery of ESFAS was taken to be the same as in the PSS: 0.01.

d. Credit for recovery of quench spray actuation was applied for the large LOCA leading to an early core damage state, since sufficient time is available for an operator to take action to actuate the sprays. (This action only affects the man-rem exposure.)

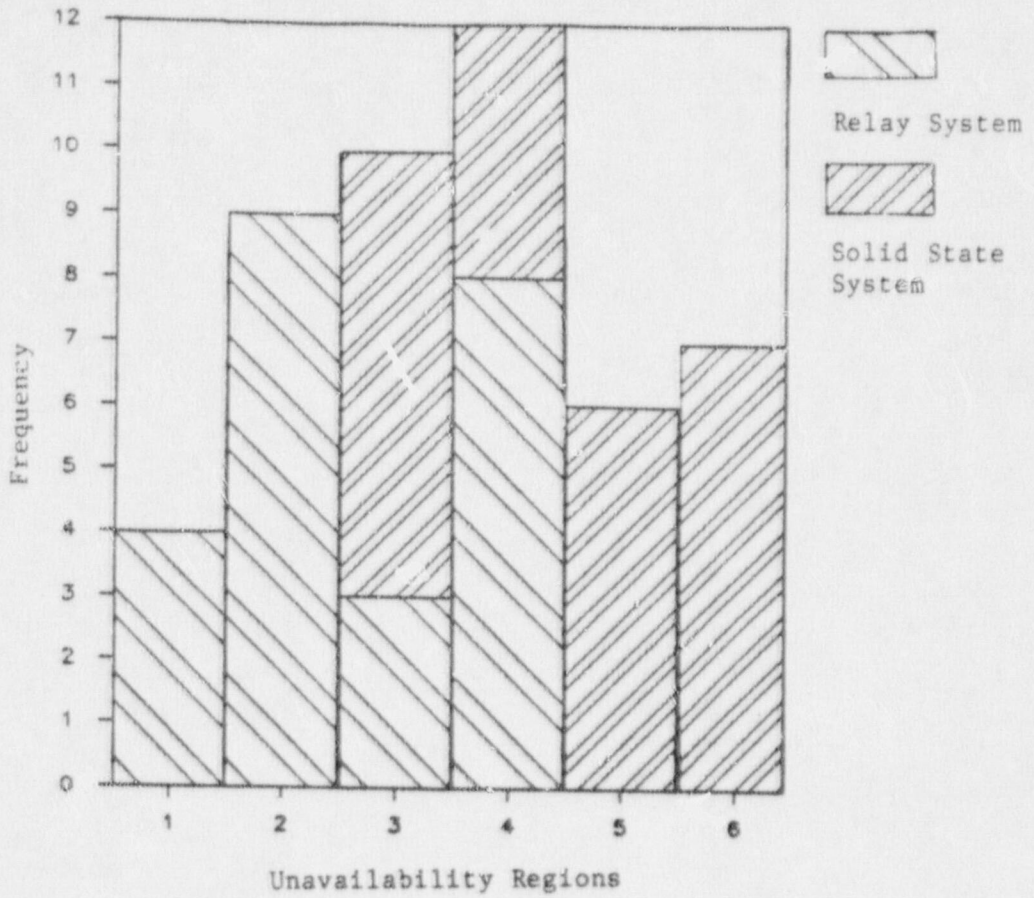
4. The risk analysis has shown that from 22 initiating events, the dominant initiating event contributor to the core damage frequency change (Case 3) was the large LOCA. Smaller contributors were the medium and small LOCAs. The dominant contributors to the man-rem exposure increase were the LOCAs with early or late core melt combined with failure of quench and recirculation sprays or loss of recirculation, respectively.

5. It was claimed that the proposed Technical Specification relaxations are applicable to all Westinghouse plants (see particularly Reference 4). The claim is based on the signal unavailability results which indicates that the unavailabilities associated with the solid state system are higher than those associated with the relay system. According to WOG, it is conservative to apply the results from risk study based on the solid state system to a plant having a relay system, assuming the plant analyses are equivalent. Since the signal unavailabilities are lower, the changes in the core damage frequency were expected by WOG to be lower in a relay plant than in a solid state plant. Thus, the signal unavailability analysis and the risk analysis results represent bounding limits for the majority of plants in question.



Region 1: (4.80E-5, 2.73E-4)
Region 2: (2.73E-4, 4.99E-4)
Region 3: (4.99E-4, 7.24E-4)
Region 4: (7.24E-4, 9.49E-4)
Region 5: (9.49E-4, 1.17E-3)
Region 6: (1.17E-3, 1.40E-3)

Figure 3.1. Distribution of 48 safety feature actuation signal unavailabilities for solid state and relay systems. (Only signals with identical logic and permissives are considered.)



Region 1: (4.80E-5, 2.73E-4)
Region 2: (2.73E-4, 4.99E-4)
Region 3: (4.99E-4, 7.24E-4)
Region 4: (7.24E-4, 9.49E-4)
Region 5: (9.49E-4, 1.17E-3)
Region 6: (1.17E-3, 1.40E-3)

Figure 3.1. Distribution of 48 safety feature actuation signal unavailabilities for solid state and relay systems. (Only signals with identical logic and permissives are considered.)

Table 3.1 Surveillance Requirements for Solid State and Relay ESFAS Designs

ESFAS Component	Solid State*		Relay System	
	Current (Base Case)	Proposed (Case 3)	Current (Base Case)	Proposed (Case 3)
Analog Channel:**				
+Test Interval (Month)	1	3	1	3
Test Time (Hour)	2	4	2	4
Maintenance Time (Hour)	1	12	1	12
Untripped Maintenance (Hour)		(6)		(6)
Logic Cabinets:				
Test Interval (Month)	2	2	1	1
Test Time (Hour)	1.5	4	3	8
Maintenance Time (Hour)	2	12	2	12
Master Relays:				
Test Interval (Month)	2	2	1	1
Test Time (Hour)	1.5	4	3	8
Maintenance Time (Hour)	2	12	6	12
Slave Relays:				
Test Interval (Month)	3	3	3	3
Test Time (Hour)	4	4	6	12
Maintenance Time (Hour)	2	12	6	12

**For the RPS Analog Channels the surveillance requirements granted previously (SER, 1985)[8] are:

	Previous	Granted	Previous	Granted
RPS Analog Channel:				
Test Interval (Month)	1	3	1	3
Test Time (Hour)	2	4	2	4
Untripped Maintenance (Hour)	1	6	1	6

*Solid State System has been used for risk analysis.
+Note that STI change is requested only for analog channels.

Table 3.2 Signal Unavailabilities (WOG Results)

Case	Unavailability of SI Signal*		Unavailability of Auxiliary Feedwater Pump Start Signal**	
	Two Train	Single Train	Two Train	Single Train
a. Solid State System				
Base	1.14E-03	2.37E-02	5.72E-04	1.09E-02
Proposed (Case 3)	1.30E-03	3.94E-02	6.39E-04	1.90E-02
b. Relay System				
Base	6.66E-04	Not given	4.80E-05	Not given
Proposed (Case 3)	8.14E-04	Not given	5.56E-05	Not given

Generated by the signal selection logic:
*Low pressurizer pressure (2/4) interlocked with permissive, P-11 (2/3).
**Steam generator water level low-low (2/4 in one loop).

Table 3.3 Results of the Risk Analysis (WOG Results)

Case	Core Damage Frequency (yr^{-1})	Man-Rem Exp.
Base	4.23E-05	288
Proposed (Case 3)	4.33E-05	293
Changes	1.0E-06 (2.4%)	5 (1.7%)

4. REVIEW OF THE UNAVAILABILITY ANALYSIS OF THE ESFAS SIGNALS

The WOG unavailability analysis of the ESFAS signals reflects by its depth and extent the importance attributed to this work by the WOG. It is obvious that the WOG is interested in achieving a reliable knowledge of the unavailability of this system in all the conceivable applications at the Westinghouse plants. This became more and more clear as the reviewers attained more and more understanding of the systems and penetrated into the intricacies of the fault tree models. As the review progressed it resulted in numerous questions and answers concerning various aspects of the unavailability analysis and the following observations are based upon this final product of the interactive review process.

The fault tree models of ESFAS for both designs; solid state and relay were evaluated with regard to adequacy of system representation including random failure modes and rates, as well as unavailability contributions due to test and maintenance, common cause failures, and human errors. From the numerous signal unavailabilities the review naturally concentrated on those which were selected by the WOG for the CDF (core damage frequency) analysis (to be reviewed in Section 5). These were: "Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)," and "Auxiliary Feedwater Start Signal Prompted by Steam Generator Level Low Low (2/4 in 1 loop)." Since the CDFs were found to be influenced more by the unavailabilities of the first signal, the review's emphasis was also concentrated on this signal.

4.1 Adequacy of System Representation

The fault trees of the above signals are provided in Appendix C of Refs. 1 and 2. The fault tree structure, which is characteristic for all the analyzed signals in the WOG analysis consists of a top fault tree, one or more middle fault trees, and then analog channel fault trees. The top fault tree describes the master and slave relays, the middle fault trees represent the logic cabinets including the permissive circuits; and the analog channel fault tree models the sensor, power supply, signal conditioning, and signal comparator circuits.

At BNL's request the WOG supplemented the original ESFAS circuit diagrams with additional detailed diagrams. These, as well as the system schematics given in Refs. 1 and 2 were compared to the system's fault trees. The fault tree models constructed by the WOG (at a level of detail down to minute electronic parts) were judged to be more than adequate for representing the systems. At that level of detail, however, it may be worthwhile to note for the sake of completeness, the omission from the trees of the loss of rack (cabinet) ventilation (or less importantly the loss of control room ventilation) which may result in a long-term failure of the ESFAS due to overheating. By the same token, mechanical failures of the cabinets were also not considered. (These very detailed fault trees might well be recommended as standard ESFAS fault tree models for future PRA work.)

4.2 Random Failures

The BNL review did not identify additional failure modes beyond those considered in the fault trees. The frequencies of various failure modes were favorably compared with data given in other data sources; e.g., with those given in the data bases for Oconee[9] and Seabrook PRAs,[10] or with those listed in a recent issue of the Military Handbook.[11]

4.3 Common Cause Failures

BNL concludes that the common cause failures were modelled satisfactorily. These included the analog channels, the logic cabinets, and the master and slave relays. For the analog channels the Atwood/Binomial failure rate method was used. For the logic cabinets as well as the master and slave relays, the beta factor method was applied. However, the potential common cause failure due to relay chattering was not included in the analysis. Due to the very low recurrence frequency at most U.S. plant sites, this omission is not expected to have a major impact on the ESFAS unavailability for the majority of the Westinghouse plants.

4.4 Human Errors

Human errors were adequately addressed in the analog channel fault trees. They were not considered, however, in the top trees which addressed the modelling of master and slave relay testing. Their omission may cause an underestimation of system unavailability mainly for the relay designs where semi. tomatic tester units are not available. Similarly, the fault trees do not model the consequences of human errors which are associated with slave relay testing when the actuated systems are not properly reconfigured from their test configurations. Although this is noted as a shortcoming of the model, it is also noted that the extended outage times, if granted, would be expected to lower the human error contribution.

4.5 Unavailability Contribution Due to Test and Maintenance

The checking of the assumptions used for proper modelling of the test and maintenance contribution to the system unavailability is one of the most important parts of the review of the system unavailability. The assumptions associated with the unavailabilities due to test and maintenance as well as comments on them follow:

A. Analog Channel Trees - (Solid state and relay designs.)

1. The fault tree model assumes that a channel is unavailable when in its bypassed condition during testing or maintenance.

2. The model assumes that all channels associated with a process parameter can be tested simultaneously. This is a conservative assumption used only for modelling purposes and is not compatible with the Technical Specification requirements concerning individual and staggered testing of these channels.

B. Top and Middle Trees (Solid state and relay designs.)

1. Only one logic train is in test or maintenance at a time.

2. During testing or maintenance the train is unavailable. In addition:

   a. for solid state systems, the testing of the logic and the permissive circuits, as well as the continuity test of the master relays are performed in bypass, and

   b. for relay systems, when the input relays are operated to test the logic combinations the associated master relay is prevented from operating.

3. During master relay (actuation) testing or maintenance the associated train is unavailable.

4. An ESFAS signal is assumed to be unavailable if equivalent slave relays in both trains are unavailable.

5. Slave relay maintenance makes only the individual slave relay unavailable.

6. The modelling of the slave relay testing, however, was found to be asymmetric for solid state and relay designs:

   a. for solid state designs, it was assumed that the slave relay test makes only the affected slave relay unavailable.

   b. for relay designs, it was assumed that the slave relay test makes the associated train unavailable.

The latter assumption used for the solid state designs reflects the practice that the actuation testing of slave relays is performed individually in a sequential process during which the actuated equipment may or may not be operated.

The assumption used for the relay design, however, reflects only the possibility that the actuation test of slave relays will be performed concurrently instead of an individual testing process. WOG characterizes this assump-

tion as conforming to general practice, and, in addition, as conservative, because the concurrent test inhibits the entire train. However, when quantifying the model, WOG takes the duration of one slave relay test. Since six slave relays are in the unavailability model of the relay design SI signal, the duration of the concurrent slave relay test is six times shorter than the total duration of a sequential testing scheme. BNL performed a sensitivity study (Appendix A) to investigate the impact of a sequential testing scheme. As shown in Appendix A, this procedure results in smaller calculated signal unavailabilities than that which would be obtained by assuming sequential slave relay testing.

In the modelling of the auxiliary feedwater pump start signal unavailability for the relay designs the question of concurrent or sequential slave relay testing does not occur because the actuation signals are directly generated by the master relays.

4.6 Audit Computations for Signal Unavailabilities

In order to audit the numerical evaluation of the fault trees performed by WOG with the WAMCUT computer code,[12] BNL used the SETS code.[13] Appropriate SETS code inputs were prepared from the fault trees and the trees were successively evaluated, i.e., first the analog channel trees, then the middle trees, and finally the top trees. The particular aim of these computer calculations were to obtain for each of the relevant signals the unavailabilities of single trains needed in the subsequent core damage frequency calculations. Not all of them were given in the submitted WOG documentation. It was desirable also to see the leading cutsets ranked according to their contribution to the train's unavailability. This information was also missing in the submittals.

As examples of the results obtained, the single train unavailabilities (Base Cases) of the "Safety Injection on Pressurizer Pressure Low (2/4) Interlocked with P-11 (2/3)" signal for solid state and relay designs are shown in Tables 4.1 and 4.2, respectively.

From an inspection of the tables one can see that the dominant contributors to the single train unavailabilities besides the expected test and maintenance are the random (mechanical and electrical) failures of the master and slave relays. Thus, the existing requirements for their relatively frequent operational testing is obviously warranted. It should also be pointed out that the unavailability contribution of the analog channels does not appear among the leading cutsets, indicating their relative insignificance.

The actual SI and AFWS pump start signal unavailability values (base and proposed cases) for single trains and for both trains of the solid state ESFAS are presented in Table 4.3. The table also displays the common cause failure contributions.

The unavailability values (base and proposed cases) of the same signal for the relay design systems are given in Table 4.4. The table presents two sets of values for each signal; one set for concurrent and another set for sequential slave relay testing. The calculation of single train and system unavailabilities for sequential slave relay testing is described in Appendix A. The table also indicates the common cause failure contributions.

The unavailability values of both Tables 4.3 and 4.4 were then used as inputs to the support state model of the Millstone Unit 3 PSS to complete the independent BNL quantification.

4.7 Results of Audit Calculations on ESFAS Signal Unavailabilities

The results of the audit runs with the SETS code were found to be in agreement with the presented unavailabilities in the WOG submittals. Therefore, BNL concurs with the following findings of the WOG unavailability analysis:

1. Analog channel contribution to signal unavailability is negligible for the solid state systems. This is also valid for the relay systems when the signals are generated through the slave relays. Considering process parameter signal diversity, the analog channel contribution is even smaller. Consequently, the BNL review supports

the finding of the WOG analysis that the question of staggered and non-staggered testing of the analog channels is not important from the point of view of ESFAS unavailability.

2. For the relay design systems when a signal is not generated through the slave relays as Table 4.4 shows; the analog channel (common cause) contribution increases to the total system unavailability. However, even in these cases, due to process parameter signal diversity, the analog channel contribution may still remain relatively small.

3. Generally, common cause failures (logic trains, master and slave relays) are the main contributors (60-90%) to the ESFAS system unavailability.

Table 4.1 Dominant Cutsets for Solid State ESFAS Single Train Based Upon Safety Injection on Pressurizer Pressure Low (2/4) Interlocked with P-11 (2/3) - Base Case

Term #	Prob. of Term	Cutset	Description
1	3.1200E-03	TAT	Train A unavailable due to test*
2	1.8500D-03	SRC1T	Slave relay (C1...D3) unavailable due to test
3	1.8500E-03	SRC2T	
4	1.8500E-03	SRC3T	
5	1.8500E-03	SRD1T	
6	1.8500E-03	SRD2T	
7	1.8500E-03	SRD3T	
8	1.7800E-04	SSPSB	Failure of SSPS to generate actuation signal
9	4.3200E-04	SRC1MB	Slave relay (C1...D3) fails due to mechanical binding
10	4.3200E-04	SRC2MB	
11	4.3200E-04	SRC3MB	
12	4.3200E-04	SRD1MB	
13	4.3200E-04	SRD2MB	
14	4.3200E-04	SRD3MB	
15	3.4700E-04	MRCM	Train B master relay C unavailable due to maintenance**
16	3.4700E-04	MRDM	Train B master relay D unavailable due to maintenance**
17	2.8800E-04	MRDMB	Master relay D fails due to mechanical binding
18	2.8800E-04	MRCMB	Master relay C fails due to mechanical binding
19	2.3100E-04	SRC1M	Slave relay (C1...D3) unavailable due to maintenance
20	2.3100E-04	SRC2M	
21	2.3100E-04	SRC3M	
22	2.3100E-04	SRD1M	
23	2.3100E-04	SRD2M	
24	2.3100E-04	SRD3M	
25	1.4400E-04	GATE4TA	Inverter gate failed open
26	1.4400E-04	MXZ13TA	Multiplex IC Z13 failed short
27	1.4400E-04	PRWIRTA	Printed wiring open
28	1.4400E-04	INGATETA	Input gate failed open
29	1.4400E-04	WIRTA	Printed circuit board wiring failed open
30	1.4400E-04	GATE3TA	Output gate failed shorted

Table 4.1 (Continued)

Term #	Prob. of Term	Cutset	Description
31	1.4400E-04	MXZ7TA	Multiplex IC Z7 failed short
32	1.4400E-04	LZ12TA	Card A313 logic IC Z12 failed open
33	1.0800E-04	SRC1FS	Slave relay (C1...D3) fails shorted electrically
34	1.0800E-04	SRC2FS	
35	1.0800E-04	SRC3FS	
36	1.0800E-04	SRD1FS	
37	1.0800E-04	SRD2FS	
38	1.0800E-04	SRD3FS	
39	7.2000E-05	MRCFSB	Master relay C fails shorted
40	7.2000E-05	MRDFS	Master relay D fails shorted
41	5.4000E-05	118VAC	Loss of 118 V AC to slave relays
42	3.6000E-05	15VDCA	15 V DC power supply faults
43	3.6000E-05	48VDC	Loss of 48 V DC power to master relays
44	2.5900E-05	BTRANSTA	Bias transistor failed open
45	2.5900E-05	PTRANTA	Power transistor failed open
46	2.1000E-05	SRC1CS	Slave relay (C1...D3) contacts do not close to start component
47	2.1000E-05	SRC2CS	
48	2.1000E-05	SRC3CS	
49	2.1000E-05	SRD1CS	
50	2.1000E-05	SRD2CS	
51	2.1000E-05	SRD3CS	
52	1.8600E-05	ZD62TA	Card A313 Zener DIODE CR 62 failed short
53	1.8600E-05	ZZDDTA	Output Zener DIODE failed shorted
54	1.8600E-05	ZENDTA	Input Zener DIODE failed open
55	1.8600E-05	ZD59TA	Card A313 Zener DIODE CR 59 failed short
56	1.4000E-05	MRCCS	Master relay C contacts do not close
57	1.4000E-05	MRDCS	Master relay D contacts do not close
58	1.0800E-05	SRC1EL	Slave relay (C1...C3) fails open electrically
59	1.0800E-05	SRC2EL	
60	1.0800E-05	SRC3EL	

Table 4.1 (Continued)

Term #	Prob. of Term	Cutset	Description
61	1.0800E-05	SRD1EL	Slave relay (D1...D3) fails open electrically
62	1.0800E-05	SRD2EL	
63	1.0800E-05	SRD3EL	
64	7.2000E-06	MRDEL	Master relay D fails open electrically
65	7.2000E-06	MRCEL	Master relay C fails open electrically
66	5.4400E-06	DIODTA	Output diode failed open
67	5.4400E-06	BDIODTA	Blocking diode failed open
68	5.4400E-06	D48TA	Input diode CR 48 failed open
69	5.4400E-06	D60TA	Card A313 output diode CR 60 failed open
70	5.4400E-06	D52TA	Input diode CR 52 failed open
71	3.5300E-06	BRES1TA	Bias resistor failed shorted
72	3.5300E-06	BRESTA	
73	5.3800E-07	P38TA	Input pin 38 failed open
74	5.3800E-07	RPINTA	Reset pin shorts to ground
75	5.3800E-07	P34TA	Card A313 output pin 34 failed open
76	5.3800E-07	PIN2TA	Pin 2 failed open
77	5.3800E-07	PIN37TA	Input pin 37 failed open
78	5.3800E-07	PIN46TA	Pin 46 failed open
79	5.3800E-07	INPINTA	Input pin failed open
80	5.3800E-07	PIN1TA	Output pin to ground failed open
81	5.3800E-07	PINTA	Output pin failed open
82	2.0736E-08	GATE1TA*	Inverting gates 1 & 2 failed open
		GATE2TA	
83	7.7472E-11	RGATETA*	Reset gate failed open & pin shorts to ground
		PINSGTA	
The sum of the term values is:			2.37E-02

*Includes sequential testing of logic and master relays.
**Includes also half of the unavailability due to logic maintenance.

Table 4.2 Dominant Cutsets for Relay ESFAS Single Train Based Upon Safety Injection on Pressurizer Pressure Low (2/4) Interlocked with P-11 (2/3) - Base Case

Term #	Prob. of Term	Cutset	Description
1	1.1111E-02	TAT	Train A unavailable due to test*
2	9.2600E-04	MRAM	Train A unavailable due to maintenance of master relay and logic
3	6.9400E-04	SRA1M	Slave relay (A1...B3) unavailable due to maintenance
4	6.9400E-04	SRA2M	
5	6.9400E-04	SRA3M	
6	6.9400E-04	SRB1M	
7	6.9400E-04	SRB2M	
8	6.9400E-04	SRB3M	
9	4.3200E-04	SRA1MB	Slave relay (A1...B3) fails due to mechanical binding
10	4.3200E-04	SRA2MB	
11	4.3200E-04	SRA3MB	
12	4.3200E-04	SRB1MB	
13	4.3200E-04	SRB2MB	
14	4.3200E-04	SRB3MB	
15	1.4400E-04	MRAMB	Master relay A unavailable due to mechanical binding
16	1.0800E-04	SRA1FS	Slave relay (A1...B3) fails shorted
17	1.0800E-04	SRA2FS	
18	1.0800E-04	SRA3FS	
19	1.0800E-04	SRB1FS	
20	1.0800E-04	SRB2FS	
21	1.0800E-04	SRB3FS	
22	5.4000E-05	125VDCA	Loss of 125 V DC power
23	3.6000E-05	MRAFS	Master relay A fails shorted
24	2.1000E-05	SRA1TCS	Test relay (A1...B3) contacts fail open
25	2.1000E-05	SRA2TCS	
26	2.1000E-05	SRA3TCS	
27	2.1000E-05	SRB1TCS	
28	2.1000E-05	SRB2TCS	
29	2.1000E-05	SRB3TCS	

Table 4.2 (Continued)

Term #	Prob. of Term	Cutset	Description
30	2.1000E-05	SRA1CS	
31	2.1000E-05	SRA2CS	
32	2.1000E-05	SRA3CS	Slave relay (A1...B3) contacts do not close
33	2.1000E-05	SRB1CS	
34	2.1000E-05	SRB2CS	
35	2.1000E-05	SRB3CS	
36	1.0800E-05	SRA1	
37	1.0800E-05	SRA2	
38	1.0800E-05	SRA3	Slave relay (A1...B3) fails open
39	1.0800E-05	SRB1	
40	1.0800E-05	SRB2	
41	1.0800E-05	SRB3	
42	6.9800E-06	MRACS	Master relay A contacts do not close
43	6.9800E-06	MRARCS	Reset relay contacts fail open
44	6.9800E-06	TEST1	Test contacts fail open
45	3.6000E-06	MRA	Master relay A fails open
46	1.3000E-06	BCONT1	Blocking contacts fail open
47	1.3000E-06	MRARSW	Reset switch contacts fail open
48	2.3148E-07	BCHAN2*	
		BCHAN3*	Bistable channel 2,3, and 4 do not remove power
		BCHAN4	
49	2.3148E-07	BCHAN1*	
		BCHAN3*	Bistable channel 1,3, and 4 do not remove power
		BCHAN4	
50	2.3148E-07	BCHAN1*	
		BCHAN2*	Bistable channel 1,2, and 4 do not remove power
		BCHAN4	
The sum of the term values is:		2.11 E-02	

*Includes sequential testing of logic, master relay, and concurrently performed slave relay tests.

Table 4.3 Unavailabilities of ESFAS Signals - Solid State System

	Unavailability of the Safety Injection Signal			Unavailability of the Auxiliary Feedwater Pump Start Signal		
	Base Case	Proposed Case		Base Case	Proposed Case	
Single Train	2.37E-02	3.94E-02		1.09E-02	1.90E-02	
Two Trains	1.14E-03	1.30E-03		5.72E-04	6.39E-04	
Common Cause Contributions	Slave Relays:		5.18E-04	Slave Relays:		1.73E-04
	Master Relays:		1.15E-04	Master Relays:		5.76E-05
	Logic Cabinets:		3.17E-04	Logic Cabinets:		2.60E-04
	Analog Channels:		1.50E-05	Analog Channels:		1.50E-05
	Total		9.65E-04	Total		5.06E-04

Table 4.4 Unavailabilities of ESFAS Signals - Relay System

	Unavailability of the Safety Injection Signal		Unavailability of the Auxiliary Feedwater Pump Start Signal	
	Base Case	Proposed Case	Base Case	Proposed Case
Single Train				
-Concurrent Slave Relay Testing	2.11E-02	4.45E-02	9.70E-03	2.55E-02
-Sequential Slave Relay Testing	3.50E-02	7.23E-02	9.70E-03	2.55E-02
Two Trains				
-Concurrent Slave Relay Testing	6.66E-04	8.14E-04	4.80E-05	5.56E-05
-Sequential Slave Relay Testing	7.35E-04	9.68E-04	4.80E-05	5.56E-05
Common Cause Contributions	Slave Relays:	5.18E-04	Slave Relays:	---
	Master Relays:	2.88E-05	Master Relays:	2.88E-05
	Logic Cabinets:	1.26E-06	Logic Cabinets:	0.0
	Analog Channels:	1.50E-05	Analog Channels:	1.50E-05
	Total	5.63E-04	Total	4.80E-05

5. CORE DAMAGE FREQUENCY CALCULATIONS

5.1 Objectives

This section describes the approach and the results of Core Damage Frequency (CDF) Calculations for the Millstone Unit 3 power plant performed at BNL.

The objectives of the CDF calculations were the following:

a. To perform an independent evaluation of the impact of proposed Technical Specification modifications on the CDF by applying an approach similar to that of the WOG (i.e. similar assumptions and conditions),

b. To check the WOG's claim that the core damage frequency increase obtained for a plant having a solid state ESFAS design is bounding for plants with relay ESFAS designs and if it is not bounding, to what extent,

c. To estimate the sensitivity of the CDF to the assumption of concurrent vs. sequential testing of slave relays at relay design plants, and

d. To determine an overall bounding CDF increase for the ESFAS, which if found acceptable by the NRC would render the proposed Technical Specification modifications generally applicable to the majority of Westinghouse plants (i.e., solid state and relay; 2/4 and 2/3 logic)

The CDF calculations represent the most important part of the review. Since they are based on the Millstone 3 PSS and the WOG's modifications, they might seem to be somewhat complicated. For the sake of better understanding, therefore, they will be presented in a more detailed form in the subsections below.

5.2 Calculational Approach

To validate the WOG calculations, BNL used the following approach:

1. Instead of a single typical Safety Injection Signal representing all types of actuation signals as was done in the Millstone 3 PSS, the WOG procedure and the BNL review used two kinds of ESFAS signals for various initiators. Table 5.1 identifies the leading internal initiators of the Millstone 3 PSS and the associated ESFAS and Process Parameter Signals that would be triggered by each initiating event.

2. Conforming to the success criteria used in the Millstone 3 PSS, only one train of Safety Systems in the ECCS was required for accident mitigation and any one auxiliary feedwater train (out of three) was required to be operable for the success of that system. Failure to manually start at least one auxiliary feedwater train was assumed to be .01 (the same value that was assumed in the WOG analysis).

3. Signal unavailabilities from both types of ESFAS design; solid state and relay were propagated through the support system state model of the Millstone 3 PSS. In the WOG calculations only solid state ESFAS unavailabilities were applied.

4. For the relay design, two signal unavailabilities were used (representing concurrent and sequential slave relay testing, respectively.)

5. For each signal unavailability, two numerical values were considered; the one corresponding to the base case, and the one corresponding to the proposed case (denoted as Case 3 in the WOG documents).

6. The probabilities for the failure of recovery of ESFAS signals were the same as those in the WOG analysis:

- 1.0 (no recovery) for large LOCA
- 0.1 for medium LOCA
- 0.01 for all other initiators

These probabilities were taken into account via the support state model.

7. The support state probabilities developed in conjunction with the initiators were propagated through all the event tree models where the support state probabilities were significantly dependent on the ESFAS unavailability. For these event trees the CDFs were evaluated in both of the cases; the base and the proposed case. The ESFAS dependency of the event trees through the support states (see more about this below) was determined by an earlier screening review. initiators whose associated support state probabilities were found completely or practically independent of ESFAS, the CDFs obtained in the Millstone 3 PSS were accepted without any changes.

   Section A and Section B of Table 5.2 list the ESFAS-dependent and the ESFAS-independent initiators with their original CDFs given in the Millstone 3 PSS. Section A of Table 5.2 contains several other quantities as well whose roles in the total CDF calculations will be discussed later.

   The sum of CDFs of ESFAS-independent initiators (see Subtotal B of Section B of Table 5.2) is

$$\sum_{i=15}^{21} (CDF)_i = 1.956E\text{-}05 \approx 1.96E\text{-}05(yr^{-1}),$$

   where i denotes the i^{th} initiating event in Table 5.2. This sum represents the total ESFAS-independent contribution to be used in Table 5.11, where the calculation of total CDFs is presented.

5.3 Support State Model and Accident Sequence Representation in the Millstone 3 PSS

In various probabilistic risk studies of reactor accidents, the unavailability of the ESFAS system is usually incorporated into either the event trees or into the support state model. The Millstone 3 PSS incorporated the ESFAS into the support state model. The Millstone support state model includes, besides the ESFAS system, the electrical power, the emergency generator load sequencer, and the service water systems.

The support system model is analyzed conditional on the initiating event and the partial or total unavailability of the above support systems. Figure 5.1 shows the support state model of the Millstone 3 PSS for initiators where the ESFAS is important. The model results in 72 states, which by their impact on the frontline systems, can be reduced to 8 unique support states. The definition of these support states is given in Table 5.3.

It is clear from the model shown in Figure 5.1 that the probability of being in any particular support state will depend on the unavailabilities of the individual ESFAS trains and the whole ESFAS. Any changes in these unavailabilities will impact the state probabilities.

In the Millstone 3 PSS the support state probabilities are referred to as support state split fractions. By using the support state technique the event trees of the Millstone 3 PSS themselves do not involve the ESFAS, but each tree associated with an initiator has to be evaluated for each of the 8 support states, which do. The procedure leads to the determination of the CDFs for individual accident sequences, or for several similar sequences (Plant Damage States, PDS) or for the sum of all sequences (sum of all the Plant Damage States) in a given tree.

Corresponding to the above description, e.g., the frequency of an accident sequence in the Millstone 3 PSS can be represented by the symbolic equation:

Frequency of an accident sequence to PDS-X =

IE*	initiating event frequency,
SSP(IE,SJ)*	support state probability for state J,
TOP_1(IE,SJ)*	
TOP_2(IE,SJ)*	logical union of conditional probabilities of top
.....	events in event tree IE for support state J.

This representation of accident sequences significantly facilitates the study of the impact of unavailability changes of support systems to the core damage frequencies. It is easy to see that whenever an accident sequence is already quantified and there is a change in the unavailability of a support system, in order to obtain the new frequency of the accident sequence only the ratio of the new and old support state probabilities needs to be calculated.

5.4 Calculation of Support State Probabilities

To determine the variation of the support state probabilities corresponding to the variation of the ESFAS unavailabilities due to changes in the test and maintenance times, a SETS-code computer model was constructed. The computer model maps the Millstone Unit 3 support state model shown in Fig. 5.1 and computes its state probabilities regrouped into the eight main states defined in Table 5.3.

The following cases were computed with the SETS-code:

A. For Solid State ESFAS:

1. Reproduction of Millstone 3 PSS Support State Probabilities.

This was needed in order to check whether BNL's understanding of the original Millstone 3 PSS support state model was correct or not. In addition, the reproduced support state probabilities served as reference probabilities for requantification of the ESFAS-dependent accident sequences.

2. Support State Probabilities for Large LOCA (base and proposed cases).

As input unavailabilities to the support state model, the "Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)" safety injection signal unavailabilities were used without considering any human recovery actions given a complete loss of the signal.

3. Support State Probabilities for Medium LOCA (base and proposed cases).

As input to the support state model, the above safety injection signal unava labilities were used with a failure probability of 0.1 for signal recovery (given a complete loss of the signal).

4. Support State Probabilities for Small LOCA and Steam Generator Tube Ruptures (base and proposed cases).

As input to the support state model, the above safety injection signal unavailabilities were used with a failure probability of 0.01 for signal recovery (given a complete loss of the signal).

5. Support State Probabilities for Other Initiators i.e., other than LOCAs or Steam Generator Tube Rupture (base and proposed cases).

As input to the support state model, the "Auxiliary Feedwater Pump Start" signal unavailabilities were used with a failure probability of 0.01 for signal recovery (given a complete loss of the signal).

Table 5.4 lists the results obtained for all of these cases. The underlined values agree completely with those given recently by WOG in Ref. 5.

B. For Relay ESFAS:

Except Case 1 (which was performed as a check to verify the BNL model against the Millstone results), all the previous cases (with similar signal recovery failure probabilities) were run twice:

- for signal unavailabilities when the testing of the slave relays was assumed to be carried out concurrently, and
- for signal unavailabilities, when the testing of the slave relays was assumed to be carried out sequentially.

Tables 5.5 and 5.6 show the results obtained for concurrent and sequential slave relay testing, respectively. Note, that the support state probabilities for "Other Initiators" are the same for both cases; concurrent and sequential slave relay testing. The reason for this, as was mentioned in Section 4, is that in the unavailability model of the relay "Auxiliary Feedwater Pump Start" signal, there is no slave relay to be tested. The actuation signal generated by the master relay is assumed to directly start the associated auxiliary feedwater train.

5.5 Requantification of ESFAS-Dependent Event Trees

According to the WOG analysis, the large and medium LOCA event trees are the most sensitive to the unavailability changes of the ESFAS. Therefore, these event trees were completely requantified at BNL.

In Plant Damage State vs. Support State representation, Tables 5.7.A and 5.7.B display the large LOCA CDFs for the solid state ESFAS in the base and proposed cases, respectively. Tables 5.7.C and 5.7.D display the large LOCA CDFs for the relay ESFAS, when concurrent slave relay testing is assumed. Tables 5.7.E and 5.7.F show also the large LOCA CDFs for relay ESFAS, when the slave relay testing is assumed to be sequential.

A similar set of tables, Tables 5.8.A through 5.8.F present the CDFs for medium LOCA.

In order to validate the CDF calculations performed by the WOG, the CDFs for individual dominant large and medium LOCA sequences were also determined at BNL. These sequences occur mainly in support states, S1 through S4. Table 5.9 lists the results of the calculation for solid state ESFAS compared with the CDFs given by WOG in Ref. 5. The table does not list the dominant

accident sequences in support state S1 because these do not differ to any degree from those originally determined in the Millstone 3 PSS.

Table 5.9 also lists the requantified dominant accident sequences for all the initiators whose associated support states are ESFAS-dependent. An inspection of the table shows there is a very good agreement between the results of WOG and BNL for those sequences which were identified in both of the calculations. However, BNL identified several dominant sequences not listed in Ref. 5. These sequences are noted in the table with lower case letters adjoining to the WOG serial number of the last commonly identified accident sequence.

Table 5.10 presents the results of the CDF calculations for the dominant sequences for relay ESFAS signal unavailabilities.

Since the CDF values were already determined in Tables 5.7.A through F and 5.8.A through F for the large and medium LOCA event trees respectively, from Tables 5.9 and 5.10 only "the sums of the dominant sequences w/o large and medium LOCAs" values will be used for the evaluation of total CDF values in the following section.

5.6 Determination of Total Core Damage Frequencies

To determine the total CDFs the partial results obtained in previous subsections are integrated here.

The various CDF contributions are summarized in Table 5.11. Most of the contributions are taken directly from other tables presented earlier. Some entries into Table 5.11, however, were obtained by some additional calculation.

The descriptions of these entries are given below:

1,2. The CDF contributions from the large and medium LOCAs are taken from Tables 5.7.A through F and 5.8.A through F, respectively.

- ESFAS-dependent initiators (other than large and medium LOCAs):

3. The CDFs of the dominant accident sequences in support state S1 are essentially insensitive to ESFAS signal unavailability changes. Therefore, the sum of the Millstone 3 PSS values was taken from Table 5.2 Part A.

4. The sum of the CDFs of the dominant accident sequences in support states S2 to S8 were calculated in Tables 5.9 and 5.10. These sums represent the entries into Table 5.11. The CDF contributions from non-dominant sequences were determined for each individual initiator in Table 5.2 Part A. The table also indicates their sums for the subgroup consisting of small LOCA and steam generator tube rupture and for the subgroup consisting of "other" initiators. Subgroups had to be formed because the signal unavailabilities for the two groups are different.

5. The CDF entries into Table 5.11 from the group of small LOCA and steam generator tube rupture were calculated by requantifying the group sum value given in Table 5.2. Part A with the assumption that each of the constituent sequences were in Support State 2.

6. The CDF entries into Table 5.11 from the group of "other than small LOCA or steam generator tube rupture initiators" were calculated by requantifying the group sum value given in Table 5.2 Part A with the assumption that all of the constituent sequences were in Support State 2.

The assumption that the above non-dominant sequences are in the support state S2 is considered to be conservative because it results in a significant change of CDF from base case to the proposed one. Presumably, WOG either neglected the contributions of these sequences or assumed that they were in support state S1.

- ESFAS-Independent Initiators:

7. The CDF contribution due to these initiators was given in Table 5.2 Part B. This value was taken from there without any alteration.

The total CDFs for solid state and relay ESFAS designs obtained by the summation of the above entries are also displayed in Table 5.11. The table also indicates the CDF increases for the proposed cases.

5.7 Discussions of the Results

A comparison of the total CDF values in Tables 5.11 reveal the following:

1. The CDFs associated with the relay ESFAS are smaller than the CDFs associated with the solid state ESFAS in the base cases. In this respect, the results of BNL are in agreement with those of the WOG.

2. The increase of the CDF from the base case to the proposed case calculated by BNL for the solid state ESFAS (2.8%) can be considered to be in a rough but acceptable agreement with the value (2.4%) obtained by the WOG.

3. The increases of the CDF from the base case to the proposed case calculated by BNL for the relay ESFAS are bigger than the increase obtained for solid state ESFAS. This is at variance with the claim of WOG, which stated that the CDF increase for the relay ESFAS was bounded by the CDF increase obtained for the solid state ESFAS, but did not do any calculation to prove the claim.

4. If the CDF calculation had been carried out for the relay ESFAS by WOG and they had assumed sequential slave relay testing as they did in the risk analysis for the solid state ESFAS, they would have obtained a CDF increase about double the value obtained for the solid state ESFAS.

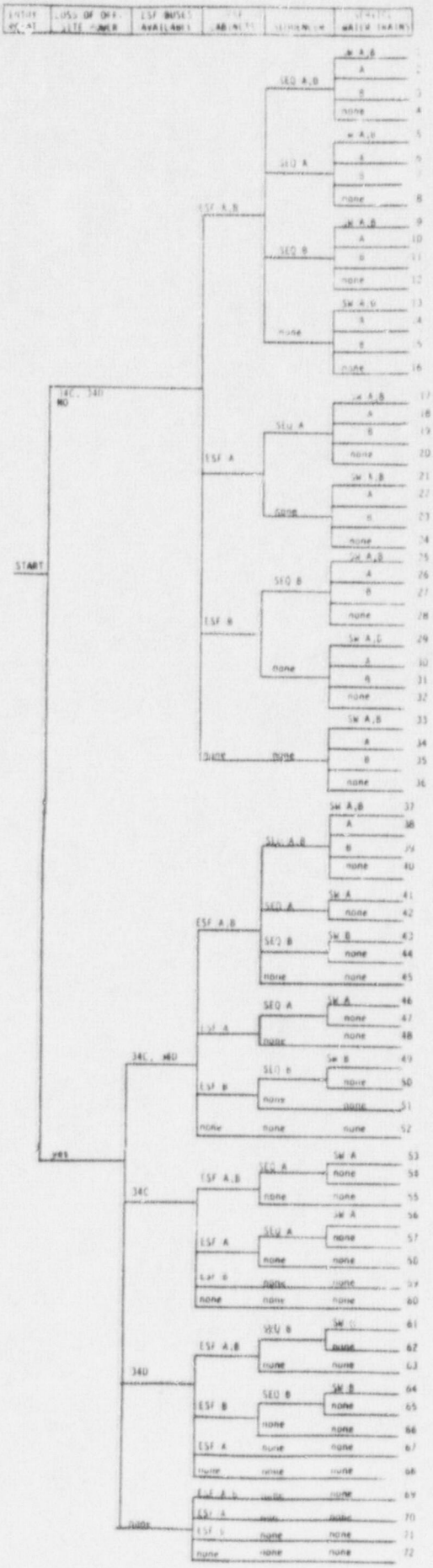


Figure 5.1. Millstone Unit 3
Support State Model

Table 5.1 Accident Initiators, ESFAS and Process Parameter Signals Used in the CDF Calculations

Initiating Event	Description	ESFAS Signal	Process Parameter Signal
1	Large LOCA	Safety Injection	Low Pressurizer Pressure (2/4) interlocked with Permissive, P-11 (2/3).
2	Medium LOCA		
3	Small LOCA		
4	Steam Generator Tube Rupture		
5	Steam Break Inside Containment	Auxiliary Feedwater Pump Start	Steam Generator Level Low Low (2/4 in one loop)
6	Steam Break Outside Containment		
7	Loss of RCS Flow		
8	Loss of Main Feedwater		
9	Primary to Secondary Power Mismatch		
10	Turbine Trip		
11	Reactor Trip		
12	Core Power Excursion		
13	Spurious Safety Injection		
14	Loss of Offsite Power		
15	Incore Instrumentation Tube Failure		
16	Interfacing Systems LOCA - V Sequence		
17	Loss of One Service Water Train		
18	Loss of One Vital DC Bus 1 or 2		
19	Loss of Both Vital DC Busses		
20	Loss of Vital AC Bus 1 or 2		
21	Loss of Vital AC Bus 3 or 4		
22*	Anticipated Transients without Scram	ESFAS Signal+ Reactor Trip	See above

*The ATWS event tree is included in the event trees of other initiators.

Table 5.2 Internal Core Damage Frequencies with Recovery by Initating Events in the Millstone PSS.

A. Initiating Events with ESFAS Dependent Event Trees

Initiating Event,(i)	Description	Core Damage Frequency CDF_i, (yr^{-1})	CDF Contribution of Dominant Sequences (yr^{-1})		CDF Contribution of Non-Dominant Sequences (yr^{-1})
			Support State 1	Support States 2-8	Support States 1-8
1	Large LOCA	2.37E-06	2.29E-06	---	8.0 E-08
2	Medium LOCA	5.49E-06	5.32E-06	1.38E-07	3.0 E-08
3	Small LOCA	1.58E-06	1.39E-06	1.46E-08	1.75E-07
4	Steam Generator Tube Rupture	1.66E-06	8.52E-07	5.57E-07	2.51E-07
5	Steam Break Inside Containment	2.69E-08*	2.69E-08	---	---
6	Steam Break Outside Containment	3.51E-06	2.78E-06	5.56E-07	1.74E-07
7	Loss of RCS Flow	5.23E-07	1.20E-07	7.89E-08	3.24E-07
8	Loss of Main Feedwater	7.77E-07	2.89E-07	2.12E-07	2.76E-07
9	Primary to Secondary Power Mismatch	4.08E-06	2.07E-06	1.60E-06	4.11E-07
10	Turbine Trip	2.48E-06	1.15E-06	9.73E-07	3.57E-07
11	Reactor Trip	3.23E-06	1.49E-06	1.27E-06	4.80E-07
Subtotal A		2.57E-05	1.78E-05	5.40E-06	2.56E-06
Subtotal A w/o Large and Medium LOCAs		1.79E-05	1.02E-05	5.26E-06	2.45E-06
Sum of i=3,4			2.24E-06		4.26E-07
Sum of i=5,11			7.93E-06		2.02E-06

*The CDF for this initiator is assumed to be completely associated with support state S1.

Table 5.2 (Continued)

B. Initiating Events with "ESFAS" Independent" Event Trees

Initiating Event,(i)	Description	Frequency CDF_i,(yr^{-1})
12	Core Power Excursion	7.65E-08
13	Spurious Safety Injection	5.32E-08
14	Loss of Offsite Power	6.68E-06
15	Incore Instrumentation Tube Failure	1.60E-07
16	Interfacing Systems LOCA - V Sequence	1.90E-06
17	Loss of One Service Water Train	7.10E-07
18	Loss of One Vital DC Bus 1 or 2	2.37E-06
19	Loss of Both Vital DC Busses	6.31E-10
20	Loss of Vital AC Bus 1 or 2	4.16E-06
21	Loss of Vital AC Bus 3 or 4	3.45E-06
Subtotal B		1.96E-05
Total A + B		4.53E-05

Table 5.3 Millstone Unit 3 Support States

Support State	Offsite Electrical Power Available	ESF Buses Energized	ESFAS Trains Actuated	EGLS Trains Actuated	Service Water Trains Available
1	Yes	34C+34D	A+B	A+B	A+B
2	Yes	34C+34D	A or B	A or B	A or B
3	Yes	34C+34D	A or B	A or B	None
4	Yes	34C+34D	None	None	None
5	No	34C+34D	A+B	A+B	A+B
6	No	34C or 34D	A or B	A or B	A or B
7	No	None	A or B	None	None
8	No	None	None	None	None

Table 5.4 Probabilities of Support States Generated by Solid State ESFAS Signal Unavailabilities[+]

Support State	Millstone[++]	Large LOCA		Medium LOCA		Small LOCA, Steam Generator Tube Rupture		Other Initiators	
		Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case
S1	9.96E-01	9.50E-01	9.18E-01	9.93E-01	9.90E-01	9.97E-01	9.97E-01	9.97E-01	9.97E-01
S2	4.02E-03	4.89E-02	8.03E-02	6.41E-03	9.54E-03	2.16E-03	2.47E-03	1.90E-03	2.06E-03
S3	2.74(-7) [2.55E-07]*	6.19E-05	8.76E-05	5.59E-06	8.23E-06	5.96E-07	8.60E-07	3.61E-07	5.17E-07
S4	1.61E-07	1.14E-03	1.30E-03	1.14E-04	1.30E-04	1.14E-05	1.30E-05	5.72E-06	6.39E-06
S5	3.03E-04	2.83E-04	2.74E-04	3.01E-04	3.00E-04	3.02E-04	3.02E-04	3.02E-04	3.02E-04
S6	4.92E-06	2.31E-05	3.23E-05	5.61E-06	6.56E-06	4.33E-06	4.42E-06	4.25E-06	4.30E-06
S7	6.23E-08 [6.49E-08]*	3.75E-07	5.20E-07	8.57E-08	9.22E-08	7.65E-08	7.71E-08	7.59E-08	7.63E-06
S8	1.06E-10 [9.63E-11]**	3.50E-07	3.99E-07	3.88E-08	4.42E-08	7.53E-09	8.59E-09	3.78E-09	4.22E-09

+ Safety injection signal unavailabilities are applied for all of the LOCAs and for the steam generator tube rupture accident. For other initiators the auxiliary feedwater system actuation signal unavailabilities are applied.

++ There is a good agreement between the values calculated at BNL and those given in Millstone PSS if it is not indicated otherwise. Bracketed values are given in Millstone PSS.

* Error in original Millstone PSS calculations.

** Rounding differences only.

Underlined values are used in individual accident sequence calculations by WOG. Within rounding errors there is complete agreement between the results of BNL and WOG.

Table 5.3 Probabilities of Support States Generated by Relay ESFAS Signal Unavailabilities+
Concurrent Slave Relay Testing

Support State	Large LOCA		Medium LOCA		Small LOCA, Steam Generator Tube Rupture		Other Initiators	
	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case
S1	9.55E-01	9.08E-01	9.94E-01	9.89E-01	9.98E-01	9.97E-01	9.98E-01	9.97E-01
S2	4.38E-02	9.04E-02	5.89E-03	1.06E-02	2.10E-03	2.57E-03	1.88E-03	2.19E-03
S3	5.77E-05	9.60E-05	5.15E-06	9.08E-06	5.52E-07	9.45E-07	3.61E-07	6.26E-07
S4	6.66E-04	8.14E-04	6.54E-05	8.14E-05	6.64E-06	8.14E-06	4.80E-07	5.56E-07
S5	2.88E-04	2.71E-04	3.01E-04	3.00E-04	3.02E-04	3.02E-04	3.02E-04	3.02E-04
S6	2.16E-05	3.53E-05	5.46E-06	6.87E-06	4.31E-06	4.45E-06	4.24E-06	4.34E-06
S7	3.51E-07	5.67E-07	8.46E-08	9.43E-08	7.64E-08	7.73E-08	7.59E-08	7.65E-08
S8	2.05E-07	2.50E-07	2.26E-08	2.77E-08	4.90E-09	5.38E-09	3.17E-10	3.67E-10

+Safety injection signal unavailabilities are applied for all of the LOCAs and for the steam generator tube rupture accident. For other initiators the auxiliary feedwater system actuation signal unavailabilities are applied.

Table 5.6 Probabilities of Support States Generated by Relay ESFAS Signal Unavailabilities+
Sequential Slave Relay Testing

Support State	Large LOCA		Medium LOCA		Small LOCA, Steam Generator Tube Rupture		Other Initiators	
	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case
S1	9.27E-01	8.53E-01	9.91E-01	9.83E-01	9.97E-01	9.97E-01	9.98E-01	9.97E-01
S2	7.15E-02	1.46E-01	8.66E-03	1.61E-02	2.38E-03	3.13E-03	1.88E-03	2.19E-03
S3	8.04E-05	1.42E-04	7.49E-06	1.38E-05	7.86E-07	1.41E-06	3.61E-07	6.26E-07
S4	7.35E-04	9.68E-04	7.35E-05	9.68E-05	7.35E-06	9.68E-06	4.80E-07	5.56E-07
S5	2.77E-04	2.54E-04	3.00E-04	2.98E-04	3.02E-04	3.02E-04	3.02E-04	3.02E-04
S6	2.98E-05	5.16E-05	6.29E-06	8.54E-06	4.39E-06	4.62E-06	4.24E-06	4.34E-06
S7	4.80E-07	8.25E-07	9.04E-08	1.06E-07	7.69E-08	7.85E-08	7.59E-08	7.65E-08
S8	2.76E-07	2.97E-07	2.50E-08	3.29E-08	4.86E-09	6.40E-09	3.17E-10	3.67E-10

+Safety injection signal unavailabilities are applied for all of the LOCAs and for the steam generator tube rupture accident. For other initiators the auxiliary feedwater system actuation signal unavailabilities are applied.

Table 5.7.A Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
Base Case

Unavailability of ESFAS: One Train = 2.37E-02
Both Trains = 1.14E-03
CC Failures = 9.65E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.50E-01	1.30E-06	1.76E-07	4.17E-10	5.62E-11	7.06E-07	1.42E-09	2.34E-10	2.19E-06
S2	4.89E-02	8.92E-07	4.36E-08	7.37E-09	3.60E-10	3.92E-08	1.55E-09	3.37E-10	9.85E-07
S3	6.19E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.40E-08	2.40E-08
S4	1.14E-03	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	4.42E-07	4.42E-07
S5	2.83E-04	3.88E-10	5.24E-11	1.24E-13	<1E-13	2.11E-10	4.24E-13	<1E-13	6.52E-10
S6	2.31E-05	4.22E-10	2.05E-11	3.47E-12	1.64E-13	1.86E-11	6.48E-13	1.41E-13	4.65E-10
S7	3.75E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.46E-10	1.46E-10
S8	3.50E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.36E-10	1.36E-10
Sum	1.00E-00	2.19E-06	2.19E-07	7.79E-09	4.17E-10	7.45E-07	2.97E-09	4.68E-07	3.64E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.7.B Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
Proposed Case

Unavailability of ESFAS: One Train = 3.94E-02
Both Trains = 1.30E-03
CC Failures = 9.65E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.18E-01	1.26E-06	1.67E-07	4.03E-10	5.44E-11	6.82E-07	1.37E-09	2.26E-10	2.11E-06
S2	8.03E-02	1.46E-06	7.15E-08	1.21E-08	5.91E-10	6.43E-08	2.54E-09	5.53E-10	1.62E-06
S3	8.76E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.40E-08	3.40E-08
S4	1.30E-03	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.04E-07	5.04E-07
S5	2.74E-04	3.75E-10	5.07E-11	1.20E-13	<1E-13	2.03E-10	4.10E-13	<1E-13	6.31E-10
S6	3.23E-05	5.89E-10	2.88E-11	4.85E-12	2.37E-13	2.59E-11	1.02E-12	1.97E-13	6.51E-10
S7	5.20E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.02E-10	2.02E-10
S8	3.99E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.55E-10	1.55E-10
Sum	1.00E-00	2.72E-06	2.42E-07	1.25E-08	6.45E-10	7.47E-07	3.92E-09	5.40E-07	4.27E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.7.C Core Damage Frequency for Large LOCA (yr^{-1})
Relay ESFAS
Base Case
Concurrent Slave Relay Testing

Unavailability of ESFAS: One Train = 2.11E-02
Both Trains = 6.66E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.55E-01	1.31E-06	1.77E-07	4.19E-10	5.65E-11	7.10E-07	1.43E-09	2.35E-10	2.20E-06
S2	4.38E-02	7.99E-07	3.91E-08	6.60E-09	3.22E-10	3.51E-08	1.39E-09	3.02E-10	8.82E-07
S3	5.77E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.24E-08	2.24E-08
S4	6.66E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.58E-07	2.58E-07
S5	2.85E-04	3.91E-10	5.28E-11	1.25E-13	<1E-13	2.12E-10	4.27E-13	<1E-13	6.57E-10
S6	2.16E-05	3.95E-10	1.92E-11	3.24E-12	1.53E-13	1.74E-11	6.06E-13	1.32E-13	4.35E-10
S7	3.51E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.37E-10	1.37E-10
S8	2.05E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	7.97E-11	7.97E-11
Sum	1.00E-00	2.11E-06	2.16E-07	7.02E-09	3.79E-10	7.45E-07	2.82E-09	2.81E-07	3.37E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.7.6 Core Damage Frequency for Large LOCA (yr^{-1})
Relay ESFAS
Proposed Case
Concurrent Slave Relay Testing

Unavailability of ESFAS: One Train = 4.45E-02
Both Trains = 8.14E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.08E-01	1.25E-06	1.65E-07	3.99E-10	5.38E-11	6.75E-07	1.36E-09	2.24E-10	2.09E-06
S2	9.04E-02	1.64E-06	8.05E-08	1.36E-08	6.65E-10	7.24E-08	2.86E-09	7.35E-10	1.82E-06
S3	9.60E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.73E-08	3.73E-08
S4	8.14E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.16E-07	3.16E-07
S5	2.71E-04	3.71E-10	5.01E-11	1.19E-13	<1E-13	2.01E-10	4.06E-13	<1E-13	6.24E-10
S6	3.53E-05	6.44E-10	3.15E-11	5.30E-12	2.59E-13	2.83E-11	1.11E-12	2.15E-13	7.11E-10
S7	5.67E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.20E-10	2.20E-10
S8	2.50E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.11E-10	1.11E-10
Sum	1.00E-00	2.89E-06	2.46E-07	1.40E-08	7.20E-10	7.47E-07	4.22E-09	3.54E-07	4.27E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.7.E Core Damage Frequency for Large LOCA (yr^{-1})
Relay ESFAS
Base Case
Sequential Slave Relay Testing

Unavailability of ESFAS: One Train = 3.50E-02
Both Trains = 7.35E-04
CC Failures = 5.63E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.27E-01	1.27E-06	1.72E-07	4.07E-10	5.48E-11	6.89E-07	1.39E-09	2.28E-10	2.14E-06
S2	7.15E-02	1.30E-06	6.37E-08	1.08E-08	5.26E-10	5.73E-08	2.27E-09	4.93E-10	1.44E-06
S3	8.04E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.12E-08	3.12E-08
S4	7.35 -04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.85E-07	2.85E-07
S5	2.77E-04	3.79E-10	5.12E-11	1.21E-13	<1E-13	2.06E-10	4.15E-13	<1E-13	6.37E-10
S6	2.98E-05	5.44E-10	2.64E-11	4.47E-12	2.11E-13	2.40E-11	8.35E-13	1.82E-13	5.99E-10
S7	4.80E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.87E-10	1.87E-10
S8	2.26E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	8.77E-11	8.77E-11
Sum	1.00E-00	2.57E-06	2.36E-07	1.12E-08	5.82E-10	7.47E-07	3.66E-09	3.17E-07	3.89E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.7.F Core Damage Frequency for Large LOCA (yr^{-1})
Relay ESFAS
Proposed Case
Sequential Slave Relay Testing

Unavailability of ESFAS: One Train = 7.23E-02
Both Trains = 9.68E-04
CC Failures = 5.63E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	8.53E-01	1.17E-06	1.55E-07	3.74E-10	5.05E-11	6.34E-07	1.27E-09	2.10E-10	1.96E-06
S2	1.46E-01	2.65E-06	1.30E-07	2.20E-08	1.07E-09	1.17E-07	4.62E-09	1.19E-09	2.95E-06
S3	1.42E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.51E-08	5.51E-08
S4	9.68E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.75E-07	3.75E-07
S5	2.54E-04	3.48E-10	4.70E-11	1.11E-13	<1E-13	1.88E-10	3.80E-13	<1E-13	5.85E-10
S6	5.16E-05	9.41E-10	4.6[illegible]-11	7.75E-12	3.79E-13	4.14E-11	1.63E-12	3.15E-13	1.04E-09
S7	8.24E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.20E-10	3.20E-10
S8	2.97E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.15E-10	1.15E-10
Sum	1.00E-00	3.83E-06	2.85E-07	2.24E-08	1.13E-09	7.51E-07	5.89E-09	4.32E-07	5.34E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table 5.8.A Core Damage Frequency for Medium LOCA (yr^{-1})
Solid State ESFAS
Base Case

Unavailability of ESFAS: One Train = 2.37E-02
Both Trains = 1.14E-03
CC Failures = 9.65E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.93E-01	3.85E-06	2.92E-07	1.23E-09	9.36E-11	1.16E-06	2.34E-09	3.85E-10	5.31E-06
S2	6.41E-03	2.20E-07	1.04E-08	1.82E-09	8.57E-11	7.23E-09	2.85E-10	6.21E-11	2.40E-07
S3	5.59E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.42E-09	3.42E-07
S4	1.14E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	6.96E-08	6.96E-08
S5	3.01E-04	1.17E-09	8.86E-11	3.74E-13	<1E-13	3.52E-10	7.09E-13	1.13E-13	1.61E-09
S6	5.61E-06	1.92E-10	9.09E-12	1.59E-12	<1E-13	6.29E-12	2.47E-13	<1E-13	2.10E-10
S7	8.57E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.24E-11	5.24E-11
S8	3.88E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.36E-11	2.36E-11
Sum	1.00E-00	4.07E-06	3.02E-07	3.05E-09	1.79E-10	1.17E-06	2.63E-09	7.35E-08	5.62E-06

Definitions of Plant Damage States:
AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.8.B Core Damage Frequency for Medium LOCA (yr^{-1})
Solid State ESFAS
Proposed Case

Unavailability of ESFAS: One Train = 3.94E-02
Both Trains = 1.30E-03
CC Failures = 9.65E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.90E-01	3.84E-06	2.91E-07	1.23E-09	9.33E-11	1.16E-06	2.33E-09	3.84E-10	5.30E-06
S2	9.54E-03	3.27E-07	1.54E-08	2.70E-09	1.28E-10	1.08E-08	4.24E-10	9.25E-11	3.57E-07
S3	8.23E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.03E-09	5.03E-09
S4	1.30E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	7.94E-08	7.94E-08
S5	3.00E-04	1.16E-09	8.83E-11	3.73E-13	<1E-13	3.51E-10	7.07E-13	1.13E-13	1.61E-09
S6	6.56E-06	2.25E-10	1.06E-11	1.86E-12	<1E-13	7.34E-12	2.89E-13	<1E-13	2.45E-10
S7	9.22E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.63E-11	5.63E-11
S8	4.42E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.70E-11	2.70E-11
Sum	1.00E-00	4.17E-06	3.06E-07	3.93E-09	2.21E-10	1.17E-06	2.75E-09	8.50E-08	5.74E-06

Definitions of Plant Damage States:

AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.8.C Core Damage Frequency for Medium LOCA (yr^{-1})
Relay ESFAS
Base Case
Concurrent Slave Relay Testing

Unavailability of ESFAS: One Train = 2.11E-02
Both Trains = 6.66E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.94E-01	3.85E-06	2.92E-07	1.23E-09	9.36E-11	1.16E-06	2.34E-09	3.85E-10	5.31E-06
S2	5.89E-03	2.02E-07	9.56E-09	1.67E-09	7.87E-11	6.64E-09	2.62E-10	5.71E-11	2.21E-07
S3	5.15E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.15E-09	3.15E-09
S4	6.64E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	4.05E-08	4.05E-08
S5	3.01E-04	1.17E-09	8.86E-11	3.74E-13	<1E-13	3.52E-10	7.09E-13	1.13E-13	1.61E-09
S6	5.45E-06	1.87E-10	8.85E-12	1.55E-12	<1E-13	6.12E-12	2.40E-13	<1E-13	2.04E-10
S7	8.40E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.17E-11	5.17E-11
S8	2.26E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.37E-11	1.37E-11
Sum	1.00E-00	4.05E-06	3.02E-07	2.90E-09	1.74E-10	1.17E-06	2.60E-09	4.42E-08	5.58E-06

Definitions of Plant Damage States:
AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.8.9 Core Damage Frequency for Medium LOCA (yr^{-1})
Relay ESFAS
Proposed Case
Concurrent Slave Relay Testing

Unavailability of ESFAS: One Train = 4.45E-02
Both Trains = 8.14E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.89E-01	3.84E-06	2.91E-07	1.23E-09	9.33E-11	1.16E-06	2.33E-09	3.84E-10	5.30E-06
S2	1.06E-02	3.62E-07	1.70E-08	2.99E-09	1.42E-10	1.20E-08	4.69E-10	1.02E-10	3.95E-07
S3	9.08E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.55E-09	5.55E-09
S4	8.14E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	4.97E-08	4.97E-08
S5	3.00E-04	1.16E-09	8.82E-11	3.73E-13	<1E-13	3.51E-10	7.06E-13	1.13E-13	1.61E-09
S6	6.87E-06	2.06E-10	1.11E-11	1.95E-12	<1E-13	7.69E-12	3.03E-13	<1E-13	2.57E-10
S7	9.43E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.76E-11	5.76E-11
S8	2.77E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.69E-11	1.69E-11
Sum	1.00E-00	4.20E-06	3.08E-07	4.22E-09	2.36E-10	1.17E-06	2.80E-09	5.58E-08	5.75E-06

Definitions of Plant Damage States:
AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.8.E Core Damage Frequency for Medium LOCA (yr^{-1})
Relay ESFAS
Base Case
Sequential Slave Relay Testing

Unavailability of ESFAS: One Train = 3.50E-02
Both Trains = 7.35E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.91E-01	3.84E-06	2.91E-07	1.23E-09	9.34E-11	1.16E-06	2.34E-09	3.84E-10	5.30E-06
S2	8.66E-03	2.97E-07	1.[illegible]E-08	2.46E-09	1.16E-10	9.77E-09	3.85E-10	8.34E-11	3.24E-07
S3	7.49E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	4.58E-09	4.58E-09
S4	7.35E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	4.49E-08	4.49E-08
S5	3.00E-04	1.17E-09	8.83E-11	3.73E-13	<1E-13	3.51E-10	7.07E-13	1.13E-13	1.60E-09
S6	6.29E-06	2.15E-10	1.02E-11	1.78E-12	<1E-13	7.05E-12	2.77E-13	<1E-13	2.35E-10
S7	9.04E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.53E-11	5.53E-11
S8	2.50E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.52E-11	1.52E-11
Sum	1.00E-00	4.14E-06	3.05E-07	3.69E-09	2.10E-10	1.17E-06	2.73E-09	5.50E-08	5.67E-06

Definitions of Plant Damage States:
AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.8.F Core Damage Frequency for Medium LOCA (yr^{-1})
Relay ESFAS
Proposed Case
Sequential Slave Relay Testing

Unavailability of ESFAS: One Train = 7.23E-02
Both Trains = 9.68E-04
CC Failures = 5.63E-04
Failure of SI Signal Recovery = 1.00E-01

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.83E-01	3.81E-06	2.89E-07	1.22E-09	9.26E-11	1.15E-06	2.31E-09	3.81E-10	5.26E-06
S2	1.61E-02	5.52E-07	2.60E-08	4.56E-09	2.16E-10	1.82E-08	7.16E-10	1.56E-10	6.02E-07
S3	1.38E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	8.43E-09	8.43E-09
S4	9.68E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	5.91E-08	5.91E-08
S5	2.98E-04	1.15E-09	8.77E-11	3.71E-13	<1E-13	3.49E-10	6.98E-13	1.12E-13	1.60E-09
S6	8.54E-06	2.93E-10	1.38E-11	2.42E-12	<1E-13	9.56E-13	3.76E-13	<1E-13	3.19E-10
S7	1.06E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	6.53E-11	6.53E-11
S8	3.29E-08	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.01E-11	2.01E-11
Sum	1.00E-00	4.36E-06	3.15E-07	5.78E-09	3.09E-10	1.17E-06	3.03E-09	6.82E-08	5.93E-06

Definitions of Plant Damage States:

AEC Medium LOCA, Early Melt
AEC1 Medium LOCA, Early Melt, Failure of Recirculation Spray
AE Medium LOCA, Early Melt, No Containment Cooling
ALC Medium LOCA, Late Melt
ALC1 Medium LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Medium LOCA, Late Melt, Failure of Quench Spray
AL Medium LOCA, Late Melt, No Containment Cooling

Table 5.9 Dominant Accident Sequence Frequencies for Solid State ESFAS†

Initiating Event	WOG #	Sequence (Only Failed Top Events)	Support State	Core Damage Frequency, [yr^{-1}] WOG Results ++ Base Case	WOG Results ++ Proposed Case	BNL Results Base Case	BNL Results Proposed Case
1. Large LOCA	1	R1	S2	8.87E-07	1.46E-06	8.88E-07	1.46E-06
(See also total	2	R1, R3	S2	4.34E-08	7.11E-08	4.34E-08	7.12E-08
CDFs in Tables	3	ACC	S2	3.61E-08*	5.91E-08*	3.48E-08	5.71E-08
5.7.A and B)	4	QS, R1	S2	7.33E-09	1.20E-08	7.34E-09	1.20E-08
	5	LP1, HP1	S2	4.41E-09*	7.23E-09*	4.26E-09	6.98E-09
	6	LP1, R1	S2	4.03E-09	6.61E-09	4.04E-09	6.62E-09
	6a	LP1, R1	S3	---	---	2.40E-08	3.39E-08
	7	LP1, QS, HP1	S4	4.41E-07	5.03E-07	4.41E-07	5.03E-07
2. Medium LOCA°	8	R2	S2	2.20E-07	3.27E-07	2.20E-07	3.27E-07
(See also total	9	R2, R3	S2	1.04E-08	1.54E-08	1.04E-08	1.54E-08
CDFs in Tables	10	ACC	S2	7.18E-09	1.07E-08	7.17E-09	1.07E-08
5.8.A and B)	11	HP2, OA1, QS	S4	6.95E-08	7.93E-08	6.95E-08	7.93E-08
3. Small LOCA°°	12	HP2, OA2, QS	S4	1.03E-06	1.18E-06	1.03E-06	1.18E-06
4. Steam Gen.	13	AF2, R2	S2	2.08E-07	2.39E-07	2.07E-07	2.38E-07
Tube Rupture°°	13a	AF2, OA3	S2	---	---	9.03E-08	1.04E-07
5. Steamline Break Inside Cont.†				---	---	---	---
6. Steamline	14	AF2, R2	S2	1.78E-07	1.93E-07	1.77E-07	1.93E-07
Break Outside	14a	AF2, OA3	S2	---	---	8.54E-08	9.27E-08
Cont.†							
7. Loss of	14b	AF1, OA7, QS	S4	---	---	2.80E-08	3.13E-08
Reactor Coolant							
System Flow†							
8. Loss of	14c	AF1, R2	S2	---	---	4.46E-08	4.84E-08
Main Feedwater†	14d	AF1, OA7, QS	S4	---	---	4.16E-08	4.65E-08
9. Primary to	15	AF1, R2	S2	2.35E-07	2.54E-07	2.34E-07	2.54E-07
Secondary Mis-	15a	AF1, OA7	S2	---	---	1.16E-07	1.26E-07
match†	15b	AF1, OA7, QS	S4	---	---	2.19E-07	2.44E-07
	15c	S2(HP2,OA1',QS)	S7	---	---	2.84E-07	2.85E-07
10. Turbine	15d	AF1, R2	S2	---	---	1.43E-07	1.55E-07
Trip†	15e	AF1, OA7	S2	---	---	7.04E-08	7.64E-08
	15f	AF1, OA7, QS	S4	---	---	1.33E-07	1.49E-07
	15g	S2(HP2,OA1',QS)	S7	---	---	1.72E-07	1.73E-07

Table 5.9 (Continued)

Initiating Event	WOG #	Sequence (Only Failed Top Events)	Support State	Core Damage Frequency, [yr^{-1}] WOG Results ++ Base Case	WOG Results ++ Proposed Case	BNL Results Base Case	BNL Results Proposed Case
11. Reactor Trip†	16	AF1, R2	S2	1.86E-07	2.01E-07	1.85E-07	2.01E-07
	16a	AF1, OA7	S2	-	-	9.15E-08	9.94E-08
	16b	AF1, OA7, QS	S4	-	-	1.73E-07	1.93E-07
	16c	S2(HP,OA1',QS)	S7	-	-	2.25E-07	2.26E-07
Total				3.59E-06	4.62E-06	5.50E-06	6.70E-06
Total, w/o Large and Medium LOCAs				1.84E-06	2.07E-06	3.75E-06	4.12E-06

+ The Table does not display sequences in support state S1.

++ Given in Ref. 5.

* WOG uses for R3 a value of 2.01E-03, instead of that given in Millstone PSS; 3.79E-02.

° Failure of SI signal recovery: 1.00E-01

°° Failure of SI signal recovery: 1.00E-02

† Failure of auxiliary feedwater start signal recovery: 1.0' E-02

Table 5.10 Dominant Accident Sequence Frequencies for Relay ESFAS+

Initiating Event	WOG #	Sequence (Only Failed Top Events)	Support State	Core Damage Frequency, [yr^{-1}] Concurrent Slave Relay Testing		Sequential Slave Relay Testing	
				Base Case	Proposed Case	Base Case	Proposed Case
1. Large LOCA (See also total CDFs in Tables 5.7.C - F)	1	R1	S2	7.96E-07	1.65E-06	1.30E-06	2.66E-06
	2	R1, R3	S2	3.89E-08	8.05E-08	6.34E-08	1.30E-07
	3	ACC	S2	3.12E-08	6.45E-08	5.09E-08	1.04E-07
	4	QS, R1	S2	6.58E-09	1.36E-06	1.07E-08	2.18E-08
	5	LP1, HP1	S2	3.82E-09	7.89E-09	6.23E-09	1.27E-08
	6	LP1, R1	S2	3.62E-09	7.48E-09	5.91E-09	1.20E-08
	6a	LP1, R1	S3	2.24E-08	3.73E-08	3.12E-08	5.49E-08
	7	LP1, QS, HP1	S4	2.57E-07	3.15E-07	2.84E07	3.75E-07
2. Medium LOCA° (See also total CDFs in Tables 5.8.C - F)	8	R2	S2	2.02E-07	3.62E-07	2.97E-07	5.52E-07
	9	R2, R3	S2	9.56E-09	1.70E-08	1.41E-08	2.60E-08
	10	ACC	S2	6.59E-09	1.18E-08	9.69E-09	1.81E-08
	11	HP2, OA1, QS	S4	4.05E-08	4.96E-08	4.48E-08	5.11E-08
3. Small LOCA°°	12	HP2, OA2, QS	S4	6.00E-07	7.39E-07	6.64E-07	8.78E-07
4. Steam Gen. Tube Rupture°°	13	AF2, R2	S2	2.02E-07	2.48E-07	2.29E-07	3.01E-07
	13a	AF2, OA3	S2	8.81E-08	1.08E-07	9.97E-08	1.32E-07
5. Steamline Break Inside Cont.†				---	---	---	---
6. Steamline Break Outside Cont.†	14	AF2, R2	S2	1.74E-07	2.05E-07		
	14a	AF2, OA3	S2	8.42E-08	9.85E-08		
7. Loss of Reactor Coolant System Flow†	14b	AF1, OA7, QS	S4	2.35E-08	2.72E-08	Same values as those for the concurrent slave relay testing.	
8. Loss of Main Feedwater†	14c	AF1, R2	S2	4.40E-08	5.14E-08		
	14d	AF1, OA7, QS	S4	3.49E-08	4.05E-08		
9. Primary to Secondary Mismatch†	15	AF1, R2	S2	2.31E-07	2.70E-07		
	15a	AF1, OA7	S2	1.14E-07	1.34E-07		
	15b	AF1, OA7, QS	S4	1.84E-07	2.12E-07		
	15c	S2(HP2,QA1',QS)	S7	2.39E-07	2.48E-07		
10. Turbine Trip†	15d	AF1, R2	S2	1.41E-07	1.65E-07		
	15e	AF1, OA7	S2	6.94E-08	8.12E-08		
	15f	AF1, OA7, QS	S4	1.12E-07	1.30E-07		
	15g	S2(HP2,OA1',QS)	S7	1.44E-07	1.51E-07		

Table 5.10 (Continued)

Initiating Event	WOG #	Sequence (Only Failed Top Events)	Support State	Core Damage Frequency, [yr^{-1}] Concurrent Slave Relay Testing: Base Case	Concurrent Slave Relay Testing: Proposed Case	Sequential Slave Relay Testing: Base Case	Sequential Slave Relay Testing: Proposed Case
11. Reactor Trip†	16	AF1, R2	S2	1.82E-07	2.14E-07	Same values as those for the concurrent slave relay testing.	
	16a	AF1, OA7	S2	9.02E-08	1.06E-07		
	16b	AF1, OA7, QS	S4	1.45E-07	1.68E-07		
	16c	S2(HP2,OA1',QS)	S7	2.22E-07	1.90E-07		
Total				4.55E-06	6.20E-06	5.34E-06	7.82E-06
Total, w/o Large and Medium LOCAs				3.13E-06	3.50E-06	3.23E-06	3.80E-06

+ The table does not display sequences in support state S1.
° Failure of SI signal recovery: 1.00E-01.
°° Failure of SI signal recovery: 1.00E-02.
† Failure of auxiliary feedwater start signal recovery: 1.00E-02.

Table 5.11 Summary of Core Damage Frequency Calculations

		Core Damage Frequency, (yr^{-1})					
				Relay ESFAS			
		Solid State ESFAS		Concurrent Slave Relay Testing		Sequential Slave Relay Testing	
	Contributors to CDF	Base Case	Proposed Case	Base Case	Proposed Case	Base Case	Proposed Case
1	Large LOCA (Tables 5.7.A - F)	3.64E-06	4.27E-06	3.37E-06	4.27E-06	3.89E-06	5.34E-06
2	Medium LOCA (Tables 5.8.A - F)	5.62E-06	5.74E-06	5.58E-06	5.75E-06	5.67E-06	5.93E-06
3	Dominant Accident Sequences in Support State 1 (w/o Large & Medium LOCAs, Table 5.2. Part A)	1.02E-05	1.02E-05	1.02E-05	1.02E-05	1.02E-05	1.02E-05
4	Dominant Accident Sequences in Support States 2-8, (w/o Large & Medium LOCAs, Tables 5.9 and 5.10)	3.75E06	4.12E-06	3.13E-06	3.50E-06	3.23E-06	3.80E-06
5	Contribution of Non-dominant Small LOCA and Steam Gen. Rupture Sequences assumed all to be in Support State 2 (Base value in Table 5.2 Part A)	2.29E-07	2.62E-07	2.23E-07	2.73E-07	2.52E-07	3.33E-07
6	Contribution of Non-dominant Sequences from Steam Break Inside Cont. through Reactor Trip Initiators assumed all to be in State 2 (Base Value in Table 5.2 Part A	9.51E-07	1.03E06	9.37E-07	1.10E-06	9.37E-07	1.10E-06
7	Accident Sequences not affected by changes of ESFAS Signal Unav. (Table 5.2 Part B)	1.96E-05	1.96E-05	1.96E-05	1.96E-05	1.96E-05	1.96E-05
Total		4.40E-05	4.52E-05	4.30E-05	4.47E-05	4.38E-05	4.63E-05
Changes in CDF, (Δ)			1.2E-06		1.7E-06		2.5E-06
Changes in CDF, %			2.7		4.0		5.7

6. OVERALL COMMENTS AND FINDINGS

6.1 Comments on the WOG Methodology

The justification analyses that accompanied the WOG's request to modify the STI and AOT requirements for the ESFAS consisted of very detailed actuation signal unavailability calculations and a "bounding" plant-specific risk analysis intended to be valid for the majority of Westinghouse plants. The WOG argument of key importance for acceptance of the proposed STI/AOT modifications by the NRC is the rather slight increase in core damage frequency (2.4%) and man-rem exposure (1.7%) of a representative Westinghouse plant. The WOG states that the analyses and results are consistent with the planned NRC guidelines for requesting STI/AOT modifications. The following is quoted from the summary of Ref.2:

> "These increases are consistent with the guidelines established in the final draft copy of "Risk Methodology Guide for AOT and STI Modifications" (Reference 29) which states "the change in core melt frequency should be small compared to the Commission's Safety Goal." The analysis also shows that there is only a small increase in public risk. All increases are well within the uncertainties of a plant risk analysis. Additionally, these changes represent substantial financial benefits to the utilities." (Reference 29 quoted above is denoted as Ref.14 in the present report.)

The Risk Methodology Guide quoted above actually states that the small core damage frequency and man-rem exposure changes are necessary but not sufficient conditions for accepting STI/AOT modification requests. The guide suggests that in addition to a demonstration of small core damage frequency (man-rem exposure) increase, it should be demonstrated that the single downtime risk (associated exposure) increase also be within acceptable limits. (Single downtime risk is the probability of a core damage occurring in one downtime when a component or a train is down. It is obtained as the product of the conditional core damage frequency given a component or a train is down and the time period during which this condition exists.) The WOG

justification analyses did not make any attempt to satisfy the "sufficient" conditions for acceptance.

In order to demonstrate the feasibility of the additional analysis required to fulfill the "sufficient" conditions for acceptance (as outlined in the guide) within the framework of WOG's risk analysis, BNL evaluated the conditional core damage frequencies for the Millstone 3 large LOCA event tree assuming various parts of the solid state ESFAS (analog channel, one logic train, etc.) to be down (unavailable). The results of these example calculations are presented in Appendix B. BNL recognizes that the guide's suggestions have not yet been made requirements by the NRC for approval of LCO changes. However, these calculations have been included by BNL to form a complete review.

6.2 Findings on ESFAS Signal Unavailabilities

From the depth and extent of the ESFAS signal unavailability analysis, it is clear that the WOG has performed a really thorough study of the ESFAS designs presently used at the plants. In this respect an excellent job was done on the solid state systems as well as on the relay system designs. The following items highlight the BNL findings in this area:

1. BNL concurs with the WOG's finding that the unavailability contributions of the analog channels for the ESFAS logic designs are small and that they become even smaller when one considers process parameter signal diversity. Therefore, whether the analog channels are tested on a staggered or non-staggered basis, there is negligible effect on the ESFAS signal unavailability.

2. Human errors associated with testing and maintenance activities for the logic as well as the master and slave relays were not modelled in the topical report. We note this as a shortcoming of the model. However, although not part of the quantification, it is noted that the requested extended allowed outage times, if granted, would be expected to lower the human error contribution.

6.3 Findings on Core Damage Frequency

1. The BNL review calculations provided a CDF frequency increase of 2.8% for solid state plants if the LCO modifications proposed by the WOG are accepted. The value obtained is in acceptable agreement with the value assessed by WOG (i.e., 2.4%) in its Justification Risk Analysis.

2. The increase of the CDF for relay plants calculated by BNL when the same conditions were used for relay ESFAS unavailability as the WOG (i.e., concurrent slave relay testing) is: 4.0%. This value is at variance with the WOG's expectation. The WOG stated that the CDF increases at relay plants would be "bounded" by the CDF increase obtained at a representative solid state plant. The WOG did not do any calculational effort, however, to prove this expectation. As a sensitivity study, BNL also performed a calculation to see the effect that a sequential testing scheme would have on the CDF. The results of the sensitivity study yielded a CDF increase of 5.7%.

3. As part of the review, BNL pointed out that the use of Millstone Unit 3 as a reference plant may not fully bound the change in CDF for Westinghouse plants in general because Millstone has a 2/4 ESFAS logic and other plants have 2/3 logic which produces higher unavailability. In response to BNL's concern, Westinghouse did a separate calculation, which was documented as Supplement 2, Revision 1, Addendum 2 to WCAP-10271. The calculation was performed on Millstone assuming the Millstone logic was simply changed from 2/4 to 2/3. The bottom line result yielded a 3.3% increase in CDF verses the 2.4% for the 2/4 logic designs. BNL accepts this additional calculation as a reasonable estimate for the 2/3 solid state designs. Given that the BNL analysis shows the relay designs as bounding over the solid state, and assuming that the ΔCDF increase in the solid tate designs between 2/4 and 2/3 logic would be proporti tely equivalent for the relay designs, an overall upper bound for the CDF increase due to the proposed TS changes should be less than 6% for the majority of Westinghouse-design plants.

REFERENCES

1. Andre, G. R., Howard, R. C., Jansen, R. L., and Leonelli, K., "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271, Supplement 2, February 1986.

2. Andre, G. R., Howard, R. C., Jansen, R. L., and Leonelli, K., "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271, Supplement 2, Revision 1, March 1987.

3. Westinghouse Owners Group Transmittal of Responses to NRC Questions on WCAP-10271, Supplement 2, WOG Memo No. OG-207 to Mr. James Lyons, November 7, 1986.

4. Revisions to WOG Responses to NRC Questions OG-207, WOG Memo No. OG-87-15, June 1987.

5. Westinghouse Letter No. NS-NRC-88-3308 to Mr. Marvin W. Hodges, January 1988.

6. Millstone Unit 3 Probabilistic Safety Study, Westinghouse Electr Corporation, August 1983.

7. Garcia, A. A. et al., "A Review of the Millstone 3 Probabilistic Safety Study," NUREG/CR-4142, UCID-20330, April 1986.

8. Safety Evaluation Report by NRC on WCAP-10271, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," January 11, 1985.

9. Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3, EPRI, Duke Power Company, NSAC-60, June 1984.

10. Seabrook Station Probabilistic Safety Assessment, Pickard, Lowe and Garrick, Inc. PLG-0300, December 1983.

11. Military Handbook, Reliability Prediction of Electronic Equipment, MIL-HDBK-217D, January 15, 1982.

12. Edermann, R. C., "WAMCUT, A Computer Code for Fault Tree Evaluation," Science Applications, Inc., NP-803, June 1978.

13. Worrel, R. B. and Stack, D. W., "A SETS User's Manual for the Fault Tree Analyst," Sandia National Laboratories, NUREG/CR-0465, SAND77-2051, November 1978.

14. Samanta, P. K., Vesely, W. E., Lofgren, E., and Boccio, J. L., "Risk Methodology Guide for AOT and STI Modifications," Final Draft, Brookhaven National Laboratory, December 1986.

APPENDIX A: Safety Injection Signal Unavailabilities for Relay ESFAS for Concurrent and Sequential Slave Relay Testing

The purpose of this appendix is to document a sensitivity study which demonstrates the difference in safety injection (SI) signal unavailabilities for relay ESFAS designs if sequential rather than concurrent slave relay testing is assumed. The demonstration will be presented in the following steps:

Step 1. It is shown on the unavailability model of the solid state SI signal, where sequentially performed individual slave relay testing was assumed by WOG, that there is an easily usable, simple, relationship between two-train and single-train unavailabilities which very accurately approximates the computer calculations.

Step 2. A similar relationship between the two-train and single-train unavailabilities is given for the relay SI signal. This step describes the WOG modelling with the assumption of concurrent slave relay testing.

Step 3. The two-train and single-train unavailabilities are then calculated for the relay SI signal with the above relationship except that sequential slave relay testing is assumed.

The calculation is presented in detail only for the base case. A similar procedure yields the results for the proposed case.

1. Solid State ESFAS

The two-train unavailability (denoted here as ESAB) of the SI signal from the single-train unavailabilities (denoted as ESA, ESB) can be approximated by the formula:

$$ESAB = ESA * \{ESB - [TBT + n_{MR} * MRXM + n_{SR} * (SRXXT + SRXXM)]\} + CC \quad , \quad (Eq.1)$$

where (by using WOG notation, base case test and maintenance unavailabilities from Table 4.1):

ESA = ESB = 2.37E-02 unavailability of an ESFAS train,

TBT = 3.12E-03 train B unavailability due to testing sequentially the logic and the two master relays,

n_{MR} = 2 number of master relays per train,

n_{SR} = 6 number of slave relays per train,

MRXM = 3.47E-04 train unavailability due to maintenance of master relay X and half of the logic,

SRXXT = 1.85E-03 unavailability of slave relay XX due to test,

SRXXM = 2.31E-04 unavailability of slave relay XX due to maintenance, and

CC = 9.64E-04 common cause failure (see Table 4.3).

The formula accurately reproduces the value obtained by computer calculation, i.e., ESAB = 1.14E-03.

2. Relay ESFAS (Concurrent Slave Relay Testing)

The two-train unavailability of the SI signal from the single-train unavailabilities can be approximated by a similar formula reproducing the WOG results:

$$ESAB' = ESB' * \{ESA' - [TAT' + n'_{MR} * MRXM' + n'_{SR} * SRXXM']\} + CC' , \quad \text{(Eq.2)}$$

where (by using WOG notation, base case test and maintenance unavailabilities from Table 4.2):

ESA' = ESB' = 2.11E-02 unavailability of an ESFAS train, (concurrent slave relay testing),

TBT' = 1.111E-02 train A unavailability including sequential testing of the logic, master relay and concurrently performed slave relay tests (concurrent slave relay test time = test time for one slave relay),

n_{MR}' = 1 number of master relays per train,

n_{SR}' = 6 number of slave relays per train,

SRXXM' = 2.31E-04 unavailability of slave relay XX due to maintenance, and

CC' = 9.64E-044 common cause failure (see Table 4.4).

The formula again accurately reproduces the value obtained by computer calculation, i.e., ESAB' = 6.66E-04.

3. Relay ESFAS (Sequential Slave Relay Testing)

The two-train unavailability (ESAB") of the SI signal from the single-train unavailabilities can be estimated (in conformity with Eq.1) by the following formula:

$$ESAB'' = ESB'' * \{ESA'' - [TAT'' + n_{MR}' * MRXM' + n_{SR}' * (SRXXT' + SRXXM')]\} + CC' , \quad \text{(Eq.3)}$$

In Eq.(3) ESA", ESB" denote the single train unavailabilities for sequential testing and ESA" = ESB".

To be in conformity with the solid state single-train unavailability, ESA" is expressed as:

ESA" = ESA' + 5 * SRXXT' = 3.5E-02 where ESA' is the relay single train unavailability (concurrent slave relay testing),

SRXXT' = 2.78E-03 the unavailability of slave relay XX due to test. The factor 5 is necessary because ESA' only contains the test time for one slave relay.

Again, to be in conformity with Eq.1:

TAT' = TAT' - SRXXT' = 8.33E-03 train A unavailability due to testing only the logic and the master relay.

The other quantities are the same as in the previous case (n'_{MR}, n'_{SR}, TAT', MRXM', SRXXM', CC'). The formula provides the unavailability of the relay SI signal for sequential slave relay testing (base case), as; ESAB" = 7.35E-04.

Appendix B: Conditional Core Damage Frequency Calculations for Millstone 3 Large LOCA

Appendix B describes an example conditional core damage frequency calculation to demonstrate the feasibility of an analysis of this type within the framework of WOG's justification analyses.

B.1 Single and Yearly Downtime Risks

The "Risk Methodology Guide for AOT and STI Modifications"[14] emphasizes that for AOT increases, not only should the increase of the average CDF be kept small compared to the NRC's Safety Goal, but the increase of the single downtime risk and the increase of the yearly (cumulative) downtime risk should also be kept within acceptable limits.

Single downtime risk is the probability of core damage occurring in one downtime when a component or a train of a safety system is down (unavailable). The probability is calculated as the product of the duration of the downtime and of the conditional CDF given that the component or the train in question is down. The considered downtime is maximum when the downtime is taken to be equal to the AOT of the component. Because under certain circumstances the conditional CDF may be quite high, the time period during which the plant is exposed to this CDF can be critical. Therefore, when considering AOT increases, the evaluation of the given downtime risk (or man-rem exposure) may be more important than the increase of the average CDF (or increase in the average man-rem exposure).

The yearly (cumulative) downtime risk measures the average contribution of downtimes of a component or a train to the CDF. It is calculated by multiplying the single downtime risk with the projected downtime occurrences during a year. The significance of the yearly downtime risk can be seen from the following situations. For risk-prone components, the yearly (cumulative) risk can be low if the test and maintenance frequency is low even if the single downtime risk is high and needs to be controlled. On the other hand, even if the single downtime risk is low, the frequency of outages of the component can make the yearly (cumulative) risk high.

B.2 Calculation of Conditional Core Damage Frequencies

To calculate the conditional CDFs, the PRA model of the plant was used with special inputs as follows. The unavailabilities of a particular set of system components were set to unity or zero depending upon whether they were assumed to be down or in an operating state, respectively. The unavailabilities of other systems/components and failure event probabilities in the model were left intact.

Since the largest contributor to the CDF change in the WOG's risk impact analysis was due to the large LOCA initiator, BNL selected the large LOCA event tree for demonstrative conditional CDF calculations.

The conditional large LOCA CDFs were separately evaluated for each of the following test or maintenance conditions:

- no ESFAS components were down,
- an analog channel was down,
- logic train or master relays were down, and
- slave relays were down.

In each of the cases in the fault tree model of the solid state ESFAS, the unavailabilities of the components assumed to be down were set equal to unity. Simultaneously, the unavailabilities due to test and maintenance for components assumed to be operating were set equal to zero. The actuation signal unavailability expression was then solved again (with Boolean techniques by using the SETS code) and requantified. The requantified signal unavailabilities were propagated through the Millstone 3 support state model and the large LOCA event tree.

Tables B.1 through B.4 display the conditional CDFs in a Plant Damage State - Support State Matrix format for each of the above cases, respectively. Table B.5 shows the risks when testing or maintaining various ESFAS components. As was expected, testing and maintenance of the slave relays provided the greatest risk for core damage. The yearly cumulative downtime risk due to large LOCA is given in Table B.6 for various components. The sum of the

risks over all the components, including when no test/maintenance is performed, provides the average CDF. The values obtained for the base (existing) and the proposed case (Case 3) are 3.63E-06 yr^{-1} and 4.25E-06 yr^{-1}, respectively. These values are in very good agreement with those obtained by direct (not through conditional CDF) calculations in Table 5.7.a and 5.7.b.

If similar calculations were performed for all the ESFAS-dependent initiators used in the Millstone 3 PSS, that would provide the total conditional CDFs.

Table B.1 Conditional Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
No Test Period

Unavailability of ESFAS: One Train = 7.42E-03
Both Trains = 9.89E-04
CC Failures = 9.65E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.82E-01	1.35E-06	1.82E-07	4.31E-10	5.82E-11	7.30E-07	1.47E-09	2.38E-10	2.26E-06
S2	1.65E-02	3.00E-07	1.47E-08	2.48E-09	1.21E-10	1.32E-08	5.21E-10	8.78E-11	3.32E-07
S3	3.53E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.37E-08	1.37E-08
S4	9.89E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.84E-07	3.84E-07
S5	2.93E-04	4.02E-10	5.43E-11	1.29E-13	<1E-13	2.18E-10	4.39E-13	<1E-13	6.75E-10
S6	1.36E-05	2.48E-10	1.21E-11	2.04E-12	<1E-13	1.08E-11	3.80E-13	<1E-13	2.73E-10
S7	2.25E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	8.72E-11	8.72E-11
S8	3.04E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.18E-10	1.18E-10
Sum	1.00E-00	1.65E-06	1.97E-07	2.91E-09	1.79E-10	7.43E-07	1.99E-09	3.98E-07	2.99E-06

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table B.2 Conditional Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
Analog Channel Test Period

Unavailability of ESFAS: One Train = 7.60E-03
Both Trains = 9.92E-04
CC Failures = 9.65E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	9.81E-01	1.35E-06	1.82E-07	4.31E-10	5.82E-11	7.29E-07	1.47E-09	2.41E-10	2.26E-06
S2	1.68E-02	3.07E-07	1.50E-08	2.53E-09	1.24E-10	1.35E-08	5.32E-10	8.97E-11	3.39E-07
S3	3.55E-05	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.38E-08	1.38E-08
S4	9.92E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.85E-07	3.85E-07
S5	2.92E-04	4.01E-10	5.42E-11	1.29E-13	<1E-13	2.18E-10	4.38E-13	<1E-13	6.74E-10
S6	1.37E-05	2.50E-10	1.21E-11	2.05E-12	1.00E-13	1.09E-11	3.83E-13	<1E-13	2.75E-10
S7	2.27E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	8.78E-11	8.79E-11
S8	3.05E-07	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.18E-10	1.18E-10
Sum	1.00E-00	1.66E-06	1.97E-07	2.96E-09	1.82E-10	7.43E-07	2.00E-09	4.00E-07	3.00E-06

Definitions of Plant Damage States:

AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table B.3 Conditional Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
Logic & Master Relay Test Period

Unavailability of ESFAS: One Train = 8.39E-03
Both Trains = 9.65E-04
CC Failures

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00
S2	9.90E-01	1.81E-05	8.83E-07	1.49E-07	7.29E-09	7.95E-07	3.13E-08	6.83E-09	1.99E-05
S3	8.34E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.24E-07	3.24E-07
S4	8.38E-03	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.25E-06	3.25E-06
S5	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00
S6	3.00E-04	5.47E-09	2.67E-10	4.51E-11	2.20E-12	2.41E-10	9.42E-12	2.07E-12	6.03E-09
S7	4.73E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.84E-09	1.84E-09
S8	2.58E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	9.99E-11	9.99E-11
Sum	1.00E-00	1.81E-05	8.83E-07	1.49E-07	7.29E-09	7.95E-07	3.14E-06	3.59E-06	2.35E-05

Definitions of Plant Damage States:
AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table B.4 Conditional Core Damage Frequency for Large LOCA (yr^{-1})
Solid State ESFAS
Slave Relay Test Period

Unavailability of ESFAS: One Train = 5.16E-03
CC Failures = 9.65E-04

Support States		Plant Damage States							
Name	Prob	ALC	ALC1	ALC2	AL	AEC	AEC1	AE	LALO
S1	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00
S2	9.94E-01	1.81E-05	8.85E-07	1.50E-07	7.31E-09	9.97E-07	3.14E-08	6.85E-09	2.00E-05
S3	8.37E-04	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	3.25E-07	3.25E-07
S4	5.16E-03	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	2.00E-06	2.00E-06
S5	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00	0.00E-00
S6	3.01E-04	5.48E-09	2.68E-10	4.53E-11	2.20E-12	2.41E-10	9.45E-12	2.07E-12	6.05E-09
S7	4.75E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	1.84E-09	1.84E-09
S8	1.58E-06	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	<1E-13	6.15E-11	6.15E-11
Sum	1.00E-00	1.81E-05	8.85E-07	1.50E-07	7.31E-09	7.97E-07	3.14E-06	2.33E-06	2.23E-05

Definitions of Plant Damage States:

AEC Large LOCA, Early Melt
AEC1 Large LOCA, Early Melt, Failure of Recirculation Spray
AE Large LOCA, Early Melt, No Containment Cooling
ALC Large LOCA, Late Melt
ALC1 Large LOCA, Late Melt, Failure of Recirculation Spray
ALC2 Large LOCA, Late Melt, Failure of Quench Spray
AL Large LOCA, Late Melt, No Containment Cooling

Table B.5 Large LOCA Downtime Risk During A Test or Maintenance Period of Solid State ESFAS

i	Conditions	Conditional CDF, (yr^{-1}) $(CCDF)_i$	Downtime Per One				Downtime Risk Per One			
			Test Period		Maintenance Period		Test Period		Maintenance Period	
			Base Case (yr)	Proposed Case (yr)	Base Case (yr)	Proposed Case (yr)	Base Case	Proposed Case	Base Case	Proposed Case
1	No Test/Maintenance	2.99E-06	---	---	---	---	---	---	---	---
2	Analog Channels* in Test/Maintenance	3.00E-06	1.62E-03	3.24E-03	8.10E-04	9.72E-03	4.86E-09	9.72E-09	2.43E-09	2.92E-09
3	Logic Trains/Master Relays in Test/ Maintenance	2.35E-05	1.04E-03	2.78E-03	1.39E-03	8.33E-03	2.45E-08	6.53E-08	3.26E-08	1.96E-07
4	Slave Relays in Test/Maintenance	2.23E-05	5.56E-03	5.56E-03	2.78E-03	1.67E-02	1.24E-07	1.24E-07	6.19E-08	3.72E-07
	Total						1.53E-07	1.99E-07	9.69E-08	5.97E-07

*Considering four "Pressurizer Pressure Low" and three "Containment Pressure High" analog channels.

Table B.6 Yearly Cumulative Downtime Risk Due to Large LOCA - Solid St te ESFAS

i	Conditions	Conditional CDF, (yr^{-1}) $(CCDF)_i$	Cumulative Times Spent In Conditional Core Damage State				Cumulative Risk	
			Test Period		Maintenance Period			
			Base Case (yr)	Proposed Case (yr)	Base Case (yr)	Proposed Case (yr)	Base Case	Proposed Case
1	No Test/Maintenance	2.99E-06	.9471+	.9134+	---	---	2.83E-06	2.73E-06
2	Analog Channels* in Test/Maintenance	3.00E-06	1.94E-02	1.30E-02	8.10E-04	9.72E-03	6.08E-08	6.81E-08
3	Logic Trains/Master Relays in Test/ Maintenance	2.35E-05	6.25E-03	1.67E-02	1.39E-03	8.33E-03	1.80E-07	5.88E-07
4	Slave Relays in Test/Maintenance	2.23E-05	2.22E-02	2.22E-02	2.78E-03	1.67E-02	5.58E-07	8.67E-07
	Total						3.63E-06	4.25E-06

*Considering four "Pressurizer Pressure Low" and three "Containment Pressure High" analog channels.

+(1.0 - Total time of test and maintenance for all the components.)