BAW-10182A
Topical Report
February 1994

THE B&W OWNERS GROUP

Technical Specification Committee

Justification for Increasing Engineered Safety Features Actuation System (ESFAS) On-Line Test Intervals

B&W NUCLEAR SERVICE COMPANY

BAW-10182A
Topical Report
February 1994

JUSTIFICATION FOR INCREASING THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS) ON-LINE TEST INTERVALS

by

Robert S. Enzinna
Stanley H Levinson

Prepared for the B&W Owners Group
Technical Specification Committee

B&W Nuclear Technologies
P.O. Box 10935
Lynchburg, Virginia 24506-0935

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

January 3, 1994

Mr. B. P. Wunderly, Chairman
B&WOG Technical Specification Subcommittee
Crystal River, Unit 3
Mail Stop NA-2I
PO Box 219
Crystal River, FL 32629-0219

SUBJECT: NRC EVALUATION OF BWOG TOPICAL REPORT BAW-10182, "JUSTIFICATION FOR INCREASED ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS) ON-LINE TEST INTERVALS"

Dear Mr. Wunderly:

The purpose of this letter is to provide the staff's evaluation of B&W Topical Report BAW-10182 prepared by B&W Nuclear Services Company for the B&W Owners Group Technical Specification (TS) Subcommittee. This topical report was submitted to the NRC by letter dated March 2, 1992, and presents justification for extending the on-line surveillance test interval (STI) for the ESFAS channels and actuation logic from a one-montn to a three-month interval.

The staff finds this report acceptable and agrees that the STI for the ESFAS can be extended for all B&W plants (except Three Mile Island) to the requested interval. Three Mile Island was not represented in the B&W Owners Group on this issue. This acceptance is contingent upon each licensee confirming that instrument drift occurring over the proposed STI would not cause the setpoint values to exceed those values assumed in the plant safety analysis and specified in the Technical Specifications. The licensees must confirm that they have reviewed instrument channel drift information and have determined that this drift over the period of the extended STI will not cause the safety setpoint to be exceeded beyond the allowable value calculated for that channel by the setpoint methodology. Each licensee should have on-site records of the as-found and as-left values showing actual calculations and supporting data for possible future staff audits. The records should consist of monthly data over a period of at least the last 2 years with a description of the current plant-specific setpoint methodology used to derive the safety margins.

In accordance with procedures established in NUREG-0390, "Topical Reports Review Status," we request that the B&W Owners Group publish accepted revisions of BAW-10182 within three months of receipt of this letter. The accepted versions should (1) incorporate this letter and the enclosed Safety Evaluation Report (SER) between the title page and the abstract and (2) include an -A (designated accepted) following the report identification symbol.

Should our acceptance criteria or regulations change so that our conclusions as to the acceptability of this report no longer be valid, the B&W Owners Group and/or the licensees referencing this topical report will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the topical report without revision.

Should you have any questions regarding the matters discussed above on the content of the enclosed SER, please contact I. Ahmed of my staff on (301) 504-3252.

Sincerely,

Bruce A. Boger, Director
Division of Reactor Controls
and Human Factors
Office of Nuclear Reactor Regulation

Enclosure:
1. Staff Safety Evaluation Report

cc w/enclosure:
W. Russell
C. Grimes
J. Taylor (B&W)

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

Enclosure

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION
B&W OWNERS GROUP TOPICAL REPORT BAW-10182
JUSTIFICATION FOR INCREASING ESFAS ON-LINE TEST INTERVALS

1.0 INTRODUCTION

By letter dated March 2, 1992 (Reference 1), the B&W Owners Group (BWOG) submitted Topical Report BAW-10182, "Justification for Increasing Engineered Safety Features Actuation System (ESFAS) On-Line Test Intervals." This report was prepared by the B&W Nuclear Services Company and provides the technical basis to justify increasing the ESFAS on-line surveillance test interval (STI) in plant technical specifications from the current one-month to a three-month interval. The Idaho National Engineering Laboratory (INEL) assisted the staff in the review of BAW-10182. The INEL review results are documented in EGG-RTAP-10925 (Reference 2) and are summarized in this safety evaluation report. The following evaluation addresses both the acceptability of the probabilistic analysis presented in BAW-10182 and the acceptability of the proposed extension of the STI.

The methodology used in BAW-10182 is the same as that previously used in the B&WOG Topical Report BAW-10167, "Justification for Increasing the Reactor Trip System On-Line Test Intervals," which was submitted to justify the Reactor

Trip System STI extension. The staff approved BAW-10167 and suggested some specific improvements in the methodology. BAW-10182 uses the improved methodology and reflects the major differences between the three ESFAS designs in the B&W operating reactors (Baily design at ANO-1 and Oconee, Gilbert design at Crystal River 3, Bechtel design at Davis-Besse) exclusive of Three Mile Island which was not represented in the BWOG on this issue. The unavailability of each of the three ESFAS designs is modeled in the report using reliability block diagrams for both the current one-month STI and the proposed three-month STI. The analysis evaluated the impact of the proposed STI extension on core melt frequency and system unavailability to demonstrate that the proposed change did not significantly increase plant risk when compared with the current technical specification requirements.

2. EVALUATION

The staff's evaluation included the following aspects of the probabilistic risk analysis (PRA) performed by B&W to justify the proposed extension of the ESFAS test interval:

1) Models and data used for the reliability analysis
2) Quantification of the analysis models
3) Uncertainty analysis

A time-dependent model was used to dynamically represent system configuration changes associated with testing and maintenance. The source of data for the analog channel components (sensors and instrument string) and digital

subsystem components for both random and common mode failures was NUREG/CR-3289, "Common Cause Fault Rates For Instrumentation and Control Assemblies," and B&W reactor operating experience obtained from the Nuclear Plant Reliability Data System. An error factor of 10 (the largest error factor listed in WASH-1400, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," for instrumentation) was used for the ESFAS components random failure rate (lambda factor) as suggested in the staff safety evaluation report for BAW-10167. Also, as suggested by NUREG/CR-5801, "Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis," when a common-mode failure rate could not be determined from the component failure history, a beta factor (fraction of lambda factor in which two or more components are involved due to common-mode failure) was used. The random failure rates of the ESFAS components assumed in BAW-10182 were compared to a generic failure rate data base compiled by INEL in EGG-SSRE-8875, "Generic Component Failure Data Base for Light Water and Liquid Sodium Reactors PRAs," and both failure rates and error factors were found to be in close agreement.

A time-dependent quantification calculation was performed by B&W using reliability block diagrams and computer codes for each of the three B&W plant ESFAS designs. The analysis considered core melt frequencies (CMF) due to ESFAS failure for both the current one-month test interval and the proposed three-month test interval over a typical 18-month fuel cycle. This analysis was performed for: (1) six different loss of coolant accident (LOCA) events (including transient-induced LOCAs), each of which challenges different ESFAS

parameters and requires a different ESFAS response; and (2) an aggregate case to bound all challenging events. The time-dependent results were then integrated to obtain an average CMF and any incremental difference in the CMF due to an increase in the test interval. BAW-10182 calculations show the incremental risk for a three-month ESFAS STI per reactor-year to vary from 1.45×10^{-7} to 2.03×10^{-8} for the three ESFAS designs, while the corresponding risk for the existing one-month STI varied from 4.0×10^{-7} to 2.11×10^{-8}. Thus, the analysis indicated that the impact on CMF of increasing the ESFAS test interval from one to three months is negligible.

An analysis of the change in CMF can also be utilized to determine changes in ESFAS unavailability. However, the B&WOG report did not present changes in ESFAS unavailability separate from the CMF results. To investigate the potential change in ESFAS unavailability, the staff duplicated the analysis for the Baily ESFAS design using BAW-10182 parameters and the time-dependent unavailability computer code FRANTIC. The analysis results showed an ESFAS unavailability increase by a factor of three, corresponding to the test interval increase (one to three months). However, CMF does not change in direct proportion to ESFAS unavailability because of other factors, such as, the reduced probability of human error when the test interval is extended. This is one of the motivations to develop and implement risk-based changes to the technical specification test intervals.

To determine the change in CMF as a result of a factor of three increase in ESFAS unavailability, the staff recalculated the risk using an ESFAS failure

probability increased by a factor of three in the Oconee plant PRA using the fault tree/event tree analysis computer code IRRAS. The results showed negligible increase in CMF.

To test the robustness of the CMF analysis results, the staff also performed an uncertainty analysis for each of the three B&W plant ESFAS designs and both the current and proposed ESFAS test intervals using a Monte Carlo computer code and an error factor of ten (an order of magnitude variation in the failure rates in either direction from the median to the lower and upper bound values). The uncertainty analysis (6000 iterations) indicated that there is a 95% probability with 95% confidence (95%/95%) that the change in CMF associated with increasing the ESFAS test interval to three months is negligible. The staff further compared the B&WOG analyses with three PRAs discussed in NUREG/CR-4550, "Analysis of Core Damage Frequency: Surry, Unit 1 Internal Event," and found the analysis conclusion to be consistent with those in NUREG/CR-4550.

While the generic analysis of risk on the extended STI is considered acceptable, it does not consider the plant-specific effects of drift in both sensors and instrument strings. These plant-specific effects should be assessed and factored into the analysis in order to maintain the validity of the assumed failure rates. Therefore, each licensee referencing BAW-10182 should confirm that they have reviewed drift information including as-found and as-left values for each ESFAS instrument channel involved and determined that drift occurring in that channel over the period of the extended STI will

not cause the setpoint value to exceed the allowable values as calculated for that channel by their setpoint methodology (instrument drift is defined as the portion between the upper leave-alone zone and the allowable value). Each referencing licensee should also maintain onsite records showing the actual setpoint calculations and supporting data that are available in order to permit possible future staff audit. The data should consist of monthly information taken over at least the last 2 years, and a description of the current plant-specific setpoint methodology used to derive the safety margins.

3. CONCLUSION

Based on the above, the staff concludes that the data and analyses in BAW-10182 adequately demonstrate a negligible change in CMF and risk, and thus extending the ESFAS surveillance test interval from the current one-month to three-month interval is, therefore, acceptable. The staff also notes, however, that licensees referencing topical report BAW-10182 should 1) include a plant-specific analysis of setpoint drift for the extended surveillance interval to confirm the validity of the assumed analysis failure rates, 2) maintain onsite records showing actual setpoint calculations and information over at least the last 2 years, and 3) include a description of the current plant-specific setpoint methodology used to derive the safety margins.

4. REFERENCES

1. BWOG Letter (J. Taylor) to NRC (Scott Newberry), dated March 2, 1992

2. INEL Letter (C.F. Obenchain) to NRC (L.C. Ruth), dated October 18, 1993

EXECUTIVE SUMMARY

The purpose of this analysis is to provide a technical basis to justify increasing the Engineered Safety Features Actuation System (ESFAS)[1] on-line test intervals. The Babcock & Wilcox Owners Group (B&WOG) proposes to increase the test interval from one month to three months.

The analysis was performed on a generic basis. Three configurations of the ESFAS were modeled to reflect the major differences between the three ESFAS designs. ANO-1 and Oconee have a Bailey-designed ESFAS, Crystal River-3 has a Gilbert-designed ESFAS, and Davis-Besse has a Bechtel-designed ESFAS. All of the ESFAS designs have three or four redundant analog subsystems that monitor pertinent plant parameters, generally reactor coolant pressure and reactor building pressure. All three designs have two redundant actuation subsystems that each actuate one of the redundant trains of Engineered Safeguards (ES) devices, including high pressure injection (HPI), low pressure injection (LPI), reactor building isolation, reactor building cooling, and reactor building spray.

The methodology used to evaluate the test intervals for the ESFAS is the same as used for the B&WOG submittal justifying the Reactor Trip System (RTS) test interval extension, Topical Report BAW-10167. The Nuclear Regulatory Commission has reviewed and approved the RTS test interval extension submittal and issued an SER. The methodology has been changed only slightly and incorporates improvements suggested by the SER. The methodology used in BAW-10167 and here is based upon reliability block diagrams (RBDs) and contains the features that are important for technical specification submittals, including: time-dependent modeling, emphasis on operating experience data, inclusion of common mode failures (mechanical and human-caused), and uncertainty analysis.

---

[1] ESFAS is called Engineered Safeguards Actuation System (ESAS) at ANO-1 and Crystal River-3, and Safety Features Actuation System (SFAS) at Davis-Besse.

A time-dependent model was used to dynamically represent system configuration changes associated with testing and maintenance. The analysis placed heavy emphasis on the use of operating experience data. Data, based on industry-wide operating experience derived from Licensee Event Reports (Atwood and Meachum, Common Cause Fault Rates for Instrumentation and Control Assemblies, NUREG/CR-3289), were used as a source of failure rates for sensors and instrument strings. Failure history for other ESFAS components, such as logic modules and relays, was based on B&WOG operating experience obtained from Nuclear Plant Reliability Data System (NPRDS).

ESFAS contribution to core melt frequency was examined for a spectrum of different Loss of Coolant Accident (LOCA) events (including transient-induced LOCAs), each of which challenges different ESFAS parameters and requires a different ESFAS response. Core melt frequency due to ESFAS failure was determined through a synthesis of the ESFAS reliability in response to various challenging events, the ESFAS challenge rate for the events, and the consequence of ESFAS non-response, in terms of the time available to avert core melt. Thus, the ESFAS failure modes were modeled with RBDs, quantified with operating history, and placed into common perspective with respect to impact on (core melt) risk.

Time-dependent plots were made showing core melt frequency due to ESFAS failure for both one- and three-month test intervals over a typical 18-month fuel cycle. The plots explicitly show the effect of surveillance testing on core melt risk. The time-dependent plots were used to ensure that there were not any risk vulnerabilities (i.e., unacceptable risk peaks) that might result from changing test intervals.

Time-dependent results were then integrated to obtain the average core melt risk due to ESFAS failure for both one-month and three-month test intervals, as well as the incremental difference in core melt frequency attributable to increasing the test interval for ESFAS from one to three months. The estimated mean incremental risk associated with extending the test interval to three months varied from 1.45×10^{-7} to 2.03×10^{-8} per reactor-year for the three ESFAS

designs. Thus, the impact of increasing the ESFAS test interval from one to three months is small.

Uncertainty analysis was performed to test the robustness of the results in light of data uncertainties. A Monte Carlo analysis was performed using error factors of ten for all failure rates including random and common mode. An error factor of ten represents an order of magnitude variation in the failure rates in either direction from the medians to the lower and to the upper bound values. The uncertainty analysis indicates that there is a 95 percent probability with 95 percent confidence (95%/95%) that the incremental core melt frequency associated with increasing the ESFAS test intervals to three months is less than 4.94×10^{-7} per reactor-year for the Bailey design, 9.57×10^{-8} per reactor-year for the Gilbert design, and 2.69×10^{-7} per reactor-year for the Bechtel design. These results show that, even with an order of magnitude uncertainty in the data, the incremental risk from extending the ESFAS test interval to three months is small.

Therefore, the B&WOG proposes to increase the ESFAS test interval from one to three months and concludes that the effect on plant risk is insignificant.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AAL	Auto Actuation Logic
ANO-1	Arkansas Nuclear One Unit 1
AOT	Allowed Outage Time
BWNS	B&W Nuclear Service Company
BWST	Borated Water Storage Tank
B&W	Babcock & Wilcox
B&WOG	Babcock & Wilcox Owners Group
CDF	Cumulative Distribution Function
CR-3	Crystal River Unit 3
D-B	Davis-Besse
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFIC	Emergency Feedwater Initiation & Control
EPRI	Electric Power Research Institute
ES	Engineered Safeguards
ESFAS	Engineered Safety Features Actuation System
HPI	High Pressure Injection
INPO	The Institute of Nuclear Plant Operations
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LPI	Low Pressure Injection
MTTR	Mean-Time-To-Repair
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
NSS	Nuclear Steam System

PDF	Probability Density Function
PRA	Probabilistic Risk Assessment
RB	Reactor Building
RBD	Reliability Block Diagram
RC	Reactor Coolant
RCS	Reactor Coolant System
RPS	Reactor Protection System
RTS	Reactor Trip System
SAR	Safety Analysis Report
STI	Surveillance Test Interval

1. INTRODUCTION

The purpose of this investigation is to show that extended test intervals for the Engineered Safety Features Actuation System (ESFAS) would not decrease plant safety. A technical justification is provided supporting an increased test interval of three months for the ESFAS. Extensions for actuated Engineered Safeguards (ES) devices, such as pumps and valves, are not proposed at this time.

The investigation performed is generic and applicable to Arkansas Nuclear One-1 (ANO-1), Oconee 1,2&3 (Oconee), Crystal River-3 (CR-3), and Davis-Besse (D-B), all of which have Babcock & Wilcox (B&W) Nuclear Steam Systems (NSS). There are three significantly different design configurations that must be accounted for by the ESFAS evaluation. Consequently, three separate models have been developed, one patterned after the Oconee and ANO-1 configurations, one for the CR-3 configuration, and the other for the D-B configuration; these were designed by Bailey, Gilbert, and Bechtel, respectively. Details concerning the similarities and differences of these designs are discussed in Section 2. The tests performed on the ESFAS are also described in Section 2, as well as proposed changes to the test frequencies.

The modeling of ESFAS uses the same methodology as developed for Topical Report BAW-10167 [1,2,3] which justified extended test intervals for the B&W Reactor Trip System. Reliability block diagrams (RBDs) were used to model the ESFAS designs. The ESFAS models constructed for the Bailey, Gilbert, and Bechtel designs include sensors and signal processing equipment, trip logic devices, output devices, and supporting power supplies. The effects of ESFAS testing on core melt frequency are included in the model. The PACRAT computer code was used to calculate the time-dependent core melt risk contribution of ESFAS for the existing one-month, as well as for the proposed three-month test intervals. The PACRAT code and other software used in this evaluation, and the modeling methodology are discussed in Section 3.

Random and common mode failures were accounted for and operating experience was used to support the evaluation. Data derived from Licensee Event Reports (LERs)

by EG&G [4] was used for the sensors and instrument strings (i.e., the analog subsystems). B&W Owners Group (B&WOG) operating experience from the Nuclear Plant Reliability Data System (NPRDS) was used to provide random and common mode failure rates for the logic components (i.e., the digital subsystems). B&WOG and generic experience was used to provide ESFAS challenging event frequencies. The data evaluation is described in Section 4.

Time-dependent determinations of core melt frequency due to ESFAS failure for the spectrum of challenging events were made using best-estimate data. ESFAS contribution to core melt frequency was estimated for one-month and three-month test intervals, as well as the incremental core melt frequency associated with extension from one-month to three-month testing. A Monte-Carlo analysis was performed on the time-averaged results to indicate the influence of data uncertainties. The quantification and uncertainty analysis are discussed in Sections 5 and 6.

2. GENERAL DESCRIPTION OF HARDWARE AND TESTING

The various B&WOG utilities have different names and acronyms for their safety features actuation systems; for simplicity, this report will refer to them all as "ESFAS." The design features of the ESFAS have been described in other documents including docketed Safety Analysis Reports (SARs). Therefore, a full description of the ESFAS is unnecessary and a summary description of the most important features is provided. These features are shown in Figures 2-1 through 2-3, reproduced from the SARs. More drawings describing the ESFAS are available from the SARs.

This evaluation is applicable to Oconee, ANO-1, CR-3, and D-B. There are three different ESFAS designs at these plants. Consequently the evaluation grouped the plants into three groups reflecting the Bailey (ANO-1 and Oconee), Gilbert (CR-3), and Bechtel (D-B) supplied ESFAS. The following sections describe the fundamental differences. These differences are accounted for in the analysis.

Although there are some differences in implementation, all of the ESFAS designs have three or four redundant analog subsystems that monitor pertinent plant parameters, generally reactor coolant (RC) and reactor building (RB) pressure, to actuate Engineered Safeguards (ES) devices that loosely translate into four functional groups: high pressure injection (HPI), low pressure injection (LPI), RB isolation and cooling, and RB spray. All three designs have two redundant actuation subsystems (i.e., digital subsystems) arranged in a one-out-of-two logic that is implemented by actuating one train of ES devices off of each ESFAS actuation subsystem.

2.1. Important Hardware Features

2.1.1. Bailey Design

Highlights of the Bailey design are:

- General[1] coincidence logic.
- Three analog channels (two-out-of-three coincidence) feeding two actuation (i.e., digital) subsystems.
- Centralized design. In each actuation subsystem, there is one coincidence logic module (called "trip logic module") for each ESFAS function. Each trip logic module, containing the two-out-of-three logic, can drive multiple "unit control modules," one for each actuated ES device or group of related devices.
- Sensed parameters include RC pressure and RB pressure.
- ANO-1 has analog sensors for RB pressure. Oconee uses analog sensors for high RB pressure and digital pressure switches for high-high RB pressure.

Features of the Bailey ESFAS are shown schematically in Figure 2-1. The ANO-1 ESFAS is shown as representative of both ANO-1 and Oconee ESFAS. The relatively minor differences between Oconee and ANO-1 ESFAS are noted in the applicable portions of the report.

---

[1] Coincident trip of different plant parameters will actuate ESFAS.

2.1.2. Gilbert Design

Highlights of the Gilbert design are:

- General[2] coincidence logic.
- Three analog channels (two-out-of-three coincidence) feeding two actuation (i.e., digital) subsystems.
- Distributed design. In each actuation subsystem, there are three channels of relays (actuated by the three analog subsystems) for each ESFAS function. These relays drive two-out-of-three coincidence logic matrices (called "auto actuation logic"). There is a separate auto actuation logic (AAL) matrix for each actuated component.
- Sensed parameters include RC pressure and RB pressure.
- Has digital pressure switches for RB pressure.

Figure 2-2 shows the Gilbert ESFAS.

2.1.3. Bechtel Design

Highlights of the Bechtel design are:

- Local[3] coincidence logic.
- Four analog channels (two-out-of-four coincidence) feeding four channels of "system logic" that are arranged in two-out-of-two pairs to form two actuation (i.e., digital) subsystems.

---

[2] Coincident trip of different plant parameters will actuate ESFAS.

[3] Coincident trips must be of the same plant parameter to actuate ESFAS.

- Distributed design. Within each of the four "system logic" channels, there are from one to nine "output modules" for each of five ESFAS functions (called "incident levels"). Each of the many output modules contains a two-out-of-four coincidence logic for each applicable plant parameter. The four channels of output modules are arranged such that each ES device is actuated by a coincident trip from two output modules in separate channels. (The redundant device in the other ES train is actuated by output modules in the remaining two channels.) Several ES devices within the same ES "system" and train may actuate from the same pair of output modules.

- Sensed parameters include RC pressure, RB pressure, RB radiation, and BWST level.

- Has analog sensors for RB pressure.

The Bechtel ESFAS is illustrated in Figure 2-3.

2.1.4. Power Supplies

The ESFAS analog sensors have individual power supplies. Failures of individual sensor power supplies cause erratic sensor readings and are equivalent to sensor failure.

Power is also required for operation of the signal conditioning and logic modules within ESFAS. This power comes from internal ESFAS DC power supplies and/or vital buses. For ESFAS components that energize-to-trip, power supply failures would prevent actuation. However, many components within ESFAS deenergize-to-trip, that is, fail safe upon loss of power.

For the Bailey design, the analog channels will trip upon loss of power. An exception is the high-high RB pressure channels at Oconee that need vital AC to trip; this parameter is used only to actuate RB spray. The digital subsystems at the Bailey plants will fail in the unactuated state upon loss of power because the trip logic modules energize-to-trip (using ESFAS -15V DC internal power

supplies) and the output relays in the unit control modules energize-to-trip (using vital AC).

For the Gilbert design, the analog channels deenergize-to-trip and, therefore, will fail safe upon loss of power. The digital subsystems also deenergize-to-trip, and, therefore, will go to the actuated state upon loss of power, except for the spray pump actuation logic, which is energize-to-trip. However, for a LOOP event, vital DC and AC power would be needed to keep the 4160 bus undervoltage relaying and ESFAS time delay relays energized, which blocks ESFAS actuation until the emergency diesel generators (EDGs) are on-line.

For the Bechtel design, both the analog and digital subsystems deenergize-to-trip, and, therefore, will go to the actuated state upon loss of power. However, for a LOOP event, vital AC and DC power would be needed for the 4160 bus undervoltage relaying, and ESFAS internal power supplies would be needed to k sequencer and output modules energized, which block ESFAS actuation until the EDGs are on-line.

Power for the actuated ES devices is outside the scope of this study. However, for ESFAS challenging events that involve an unpowered ES train, the study recognizes that ESFAS must actuate the powered ES train. This study does not address changes to the test intervals for the ES devices or their power supplies.

2.2. Testing and Maintenance Features

This study addresses the proposed changes to the current one-month test intervals for those components that are tested on-line. The proposed changes that were evaluated are noted below, *in italics*. This consists of extending the test interval for the ESFAS analog and digital (i.e., actuation) subsystems from one month to three months. For other tests that are not currently performed monthly, such as visual channel checks and response time tests, no changes are proposed at this time.

In addition, no test interval changes are proposed at this time for the components that are outside of the ESFAS system (and ESFAS Technical

Specifications) scope, specifically, the actuated ES devices and those power supply components that are external to the ESFAS cabinets, such as station batteries, inverters, and 4160V bus undervoltage relaying.

The following sections summarize the testing and maintenance features of the ESFAS components. There are some variations in the testing and maintenance schemes for the utilities with the three ESFAS designs. The most significant of these are noted in the following descriptions.

2.2.1. Analog Subsystem Testing: Sensors

Sensor testing includes the following:

- Full off-line test and calibration at shutdown (18-month test interval).
- Channel check consisting of visual comparison of analog sensor output against other channels (each shift).
- RB pressure sensors (analog sensors and digital switches) are exercised monthly at the plants where they are accessible (D-B and CR-3). For D-B this test results in bypass of the sensor during the test. *It is proposed that this test interval be changed to three months.*

2.2.2. Analog Subsystem Testing: Instrument Strings

For this study, an "instrument string" includes all electrical components from a sensor to the corresponding bistable(s). This includes the dedicated sensor power supply, signal conditioning, and the bistable(s), but excludes the sensor. Instrument string testing is summarized below:

- Monthly functional test of each channel. *It is proposed that this test interval be changed to three months.*

  For the Bechtel design, the functional tests are staggered (one of the four channels is tested per week). The testing requires individual instrument strings of the applicable channel to be bypassed, one plant parameter at a time. (The coincidence logic downstream of the instrument string is not bypassed, therefore all four channels can trip with two-out-of-three inputs of the tested parameter or two-out-of-four inputs of any other parameter.)

  For the Bailey and Gilbert designs, the three redundant channels are tested sequentially. The applicable channel is tripped during the functional test.

  For all three designs, each plant parameter is tested separately, in turn, by substituting a false signal downstream of the sensor.

2.2.3. Maintenance of Test-Failed Sensors and Instrument Strings

Maintenance is undertaken if the sensors or instrument strings are determined to be inoperable, following the guidelines of the applicable Technical Specifications. The Technical Specifications in effect during performance of this study were used, except for CR-3, for which the Revised Standard Technical Specifications [5] were used. Single channels (sensors or instrument strings) that fail are generally required by Technical Specifications to be tripped within one hour. Once tripped, the components are repaired and returned to service at the first opportunity. If, at the plants with the three-channel ESFAS designs, the tripped channel cannot be repaired before the next scheduled surveillance test, then the reactor must be shutdown because the test cannot proceed without causing an unwanted ESFAS actuation.

If failure of multiple analog channels is discovered, Technical Specifications require that the reactor be shutdown within a specified length of time to a mode where ESFAS operability is not required. For the Bailey plants, hot shutdown is

required within 12 hours, and if not repaired within 48 more hours, then cold shutdown is required within 24 hours. For the Gilbert plant, hot shutdown is required within 13 hours for RC pressure or cold shutdown is required within 37 hours for RB pressure. For the Bechtel plant, cold shutdown is required within 37 hours for radiation detection channels or hot shutdown is required within 13 hours for the other parameters. During this time, the reactor can return to power if the affected components are repaired and returned to service. (However, the RBD model assumes that the full allowed time will be used).

With the proposed test interval, the analysis assumes the same ACTION statement times as with the one-month test interval.

2.2.4. Digital (Actuation) Subsystem Testing

The designs of the three ESFAS systems vary in the way testing is accommodated in the digital subsystems. Each designer has approached in a different way the problem of how to test the operability of ESFAS actuation logic without producing a spurious actuation:

- All of the B&WOG utilities have monthly functional testing of the digital subsystems for their respective ESFAS designs. *It is proposed that this test interval be changed to three months.*

- The Bailey digital subsystem has centralized coincidence logic (i.e., there is one trip logic module per function in each digital subsystem). The Bailey digital subsystem on-line functional test has two parts:

  The two-out-of-three logic of each trip logic module is tested by tripping its inputs one at a time. This results in a half-trip of each trip module.

  The circuitry from the coincidence logic to the unit controller of each ES device is tested by means of a logic test module and a half-wave signal that tests the electrical continuity without causing a spurious actuation.

- The Gilbert design has distributed coincidence logic (i.e., each actuated ES device has its own auto actuation logic (AAL) matrix). There are two on-line functional tests that affect the digital subsystems:

  Test trips sent separately from each of the three analog channels terminate with half-trips in all of the applicable two-out-of-three AAL matrices in each of the two actuation subsystems.

  In another test procedure, each AAL matrix is tested separately by tripping one combination of two of its inputs, during which time the output of the applicable matrix is blocked to prevent spurious equipment actuation. Since each actuated device has its own AAL matrix, only a single ES device at a time is affected. The matrix tests rotate so that all three combinations of two are tested in three sequential months.

- The Bechtel design has four channels of coincidence logic that the utility tests on a staggered schedule concurrent and integrated with the tests of the four analog channels. The Bechtel coincidence logic is distributed among many output modules, each one containing a two-out-of-four coincidence logic for each applicable plant parameter. Each output module is functionally tested separately as follows:

  Each coincidence logic circuit has a fifth input from a test circuit; the trip of one-out-of-four inputs from the analog channels coincident with the "fifth channel" test trip satisfies the two-channel coincidence required to trip the output module. The trip of the output module results in a half-trip of the applicable output module pair; the associated ES devices do not trip because each output module output is "AND-ed" with one from a complimentary channel.

2.2.5. Maintenance of Test-Failed Digital Subsystems

Detection of faulty components in the digital subsystems results in certain actions being taken that are dictated by Technical Specifications. In general, repair is initiated either with the affected component(s) tripped or with shutdown of the reactor required within a certain length of time (that varies from plant to plant). The Technical Specifications in effect during performance of this study were used, except for CR-3, for which the Revised Standard Technical Specifications [5] were used; the following is a summary of the Technical Specifications that were used for each plant.

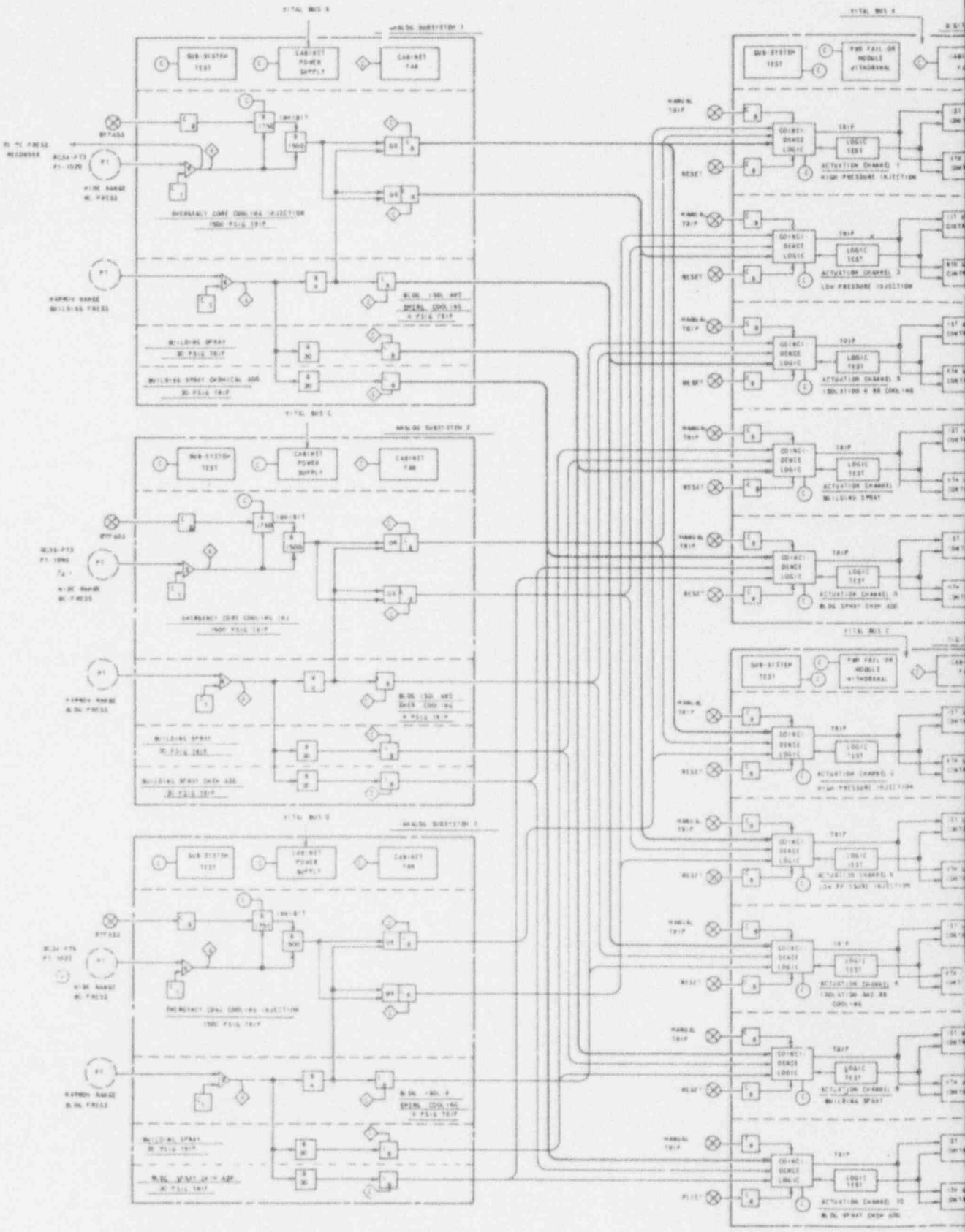
For the Bailey plants, the length of time that the reactor can operate with inoperable digital subsystem component(s) before the reactor must be in hot shutdown varies from 24 to 36 hours. For ANO-1, component failure in the digital subsystems results in invoking the Emergency Core Cooling System (ECCS) Technical Specification for the associated ES component(s); consequently, the length of time that the reactor can operate with the inoperable digital subsystem component(s) before the reactor must be in hot shutdown is 36 hours. For Oconee, the length of time that the reactor can operate with inoperable digital subsystem component(s) before the reactor must be in hot shutdown is 24 hours. For both ANO-1 and Oconee, cold shutdown follows after an additional 72 hours.

For the Gilbert plant, component failure in the digital subsystems (automatic actuation logic) results in invoking the ECCS Technical Specification for the associated ES component(s). Consequently, the length of time that the reactor can operate with the inoperable digital subsystem component(s) varies according to the affected device(s). For example, the allowed outage time is 72 hours for one failed train of HPI and 7 days for one failed train of RB cooling, followed by hot shutdown within 12 hours if HPI is affected, or cold shutdown in 36 hours if RB cooling is affected.

For the Bechtel plant, failures in the digital subsystems require that the affected component(s) be tripped or that shutdown be initiated within one hour to bring the reactor to cold shutdown within the next 36 hours.

During these periods the reactor can return to power if the affected component(s) are repaired and returned to service (however the RBD model assumes that the full allowed time will be used).

With the proposed test interval, the analysis assumes the same ACTION statement times as with the one-month test interval.



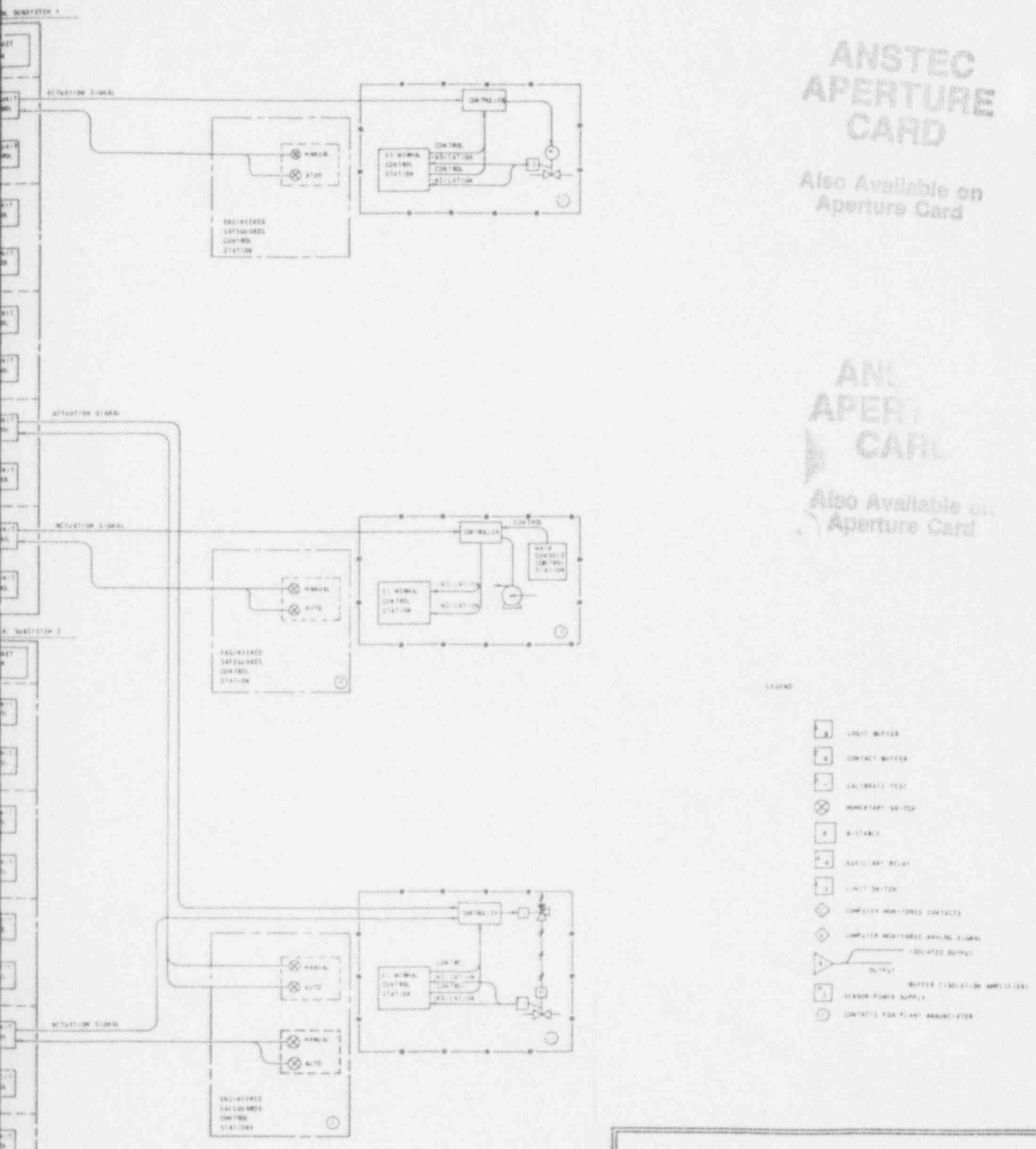
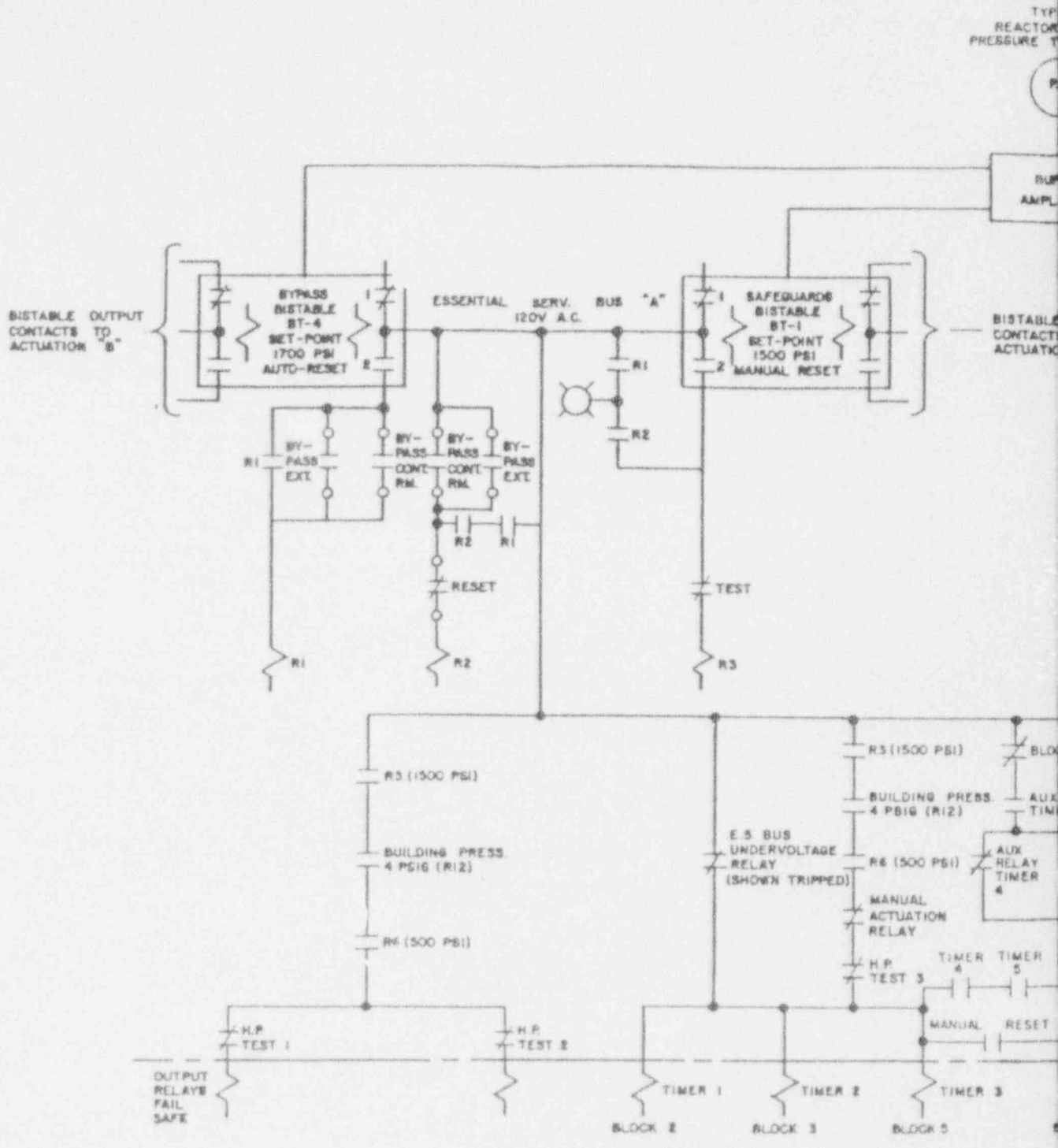


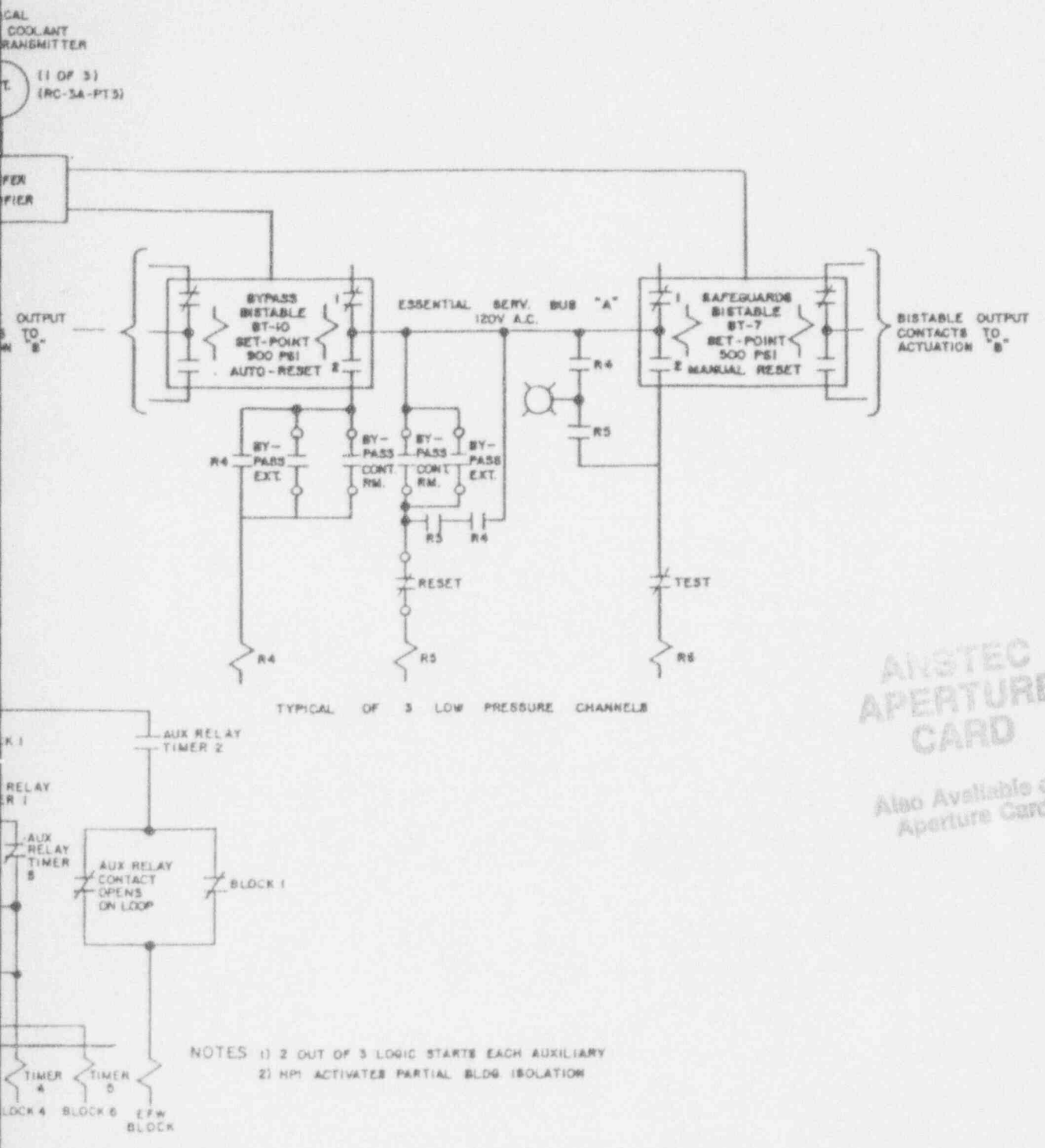
FIGURE 2-1

BAILEY ESFAS BLOCK DIAGRAM (ANO-1)



TYPICAL OF 3 CHANNELS

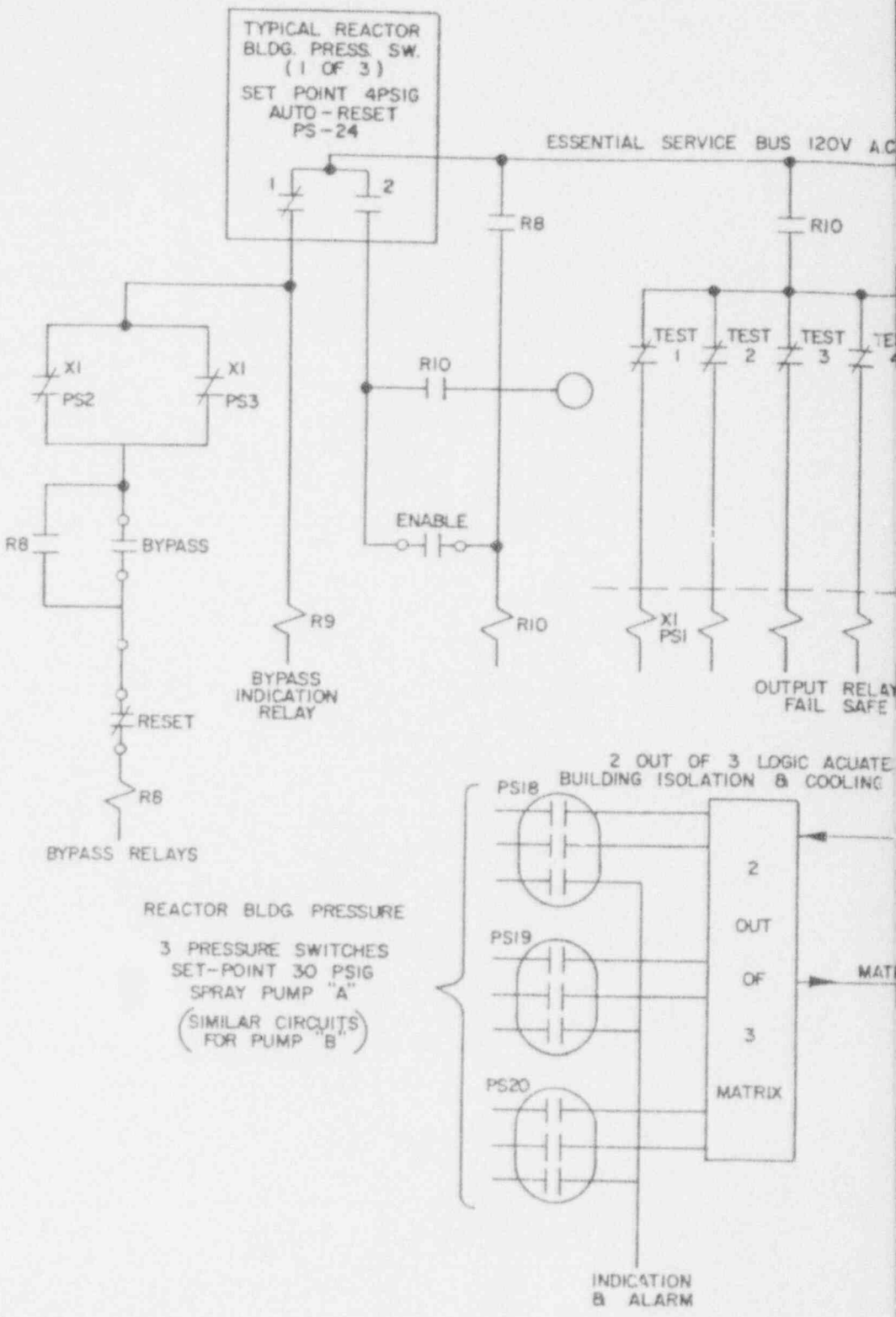
HIGH PRESSURE INJECTION & LOADING SEQUENCE "A"



NOTES 1) 2 OUT OF 3 LOGIC STARTS EACH AUXILIARY
2) HPI ACTIVATES PARTIAL BLDG ISOLATION

FIGURE 2-2 (SHEET 1 OF 2)

GILBERT ESFAS DIAGRAM (CR-3)


TYPICAL REACTOR BLDG. PRESS. SW. (1 OF 3)
SET POINT 4PSIG
AUTO - RESET
PS - 24
ESSENTIAL SERVICE BUS 120V A.C
1
2
R8
R10
TEST 1
TEST 2
TEST 3
X1
PS2
X1
PS3
R10
ENABLE
R8
BYPASS
R9
R10
X1
PS1
BYPASS INDICATION RELAY
OUTPUT RELAY FAIL SAFE
RESET
R8
BYPASS RELAYS
2 OUT OF 3 LOGIC ACUATE
BUILDING ISOLATION & COOLING
PSI8
PSI9
PS20
2
OUT
OF
3
MATRIX
REACTOR BLDG. PRESSURE
3 PRESSURE SWITCHES
SET-POINT 30 PSIG
SPRAY PUMP "A"
(SIMILAR CIRCUITS FOR PUMP "B")
INDICATION & ALARM

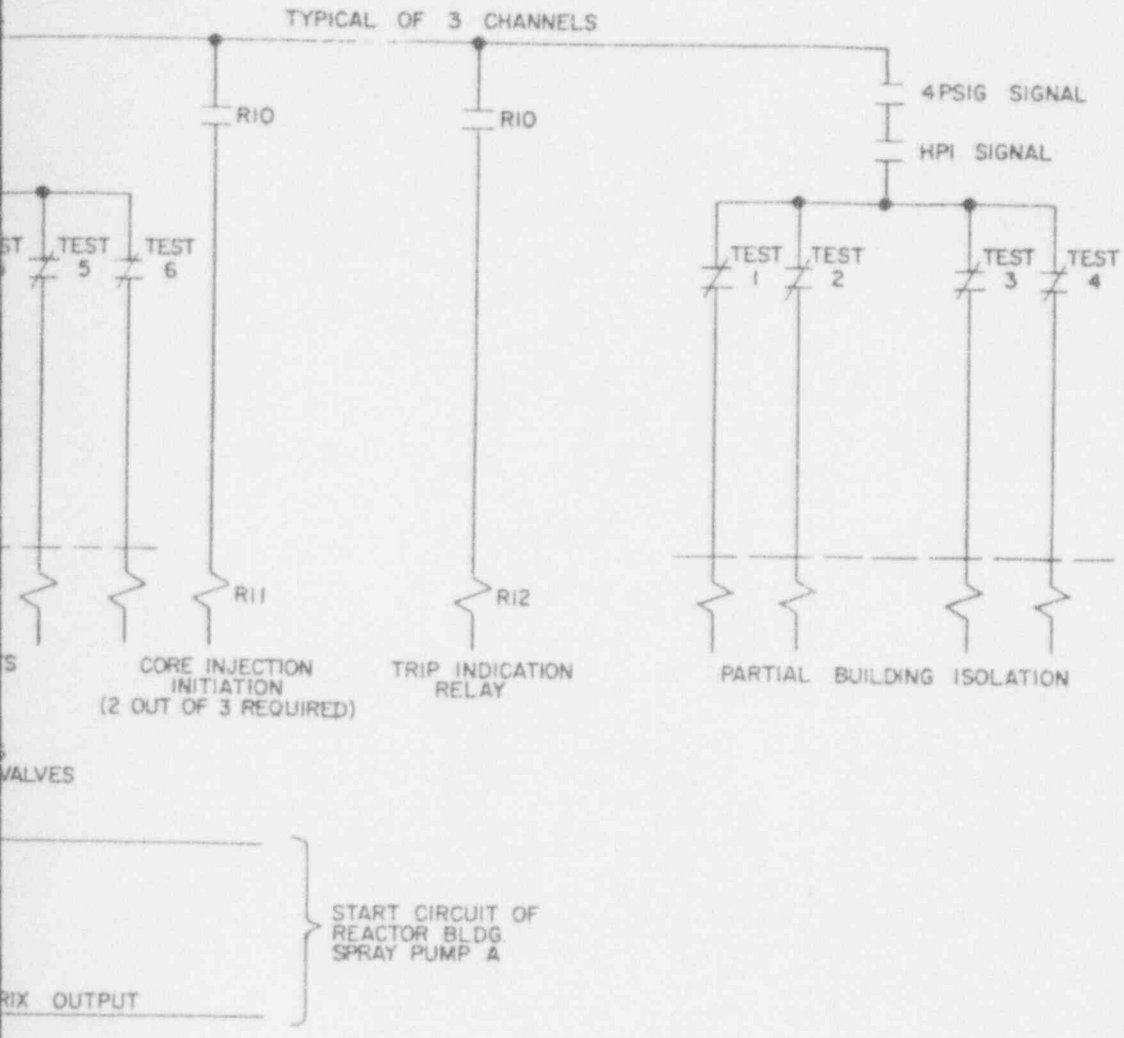
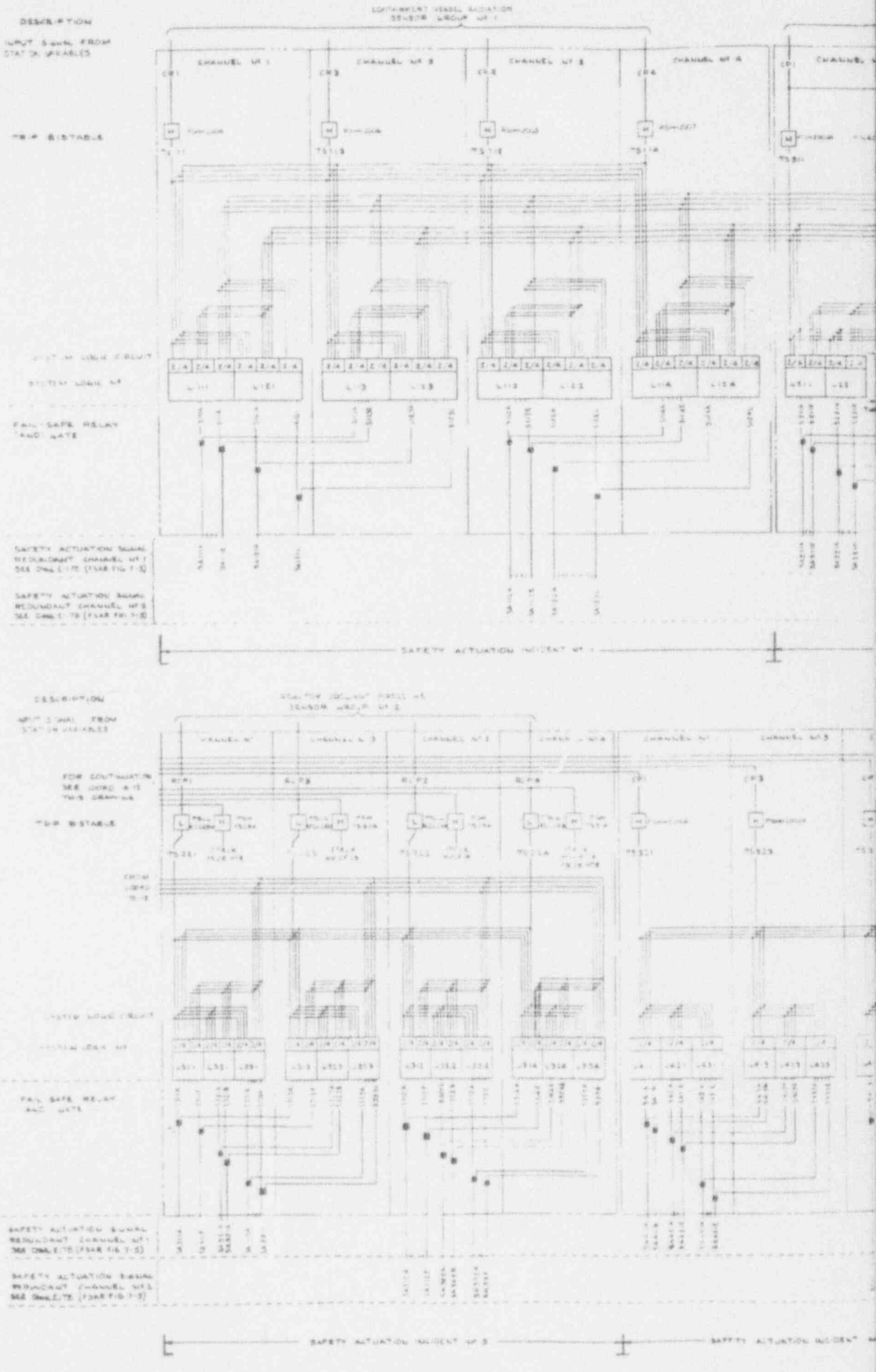


FIGURE 2-2 (SHEET 2 OF 2)

GILBERT ESFAS DIAGRAM (CR-3)


DESCRIPTION
INPUT SIGNAL FROM STATION VARIABLES
FOR BISTABLE
CHANNEL N° 1
CHANNEL N° 3
CHANNEL N° 2
CHANNEL N° 4
FAIL-SAFE RELAY "AND" GATE
SAFETY ACTUATION SIGNAL REDUNDANT CHANNEL N° 1
SAFETY ACTUATION SIGNAL REDUNDANT CHANNEL N° 3
SAFETY ACTUATION INCIDENT N° 1
DESCRIPTION
INPUT SIGNAL FROM STATION VARIABLES
FOR CONTINUATION SEE CORD. A-12 THIS DRAWING
FOR BISTABLE
FAIL SAFE RELAY AND GATE
SAFETY ACTUATION SIGNAL REDUNDANT CHANNEL N° 1
SAFETY ACTUATION SIGNAL REDUNDANT CHANNEL N° 2
SAFETY ACTUATION INCIDENT N° 3

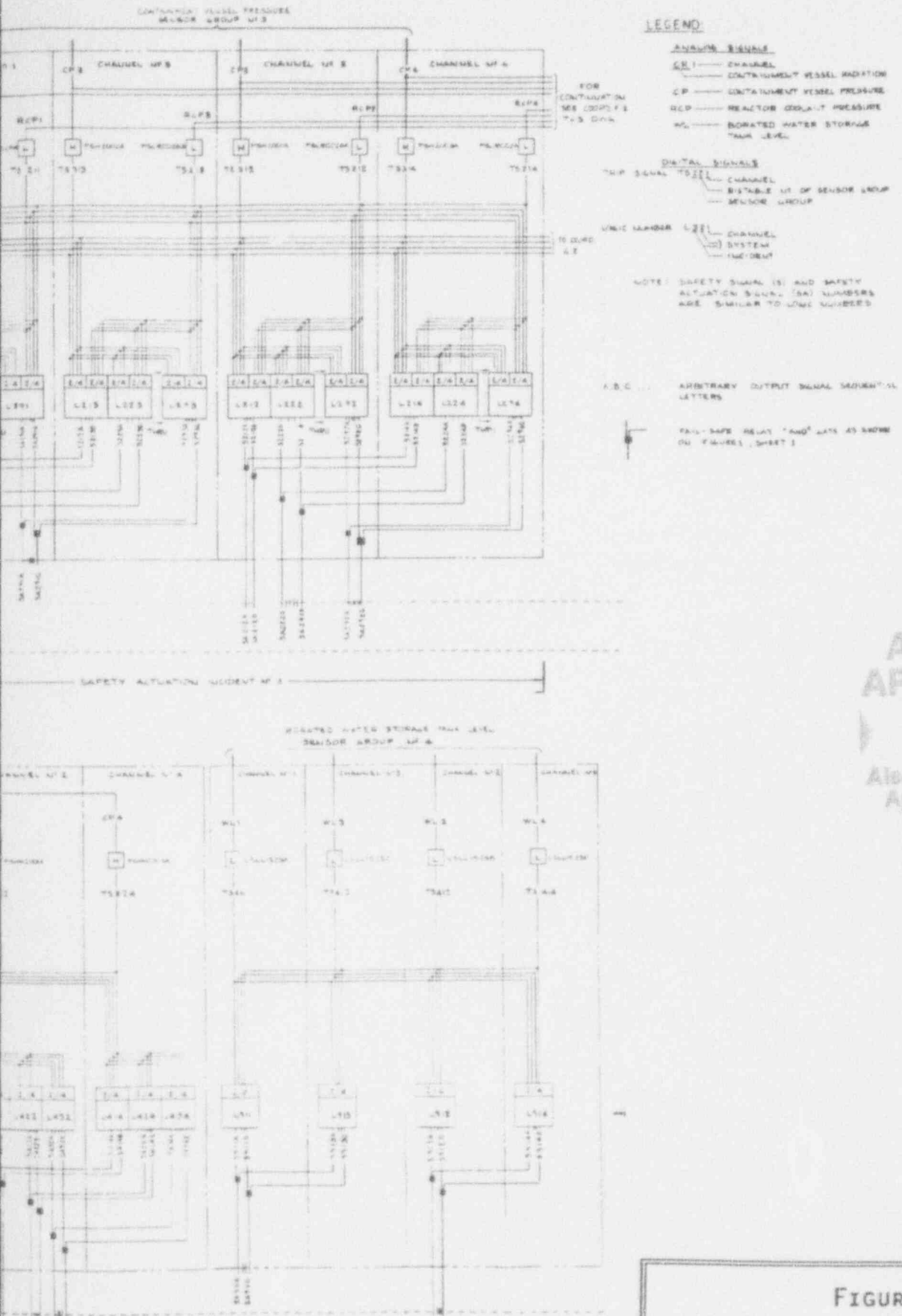


FIGURE 2-3

BECHTEL ESFAS SIGNAL DIAGRAM (D-B)

3. DESCRIPTION OF MODELS USED FOR RELIABILITY EVALUATION

The methodology used to evaluate the test intervals for the ESFAS is the same as used for the B&WOG submittal on Reactor Trip System (RTS) test interval extension, Topical Report BAW-10167 [1,2]. The Nuclear Regulatory Commission (NRC) [3] has reviewed and approved the RTS test interval extension submittal. The methodology documented in BAW-10167, and used here, is based upon RBDs and contains the features that are important for technical specification submittals, including: time dependent modeling, emphasis on operating experience data, inclusion of common mode failure and human error, and uncertainty analysis. The methodology discussed in Section 3 and the data treatment discussed in Section 4 are the same as used for BAW-10167, except for the minor deviations that are noted below.

3.1. Deviations from BAW-10167 Methodology and Data

BAW-10167 evaluated the RTS reliability and risk significance for a representative (and bounding) event, namely, loss of feedwater. It also explicitly excluded manual recovery action (i.e., manual reactor trip) because it was considered a constant over all events and would unnecessarily complicate and mask the results. In the ESFAS analysis, it was not possible to choose a representative event because ESFAS actuates a much wider selection of equipment than RTS. Therefore, ESFAS reliability was examined for a spectrum of different Loss of Coolant Accident (LOCA) events, each of which challenges different ESFAS parameters and requires different ESFAS response. Failure of ESFAS to respond by actuating the appropriate devices, in itself does not disable the ES function(s), because the devices can be actuated manually independent of ESFAS. ESFAS has more functions than RTS, and the time available for appropriate operator recovery action is not constant over all ESFAS functions (for example, failure of ESFAS to actuate HPI requires more urgent operator action than failure of ESFAS to actuate RB cooling). Thus, it was necessary to include ESFAS challenge rates and recovery through manual ES actuation as a way of putting the various event scenarios that challenge ESFAS, and the respective ESFAS failure modes, into common perspective with respect to impact on (core melt) risk.

Another difference between this analysis and BAW-10167 is in the uncertainty analysis (described is Section 5). In response to comments by the reviewers of BAW-10167, the error factors on the failure data were increased to ten for all components.

In BAW-10167, common mode failure rates were excluded for some components where the data did not support their inclusion, or the rates were insignificantly small. In response to comments made by the reviewers of BAW-10167, the ESFAS analysis includes a common mode failure contribution for all components within the ESFAS system, even when the failure data did not support development of a rate. In the cases where common mode failure rates could not be obtained from the failure history, subjective (and conservative) β-factors were assigned.

In BAW-10167, for test-revealed failures, time-to-repair data was obtained from historically-derived mean-time-to-repair (MTTR) data rather than Technical Specification-dictated allowed outage time (AOT) or ACTION times. Since this was an issue in the BAW-10167 review process, the ESFAS analysis assumes that the system reliability will continue to be vulnerable to a test-revealed failure for the full length of the AOT/ACTION time dictated by Technical Specifications, even though the actual repair time may be shorter. Thus, the times used in the model are the full time allowed by Technical Specifications, from detection of the failure until the component or channel is in a "safe" state (generally tripped) or the reactor is shutdown to a "safe" state (i.e., a mode where the affected ESFAS function is no longer needed).

The analysis of component wearout is not included in the ESFAS model. Inclusion of wearout in Topical Report BAW-10167, Supplement 1 [2] was included to address Generic Issue 83-28, item 4.5.3 and applied primarily to reactor trip breakers; it is not a significant issue for ESFAS monthly test interval extension.

Evaluation of instrument drift over the proposed (i.e., longer) test interval is not evaluated in this report. An attempt to address drift on a generic basis in BAW-10167, Supplement 1 was concluded by the reviewers to be insufficient because drift was considered to be "individual to each specific plant." The reviewers determined that before implementation, each licensee should confirm that drift

will be within acceptable limits over the period of the new test interval. The B&WOG considers that to be an acceptable approach for implementation of the proposed extended ESFAS test interval.

3.2. Reliability Block Diagram Modeling

Separate RBDs were constructed to represent the three ESFAS designs, Bailey, Gilbert, and Bechtel, and are shown in Appendix A. The three ESFAS configurations are representative of all the participating B&WOG plants, specifically Oconee, ANO-1, CR-3, and D-B. Each plant's ESFAS closely matches one of these configurations.

ANO-1 and Oconee both have the Bailey design and they have only minor differences of hardware and test practices, as noted in Section 2 and/or on the Bailey RBD. These minor differences were evaluated for their reliability and core melt risk significance, and their impact was insignificant. Where these small differences exist, the most conservative choice was used for the Bailey model. Thus one model was developed, using the most limiting features, to represent both of the plants with the Bailey design.

The Gilbert and Bechtel models reflect CR-3 and D-B-specific hardware and test practices, respectively. Consequently, all of the above-listed plants are represented or bounded by the three models and the conclusions derived from the analysis apply generically to all.

The hardware configurations summarized in Section 2 are represented by these RBDs. This includes sensors for all parameters input to the ESFAS, instrumentation channels containing processing equipment and bistables, coincidence logic consisting of logic modules and/or relays, and power supplies.

The RBDs model each sensed parameter of the ESFAS trips. These include RC pressure (for low and low-low trips), and RB pressure (for high and high-high trips). In addition, the Bechtel design includes high RB radiation and low BWST level. The RBD is arranged so that individual parameters or combinations of parameters can be called upon for evaluation of ESFAS response to a selected

challenging event. For example, for an interfacing systems LOCA (i.e., LOCA outside of containment), high RB pressure will not be challenged -- therefore, when evaluating that case, the unchallenged RB pressure parameter was analytically detached from the RBD.

The top logic of the RBDs in Appendix A are shown configured for general functional logic and are not tailored for any particular event. The top logic of the RBDs reflect dependencies that are a function of ES equipment assignment to channels (e.g., for Gilbert design, successful actuation of LPI requires actuation of both LPI and HPI functions because LPI pumps are started by the HPI channels and the LPI valves are opened by the LPI channels). Quantification runs were tailored to specific challenging events by detaching unchallenged or inapplicable functions -- for example, when evaluating a small LOCA, the LPI actuation function was not needed.

The level of detail of the RBD basic events was chosen to correspond with the level of resolution of the data, with preference given to data derived from operating experience. For example, random and common mode failure data for instrumentation assemblies from NUREG/CR-3289 [4] is available at the "sensor" and "signal conditioning system" level of resolution. A "signal conditioning system" is a combination of all of the components in an instrument string from downstream of the sensor, encompassing buffer amplifier, dedicated sensor power supply, etc., up to and including the bistable(s).

For other components, such as logic modules, the level of detail of the RBDs corresponds to the utilities' NPRDS reporting scope [6], so that operating experience could be attributed to the specific ESFAS designs.

For relays, failure data was obtained from NPRDS at the relay level, however since there were so many relays, it was impractical to show each one individually on the RBD. Therefore, individual relays were combined as basic events when they were in the same channel and used for the same function. That is, relays were modeled so that if one relay failed, the basic event (e.g., 4160 volt bus undervoltage relaying) failed.

Common mode failures are treated explicitly in the RBDs. Dependent basic events are shown involving two or more redundant components. All RBD basic events involving ESFAS components have corresponding common mode failure basic events associated with them and their redundant counterparts. This includes all of the ESFAS components that are within the scope of the proposed Surveillance Test Interval (STI) changes. More information on the identification and quantification of common mode failures appears in the discussion of the data (Section 4).

Human errors are not explicitly shown on the RBDs. Errors introduced during maintenance and test activities are incorporated into the common mode failure (and random) events. Common mode failures can result from both mechanical and human causes; analysis of the data indicates difficulty in separating the human element from the common mode failure. For example, the common mode failure (and random failure) data for instrumentation came from NUREG/CR-3289 [4] and is based on operating experience from LER reviews. This source expresses the common mode failure rates in terms of lethal and non-lethal "shocks". Analysis of the LERs supporting NUREG/CR-3289 indicates that many of these "shocks" are human-caused, although it is difficult to determine the exact breakdown between human and non-human causes. Similar difficulties in interpretation were experienced when analyzing NPRDS failure data for mechanical versus human causes. Therefore, in the interest of using operating experience data wherever possible, the human element and common mode failure contribution are integrated. The preference of operating-experience-based rather than theoretically-based estimates of human error probabilities provides more meaningful results.

3.3. Testing and Maintenance Modeling

The testing model was constructed with the flexibility to examine alternative test intervals for the ESFAS analog and digital subsystems. The RBD models and the PACRAT computer code account for changes in the configuration due to testing. All component failures that are not in the fail-safe mode contribute to system unavailability (i.e., to trip on demand) until they are detected (usually through testing). Some components are tripped either for testing or subsequent repairs and therefore do not contribute to system unavailability while they are in the

safe state. Other components contribute to system unavailability because redundancy is reduced while they are bypassed during testing. Components that are not tripped upon detection of failure contribute to system unavailability further while they are inoperable awaiting repair or reactor shutdown. These dynamic changes are reflected in the model for the test intervals that are examined.

The calculations performed by the PACRAT computer code (described in Section 3.5) are time-dependent. For example, the RBDs for the Bechtel ESFAS contain basic blocks in each of the four instrument string channels that perform a test-bypass function. These are analytic switches that remove the respective channels from service at prescribed times and durations. Using the RBD as input, the PACRAT code calculates the dynamic (time-dependent) availability of the Bechtel instrument strings as they change from 2-out-of-4 logic to 2-out-of-3 logic for the test, and back to 2-out-of-4 logic as the channel is returned to service, showing the effect of channel bypass during test. Other time dependent effects become evident using time-dependent analysis. After each test, for example, there is a step improvement in system unavailability as the tested components are verified to be free of undetected failures. Between tests, there is increasing unavailability according to the exponential relationship of reliability versus time; this reflects the probability of undetected failures accumulating until the next test.

The time-dependent modeling confirms that temporary changes in system configuration do not result in brief periods of extremely poor reliability that may have been hidden if averaged over a month or a year. This type of modeling is important when trying to demonstrate the effect of Technical Specification changes. The time-dependent results are presented and discussed in Section 5.

3.3.1. Analog Subsystem Components: Sensors

The modeling of sensors includes full testing at 18-month refueling outages, monthly exercising of RB pressure sensors at some plants (those plants with sensor accessibility), and visual comparison of sensor outputs each shift. The shift check may reveal catastrophic failures, however non-catastrophic or

degraded failures (such as drift) may not be discovered until the refueling outage test (or monthly exercising, if applicable). Thus, the reliability model considered both the catastrophic and degraded failure modes for random and common mode failure rates and corresponding times-to-repair of sensors. Due to the longer exposure time (i.e. the length of time that the failure is likely to go undetected), the degraded failure modes dominate sensor unavailability.

Sensor reliability is exponentially distributed over the time interval until detection, and contributes to ESFAS unavailability accordingly. Upon detection, single failures are treated differently than multiple failures because Technical Specifications typically require shutdown when more than one sensor failure for the same parameter is affected. Following detection, the model generally assumes that, consistent with Technical Specifications, individual sensor failures will result in trip of the appropriate ESFAS channel, while multiple failures will result in reactor shutdown and repair.

3.3.2. Analog Subsystem Components: Instrument strings

The (currently monthly) functional testing of instrument strings is performed differently for the four channel and three channel ESFAS designs. At the plant with the four channel ESFAS, the instrumentation strings are bypassed during testing. The modeling for the instrument strings includes the contribution of the bypassed string to reduced redundancy, and hence reduced ESFAS availability, for the duration of the test. At the plants with the three channel ESFAS, the instrument strings are tripped during testing and there is no reduced redundancy contributed by the test.

Instrument string reliability is exponentially distributed over the period between tests, and contributes to ESFAS unavailability accordingly. Single failures are treated differently than multiple failures because Technical Specifications typically require shutdown when more than one instrument string failure for the same parameter is detected. Following detection, the models assume that, consistent with Technical Specifications, individual instrument string failures will result in trip of the appropriate ESFAS channel, while multiple failures will result in plant shutdown and repair.

3.3.3. Digital Subsystem Components

As described in Section 2, the ESFAS digital subsystems for the Bailey and Bechtel designs are tested by tripping the appropriate components. Since the functions are tripped, there is no effect on ESFAS unavailability due to reduced redundancy. For the Gilbert design, the digital subsystems (i.e., auto actuation logic) are also tested by tripping the appropriate components, however the actuations are blocked before the actuated devices. Since Gilbert uses a distributed system, only one ES device at a time is affected. Nonetheless, the model reflects a reduced redundancy during these tests.

The digital subsystem testing contributes to availability by detection of latent failures that may develop between tests. The analytical model reflects this contribution with failure rates that are exponentially distributed over the monthly test cycle (quarterly, in the case of the proposed test interval). Upon detection of digital subsystem failures at the Bailey and Bechtel plants, the Technical Specifications require reactor shutdown within the specified ACTION time limit. At the Bechtel plant (which has a four-channel ESFAS), a failed digital subsystem component can be tripped; failures in multiple channels would require reactor shutdown within the specified Technical Specification ACTION limit.

3.3.4. Modeling of Component Repair

If testing reveals a failure needing repair, then attempts to repair the affected component(s) can continue for the full extent of the Technical Specification ACTION time limit, concurrent with the prescribed ACTION. The ACTION time limit is the time allowed from detection of the failure until the component or channel is in a "safe" state (generally tripped) or the reactor is shutdown to a "safe" state (i.e., a mode where the affected ESFAS function is no longer needed). When the repair is successful, the plant may return to normal configuration. For the purpose of Technical Specification evaluation, it was assumed that the full ACTION time limits are always used, though in some cases, the repair can be done faster. Thus, the "repair-times" used in the model, during which time the system

reliability is "vulnerable," are the full time allowed by Technical Specifications.

3.4. Determining Risk Significance of ESFAS Reliability

Since the purpose of the analysis is to examine the risk-impact of ESFAS test intervals, it is necessary to isolate the impact of ES actuation failure on that risk. Plant-specific Probabilistic Risk Assessments (PRAs) were not used to extract the influence of ESFAS because all ESFAS failures may not be explicitly represented in a PRA, and when they are, the failure modes are not usually significant contributors because they are overshadowed by failure of the actuated ES devices. A secondary reason was to avoid bringing the generic applicability of plant-specific PRAs into question. Therefore, the method used was to build an ESFAS RBD model, and then modify it with generic challenge rates and recovery probabilities, for a spectrum of events. Assuming that the consequence of non-recovery is core melt, the result is the ESFAS contribution to core melt frequency.

Since ESFAS is a multi-functioned system that is designed to respond to a variety of postulated LOCA events, it was necessary to align the RBD model functionally to the challenging events. Each event has a different impact on ESFAS, with respect to parameters that are challenged and ESFAS functions that need to respond. In addition, for a given event, some ES functions (e.g., actuation of long-term RB cooling) have less urgency than others (e.g., actuation of safety injection); consequently, their actuation failures have different risk significance. These issues were addressed for each event that could challenge ESFAS and incorporated into the model to produce an "aggregate" ESFAS-induced risk model.

The risk analysis built upon the RBD model, with RBDs being generated to represent all ESFAS functions at each plant. Then the models were run for the specific events from the spectrum of LOCAs and challenged ESFAS parameters. Given a specific ESFAS challenge scenario, the risk significance was addressed as a function of the ESFAS challenge rate and the consequence of non-recovery of

ES actuation for that scenario. Thus, a perspective was given to the relative importance of various events and ESFAS functions.

The following is a description of the risk analysis process:

3.4.1. Challenging Events

The events that challenge ESFAS are LOCAs and transient-induced LOCAs of various sizes. A variety of analysis source documents were examined, including Safety Analyses, Technical Specification Bases documents, and PRA literature, to identify events that would challenge ESFAS. They were grouped according to the required ESFAS response (e.g., is LPI needed?) and by which ESFAS parameters are challenged (e.g., will the Reactor Coolant System (RCS) depressurize to the low-low pressure setpoint?).

Transient-induced LOCAs originating from loss-of-offsite-power (LOOP) events were also included. The LOOP-initiated events are significant because, with subsequent failure of emergency AC power, ESFAS must actuate the ES devices in the powered train(s) (and sequence loads, if appropriate). Other than transient-induced LOCA, the probability of coincident LOCA with LOOP was not considered to be significant from a risk perspective.

The documentation on each potential event was examined to determine, if realistic assumptions were used, whether ESFAS would be challenged, and if so, which parameters (high RB pressure, low RC pressure, etc.) would be challenged, and also which ES systems were needed to mitigate risk. Some events, such as steam line break and steam generator tube rupture, were excluded because ESFAS would not be challenged or would be ineffectual (e.g., feedwater isolation is not an ESFAS function at B&WOG plants), and therefore ESFAS would not have an impact. The complete list of ESFAS-challenging events were grouped according to similar ESFAS response with respect to challenged parameters and functions. Table 3-1 shows the challenging event classes included in the ESFAS risk evaluation.

3.4.2. Mission Success

Upon examining the challenging events for ESFAS, core damage was chosen as an appropriate measure of risk. This is because the ultimate consequences of ESFAS failure for each of the ESFAS-challenging events involved core damage. If realistic Safety Analysis assumptions are used, it is unlikely that containment failure would occur without core melt, even for large break LOCA. Thus, for each event, a determination was made of which ES functions were needed to prevent core damage. The ES functions needed to prevent core damage involve keeping the core covered, preserving RCS inventory, and providing containment heat removal for the spilled (and recirculated) coolant.

For each event, a determination was made of which ESFAS functions (i.e., ESFAS outputs) actuate the ES systems needed to prevent core damage. Generally the mission success required one-of-two of the ESFAS digital subsystems. However, the digital subsystems are divided functionally, with the ES device assignments split among the functions. (Each design has four or five ESFAS "functions," and each design has its own naming convention such as "incident level" or "actuation channel".) No individual device discrimination was made within ESFAS functions; that is, all of the outputs attached to an ESFAS function had to trip or else actuation of that function was assumed failed. There were some dependencies between functions, and these were incorporated in the RBD models. For example, sometimes two ESFAS functions must trip to fully actuate an ES system, such as in the Gilbert design, where the LPI pumps are started with the "HPI & Load Sequencing" function and the LPI valves are opened by the "LPI" function.

The RBDs were constructed, as shown in Appendix A, to reflect all functions and challenged parameters. For the computer runs, the analysis invoked the appropriate parts of the RBD to respond to each challenged event. This involved deleting credit for plant parameters whose set points would not be challenged, and identifying the ESFAS functions that would be needed to prevent core melt. The challenged parameters and ESFAS functions (in terms of the design-specific output channel names) that were invoked for each event are delineated on Tables 3-1 and 3-2.

3.4.3. Consequence

Given each event scenario and subsequent ESFAS non-response, the consequent risk-significance is contingent on the time available to avert core damage, via manual actuation of each ESFAS function that has failed to actuate automatically. This time varies depending on the severity of the LOCA, and the ESFAS function that has failed. For example, failure to actuate HPI or LPI to prevent core uncovery is generally more urgent that failure to actuate RB cooling for its long-term cooling function. The times available for manual actuation to prevent core damage were obtained or extrapolated from available accident analyses. Generally, the operator can actuate the ES equipment (independent of ESFAS) from the main control panel. As discussed in Section 4, operator failure probabilities were obtained from NUREG/CR-4834 [7], which contains time-reliability correlations based on simulator experiments.

The conditional core damage frequency upon ESFAS failure was assumed to be equivalent to the operator non-recovery probability for ES device actuation. The only recovery taken credit for was an operator action, as time allows, to actuate ES devices manually. Failure of the actuated ES devices was not included as that would de-emphasize the risk-impact of actuation failure modes. Also, no credit was taken for other recovery paths, such as equipment not actuated by ESFAS.

3.4.4. Quantification

The RBDs, coupled with the challenge rates and recovery probabilities, were evaluated with the FTAP computer code [8] to produce Boolean expressions of core melt risk for the three ESFAS designs. The Boolean equations were assembled from the FTAF-produced cut sets generated for each of the challenging events. The resulting Boolean expressions were used in PACRAT computer code [9] runs to produce time-dependent and time-averaged results, and in SAMPLE computer code [10] runs to produce time-averaged uncertainty results. The Boolean equations were developed for individual challenging events as well as the aggregate of all of the challenging events. These were used in PACRAT and SAMPLE to produce the ESFAS contribution to core melt frequency for both one-month and

three-month STIs, as well as the incremental contribution to core melt frequency associated with extension of the STI from one month to three.

3.5. Computer Codes

Construction and solution of the RBDs used B&W Nuclear Service Company's (BWNS's) IRIS workstation software, described below. RBDs were chosen over fault trees for the ESFAS because the channelized nature of the system lends itself to the RBD format, and eases verification of the model. Cut sets generated by FTAP were used in Boolean expressions for quantification by PACRAT or SAMPLE. The code used for evaluation of ESFAS failure probability was BWNS's PACRAT code, which is similar to the public domain code FRANTIC. In this evaluation, SAMPLE was used to generate the uncertainties associated with the time-averaged ESFAS results. All of these codes were previously used and reviewed by the NRC (in the B&WOG Topical Report BAW-10167), and are discussed below.

3.5.1. IRIS Reliability Workstation

BWNS's IRIS (Integrated Reliability Interactive System) [11] reliability workstation uses interactive graphics to help the engineer construct RBDs and fault trees, and is interfaced with industry-proven analytic codes FTAP [8], PACRAT [9], and SAMPLE [10] to evaluate the models. This is accomplished by menu-driven routines that allow construction and editing of RBDs, fault trees, and event trees directly on the computer screen.

In response to computer prompting, the user enters the appropriate failure rate and repair data for basic events of the model. After checking the modeling logic for completeness, inconsistencies, and errors, IRIS automatically generates the input files for the analytical codes. In this way, quality control is improved by automating the error-prone tasks associated with formatting of code input. IRIS is then used to generate report-quality drawings of the models (RBDs, fault trees, or event trees) and plots of results (time-dependencies or uncertainties) produced by the analytic codes.

In this evaluation, IRIS was used to construct the RBDs for the three ESFAS designs, produce RBD diagrams for the report, and prepare the input for the evaluation codes FTAP, PACRAT, and SAMPLE.

3.5.2. FTAP

BWNS's version of FTAP2 (Fault Tree Analysis Program) computes the system reliability and generates a list of minimal cut sets (and their probabilities) associated with an input fault tree. FTAP is very efficient because it contains automatic fault tree modularization and therefore can handle very large fault trees such as those associated with plant PRAs. It is similar in capability to Electric Power Research Institute's (EPRI's) SETS code [12]. FTAP2 was developed at the University of California, Berkeley for use by the Air Force and Navy, and is a public-domain, industry-accepted code. BWNS has made modifications to enhance its capabilities and usefulness, in accordance with our internal certification procedures. IRIS will automatically generate an input file for FTAP.

3.5.3. PACRAT

PACRAT (Probabilistic Analysis Code with Repair and Testing) was developed by BWNS and has been used for other evaluations of the Reactor Protection System (RPS) previously submitted to the NRC [13]. PACRAT computes the time-dependent and average unavailability for any system model whose failure or success can be described by a FORTRAN subroutine. The generalized form of the FORTRAN subroutine allows the system model to take the form of an RBD or fault tree, or any other model that represents system failure or success in terms of component failure or success. Typically, a fault tree or RBD is used, is reduced to representative cut sets, path sets, or Boolean expression, and is input to PACRAT in the form of a FORTRAN subroutine.

PACRAT will model a wide variety of component types including those that are nonrepairable, monitored (self-annunciating failures), and tested (staggered, sequential, etc.). The models include the effects of testing and maintenance outages and component renewals. In addition to constant failure rates, time-

dependent failure rates can be modeled to account for detectable and undetectable age (wearout) failures.

Common mode failure can be easily accounted for either by including them explicitly in the fault tree or RBD logic, or by manipulation of the cut or path sets. By using a FORTRAN subroutine to represent the system model, PACRAT is flexible enough to accommodate any treatment of common mode failure that can be written into the subroutine, including β-factors, actual operating experience, or the binomial failure rate method.

The PACRAT code calculates the time-dependent failure probability of every component and the system, and also keeps a running average of the system availability. The output of PACRAT includes the failure probability at each time step, which can be plotted to show the changes due to testing and repair, in addition to the time-averaged unavailability for the periods of interest.

The PACRAT code is similar in capability to the FRANTIC code [14]. However, PACRAT is more flexible because the system failure representation is generalized (cut sets, path sets, Boolean equations, etc.) and is not limited to cut sets.

3.5.4. SAMPLE

SAMPLE is a general purpose computer program for performing uncertainty analysis. It was first developed and used in the WASH-1400 Reactor Safety Study [15], and is a public-domain, industry-accepted code. Uncertainties are represented by random variables. The user supplies a FORTRAN function that combines the random variables in a mathematical expression modeling the physical process.

For this application, a Boolean expression is used to describe the cut sets of the system under study. The random variables are the failure probabilities. The random variables are sampled and processed through the Boolean expression; this is repeated for numerous trials of the simulation. The simulation produces a distribution for the specified physical process parameter. BWNS has made modifications in SAMPLE to enhance its capabilities, in accordance with our internal certification procedures. The input to SAMPLE, a FORTRAN subroutine

modeling the system as a Boolean expression, is automatically generated with an option in BWNS's version of FTAP.

Table 3-1

Definition of ESFAS Challenging Event Classes

Class	Description	Challenged ESFAS Parameters	Included Events
A	LOCAs that require HPI. Both trains of offsite-derived power are operational.	RC Pressure (Lo) RB Pressure (Hi) RB Pressure (Hi-Hi) BWST Level (DB only) Radiation (DB only)	• Small to medium LOCAs • Transient-induced (non-LOOP) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)
B	Similar to Class A, except that both Emergency Diesel Generators are on-line[a]. (ESFAS must actuate ES equipment in one-out-of-two trains.)	RC Pressure (Lo) RB Pressure (Hi) RB Pressure (Hi-Hi) BWST Level (DB only) Radiation (DB only)	• Transient-induced (LOOP) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)
C	Similar to Class A, except only one Emergency Diesel Generator is on-line[a]. (ESFAS must actuate ES equipment in one-out-of-one train.)	RC Pressure (Lo) RB Pressure (Hi) RB Pressure (Hi-Hi) BWST Level (DB only) Radiation (DB only)	• Transient-induced (LOOP and loss of one Emergency Diesel Generator) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)
D	LOCAs that require LPI.	RC Pressure (Lo) RC Pressure (Lo-Lo) RB Pressure (Hi) RB Pressure (Hi-Hi) BWST Level (DB only) Radiation (DB only)	• Medium to Large LOCAs
E	LOCAs that challenge only RC Pressure and are isolatable (by ESFAS)	RC Pressure (Lo)	• "V-sequence" (Interfacing Systems LOCA)
F	LOCAs that challenge only RB Pressure (i.e., too small to depressurize primary system).	RB Pressure (Hi) Radiation (DB only)	• Very small break LOCA with no secondary side heat removal available

[a] Oconee derives emergency AC power from the Keowee hydroelectric generators rather than EDGs.

Table 3-2

Mission Success Definitions

Class	Function(s) that Need to be Actuated in Response to the Challenging Event to Prevent Core Melt		ESFAS Functions Mission Success (Using Plant-Specific Function Names)[a]		Boundary Conditions
	ES Functions	ES Mission Success			
A	Injection (HPI)	1 of 2 HPI trains	D-B	1 of 2 Incident 2 1 of 2 Incident 5	None.
	Long-term Heat Removal (RB Cooling)	1 of 2 RB cooling trains, including fans, valves, coolers, and cooling water	CR-3	1 of 2 HPI/LS 1 of 2 RB Cooling <dependent on HPI/LS - must be the same channel as actuated HPI/LS>	
	HPI Recirculation	1 of 2 recirculation paths from the sump (to LPI) to HPI	ANO-1	1 of 2 Channels 1,2 1 of 2 Channels 5,6	
			Oconee	1 of 2 Channels 1,2 1 of 2 Channels 5,6	
B	Same as Event Class A	Same as Event Class A	Same as Event Class A		This challenging event requires EDCs[b], (load sequencing equipment, if required), and battery-derived power.
C	Same as Event Class A	Same as Event Class A	D-B	1 of 1 Incident 2 1 of 1 Incident 5	This challenging event requires EDGs[b] (load sequencing equipment, if required), and battery-derived power for the ESFAS subsystem associated with the powered ES train.
			CR-3	1 of 1 HPI/LS 1 of 1 RB Cooling	
			ANO-1	1 of 1 Channels 1,2 1 of 1 Channels 5,6	
			Oconee	1 of 1 Channels 1,2 1 of 1 Channels 5,6	

Class	Function(s) that Need to be Actuated in Response to the Challenging Event to Prevent Core Melt		ESFAS Functions Mission Success (Using Plant-Specific Function Names)[a]		Boundary Conditions
	ES Functions	ES Mission Success			
D	Injection (LPI)	1 of 2 LPI trains	D-B	1 of 2 Incident 2 1 of 2 Incident 3 1 of 2 Incident 5	None.
	Long-term Heat Removal (RB Cooling)	1 of 2 RB cooling trains, including fans, valves, coolers, and cooling water	CR-3	1 of 2 HPI/LS 1 of 2 LPI <dependent on HPI/LS - must be the same channel as actuated HPI/LS> 1 of 2 RB Cooling <dependent on HPI/LS - must be the same channel as actuated HPI/LS>	
	LPI Recirculation	1 of 2 recirculation paths from the sump to LPI	ANO-1	1 of 2 Channels 3,4 1 of 2 Channels 5,6	
			Oconee	1 of 2 Channels 3,4 1 of 2 Channels 5,6	
E	Isolation	1 of 2 RB Isolation, must be the line with the break (letdown line is assumed for example)	D-B	1 of 2 Incident 2	None.
			CR-3	1 of 2 RB Isolation	
			ANO-1	1 of 2 Channels 1,2	
			Oconee	1 of 2 Channels 1,2	
F[c]	Same as Event Class A	Same as Event Class A	Same as Event Class A		None.

[a] See Table 3-3 for identification of plant-specific ESFAS function names.

[b] Oconee derives emergency AC power from the Keowee hydroelectric generators rather than EDGs.

[c] While this table shows the same entries for challenging event class A and F, note in Table 3-1 that the challenged ESFAS parameters are different for the two cases.

Table 3-3

Summary Identification of Plant-Specific ESFAS Function Names

Plant	Plant-Specific ESFAS Function Names	Generic ES Function(s)
D-B	Incident 1	Partial RB Isolation
	Incident 2	HPI, RB Spray (valves), RB Cooling, Partial RB Isolation
	Incident 3	LPI, Partial RB Isolation
	Incident 4	RB Spray (pumps), Partial RB Isolation
	Incident 5	BWST Level Permissive
CR-3	HPI & Load Sequencing (HPI/LS)	HPI, LPI (pumps), RB Spray (enable), RB Coolers
	LPI	LPI (valves)
	RB Spray	RB Spray
	RB Cooling	RB Cooling (valves)
	RB Isolation	RB Isolation
ANO-1	Channels 1,2	HPI, Partial RB Isolation, RB Spray (valves)
	Channels 3,4	LPI, Partial RB Isolation, RB Spray (valves) (Note: RB Spray function is available if either HPI or LPI actuates.)
	Channels 5,6	RB Cooling, Partial RB Isolation
	Channels 7,8	RB Spray (pump)
	Channels 9,10	RB Spray (chemical addition)
Oconee	Channels 1,2	HPI
	Channels 3,4	LPI
	Channels 5,6	RB Cooling, RB Isolation
	Channels 7,8	RB Spray

4. SOURCES OF DATA FOR THE RELIABILITY EVALUATION

Emphasis was placed on the use of operating experience in the derivation of random and common mode failure rates. The same data sources were used to obtain failure rates for ESFAS components as were used for the Topical Report BAW-10167. [1,2,3] All failure rates were derived either directly or indirectly from experience collected in the Nuclear Plant Reliability Data System (NPRDS) and Licensee Event Reports (LERs) data bases.

For the digital subsystem components, such as the various logic modules and/or relays used in the ESFAS designs, B&WOG experience from the NPRDS data base (available through INPO) was used.

NUREG/CR-3289 [4] was used to develop the common mode and random failure rates for the analog channels. This includes the sensors and instrumentation strings, including signal conditioning components up to and including the bistables. The data base used in NUREG/CR-3289 coalesces industry-wide operating experience obtained from LERs.

The following describes the data evaluation for the components of the ESFAS models.

4.1. Analog Channels (Sensors and Instrument Strings)

The data used for sensors and instrument strings for both random and common mode failures were obtained from NUREG/CR-3289 [4]. NUREG/CR-3289 includes failure rate data of sensors for a variety of measured parameters. Reference [4] also includes "signal conditioning system" failure rates, which includes all of the components in an analog channel, except the sensor itself, up to and including the bistable. The instrument string also includes the dedicated sensor power supply.

The source of the data is LERs and the failure modes include both human error (such as miscalibration of bistables) and mechanical failures. The values used

in this analysis were the Baysian means reported in the NUREG. The "reduced capability fault" (i.e., degraded) data category listed in NUREG/CR-3289 was used into the analysis, as well as the complete failure "inoperability fault" data category. The "reduced capability fault" category includes non-catastrophic failures such as setpoint drift. The NUREG data that were used for this evaluation are summarized in Table 4-1.

Table 4-1 gives random failure rates (λ) and the terms that can be used to compute the common mode failure rate. For common mode failures, the NUREG expresses the failure data in terms of lethal and non-lethal shock rates, and the conditional probability of failure given a non-lethal shock. A lethal shock (which may be caused by human or hardware fault) is one that will disable all redundant channels of a component or subsystem. A non-lethal shock may or may not disable redundant channels, and conditional probabilities are provided for failure of a channel given a non-lethal shock. Full details on the derivation and interpretation of these values is contained in reference [4] and are not repeated here. However, the following example will illustrate the use of the data in Table 4-1 to calculate a common mode failure probability.

For a system with three channels, arranged in two-out-of-three logic, the common mode failure for at least two-out-of-three channels is given by:

$$\text{Common mode failure probability} \approx (1 - e^{-\omega t}) + (3p^2[1-p] + p^3)\ (1 - e^{-\mu t})$$

where:

ω = lethal shock rate

μ = non-lethal shock rate

p = conditional probability of failure given non-lethal shock

t = time period of interest

Similar to the treatment in BAW-10167, the analysis included the effect of the common mode failure of sensors and instrument strings of the same sensed parameter. B&W experience indicates that there is no evidence supporting a common mode failure between two independent sensed parameters. Also, in NUREG/CR-3289, there were no events that failed channels of unlike parameters; only the probabilities of occurrence for common mode failures between channels

of like parameters were estimated. In addition, the NRC review the B&WOG submittal [3] and of the Westinghouse Owners Group RPS submittal [18] indicates agreement with the data presented in NUREG/CR-3289 [4]. Therefore, the B&W ESFAS models only include common mode failures of like parameters.

Some of the sensors provide input to more than one bistable, e.g. low and low-low RC pressure. When more than one bistable trip is derived from the same sensor, some of the other instrument string components are also shared; however, the bistables are not shared. Since the bistable is generally the weakest component (because this is where the human interaction occurs), channel failures are not likely to affect more than one trip function. Nonetheless, the B&W model accounts for sensor dependencies, where appropriate. Since the data in NUREG/CR-3289 does not break out individual components of the instrument strings (i.e. bistables), the use of the data in the RBD assumes complete dependence when the signal from a single sensor is used in more than one bistable. This treatment is conservative.

4.2. Digital Subsystem Components

Operating experience was reviewed to quantify failure rates for digital subsystem components, including logic modules (e.g., logic buffer modules, trip logic modules, and unit control modules for the Bailey design, and output modules for the Bechtel design), logic relays (e.g., output relays for the auto actuation logic in the Gilbert design), and other modules (e.g., sequencer modules in the Bechtel design, and power supply modules). Failure rates were obtained from the operating experience data for the ten years ending January, 1990.

The operating experience included failure rates and failure descriptions from NPRDS, which included both mechanical- and human-caused failures. A specific NPRDS search was made for each logic module and relay in the ESFAS digital subsystems at the B&WOG plants.

The RBD model required discrimination of failure modes for logic modules and logic relays. Since spurious logic trips do not contribute to ESFAS failure to actuate, it was necessary to separate failure-to-trip modes from spurious-trip

modes. Most logic relays, for example, deenergize to trip; inadvertent deenergizations and subsequent spurious actuations (or half-actuations) were more numerous than events involving failure to trip (i.e., failure to deenergize) on demand. Hence, the component failure descriptions were reviewed, and the failure rates partitioned accordingly, giving emphasis to hardware and human errors that could prevent trip on demand. It is recognized that failures causing unwanted actuations are also important to plant safety, and they are addressed separately in Section 4.8.

For the other modules, such as power supply modules and sequencer modules, all of the failure modes are applicable for the determination of the reliability of ESFAS actuation because these components do not have a tripped/not-tripped mode of operation. That is, all failure modes of these components can potentially lead to the unavailability of ESFAS actuation.

The failure experience for each digital subsystem component or module was reviewed to determine if any of the failures were potentially common mode failure. Failures that occurred within one month of each other at the same plant (to account for staggered testing) were examined to determine if the mode, mechanism, or cause of failures was similar. In these instances, the information was used to partition the failure rate into random and common mode portions, from which a beta factor (and, if needed, a gamma factor) were derived. The beta factor, β, is the fraction of the random failure rate (λ) in which two or more components are involved due to common mode. (The gamma factor, γ, is the fraction of the β involving three or more components.)

Typically, it is difficult to collect and identify sufficient operating experience data to make common mode failure rate calculations with confidence. In the data for power supply modules, there was one multiple failure event in a related system (EFIC). Also, for logic relays there was one multiple failure event involving Clark relays (the type used in the Gilbert design), although they were in the same (rather than a redundant) channel. When possible, such as in these cases described above, a beta factor was derived from the data.

When the failure history of the component showed no evidence of multiple failures (e.g, none of the failures-to-trip for ESFAS logic modules involved multiple modules), it was necessary to apply engineering judgement and assume a conservative value for the beta (and gamma) factor, (i.e., β=.1, γ=.5); see Table 4-2 for a complete list of random and common mode failure rates.

Developing the common mode failure rates for groups of like components required determining the component failure combinations that would lead to system failure. For example, in the Bechtel design, there are many output modules and system failure included several two-element cut sets of output modules of like function. The failure rate of a specific component for all modes (random and common mode) is λ_t. The failure rate of a specific component due to common mode failure is equal to $\beta \cdot \lambda_t$. From reference [16], the generalized expression for a common mode failure rate of a specific two components of a group of m components (i.e., system size = m) is equal to:

$$\lambda_2 = \frac{1}{m-1}(1-\gamma)\beta\lambda_t$$

which can conservatively be reduced to:

$$\lambda_2 = \frac{1}{m-1}\ \beta\ \lambda_t$$

assuming that terms with higher order (greater than two-element cut sets) are not significant. In the Bechtel example, the above formula was used for each specific output module pair (two-element cut sets) whose failure will lead to system failure.

4.3. Miscellaneous External (i.e., Non-ESFAS) Components

Failure rates were needed for miscellaneous components associated with the external power supplies for ESFAS (internal ESFAS power supplies are included in the data discussed in Sections 4.1 and 4.2). Failure rates for batteries, inverters, and undervoltage relaying were obtained from NPRDS for B&WOG plants. Common mode failure for these components was not included in the model because the components are external to ESFAS and not within the scope of the STI

extension being evaluated. Since this analysis is interested in the relative incremental risk involved with changing the ESFAS test intervals, and external power supply test interval changes are not proposed, to include common mode failure of these components would serve only to mask the effect of test interval changes on the other components.

4.4. Applicability of Data to Extended-Test-Interval Model

The historical data bases largely represent components that have been tested monthly. Their failure rates can be expressed as failure-per-demand or failures-per-hour. As long as the modeled test frequency is monthly, a reliability analysis that assumes per-demand rates will yield the same results as one that assumes per-hour rates. This assumption is not true if the data is extrapolated to longer-than-one-month test intervals. Obviously, if failure rates are expressed per-demand, the component's probability of failure for a given challenge will remain constant regardless of how the test interval is varied. This would be optimistic and misleading. However, if failure rates are expressed per-hour, the component's probability of failure for a given challenge will be a function of the time elapsed since the last test, and would increase proportionally as the test interval increases. This would be pessimistic and may overestimate the sensitivity to test interval. Hence, modeling at extended test intervals requires ascertaining whether the failures experienced were time- or demand-related; otherwise, failure rates must be expressed per-hour to yield results that are conservative for examining the sensitivity of reliability to test interval.

The components in the data bases actually have two kinds of failure mechanisms--those that are cycle-dependent and those that are time-in-service-dependent. For example, test-related human errors (that may contribute to either random or common mode failure) are expected to be cycle-dependent; that is, their rate would increase or decrease in proportion to the number of human interactions (or tests). Other failure mechanisms, such as those that might result from exposure to environmental effects (grease, dirt, etc.), would be proportional to the amount of time-in-service. An ideal model would separate the historical failure experience into cyclic and time-related contributions, and split the failure

rates into per-demand and per-hour contributions. However, the failure records supporting NUREG/CR-3289 (LERs) and NPRDS were not sufficient to meaningfully discriminate between time-related and cyclic failure mechanisms.

The failure rate data used in this analysis were obtained from NUREG/CR-3289 and NPRDS, and are reported in terms of failures-per-hour. They are, therefore, conservative for examining ESFAS sensitivity to test interval. This conservatism applies to the human errors as well as mechanical failure modes that have cycle-dependent rather than time-in-service dependent failure mechanisms.

4.5. Time-to-Repair Data

The ESFAS reliability models, in addition to failure rates, require data for time-to-repair of test-revealed failures. The time-to-repair is a function of the time taken to discover the failure. For test-revealed failures, this is a function of the STI. Both the existing one-month test intervals and the proposed three-month test intervals were used in the analysis to determine the sensitivity of ESFAS reliability to the STI.

However, not all failure are test-revealed. Sensor failures, in particular, are usually not testable on-line (an exception is the RB pressure sensors at CR-3 and D-B that can be exercised each month). Thus, unless the failure is catastrophic (in which case it will detected at the shiftly channel check), it may not be apparent until the refueling outage or an actual ESFAS demand. This was assumed to be the case for "reduced capability faults" of sensors. Due to the longer exposure time (i.e., the length of time that the failure is likely to go undetected), the degraded failure modes ("reduced capacity faults") dominate sensor unavailability.

Once a failed component is discovered, if the failure mode is in the "unsafe" direction, the system or channel is "vulnerable" for an additional length of time until either: the failed component is repaired and restored to service, or the failed component is put in its "safe" (i.e., tripped) state, or the reactor is shutdown so that the affected ESFAS function is no longer needed. The choice of options is dictated by the Technical Specifications; the times used in the

analysis were the ACTION times prescribed by those Technical Specifications (summarized in Section 2).

For most components in this analysis, the failed component or channel was assumed tripped within one hour of when the test fails. When a second failure is discovered, as would be the case in a common mode failure, or in other situations where the Technical Specification requires shutdown, the model conservatively assumes that the reactor will be shutdown using the full ACTION time limit.

For some random failures, especially those components with plug-in design and spares in stock, component restoration can be attained in less time than allowed by the ACTION statement. However, since the purpose of this study is to evaluate the effect of proposed technical specification changes, it was conservatively assumed that the full ACTION time limit would be used. This results in the maximum analyzed "vulnerability" when a component fails in a surveillance test, and therefore over estimates the ESFAS unavailability for cases where repair and system restoration occurs faster than allowed by technical specifications.

4.6. ESFAS Challenging Event Frequencies

Challenging event frequencies were obtained from a combination of B&WOG experience, and the Oconee PRA [16]. The frequencies for the six challenging events and their sources are presented in Table 4-3.

Conventional LOCA frequencies were obtained from the Oconee PRA, which were obtained from industry operating experience. Transient-induced LOCA frequencies were obtained from B&WOG operating experience. LOCAs induced from LOOP events, with and without coincident EDG failure, were included by combining B&WOG operating experience with generic EDG failure probabilities.

The interfacing-systems LOCA frequency was extrapolated from the Oconee PRA. The Oconee plant was considered representative because the B&WOG NSS designs are similar and because ESFAS is not a significance risk contributor for interfacing systems LOCA. The potential interfacing systems LOCA pathways identified in the Oconee PRA were reviewed to determine which ones contained ESFAS-actuated

isolation valves. The frequency was re-calculated by omitting credit for the ESFAS actuation in determining the significant pathways and the ESFAS challenge rate.

4.7. Non-Recovery Probabilities

Given ESFAS failure, the time available to avert core damage depends on the severity of the LOCA and the ESFAS function that has failed. Estimates were made of the minimum time available for manual initiation of ES devices that have failed to actuate. Extrapolating from available accident analyses, conservative times were assumed for diagnosis and action to avert core melt given the specific event and failed ESFAS function.

For example, given a large LOCA and failure to actuate RB cooling, the operator was conservatively given 30 minutes to start RB cooling because the BWST takes at least 30 minutes to drain and the long-term heat sink is not needed before then. The causal relationship between failure to actuate building cooling and imminent core uncovery/melt is a conservative assumption. Some other ESFAS actuation failures are a more immediate concern, for example, LPI actuation failure for a large LOCA assumes that the operator must actuate LPI manually within 15 minutes to avoid inevitable core damage.

Operator recovery from ESFAS actuation failure requires both cognitive (diagnostic) and action tasks. The operator can initiate all of the ES equipment (independent of ESFAS) from the main control panel. Operator error probabilities for operating these controls were obtained from NUREG/CR-1278 [18]. The diagnostic (cognitive) error probabilities were obtained from NUREG/CR-4834 [7], which contains time-reliability correlations based on simulator experiments. Recovery times longer that an hour were not assigned (although in some cases, they may have been justified) because the failure probability for recovery times greater than one hour were equivalent to recovery times of one hour. The recovery times and failure probabilities are shown on Table 4-4.

Recognizing the potential importance of the assumed times for averting core damage given ESFAS failure, a sensitivity analysis was performed. The

sensitivity analysis is contained in Appendix D. In the sensitivity analysis, the time available to avert core damage was reduced to half of the values shown in Table 4-4, and the results recomputed to show that the change in risk associated with the proposed test interval extension is still acceptably small.

4.8. Spurious ESFAS Actuation Frequency

The LER data base, available through INPO, was examined for events from January 1984 through August 1990 that involved spurious ESFAS actuations at B&WOG plants.

The search identified several spurious ESFAS actuation events. It was not always possible to determine from the LER descriptions whether monthly surveillance testing played a role in these ESFAS trips. However, there were at least six events that clearly occurred during monthly surveillance testing. These events involved all three ESFAS designs. This yields a spurious ESFAS actuation frequency due to monthly surveillance testing of at least 0.12 per reactor year.

Therefore, it can be expected that extension of the STI to three months will provide some relief in the rate of spurious actuations of ES equipment.

A reduction in the rate of spurious ESFAS trips and the associated actuations of ES equipment can be expected to contribute minimally to a decrease in core melt frequency. However, due to the small numbers involved, the spurious ESFAS trip frequency is provided here as information only. The core melt risk benefit associated with spurious trip reductions was not credited in the analysis or results.

Table 4-1

ESFAS Analog Channel Components Data Summary

Component	Inoperability	Reduced Capability
RB PRESSURE SENSOR		
Random (λ)	1.90×10^{-6}/hr	3.60×10^{-6}/hr
Lethal Shock (ω)	4.50×10^{-8}/hr	2.30×10^{-7}/hr
Non-Lethal Shock (μ) (system size=3)	6.50×10^{-6}/hr	2.20×10^{-6}/hr
Non-Lethal Shock (μ) (system size=4)	5.30×10^{-6}/hr	1.80×10^{-6}/hr
Condition Probability (p)	.161	.177
RC PRESSURE SENSOR		
Random (λ)	1.90×10^{-6}/hr	3.60×10^{-6}/hr
Lethal Shock (ω)	4.50×10^{-8}/hr	2.30×10^{-7}/hr
Non-Lethal Shock (μ) (system size=3)	6.50×10^{-6}/hr	2.20×10^{-6}/hr
Non-Lethal Shock (μ) (system size=4)	5.30×10^{-6}/hr	1.80×10^{-6}/hr
Condition Probability (p)	.161	.177
RB PRESSURE (DIGITAL) SWITCH		
Random (λ)	7.70×10^{-7}/hr	6.60×10^{-6}/hr
Lethal Shock (ω)	5.40×10^{-8}/hr	1.60×10^{-7}/hr
Non-Lethal Shock (μ) (system size=6)	3.10×10^{-6}/hr	1.20×10^{-5}/hr
Condition Probability (p)	.137	.456
RADIATION SENSOR		
Random (λ)	4.50×10^{-6}/hr	6.40×10^{-6}/hr
Lethal Shock (ω)	4.20×10^{-7}/hr	2.10×10^{-6}/hr
Non-Lethal Shock (μ) (system size=4)	2.60×10^{-3}/hr	2.60×10^{-3}/hr
Condition Probability (p)	.064	.064
BWST LEVEL SENSOR		
Random (λ)	1.90×10^{-6}/hr	3.60×10^{-5}/hr
Lethal Shock (ω)	4.50×10^{-8}/hr	2.30×10^{-7}/hr
Non-Lethal Shock (μ) (system size=4)	5.30×10^{-6}/hr	1.80×10^{-6}/hr
Condition Probability (p)	.161	.177
INSTRUMENT STRINGS		
Random (λ)	3.10×10^{-6}/hr	2.00×10^{-6}/hr
Lethal Shock (ω)	2.90×10^{-7}/hr	6.40×10^{-7}/hr
Non-Lethal Shock (μ) (system size=3)	3.80×10^{-6}/hr	2.90×10^{-6}/hr
Non-Lethal Shock (μ) (system size=4)	3.10×10^{-6}/hr	2.40×10^{-6}/hr
Condition Probability (p)	.177	.244

Note:

* System size of three applies to Bailey and Gilbert designs for analog sensors (three-channels).

* System size of four applies to Bechtel design (four-channel system).

* System size of six applies to Gilbert and Bailey (Oconee) design (three-channel) for RB pressure switches because separate switches are used for each actuation subsystem.

Table 4-2

Summary of the Random Failure Rates and Beta Factors
for Digital Subsystem Components

Component	Failure Rate (/hour)	Beta (β) Factor
Trip Module	1.60×10^{-6}	a
Output Module	4.80×10^{-7}	a
Logic Buffer Module	5.08×10^{-7}	a
Unit Control Module	1.57×10^{-7}	a
Sequencer Module	3.49×10^{-6}	a
Power Supply	5.35×10^{-7}	.4
Inverter	2.58×10^{-5}	n/a
Station Battery	4.63×10^{-6}	n/a
Relay (CR-3)	1.01×10^{-7} (coil) 1.45×10^{-8} (contact)	.25
Undervoltage Relay	3.41×10^{-7}	n/a

[a] The data did not exhibit evidence of common mode failures, therefore a β-factor value of .1 was assumed.

Table 4-3

Frequencies of ESFAS Challenging Event Classes

Class	Description	Included Events	Frequency (/reactor year)	Source
A	LOCAs that require HPI. Both trains of offsite-derived power are operational.	• Small to medium LOCAs	7×10^{-4}	Oconee PRA[a] (1.5" to 4")
		• Transient-induced (non-LOOP) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)	3.7×10^{-3}	B&WOG operating experience
B	Similar to Class A, except that both Emergency Diesel Generators are on-line. (ESFAS must actuate ES equipment in one-out-of-two trains.)	• Transient-induced (LOOP) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)	5.4×10^{-4}	B&WOG operating experience
C	Similar to Class A, except only one Emergency Diesel Generator is on-line. (ESFAS must actuate ES equipment in one-out-of-one train.)	• Transient-induced (LOOP and loss of one Emergency Diesel Generator) LOCAs (e.g., PORV LOCA; Safety Valve fails to reseat)	4.3×10^{-5}	B&WOG operating experience, with generic EDG
D	LOCAs that require LPI.	• Medium to Large LOCAs	7×10^{-4}	Oconee PRA[a] (>4")
E	LOCAs that challenge only RC Pressure and are isolatable (by ESFAS).	• "V-sequence" (Interfacing Systems LOCA)	3.4×10^{-7}	Extrapolation from Oconee PRA (pathways with ESFAS actuated valves)
F	LOCAs that challenge only RB Pressure (i.e., too small to depressurize primary system).	• Very small break LOCA with (assume) no secondary side heat removal available	4.7×10^{-3} [b]	Oconee PRA[a] (3/8" to 1.5")

[a] Calculated from industry operating experience.

[b] Assumes that no feedwater is available.

Table 4-4

Manual Recovery Probabilities
for Determining Risk-Significance of ESFAS Failure Consequence

Manual Recovery Action	Applicable ESFAS Challenging Event	Time Available (after ESFAS failure) to Avert Core Melt	Probability of Non-Recovery
Initiate Safety Injection	A,B,C	30 minutes	0.013
	D	15 minutes	0.044
	F	1 hour	0.0061
Initiate RB Long-Term Cooling	A,B,C,F	at least 1 hour	0.0061
	D	at least 30 minutes	0.013
Isolate Interfacing Systems LOCA	E	at least 30 minutes	0.013
Actuate BWST Level permissive (D-B)	A,B,C,F	at least 25 minutes	0.018
	D	at least 10 minutes	0.089

5. MODEL QUANTIFICATION

5.1. Time-Dependent Analysis

The quantification for each test interval included making separate runs for each of the three ESFAS designs for all six challenging events, as well as an aggregate run where all the challenging events were accounted for in a single Boolean expression. The base cases, using the current one-month test interval, were quantified with PACRAT using best estimate (mean) failure rate data to determine the time-dependent and time-averaged core melt risk due to ESFAS failure. The one-month analyses were repeated using a three-month test interval to quantify the effect of extending the test interval. For the latter cases, the test interval for all of the ESFAS components was changed from one to three months, except for components outside the ESFAS system boundary, such as external power supplies.

Time-dependent risk plots are shown in Figures 5-1 through 5-3 for the one-month case for each of the three ESFAS designs for challenging event A. Similar results were generated for the remaining five challenging event categories for both the one-month and three-month test interval. The time-dependent plots show the instantaneous core melt frequency contribution from ESFAS indicating the effects of changes in system configuration due to ESFAS failures, testing, and maintenance. In addition, composite (time-dependent) plots of all six challenging events, displaying one-month and three-month test interval traces for each of the three ESFAS designs, are shown in Figures 5-4 through 5-6. These time-dependent results were integrated over time (18-month fuel cycle) to generate the time-averaged results discussed in Section 5.2.

The time-dependent plots were used to examine the dynamic effects of the STIs. They substantiate the validity of the RBDs, as well as the time-averaged results derived from integrating the time-dependent results. Most importantly, the time-dependent plots were used to identify any risk vulnerabilities (i.e., risk peaks) that might result from changing test intervals.

Prior to discussing specific plots, two trends that appear in the plots will be discussed. The first trend is the overall increasing core melt risk as a function of time. Degraded failure modes (e.g., drift) of some sensors may not be detectable until the refueling outage (assumed at 18-month intervals), therefore a failure during the mission time remains unrepaired and contributes to the general increasing trend. The second trend concerns the ESFAS equipment that is tested monthly. The plot shows an increasing risk until the time of the test, then a decrease in risk as the tested equipment is assumed to be returned to service failure free (i.e., confirmed working, or repaired to a working state).

5.1.1. Bailey

In Figure 5-1, showing the risk of core melt from failure of a Bailey-designed ESFAS for challenging event A, both trends are apparent. The small "ripple" at the top and bottom of each risk peak is indicative of the different Technical Specification ACTION times for different ESFAS components. The pattern repeats with a period of one month, which is the test interval for this case. As time progresses the cumulative effect of the sensors whose failu modes are untestable on-line begin to dominant the restorative effect of the monthly tested components.

Figure 5-4 shows the risk of core melt from an ESFAS failure for the Bailey design for all challenging events, and with STIs of both one month and three months. The first trace shows the one-month test interval for the composite event case and the trends are identical to the challenging event A. Thus, ESFAS's time-dependent behavior is similar for all challenging events. The second trace of Figure 5-4 shows the pattern repeating every three months, which is the test interval for that case. Comparison of the plots show that there are no time-dependent vulnerabilities that result from the extension of the test interval to three months.

5.1.2. Gilbert

Figure 5-2 shows the risk of core melt with a one-month STI from failure of a Gilbert-designed ESFAS for challenging event A. The patterns are similar to those discussed in Figure 5-1, with two differences. The first difference is that the first trend (generally increasing risk) is not apparent in the Gilbert design. This is also true in Figure 5-5, which shows the time-dependent risk for all challenging events with both one-month and three-month STIs. The reason for the flat (generally non-increasing) shape is that the reactor building pressure switches are accessible and are exercised (i.e., tested) monthly. The other sensors (reactor coolant pressure) may have degraded failure modes that are not detectable on-line, however they are not a dominant contributor to risk of core melt.

The second difference is the distinct increase in risk that occurs every month during testing. In Figure 5-2, the risk peaks occur during the AAL testing because the AAL output to individual devices is blocked one at a time for the tests. Also in Figure 5-5, depicting all six challenging events, the peaks are higher (than in Figure 5-2, depicting only challenging event A) because for the LOOP events (B and C), the undervoltage relaying input to ESFAS is risk significant. The peaks that appear along the top of the trace(s) are caused by the temporary test-related disabling of the undervoltage relaying, which affects the sequencing of the ESFAS actuated devices during the LOOP events. Therefore, if an ESFAS challenge occurs during these tests, the probability of ESFAS failure (and associated risk) rises. After the components are returned to (failure-free) service, the risk returns to a nominal value. The undervoltage relaying, although an input to ESFAS, is not part of ESFAS, and, therefore, is not within the scope of the tests whose intervals are extended from one month to three months. Figure 5-5, the risk for all challenging events, shows the same pattern of peak locations and magnitude for both the one-month and three month test intervals; the reason for this is because the undervoltage relaying testing (which occurs every month in both traces) is more risk significant than the AAL testing. Thus, the plots show no time-dependent vulnerabilities that result from the extension of the test interval from one month to three months.

5.1.3. Bechtel

Figures 5-3 and 5-6 show the risk of core melt from a Bechtel-designed ESFAS for challenging event A and all challenging events. The first trend of generally increasing risk is contributed by sensor degraded failure modes that are undetectable on-line. Although reactor building pressure sensors are exercised during on-line functional testing, other sensors, such as the BWST level sensors and reactor coolant pressure sensors, may have undetectable degraded failures (which contribute to the first trend). The second trend, rising and falling risk, occurs more frequently than the test interval. D-B, which uses the Bechtel ESFAS design, a four-channel system, has staggered testing. Therefore, each week, one channel is tested. For the three-month test interval, channel testing would occur every three weeks, as can be observed in Figure 5-6. The rise in risk occurs due to the bypass of individual ESFAS sensor string channels. These bypasses temporarily reduce the two-out-of-four logic to two-out-of-three logic. However, the magnitude of the risk peaks does not change significantly from the one-month to the three-month case; therefore, the plots show no time-dependent vulnerabilities that result from the extension of the test interval from one month to three months.

5.2. Time-Averaged Results

Table 5-1 gives a summary of the contribution to core melt frequency (risk) due to ESFAS failure for each of the challenging events, as well as the aggregate of all the challenging events, for one- and three-month test intervals. The core melt risks reported in Table 5-1 are the time-averaged risk of core melt due to ESFAS failure obtained by integrating the instantaneous ESFAS risk contained in the time-dependent plots (as computed by PACRAT). The delta (or incremental) risk is computed by subtracting the risk of core melt using a one-month test interval from the risk of core melt using a three-month test interval. Thus, the incremental risk represents the increased core melt frequency from an ESFAS failure due to the changing of the test interval from one month to three months.

Table 5-1 shows the risk is dominated by challenging events A and F. Challenging events A and F have the highest frequency of occurrence. The core melt risk for

events A and F are approximately the same on a per plant basis. This reason for this is that ESFAS failure in the Bailey and Gilbert cases (for events A and F) is dominated by RB pressure sensor and instrument string failures. In the model, event A challenges both RB pressure and RC pressure, while event F only challenges RB pressure. However, since the contribution of RC pressure sensor and instrument string failures to core melt risk is small (because no ESFAS function is solely depended on RC pressure), the core melt risk for events A and F are approximately the same. In the Bechtel case, for both events A and F, ESFAS failure is dominated by failures of the BWST level sensors and instrument strings.

Another result that can be observed from Table 5-1 is the negative risk increment for the Gilbert ESFAS for challenging event C (small break LOCA with only one train of power available). With only one powered ES train available, the test-related blocking of individual AAL outputs in the digital subsystem associated with the powered ES train is more significant. Thus, with the three-month test interval, there is a decreased likelihood that the ESFAS subsystems needed to actuate the powered ES train will be in test. This has the effect of increasing the ESFAS reliability for challenging event C.

As is shown in Table 5-1, the calculated mean contribution of ESFAS to core melt frequency (with one-month STI) ranges from 2.11×10^{-8}/reactor-year (for Gilbert) to 5.26×10^{-7}/reactor-year (for Bechtel) for the ESFAS designs analyzed. In this analysis, the risk of core melt due to ESFAS failure with a three-month test interval ranges from 4.1×10^{-8}/reactor-year (for Gilbert) to 6.1×10^{-7}/reactor-year (for Bechtel). Some previous PRA-based studies were examined to determine their consensus on the contribution of ESFAS to risk, and to see if the risk-significance compared favorably with the ESFAS risk significance calculated in this study. This compares favorably with the results expected in PRA studies for ESFAS contribution to core melt frequency.

Figure 5-7 shows the core melt risk for all the challenging events (i.e., the last entry of Table 5-1) as a function of test interval. The Bailey and Bechtel traces are relatively flat, indicating little sensitivity to the ESFAS test interval. While the Gilbert trace shows more of a slope, the overall risk is an

order of magnitude less than Bailey or Bechtel. Thus, the effect of increasing the ESFAS test interval is relatively insignificant.

The core melt risk for the Gilbert-designed ESFAS is lower than the other designs because the Gilbert-designed ESFAS at CR-3 has an RB pressure sensor design that allows exercising of the sensors (pressure switches) during the on-line functional testing. The Bailey plants do not have that feature, and hence RB sensor failures (analog sensors at ANO-1, pressure switches at Oconee) may go undetected until complete testing during the refueling outage. The Bechtel-designed ESFAS at D-B also includes exercising of the RB pressure sensors (analog sensors) during the on-line test; however, the Bechtel ESFAS has an additional function: the BWST level permissive, which offsets the advantage gained by the testable RB pressure sensors.

The mean incremental core melt frequency associated with the extension of the STI from one to three months ranges from 2.03×10^{-8}/reactor-year (Gilbert) to 1.45×10^{-7}/reactor-year (Bailey). Thus, the impact of increasing the ESFAS test interval from one to three months is small compared to the Commissioners' safety goal; accordingly, the test interval extension request is justified in light of the negligible increase in the overall core melt frequency. In addition, the time-dependent analysis shows that the change of STI from one to three months does not significantly change the conditional risk (i.e., vulnerability) due to testing.

In reference [20], Brookhaven National Laboratory performed an analysis of the risk impact of STIs at ANO-1. That study qualified the effect (on risk) of the surveillance test itself Thus, performing the test resulted in a net risk benefit as the tested component was returned to service. The surveillance tests related to ESFAS (ESAS at ANO-1) components fell into the category of "low risk impact." The consequence was that "their intervals could easily be extended without affecting risk."

Table 5-1

Summary of Time-Average Risk Results

Challenging Event[a]	ESFAS Test Interval	Core Melt Risk due to ESFAS Failure (/Rx-yr)		
		Bailey	Gilbert	Bechtel
A	One-Month	1.57e-07	4.97e-09	1.59e-07
	Three-Month	2.13e-07	1.37e-08	1.85e-07
(4.40e-03/yr)	Delta Risk[b]	5.63e-08	8.76e-09	2.60e-08
B	One-Month	1.93e-08	1.52e-09	4.14e-08
	Three-Month	2.64e-08	2.46e-09	4.94e-08
(5.40e-04/yr)	Delta Risk[b]	7.02e-09	9.45e-10	7.99e-09
C	One-Month	3.69e-09	7.65e-09	2.98e-08
	Three-Month	6.02e-09	5.93e-09	3.43e-09
(4.30e-05/yr)	Delta Risk[b]	2.33e-09	-1.72e-09	4.51e-09
D	One-Month	5.40e-08	1.69e-09	1.23e-07
	Three-Month	7.42e-08	4.70e-09	1.39e-07
(7.00e-04/yr)	Delta Risk[b]	2.02e-08	3.01e-09	1.54e-08
E	One-Month	2.54e-11	2.46e-11	9.08e-12
	Three-Month	3.39e-11	3.26e-11	1.02e-11
(3.40e-07/yr)	Delta Risk[b]	8.53e-12	7.99e-12	1.16e-12
F	One-Month	1.66e-07	5.26e-09	1.72e-07
	Three-Month	2.25e-07	1.45e-08	2.02e-07
(4.70e-03/yr)	Delta Risk[b]	5.88e-08	9.26e-09	2.96e-08
ALL	One-Month[c]	4.00e-07	2.11e-08	5.26e-07
	Three-Month[c]	5.45e-07	4.14e-08	6.10e-07
	Delta Risk[b]	1.45e-07	2.03e-08	8.35e-08

[a] The numbers in the parentheses are the frequency of occurrence for the indicated challenging event (from Section 4.6).

[b] Delta risk is computed by subtracting the risk of core melt using a one-month test interval from the risk of core melt using a three-month test interval.

[c] These values are graphically presented in Figure 5-7.

Figure 5-1: Risk of Core Melt from ESFAS Failure vs. Time
for Bailey Design - Challenging Event A - 1 Month Test Interval

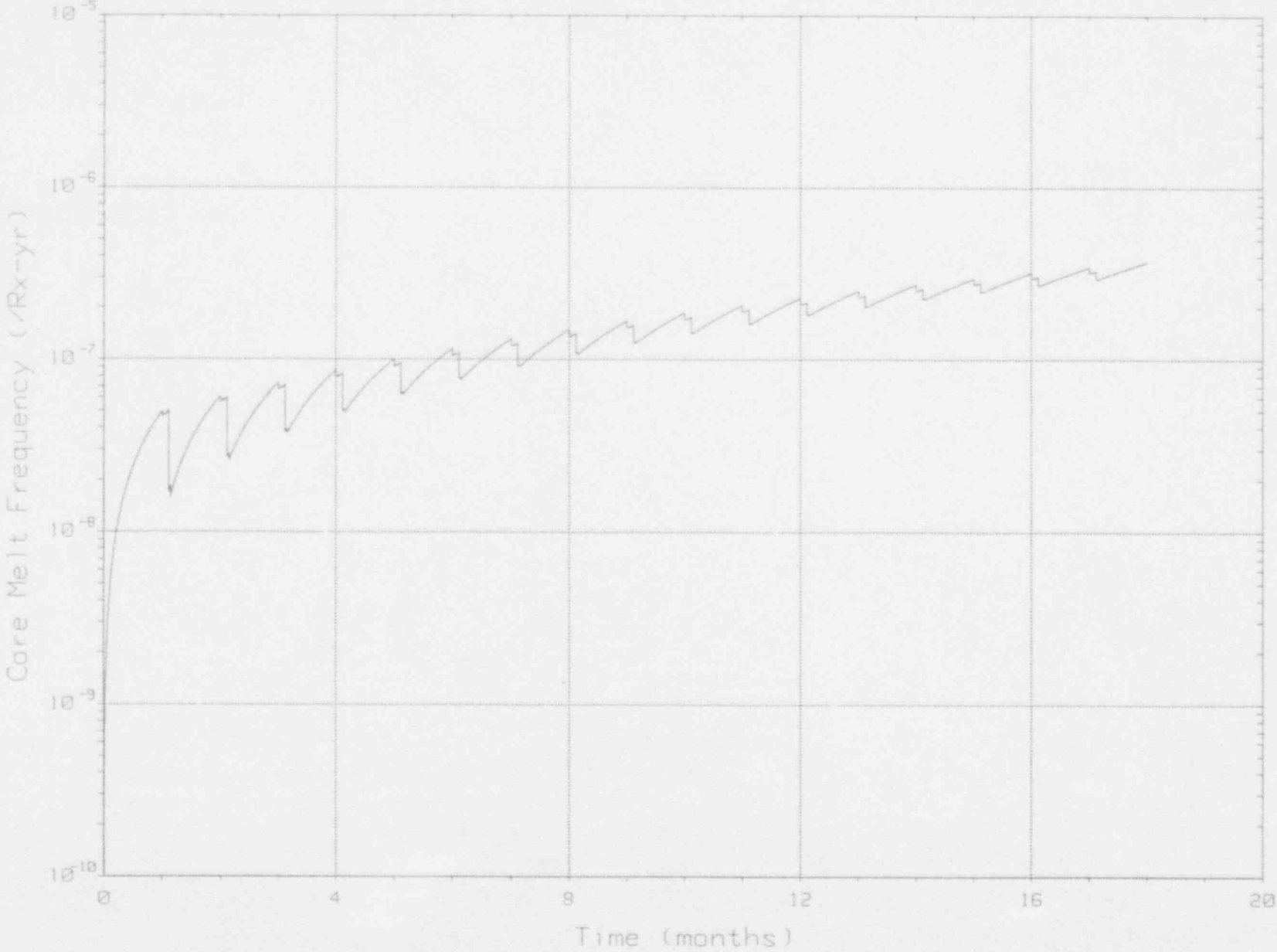


Figure 5-2: Risk of Core Melt from ESFAS Failure vs. Time
for Gilbert Design - Challenging Event A - 1 Month Test Interval

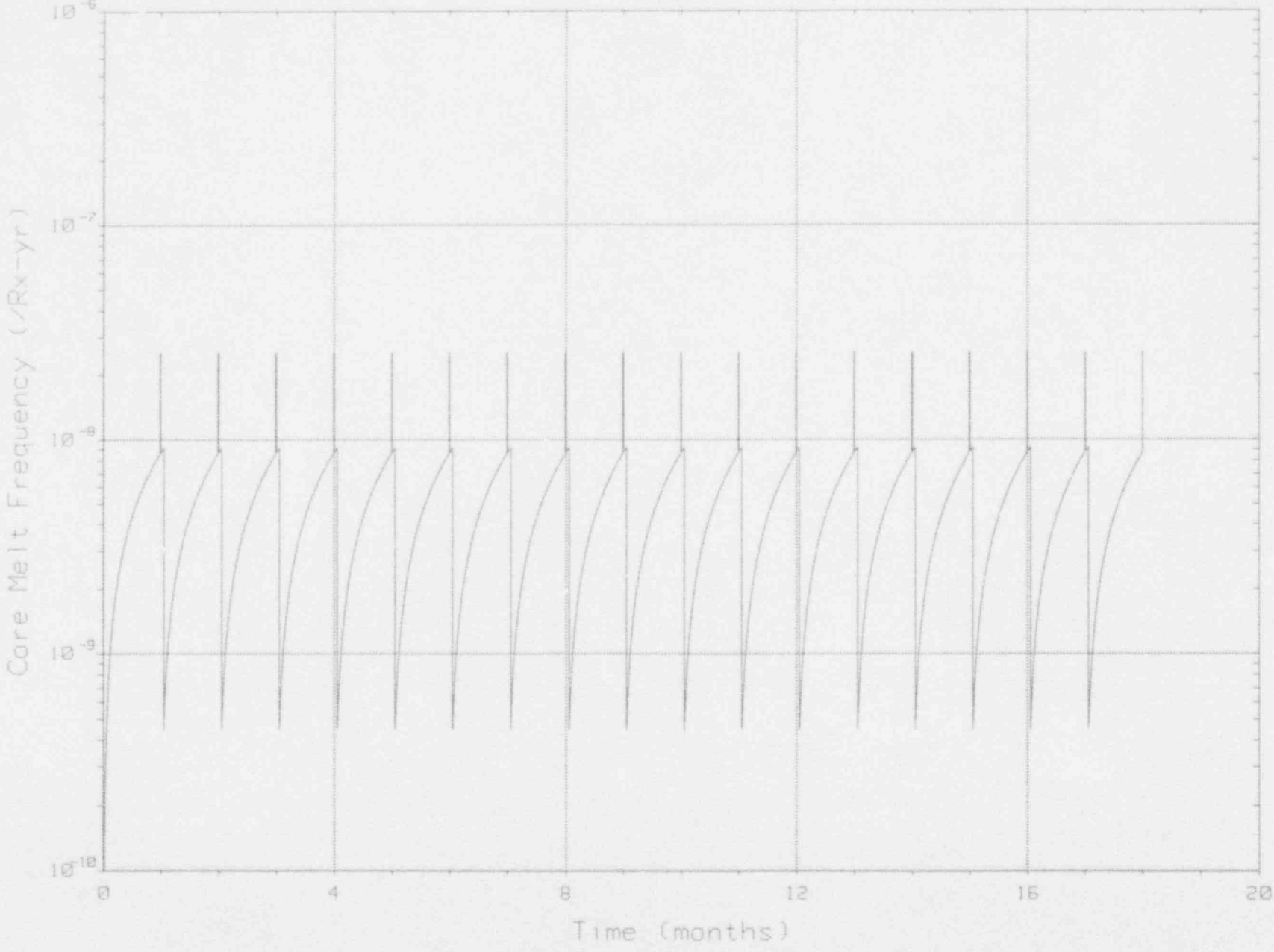


Figure 5-3: Risk of Core Melt from ESFAS Failure vs. Time
for Bechtel Design - Challenging Event A - 1 Month Test Interval

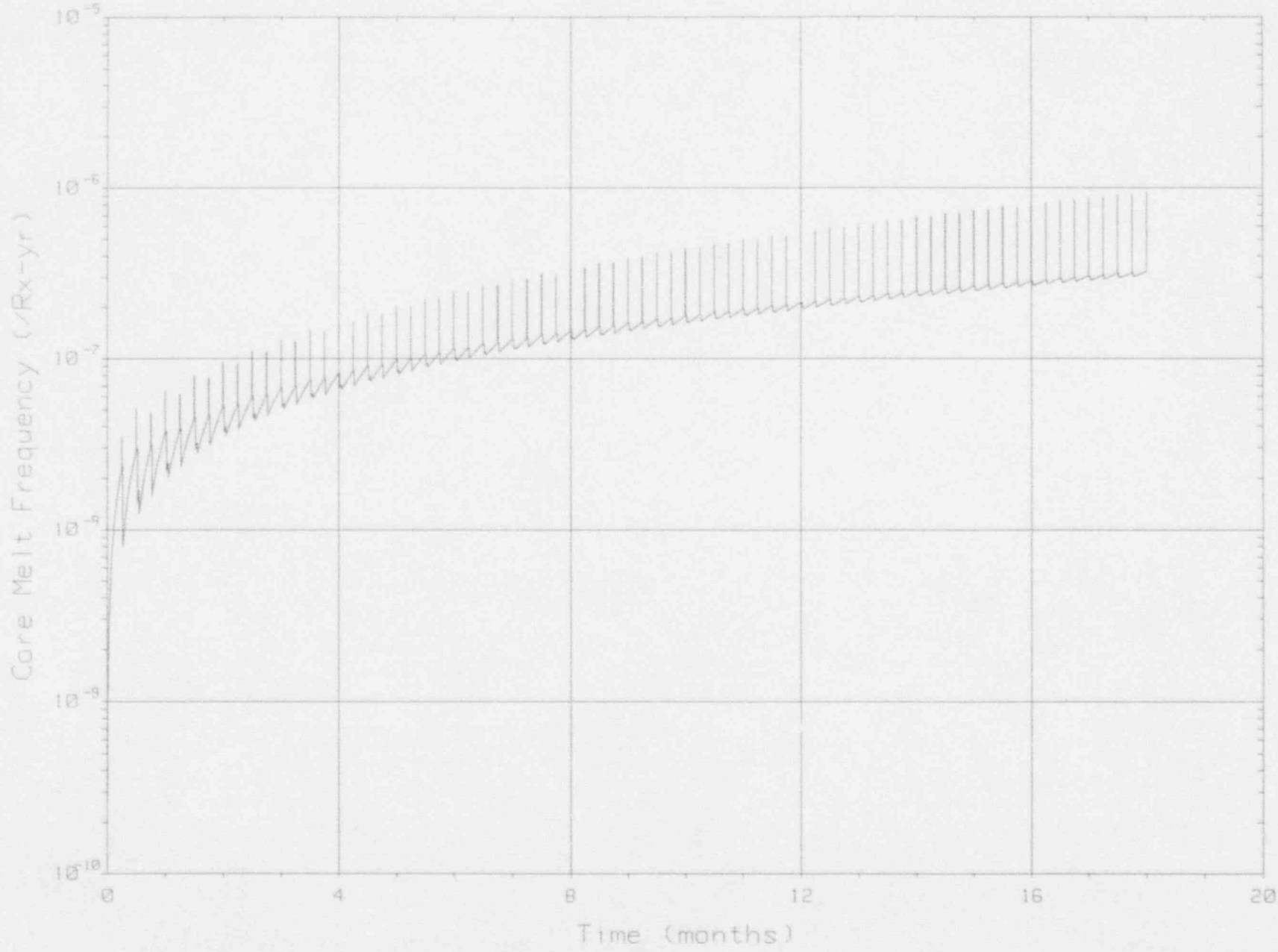


Figure 5-4: Risk of Core Melt from ESFAS Failure vs. Time
for Bailey Design - All Challenging Events - 1 & 3 Month Test Intervals

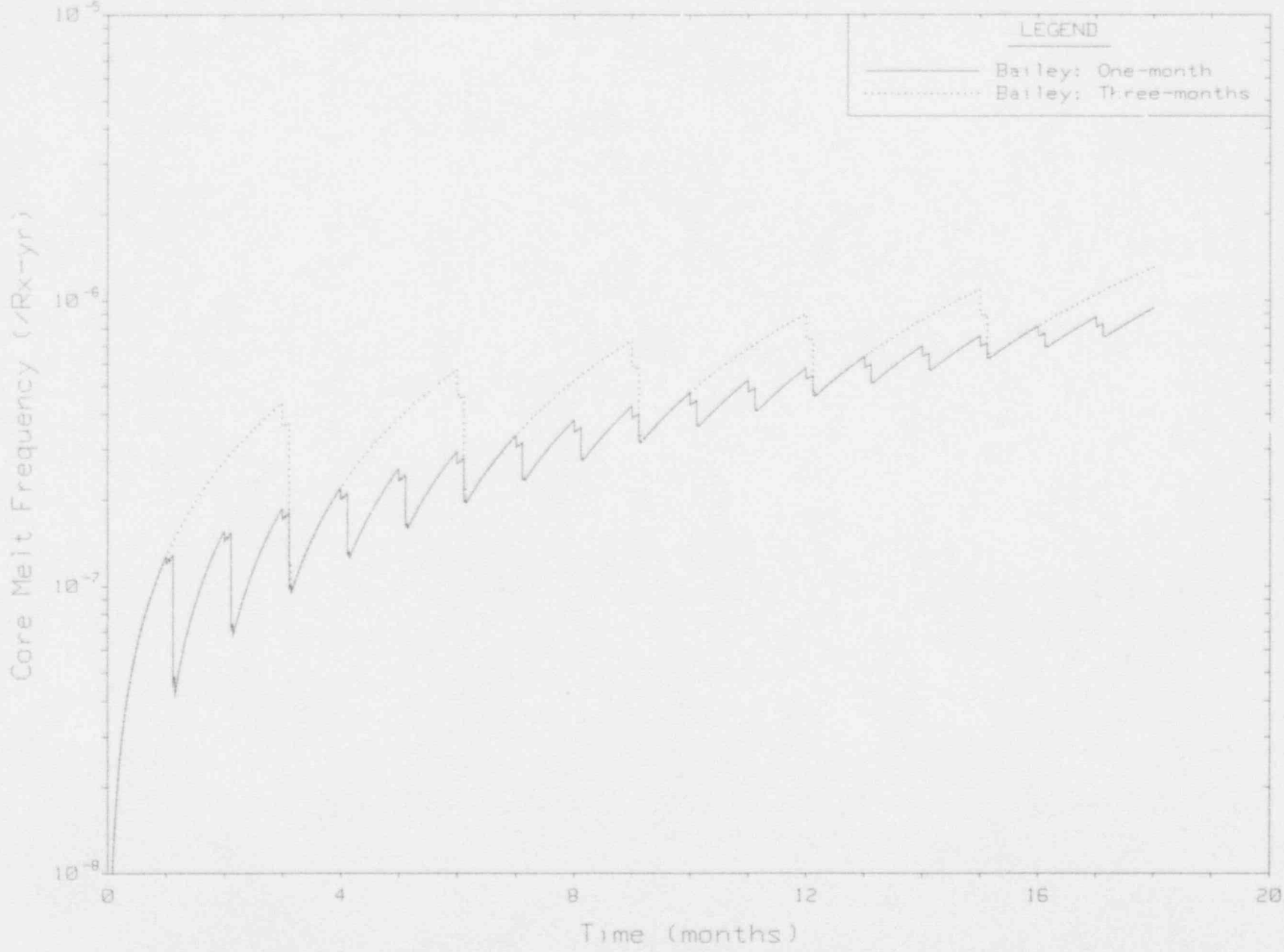


Figure 5-5: Risk of Core Melt from ESFAS Failure vs. Time
for Gilbert Design - All Challenging Events - 1 & 3 Month Test Interval

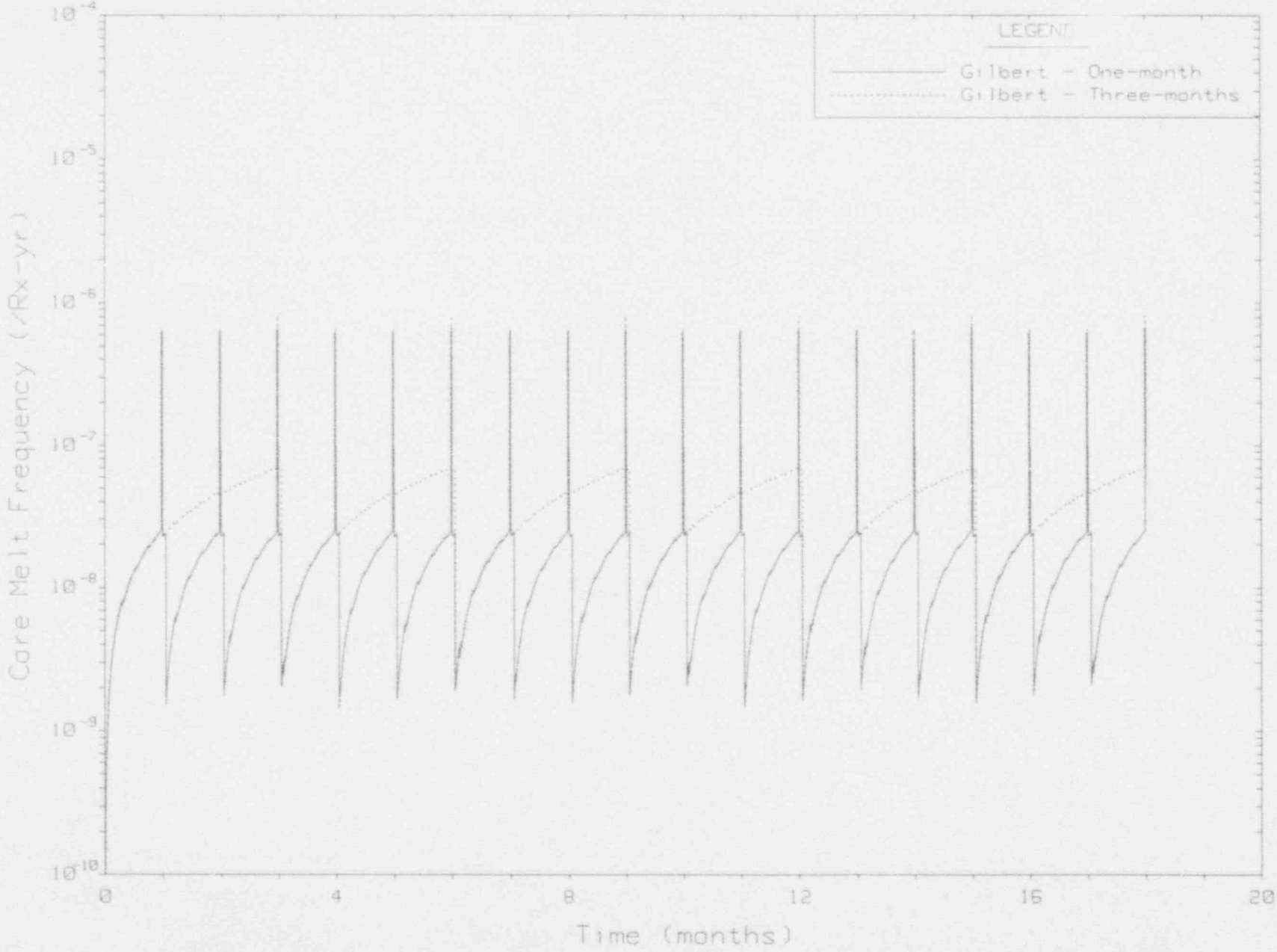


Figure 5-6: Risk of Core Melt from ESFAS Failure vs. Time
for Bechtel Design - All Challenging Events - 1 & 3 Month Test Intervals

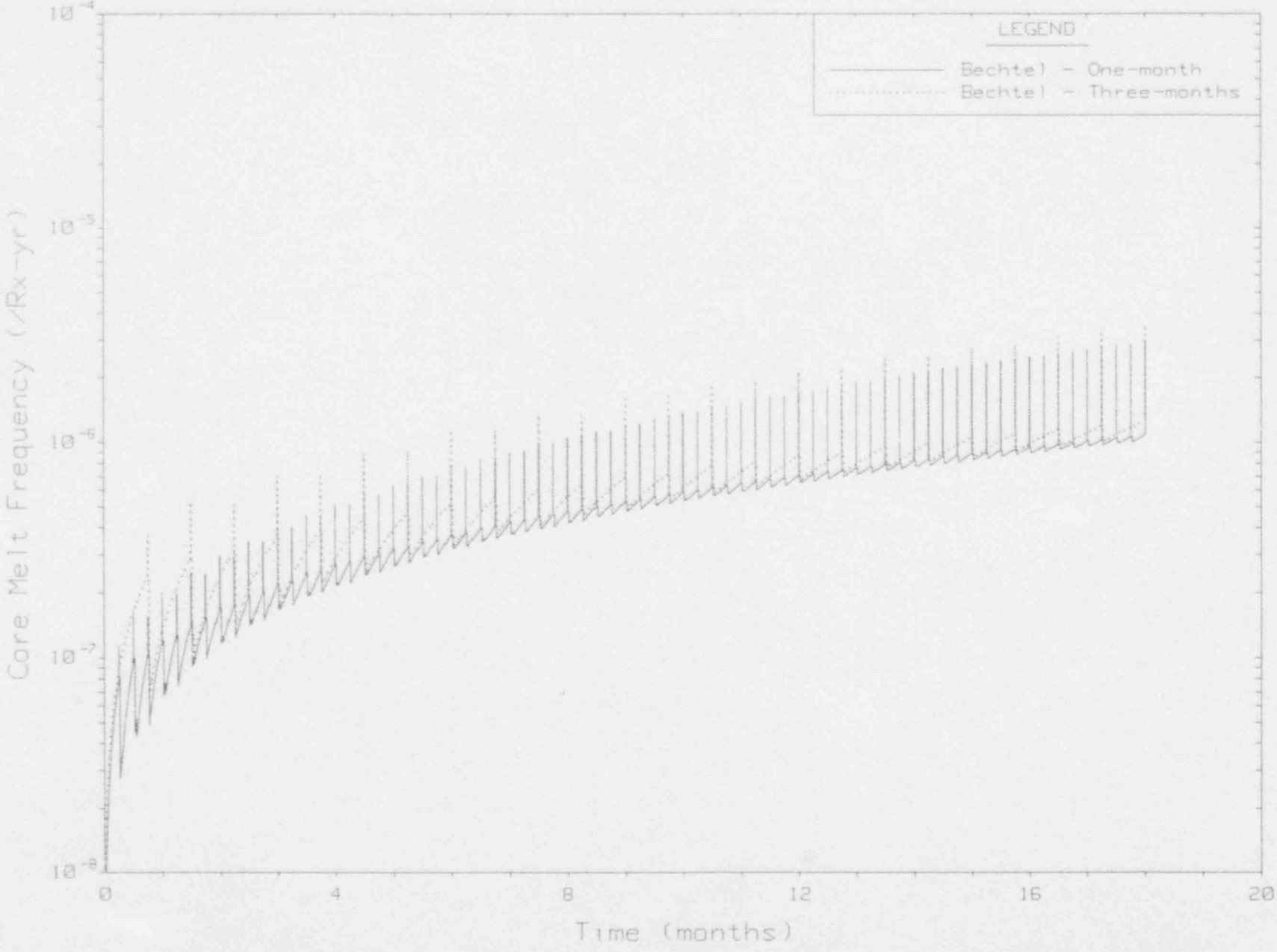
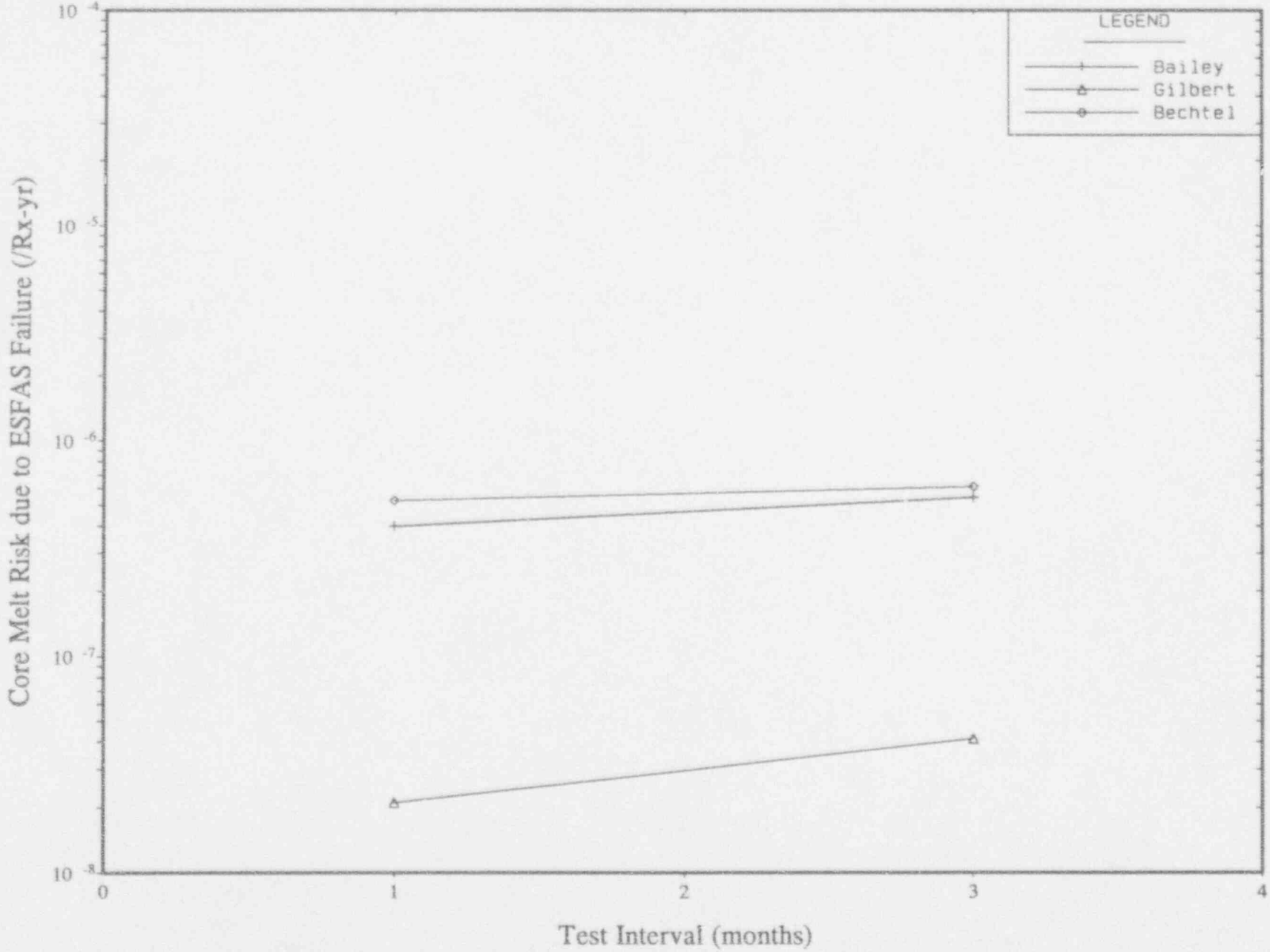


Figure 5-7: Core Melt Risk due to ESFAS Failure vs. STI
Summary of ESFAS Test Interval Extension '.nalysis



6. UNCERTAINTY ANALYSIS AND RESULTS

6.1. Uncertainty Analysis

For each of the three ESFAS designs, uncertainty analysis was performed on the time-averaged results. The purpose of the uncertainty analysis was to quantify the effect (on risk) of the uncertainty of the failure rate data as the ESFAS test interval was increased from one month to three months. The Boolean expressions derived from the RBDs that were used as input to PACRAT (as described in Section 3.4) were also used as input to the SAMPLE Monte Carlo computer code.

The Monte Carlo simulation was performed in accordance with the methodology prescribed in NUREG/CR-4350, Volume 5 [21] prepared by Sandia National Laboratory.

As with the execution of PACRAT, two sets of SAMPLE runs were made:

- Cases were run for each ESFAS design for each of the ESFAS challenging events.

- Cases were run for each ESFAS design using a composite Boolean expression representing all of the ESFAS challenging events. The composite Boolean expression was used (versus summing the results for the individual cases) so that like components required for different challenging events would have the same "sampled" value for each iteration.

Lognormal distributions were assumed for the failure rates. Error factors of ten were used for all random failures and common mode failures (for hardware failures and human errors) to define the range of uncertainty about the median values. The median values were calculated from the mean (best estimate) values, using the lognormal distribution assumption.

Six thousand trials were used in the Monte Carlo evaluation for each case. Two identical runs of 6000 trials were made for each case, using the same "sampled"

values, changing only the test interval from one month to three months. The resulting core melt frequencies from each trial were subtracted to obtain the one to three month (test interval) incremental risk resulting from ESFAS failure. The resulting incremental risk distributions describe the range of uncertainty of the time-averaged ESFAS incremental contribution to core melt frequency associated with increasing the test interval from one to three months.

Figure 6-1 shows both sets of SAMPLE cases for the Bailey ESFAS design: six[1] traces are shown. Five of the traces represent the cumulative distribution function (CDF) of the incremental risk (due to an increase in test interval from one to three months) for each of the challenging events (as labeled) that had an incremental risk contribution greater than 10^{-11}. The right-most trace (labeled "Total") represents the total incremental risk (from all six challenging events). The composite CDF appears to the right of the individual CDFs, indicating a mean value greater than any of the individual CDFs. As expected, the composite curve has a mean equal to the sum of the individual means. The median (50% value) incremental core melt frequency, as read off the "Total" trace, is approximately 5×10^{-8}/reactor-year, which is an insignificant fraction of the Commissioners' safety goal. Even with an error factor of ten for all the failure data, the 95% value of incremental core melt frequency associated with increasing the test interval from one to three months is very small (4.66×10^{-7}/reactor-year).

A similar set of traces is shown in Figures 6-2 and 6-3 for the Gilbert and Bechtel ESFAS designs. These traces conservatively represent the CDF for the incremental core melt frequency because some of the 6000 trials showed a risk benefit (reduction in core melt frequency) derived from increasing the test interval from one to three month, and these points have not been included. Both Gilbert and Bechtel ESFAS designs have surveillance tests that disable or bypass portions of the system during the test. These tests have a small impact on risk; with some trials of the Monte Carlo uncertainty analysis, the uncertainty of the failure rates were such that the resulting incremental risk was negative due to

---

[1] There are a total of seven traces (six individual challenging events plus one representing all the challenging events). The CDF for challenging event E was not plotted since its incremental risk contribution was less than 10^{-11}.

the effect of less-frequent bypassing with the three month STI. This included a few points in each of the Bechtel ESFAS cases, and many of the points for challenging events B and C (see Section 5.2) for the Gilbert ESFAS.

To generate the logarithmic plots in Figures 6-2 and 6-3, the negative risk increments (risk benefit) were removed, and the remaining values renormalized to generate a CDF. Therefore, the risk benefit is not reflected in the displayed CDFs. Because of the overwhelming risk benefit generated by challenging event C for the Gilbert ESFAS design, no CDF trace is displayed.

6.2. Uncertainty Analysis Results

Using a non-parametric one-sided tolerance limit, it was determined that the 5728^{th} value (of the 6000 ordered statistics generated by SAMPLE) represents the 95%/95% value, that is, it can be asserted with a confidence of at least 95% that 95% of a population lies below the 95%/95% value of a random sample from that population. The non-parametric approximation requires no assumption of normality.

The point-estimate value (as calculated by PACRAT) and 95%/95% values of the incremental risk of core melt due to an increased ESFAS test interval are given in Table 6-1 for each of the three ESFAS designs, and each of the challenging events and the challenging event aggregrate. The mean incremental core melt frequencies calculated by SAMPLE agree with the mean incremental core melt frequencies calculated by PACRAT. The relative closeness of the means and 95%/95% values (upper bound) shows the robustness of the best estimate incremental risk even with considering an order of magnitude variation in all the basic event failure data.

Figures 6-4 through 6-6 are the probability density functions (PDFs) of the incremental increase in core melt frequency due to changing the ESFAS test interval from one to three months for all challenging events. They are obtained from the "Total" CDFs shown in Figures 6-1 through 6-3 by differentiating the curves to convert the CDF into a PDF format. The mean and upper bound are shown explicitly on the PDF for each ESFAS design. The PDF for the Gilbert ESFAS

design (Figure 6-5) is truncated on the left side because the lower 1 percentile of the PDF showed negative values (i.e., risk benefit).

The uncertainty analysis shows 95%/95% values from 9.57×10^{-8} (Gilbert) to 4.94×10^{-7} (Bailey). The small magnitude of the upper bounds reinforces the robustness of the conclusion that increasing the ESFAS test interval from one month to three months does not significantly impact risk.

TABLE 6-1

Means and Upper Bounds of the Incremental Risk (/Reactor-year)
of Core Melt due to the Extension of the STI from
One Month to Three Months for the Three ESFAS Designs

Event	Bailey[a]		Gilbert[a]		Bechtel[a]	
	Mean[b]	95%/95%[c]	Mean[b]	95%/95%[c]	Mean[b]	95%/95%[c]
A	5.63e-08	1.98e-07	8.76e-09	3.57e-08	2.60e-08	9.53e-08
B	7.02e-09	2.47e-08	9.45e-10	3.74e-09	7.99e-09	3.03e-08
C	2.33e-09	1.00e-08	-1.72e-09	-4.43e-11	4.51e-09	1.88e-08
D	2.02e-08	7.10e-08	3.01e-09	1.09e-08	1.54e-08	5.67e-08
E	8.53e-12	3.12e-11	7.99e-12	3.31e-11	1.16e-12	5.52e-12
F	5.88e-08	1.96e-07	9.26e-09	3.71e-08	2.96e-08	1.08e-07
All[d]	1.45e-07	4.94e-07	2.03e-08	9.57e-08	8.35e-08	2.69e-07

[a] All values are given in units of 'per reactor-year'.

[b] Taken from Table 5-1, and presented here for comparative purposes.

[c] The 5728th point of the 6000 ordered statistics.

[d] These values are explicitly shown on Figures 6-4 through 6-6.

Figure 6-1: CDFs for the Incr. Risk of Core Melt due to Increased Test Int. for Bailey ESFAS (for Indiv. & All Challenging Events)

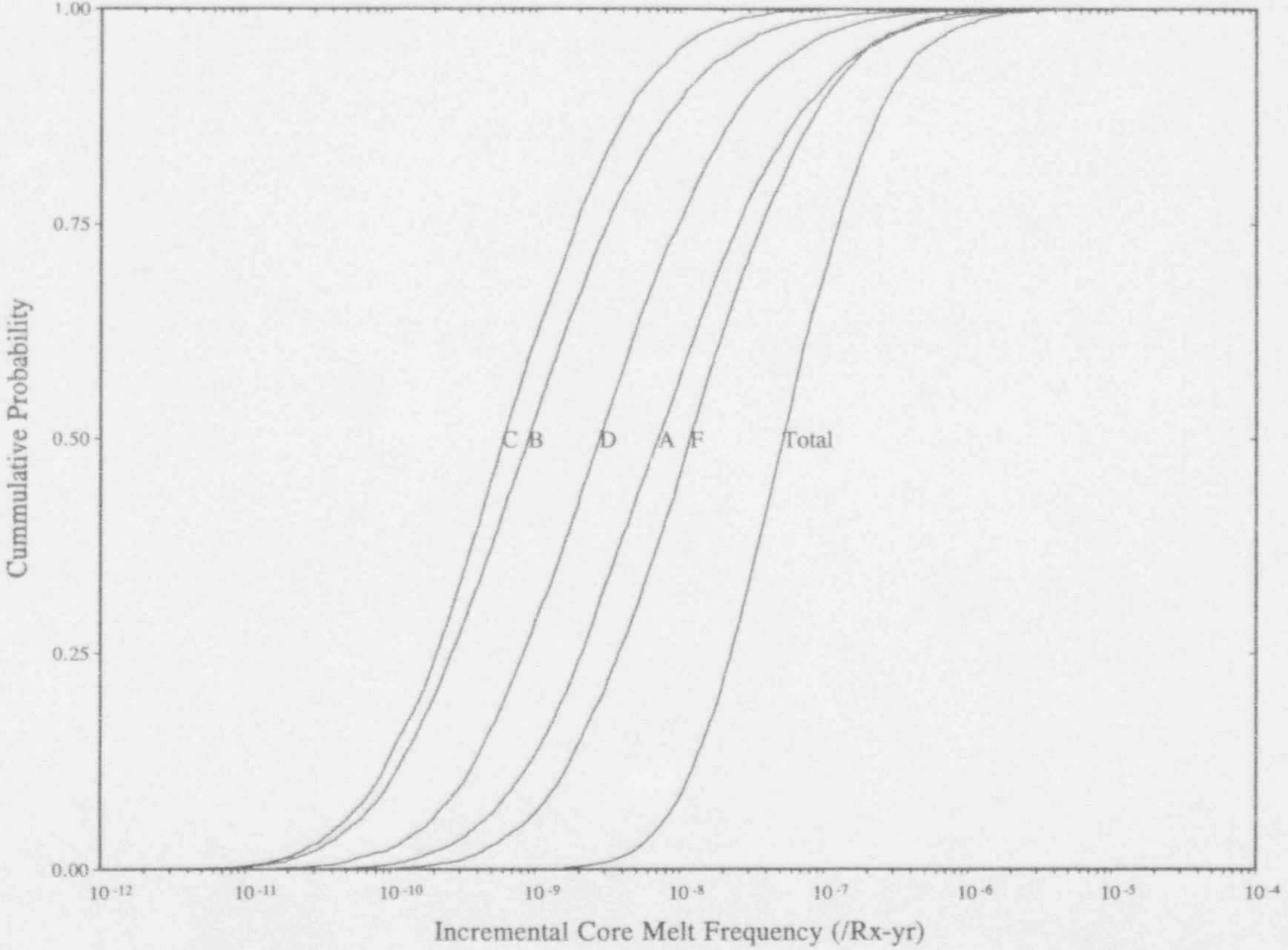


Figure 6-2: CDFs for the Incr. Risk of Core Melt due to Increased Test Int. for Gilbert ESFAS (for Indiv. & All Challenging Events)

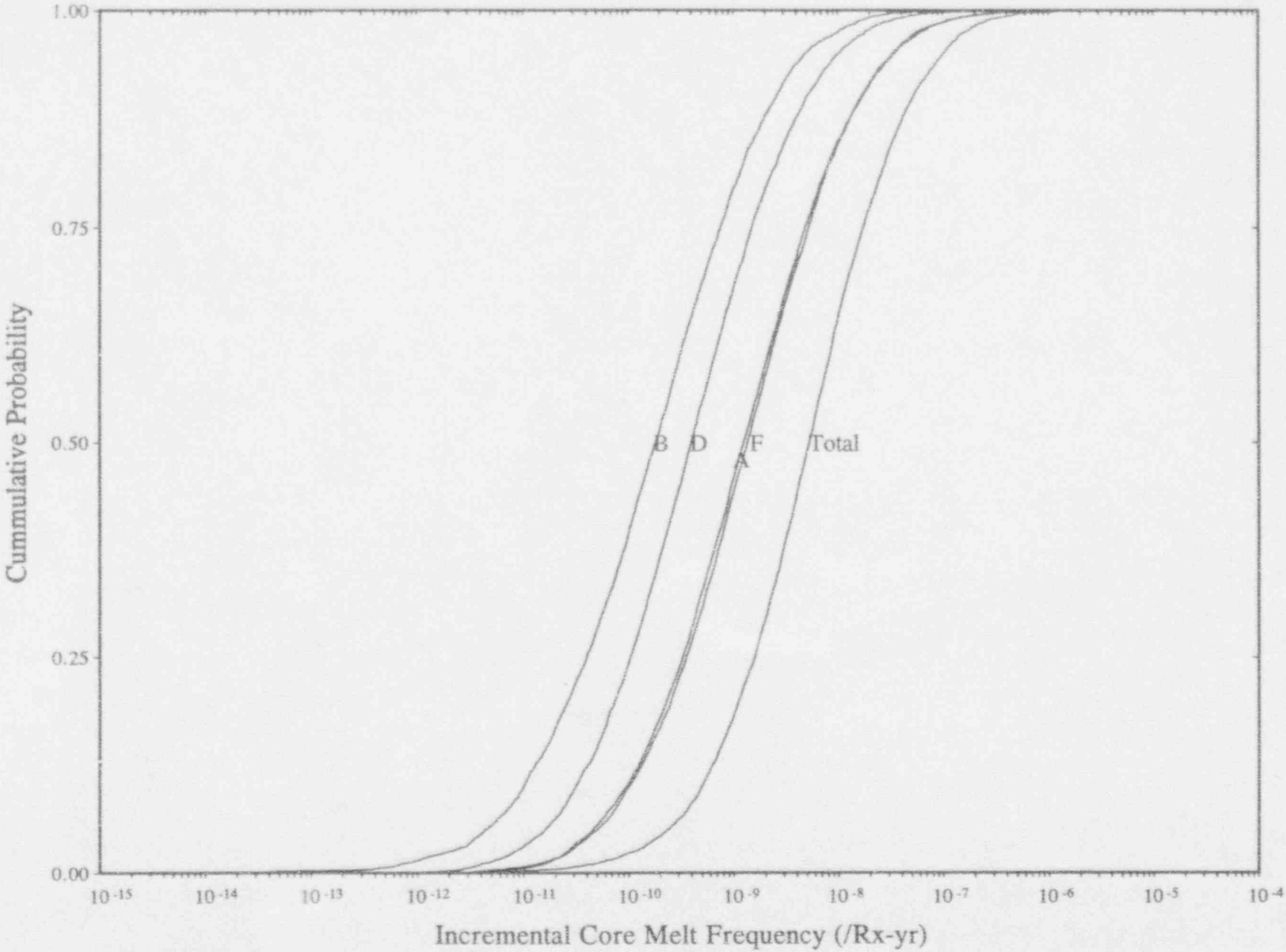


Figure 6-3: CDFs for the Incr. Risk of Core Melt due to Increased Test Int. for Bechtel ESFAS (for Indiv. & All Challenging Events)

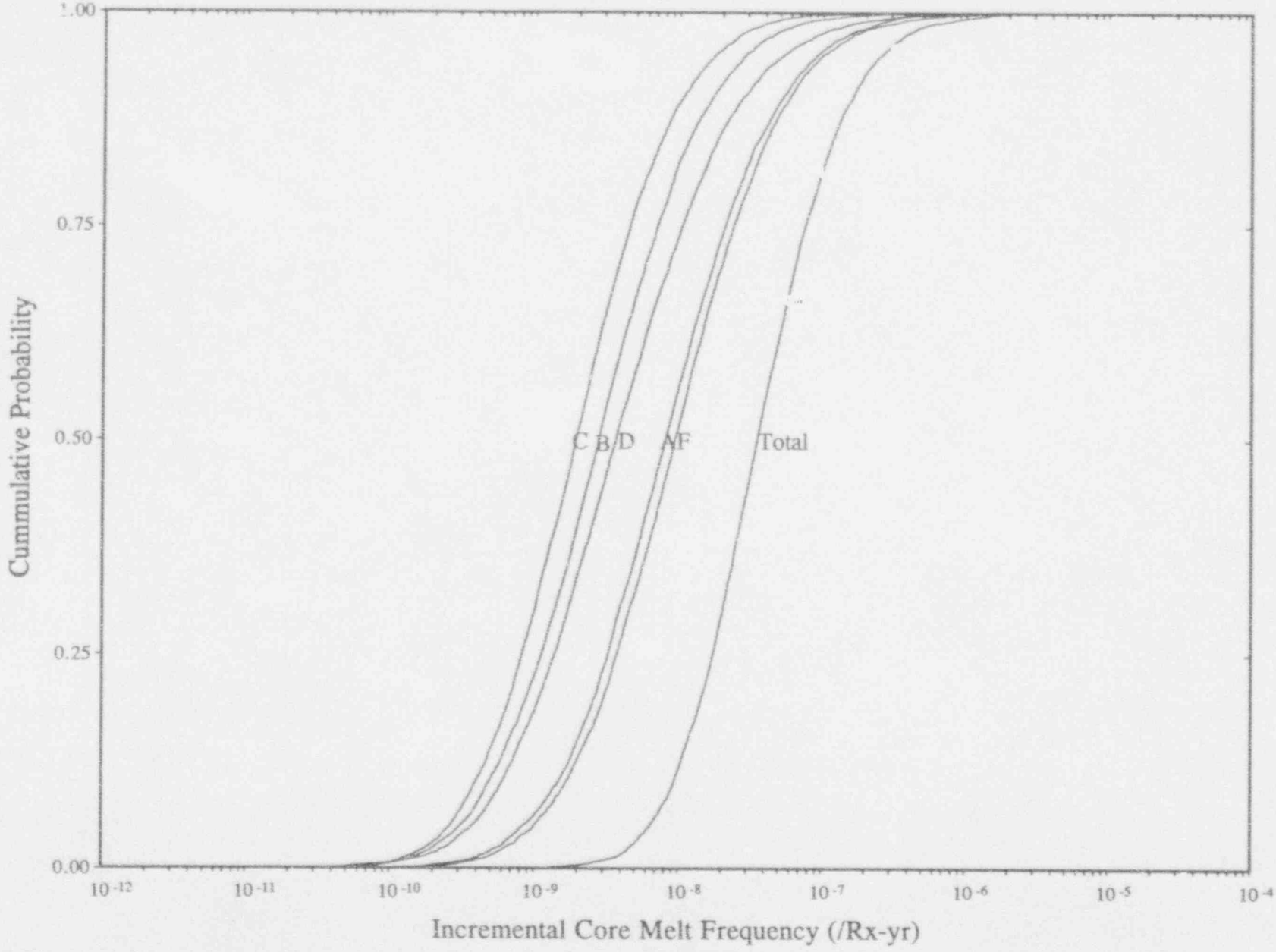


Figure 6-4: PDF for the Incremental Risk of Core Melt due to Increased Test Interval for Bailey ESFAS (for All Challenging Events)

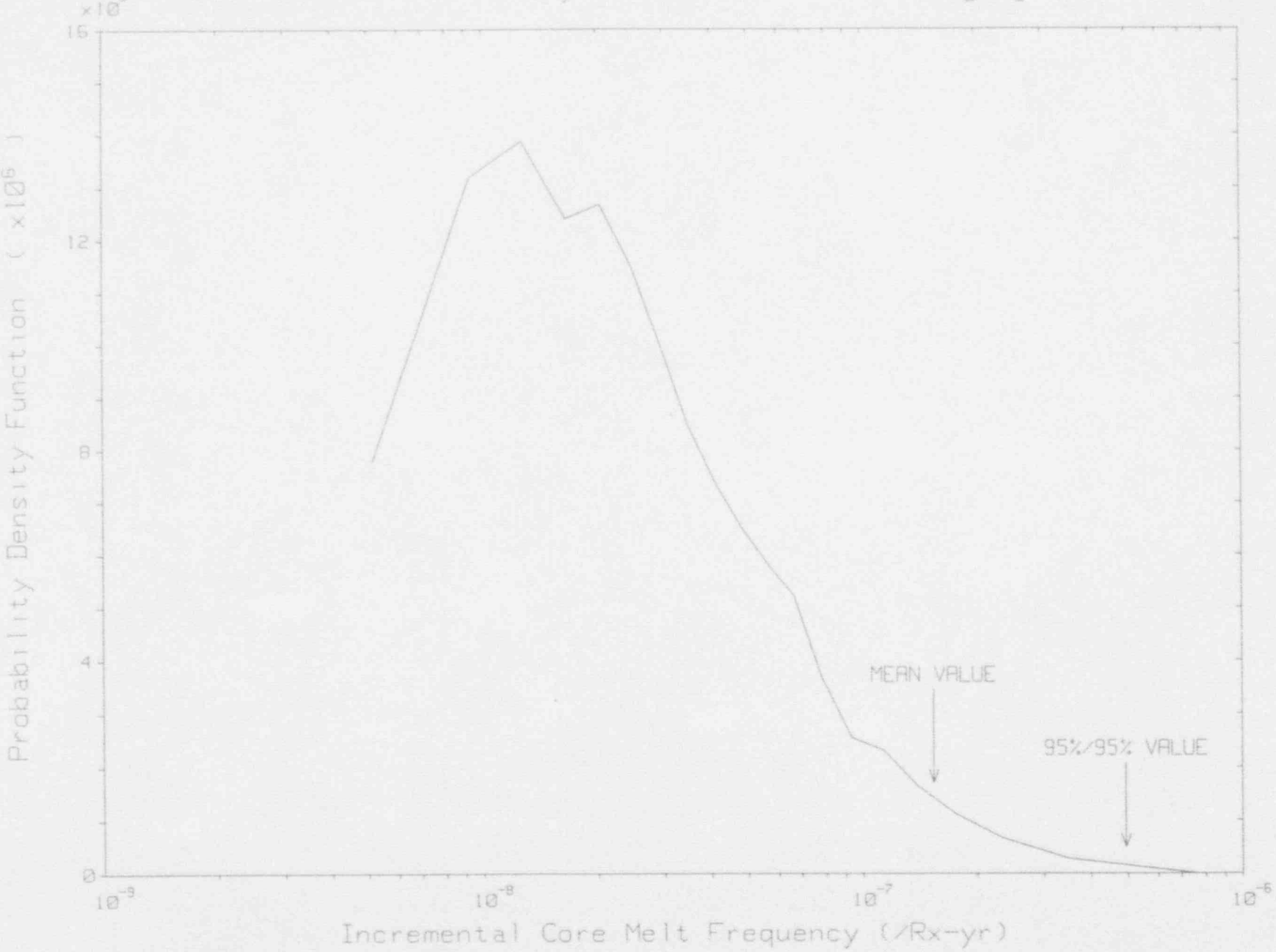


Figure 6-5: PDF for the Incremental Risk of Core Melt due to Increased Test Interval for Gilbert ESFAS (for All Challenging Events)

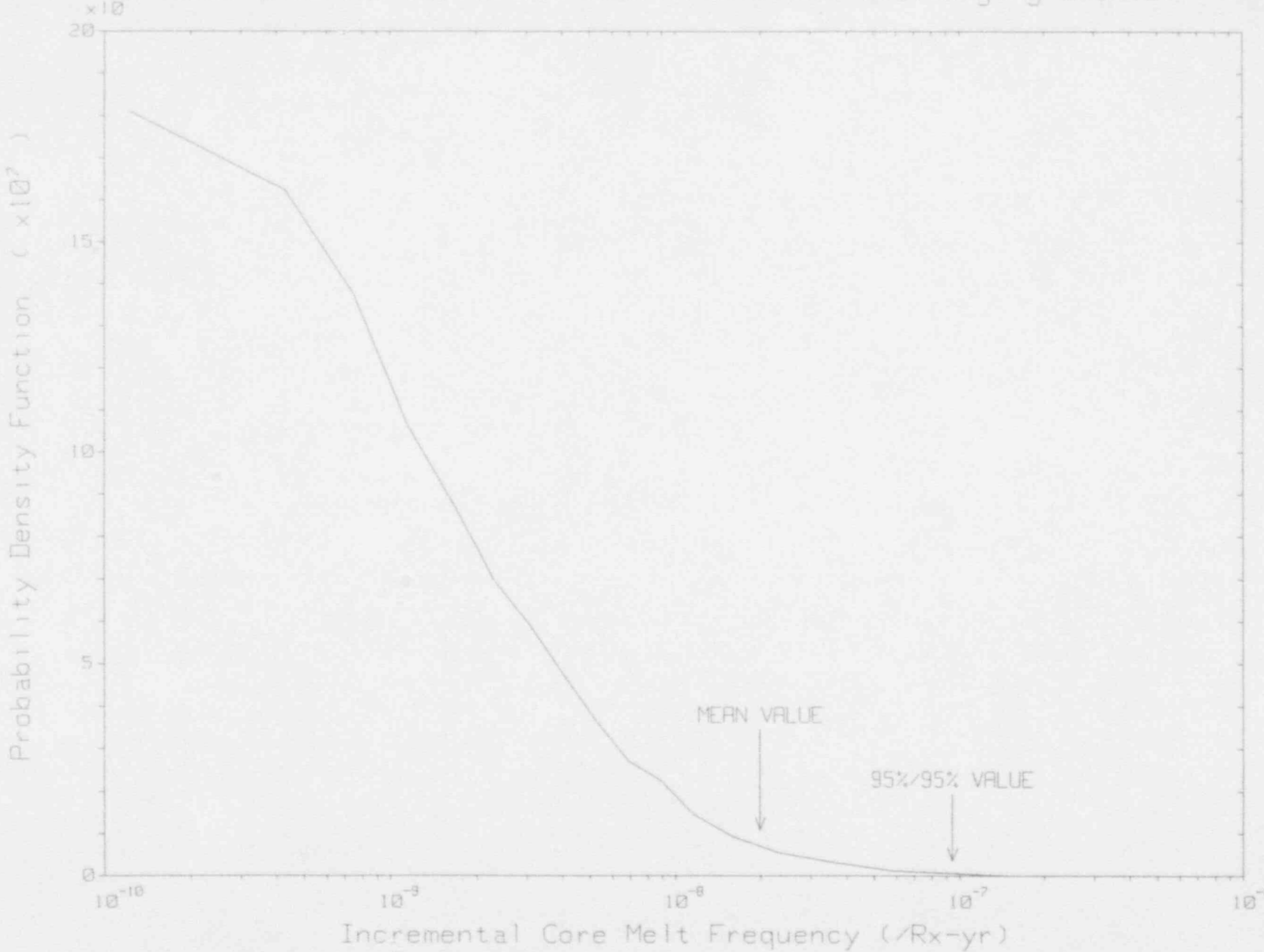
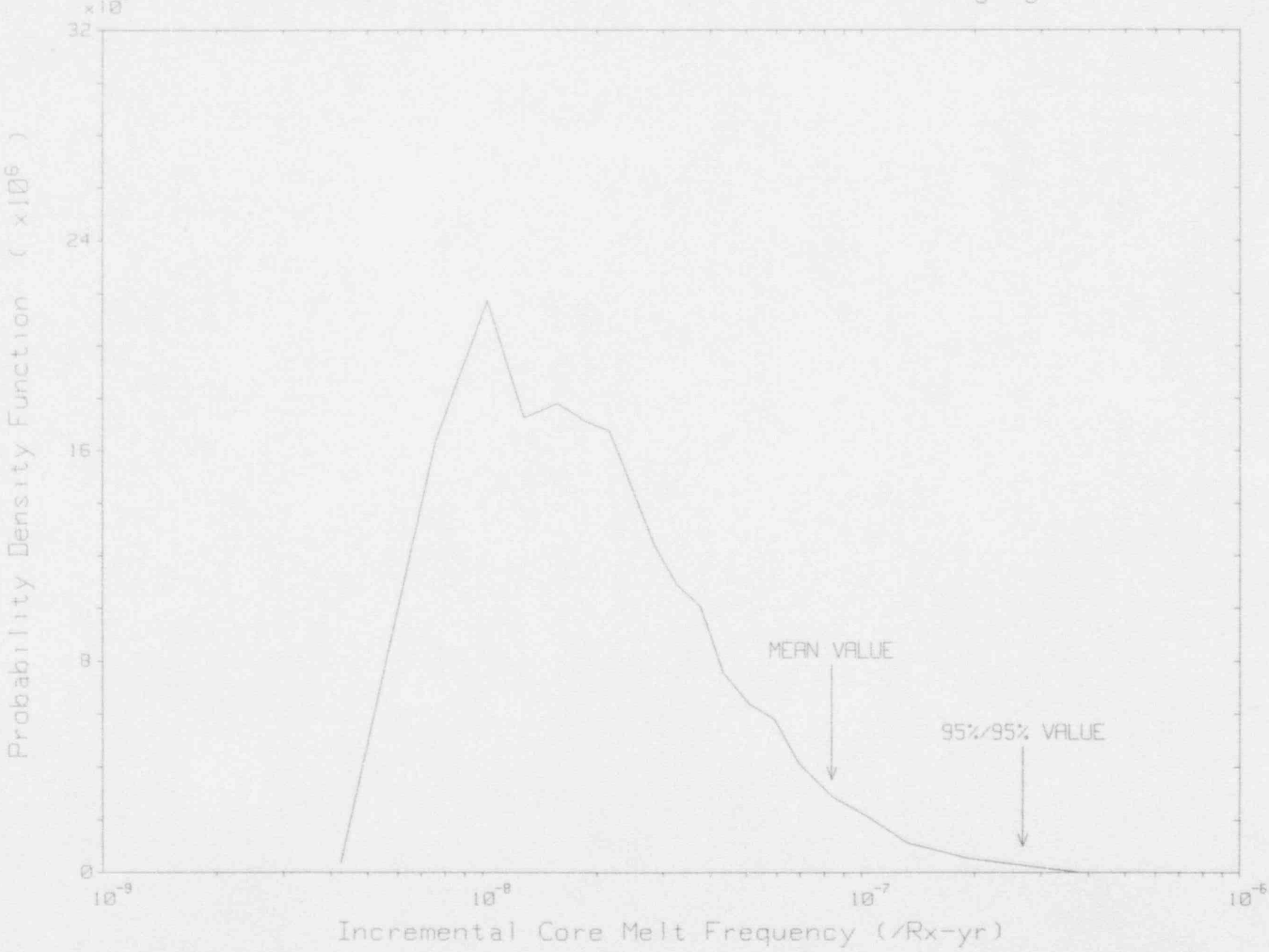


Figure 6-6: PDF for the Incremental Risk of Core Melt due to Increased Test Interval for Bechtel ESFAS (for All Challenging Events)



7. REFERENCES

[1] R. S. Enzinna, S. H. Levinson, and E. W. Swanson, "Justification for Increasing the Reactor Trip System On-Line Test Intervals," prepared for the B&WOG Availability Committee, BAW-10167, May 1986.

[2] R. S. Enzinna, S. H. Levinson, and E. W. Swanson, "Justification for Increasing the Reactor Trip System On-Line Test Intervals," prepared for the B&WOG Availability Committee, BAW-10167, Supplement Number 1: Questions & Answers, February 1988.

[3] Safety Evaluation Report, B&WOG Topical Report BAW-10167, Justification for Increasing the RTS On-Line Test Interval, Enclosure in a Letter (NRC Evaluation of BWOG Topical Report BAW-10167 and Supplement 1) from Ashok C. Thadani (NRC) to Courtney W. Smythe (BWOG), December 1988.

[4] Teresa R. Meachum and Corwin L. Atwood, Common Cause Fault Rates for Instrumentation and Control Assemblies, Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1981, prepared for the U.S. Nuclear Regulatory Commission by the Idaho National Engineering Laboratory (INEL), EGG-2258, NUREG/CR-3289, May 1983.

[5] Standard Technical Specifications - Babcock & Wilcox Plants - Draft Report for Comment, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, NUREG-1430, January 1991.

[6] NPRDS Reporting Guidance Manual, Revision 02, INPO 89-001, The Institute of Nuclear Power Operations, August 1990.

[7] Lousie M. Weston, Donnie W. Whitehead, and Norman L. Graves, Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Based Method, prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratories, Albuquerque, New Mexico, SAND87-0179, NUREG/CR-4834/1 of 2, June 1987.

[8] R. R. Willie, FTAP2, Computer-Aided Fault Tree Analysis, ORC 78-14, Operations Research Center, University of California, Berkeley, August 1978, Modifications by BWNS, NPGD-TM-536, Rev. I, BWNS, Lynchburg, Virginia, February 1991.

[9] E. Oelkers and M. J. Talian, PACRAT - Probability Analysis Code with Repair and Testing, NPGD-TM-291, Rev. 4, BWNS, Lynchburg, Virginia, March 1991.

[10] SAMPLE: General Purpose Computer Program for Uncertainty Analysis by Monte Carlo Simulation, originally by WASH-1400 Reactor Safety Study Group, modifications by BWNS, NPGD-TM-501, Rev G, BWNS, Lynchburg, Viriginia, May 1991.

[11] S. H. Levinson, User's Manual: Integrated Reliability Interactive System, IRIS, NPD-TM-28, BWNS, Lynchburg, Virginia, August 1985.

[12] R. B. Worrell and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, NUREG/CR-0465, Sandia National Laboratories, Albuquerque, New Mexico, November 1978.

[13] "Reactor Protection System," Vol. 2, Rev. 6, BAW-100085P, April 1979.

[14] W. E. Vesely, et. al., FRANTIC II - A Computer Code for Time-Dependent Unavailability Analysis, NUREG/CR-1924, U.S. Nuclear Regulatory Commission, 1981.

[15] Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, U. S. Nuclear Regulatory Commission, October 1975.

[16] Mosleh and Fleming, Procedures for Treating Common Cause Failure in Safety and Reliability Studies, Pickard, Lowe, and Garrick, Inc., NUREG/CR-4780, Volume 2 (Table C-1), January 1989.

[17] Oconee Nuclear Station Unit 3 Probabilistic Risk Assessment, Duke Power Company, transmitted in a letter dated November 30, 1990 from M.S. Tuckman (Duke Power) to NRC Document Control Desk in response to Generic Letter 88-20.

[18] A. D. Swain and H. E. Guttman, Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratories, Albuquerque, New Mexico, SAND80-0200, NUREG/CR-1278, August 1983.

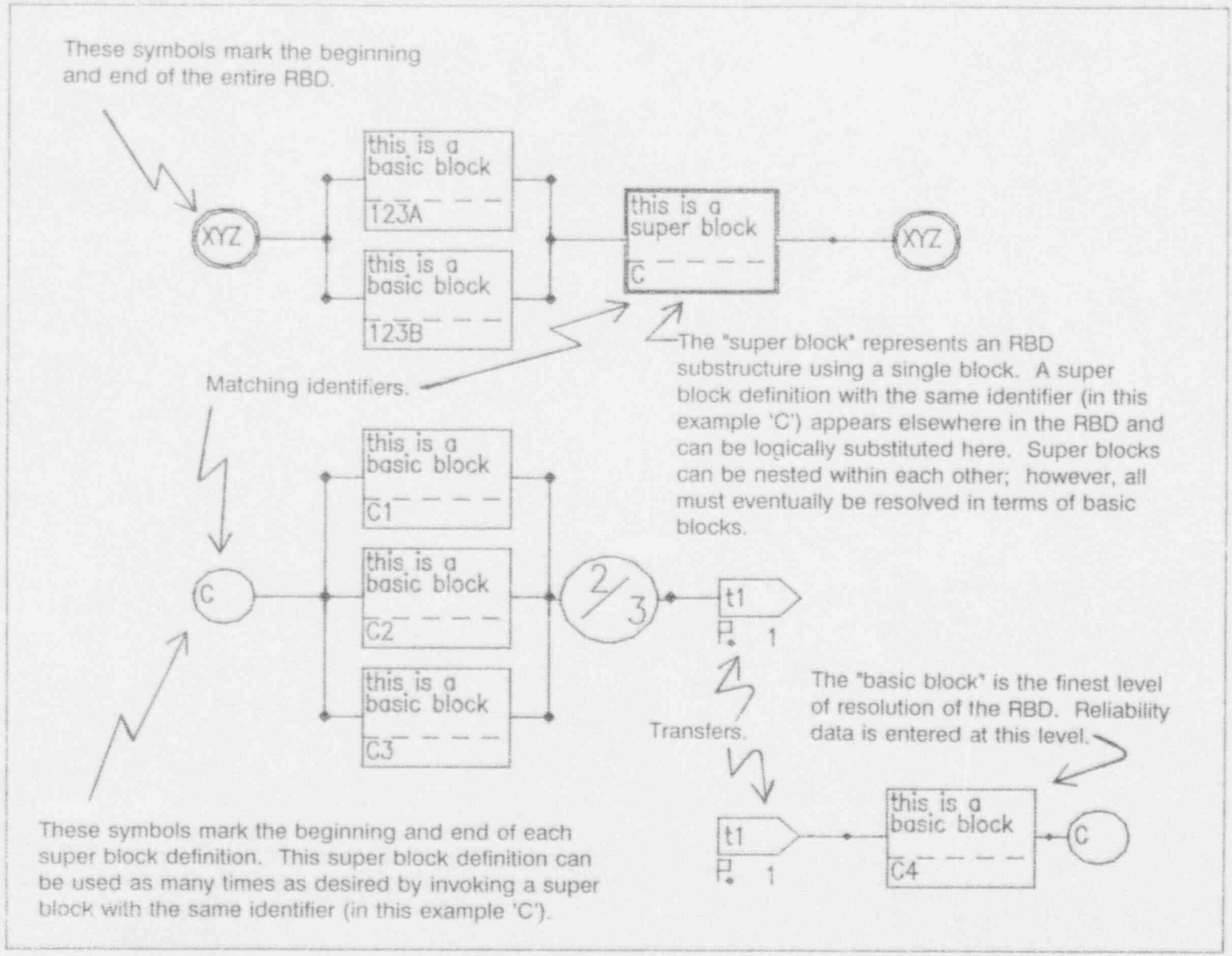
[19] F. Burrows, T. Dunning, R. Emch, S. Newberry, and M. Virgilio, Safety Evaluation by the Office of Nuclear Reactor Regulation WCAP-10271, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System", transmitted by letter from E. J. Butcher to C. O. Thomas, U.S.N.R.C., Washington D.C., Febrary 15, 1985.

[20] E. V. Lofgren, Probabilistic Risk Assessment Course Documentation, Volume 5: System Reliability and Analysis Techniques Session D - Quantification, prepared by Sandia National Laboratories, Albuquerque, New Mexico, for the U.S. Nuclear Regulatory Commission, SAND85-1495/5 of 7, NUREG/CR-4350/5 of 7, August 1985.

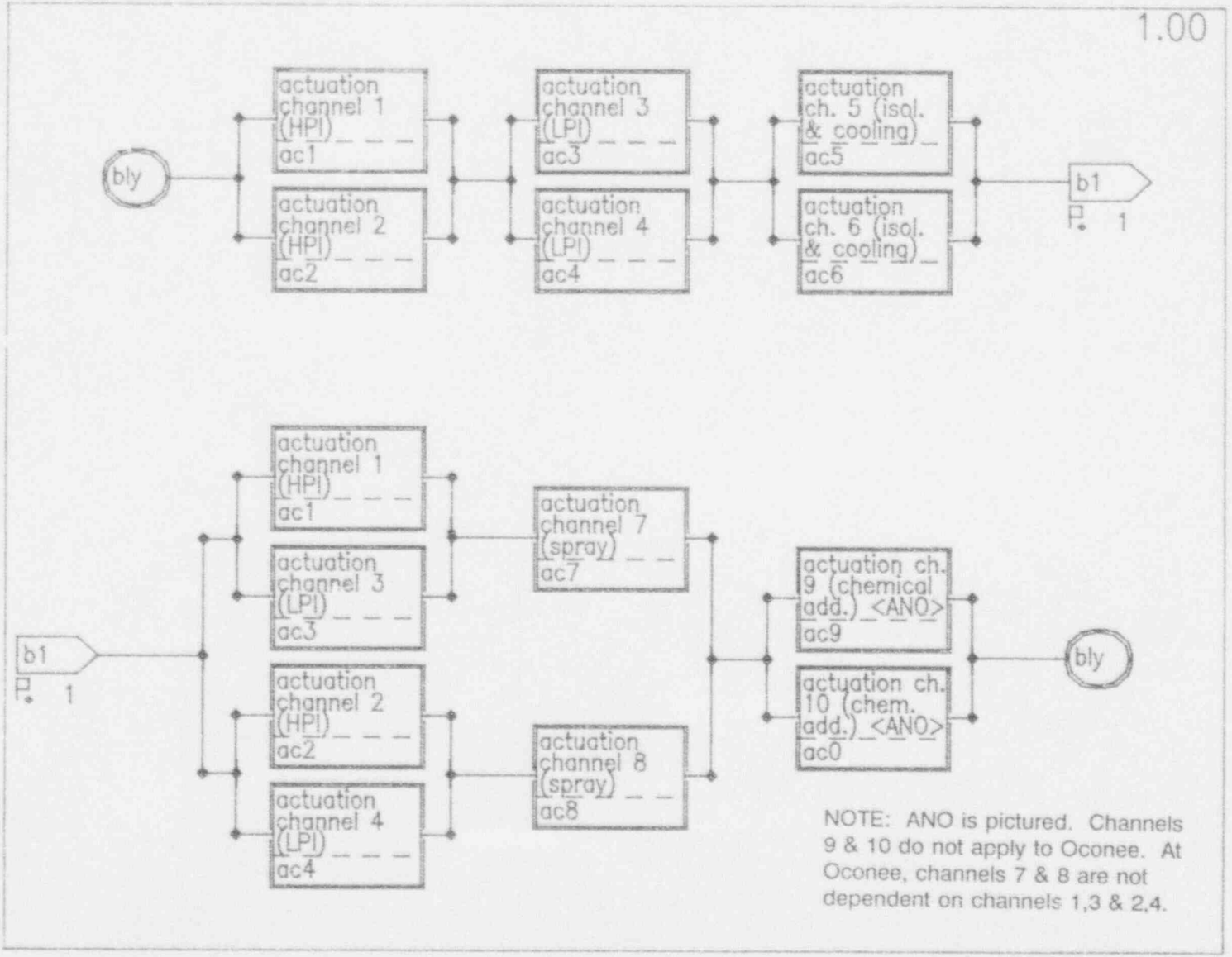
[21] P.K. Samanta, S.M. Wong, and J. Carbonaro, Evaluation of Risk Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant, prepared for the Office of Nuclear Regulatory Research by Brookhaven National Laboratory, Contract DE-AC02-76CH00016, BNL-NUREG-52024, NUREG/CR-5200, August 1988.

APPENDIX A

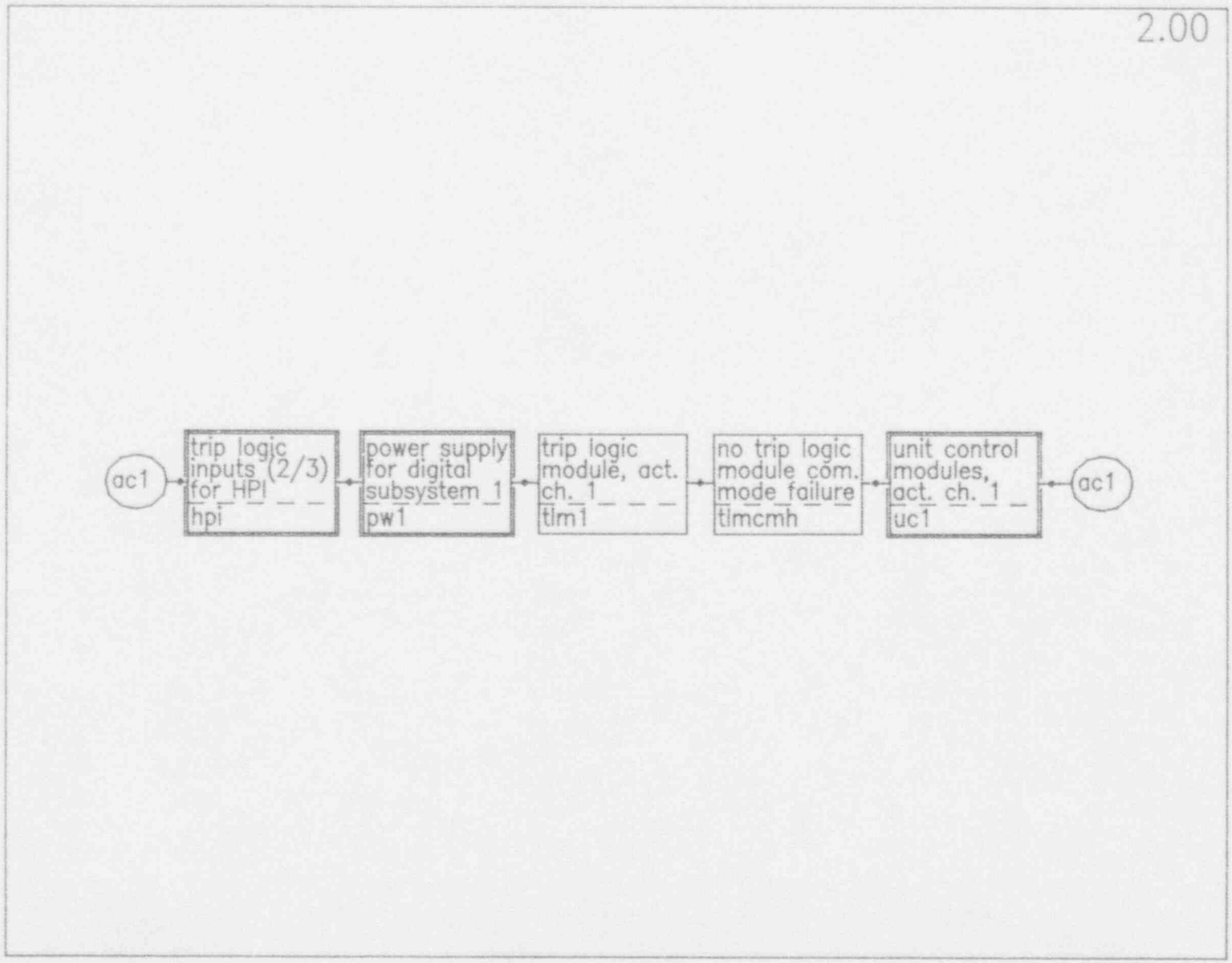
RBD for Bailey ESFAS (ANO-1 & Oconee)



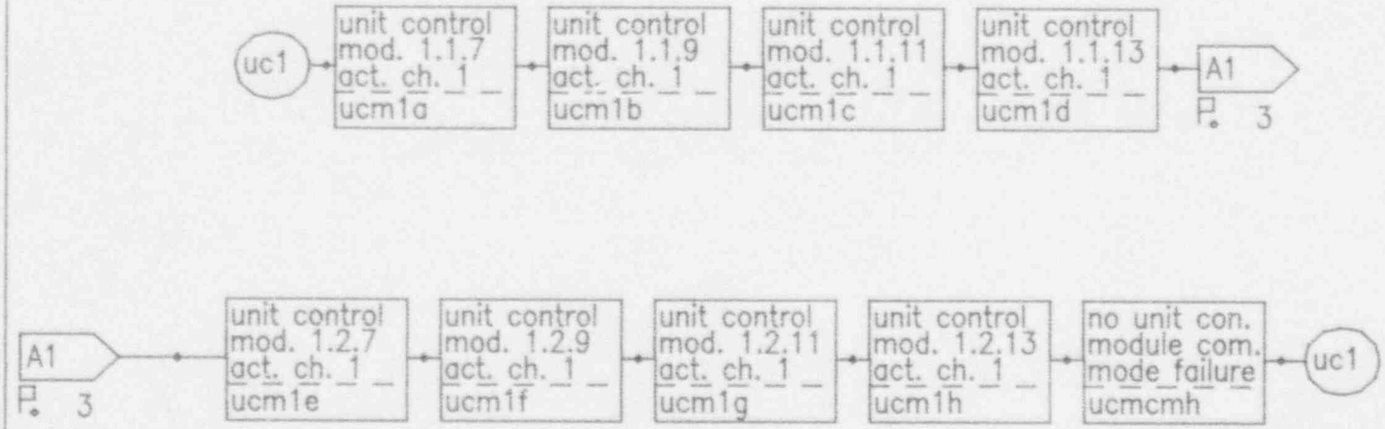
RBD Symbology Description



Bailey ESFAS (ANO-1 & Oconee)

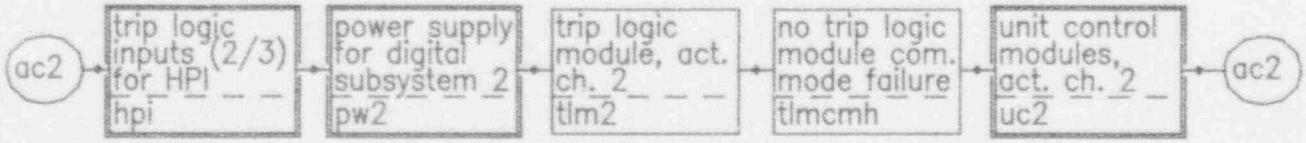


Bailey ESFAS (ANO-1 & Oconee)

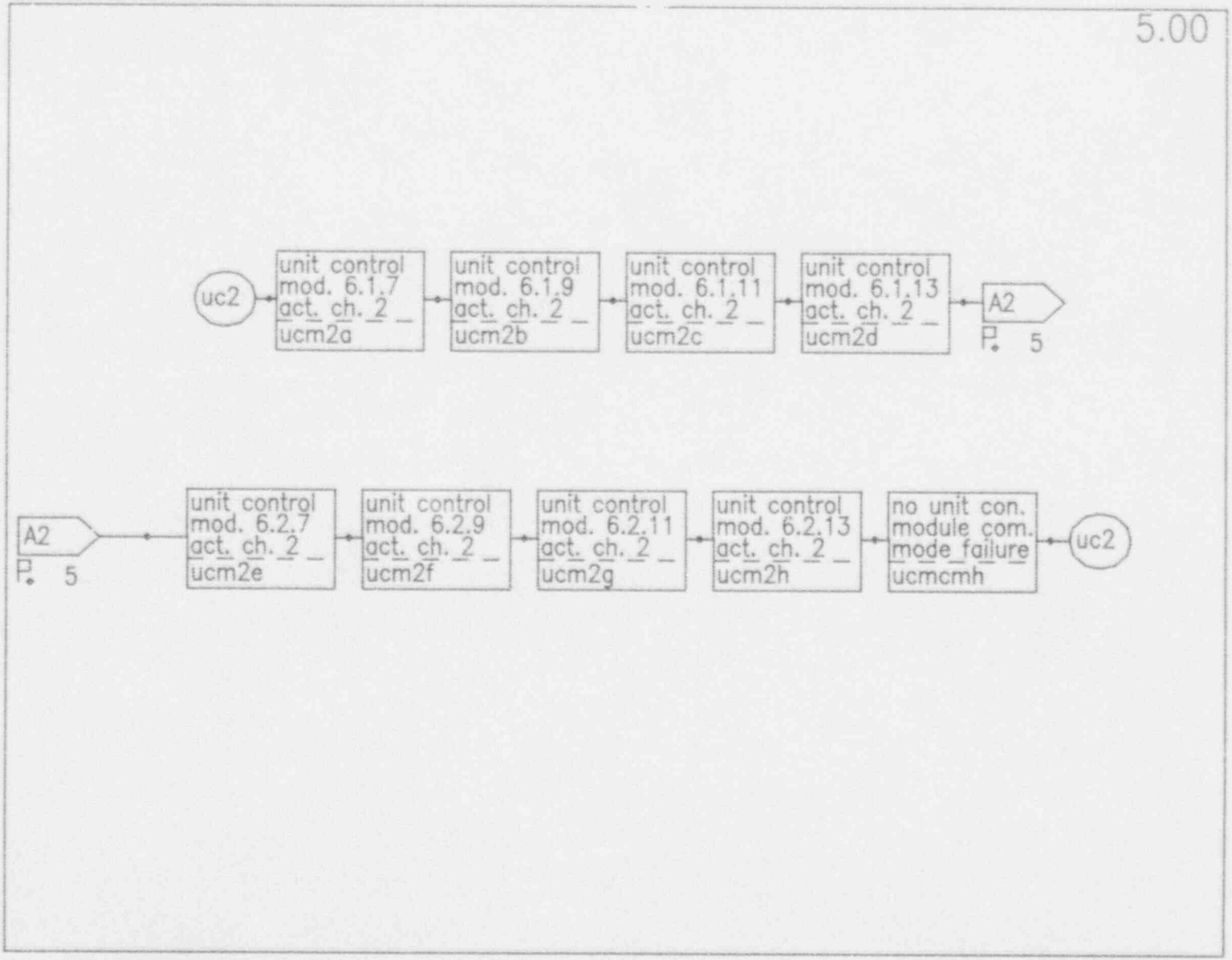


NOTE: Channels 1 through 10 unit control modules (UCMs) for ANO are shown. UCMs for Oconee channels 1 through 8 are similar.

Bailey ESFAS (ANO-1 & Oconee)

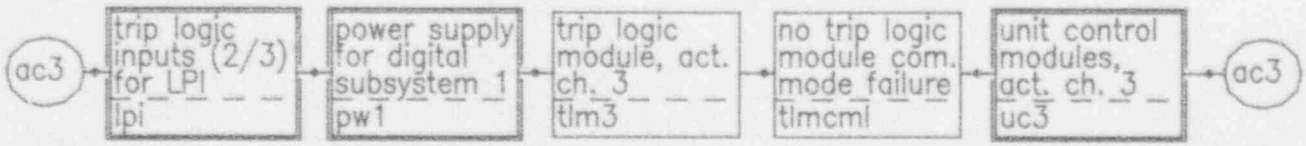


Bailey ESFAS (ANO-1 & Oconee)

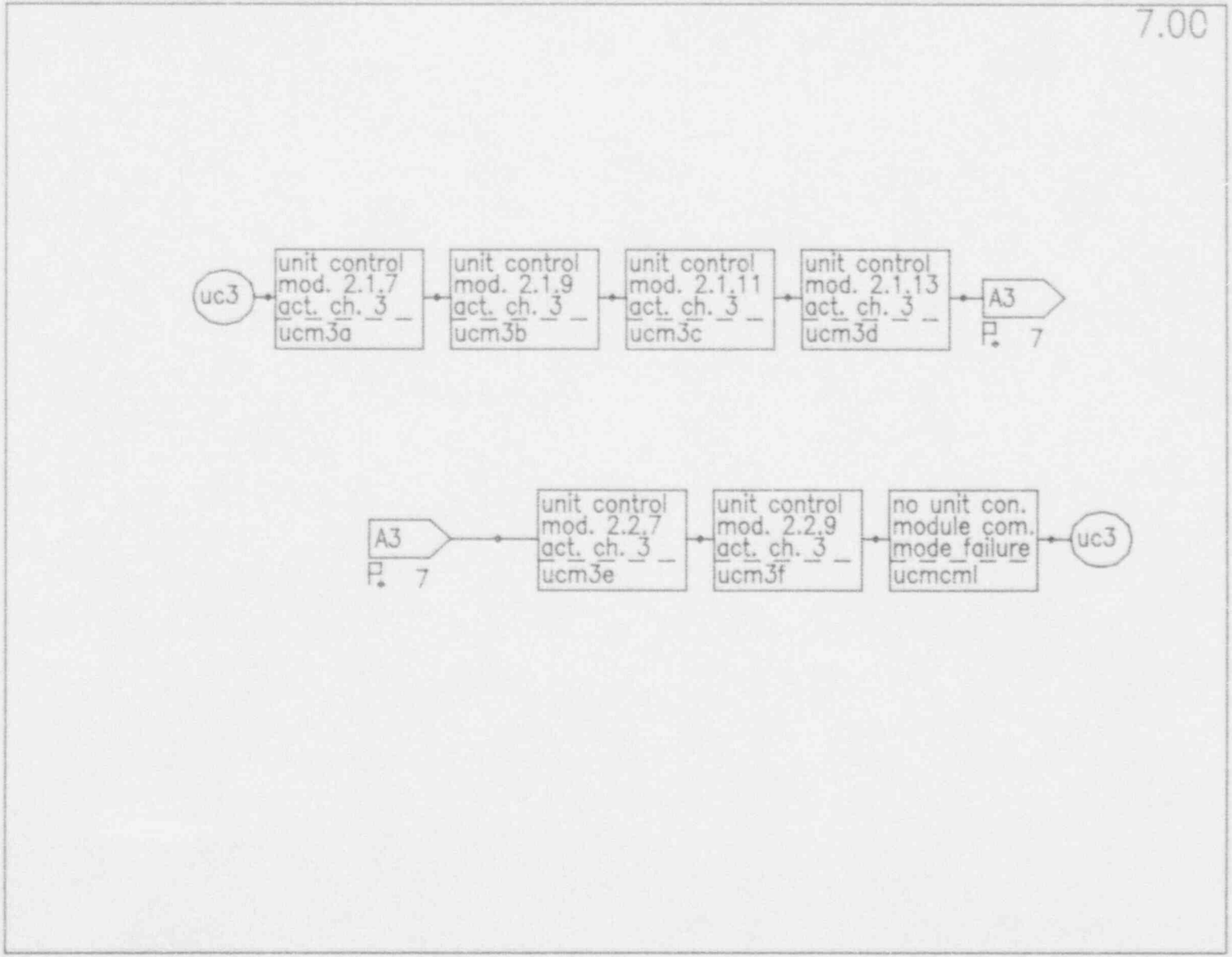


Bailey ESFAS (ANO-1 & Oconee)

6.00

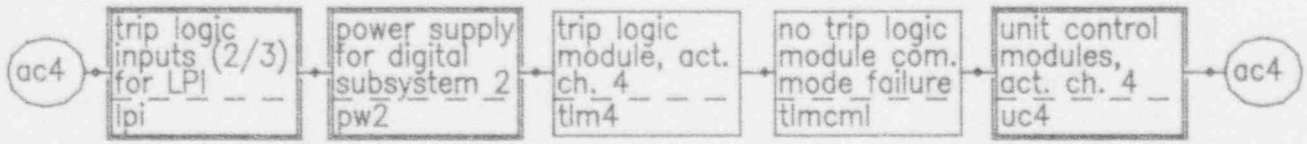


Bailey ESFAS (ANO-1 & Oconee)

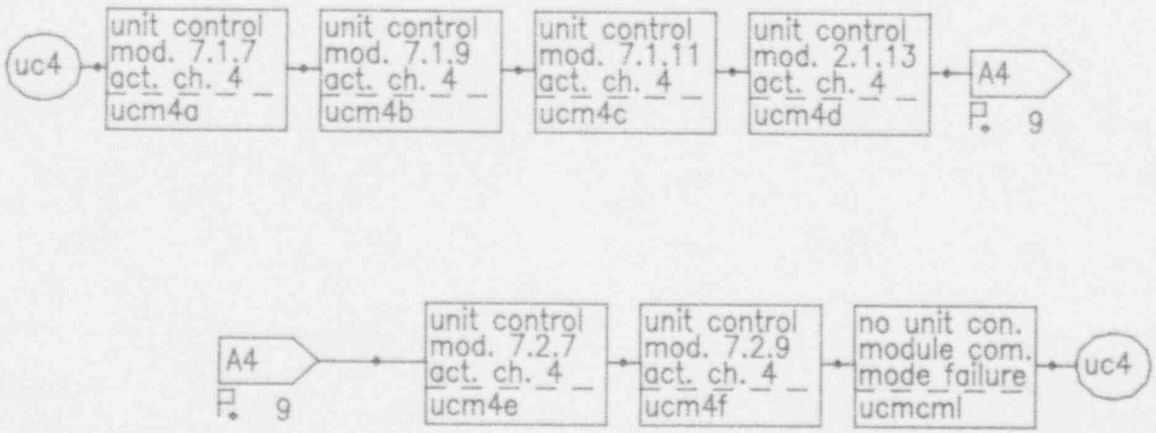


Bailey ESFAS (ANO-1 & Oconee)

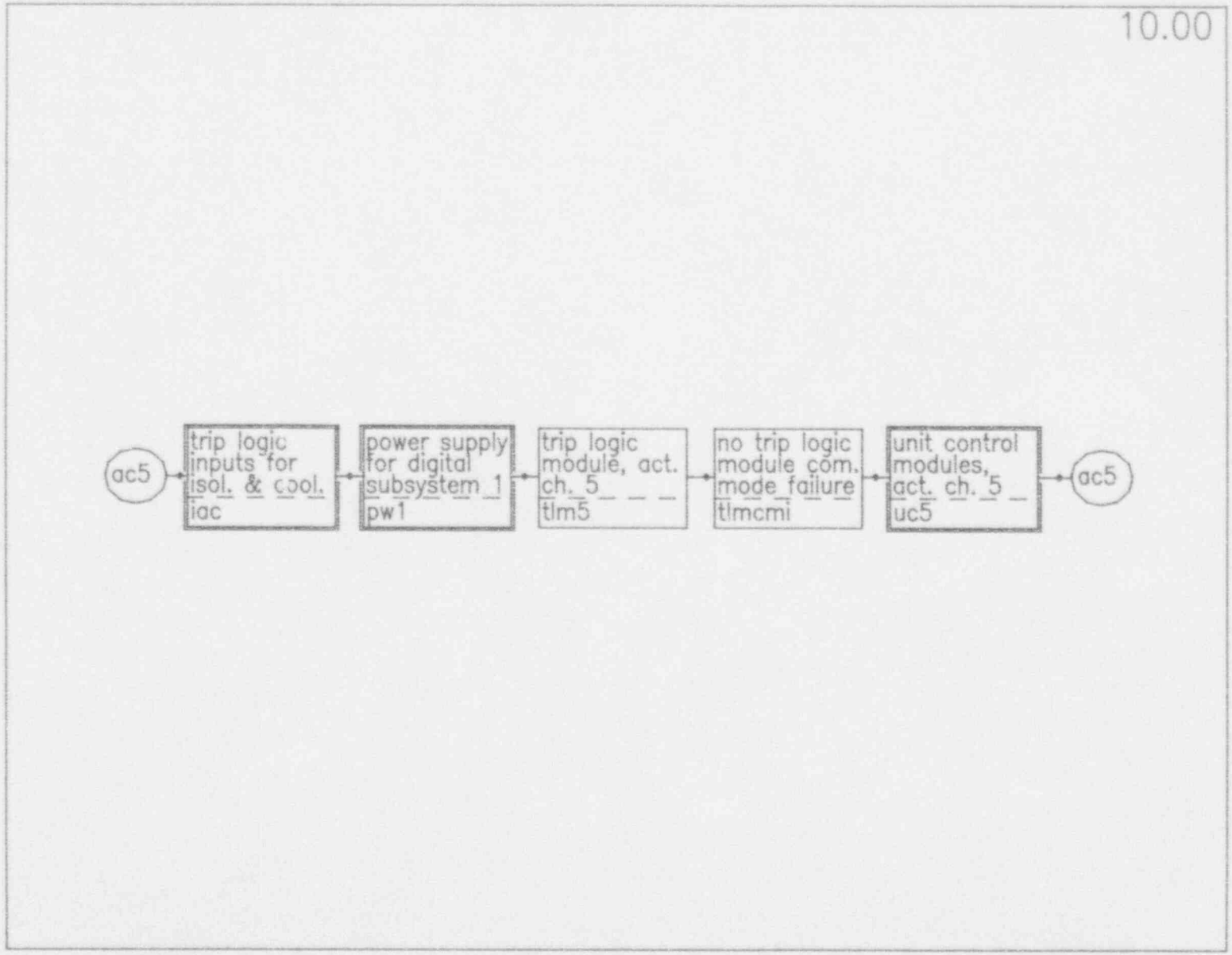
8.00



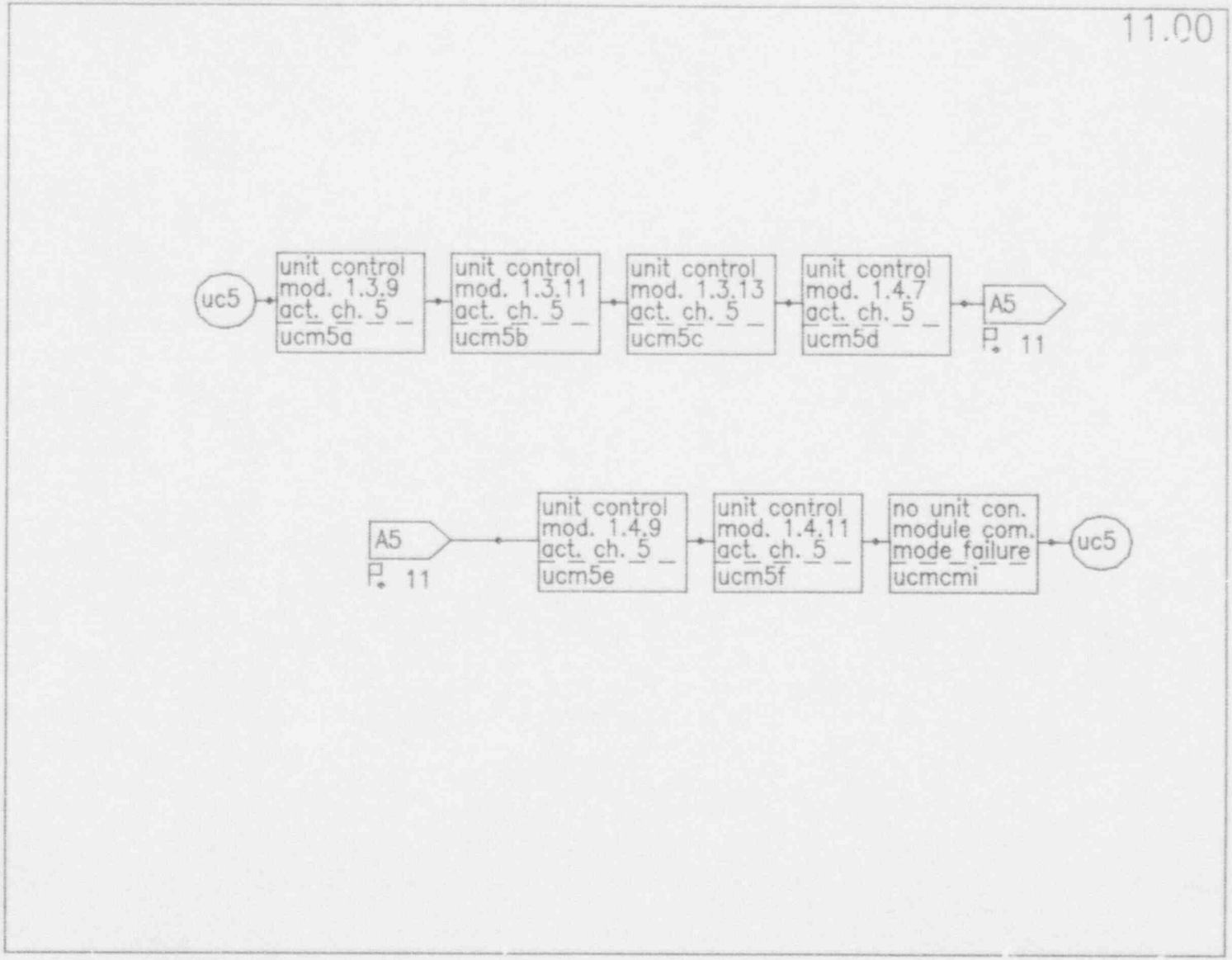
Bailey ESFAS (ANO-1 & Oconee)



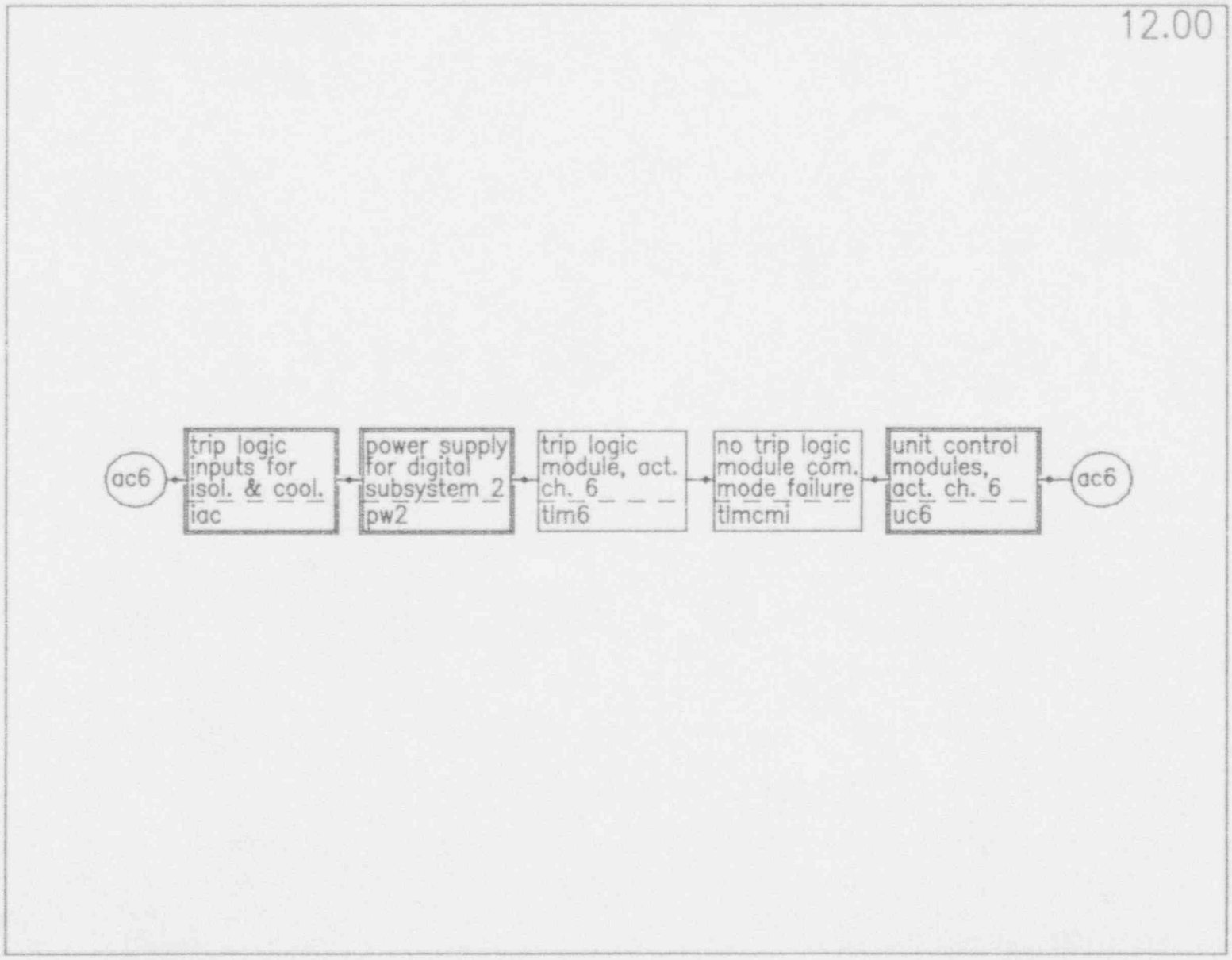
Bailey ESFAS (ANO-1 & Oconee)



Bailey ESFAS (ANO-1 & Oconee)

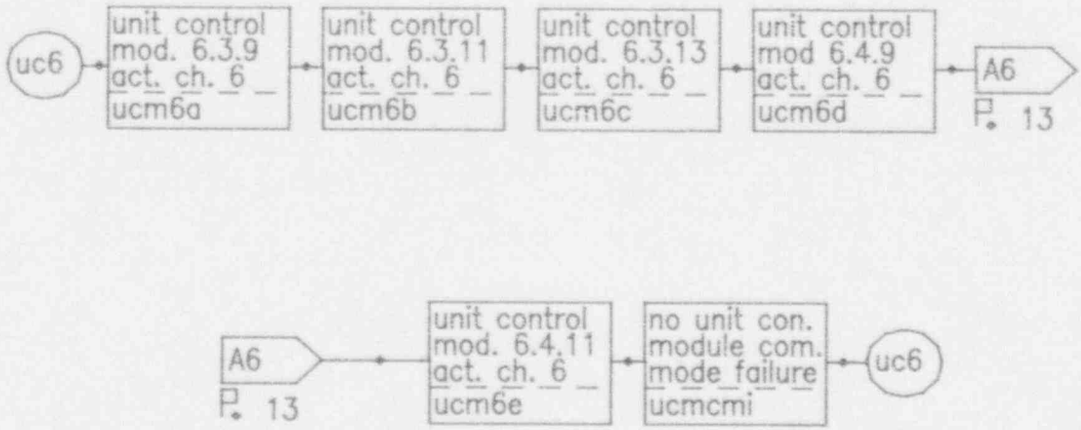


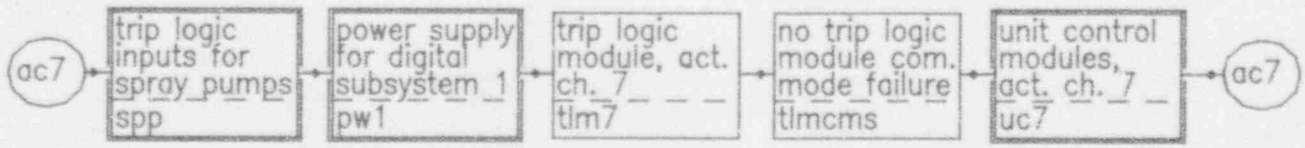
Bailey ESFAS (ANO-1 & Oconee)



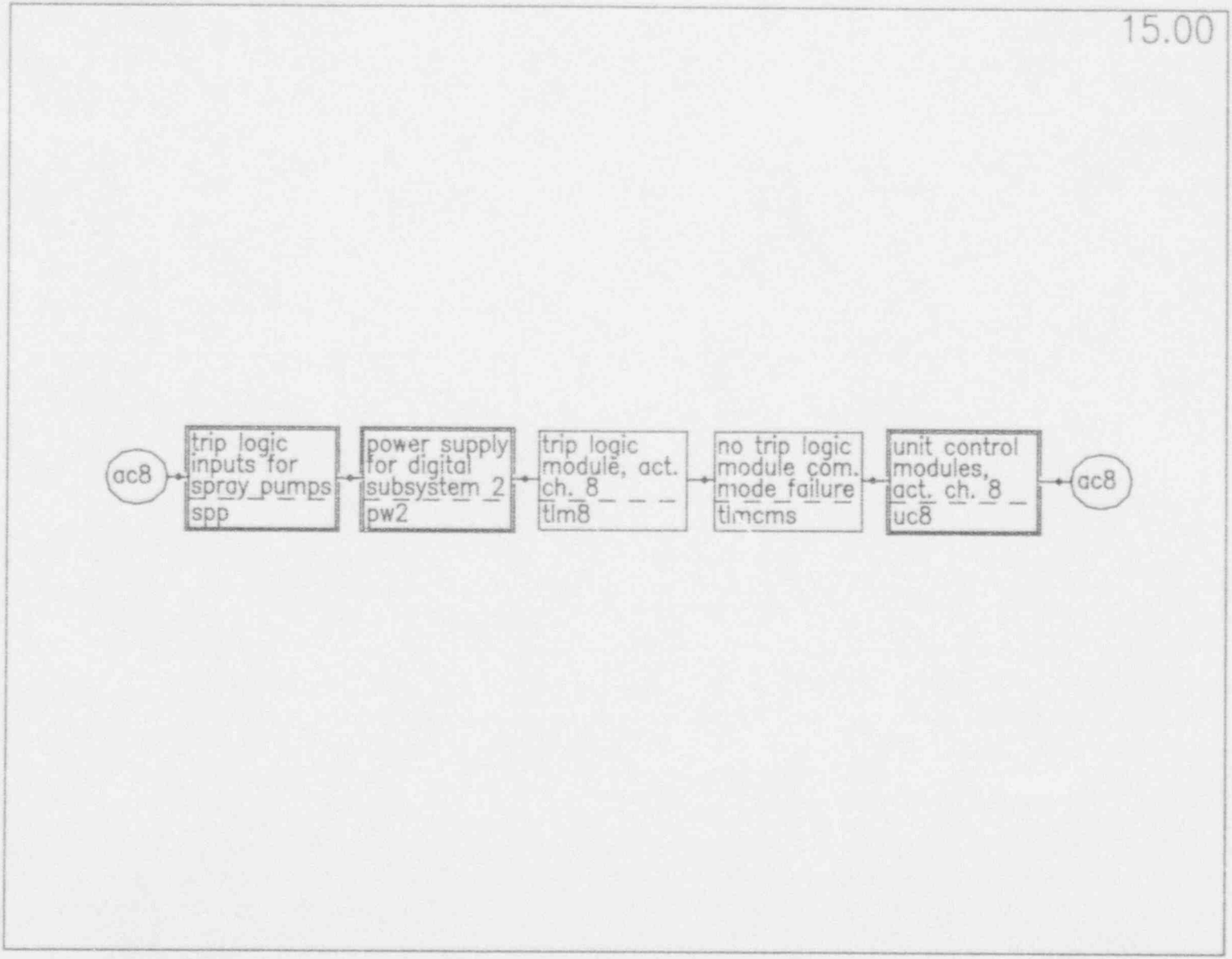
Bailey ESFAS (ANO-1 & Oconee)

13.00

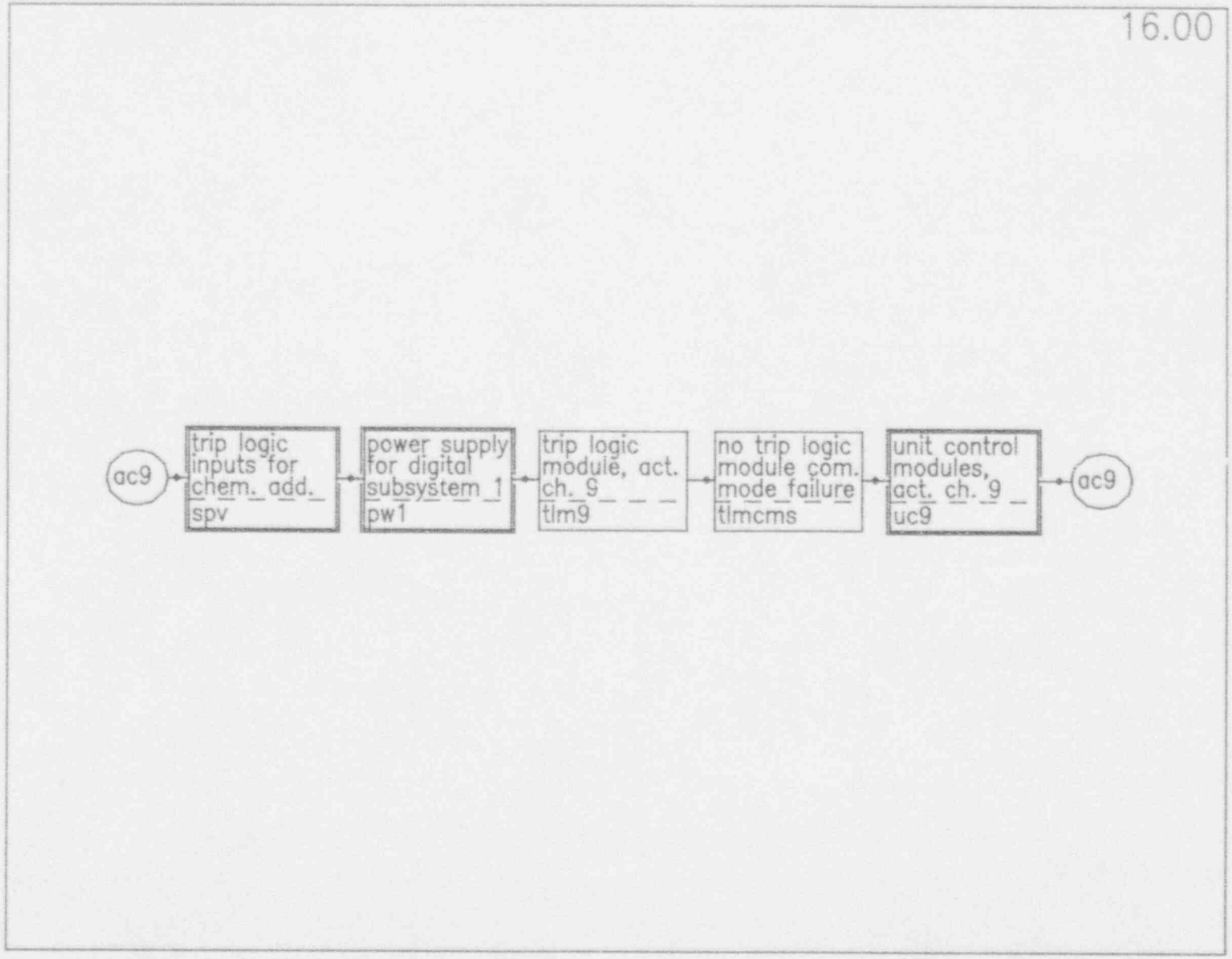

uc6
unit control
mod. 6.3.9
act. ch. 6
ucm6a
unit control
mod. 6.3.11
act. ch. 6
ucm6b
unit control
mod. 6.3.13
act. ch. 6
ucm6c
unit control
mod 6.4.9
act. ch. 6
ucm6d
A6
P. 13
A6
P. 13
unit control
mod. 6.4.11
act. ch. 6
ucm6e
no unit con.
module com.
mode failure
ucmcmi
uc6



Bailey ESFAS (ANO-1 & Oconee)

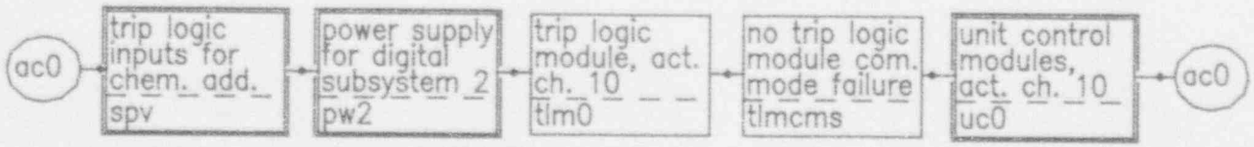


Bailey ESFAS (ANO-1 & Oconee)

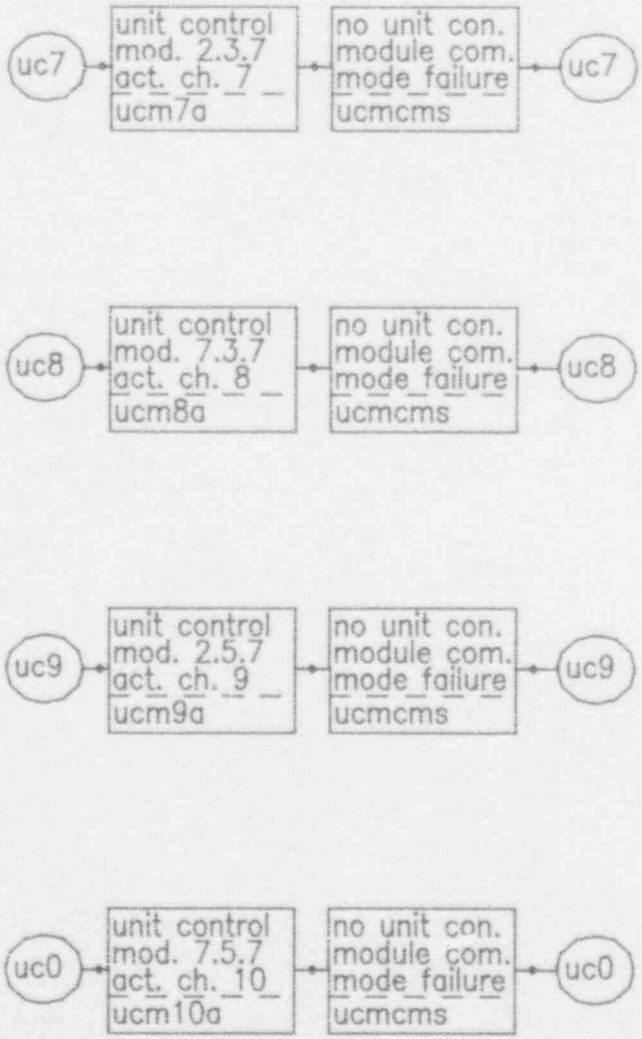


Bailey ESFAS (ANO-1 & Oconee)

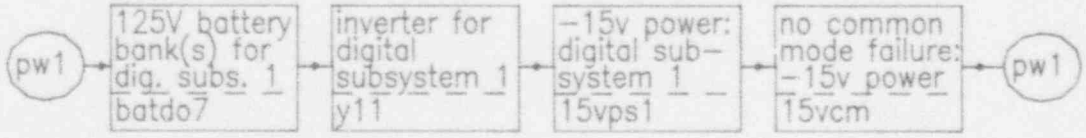
17.00



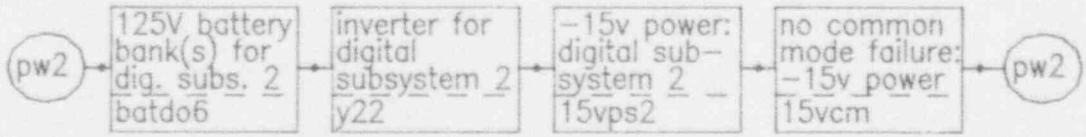
Bailey ESFAS (ANO-1 & Oconee)



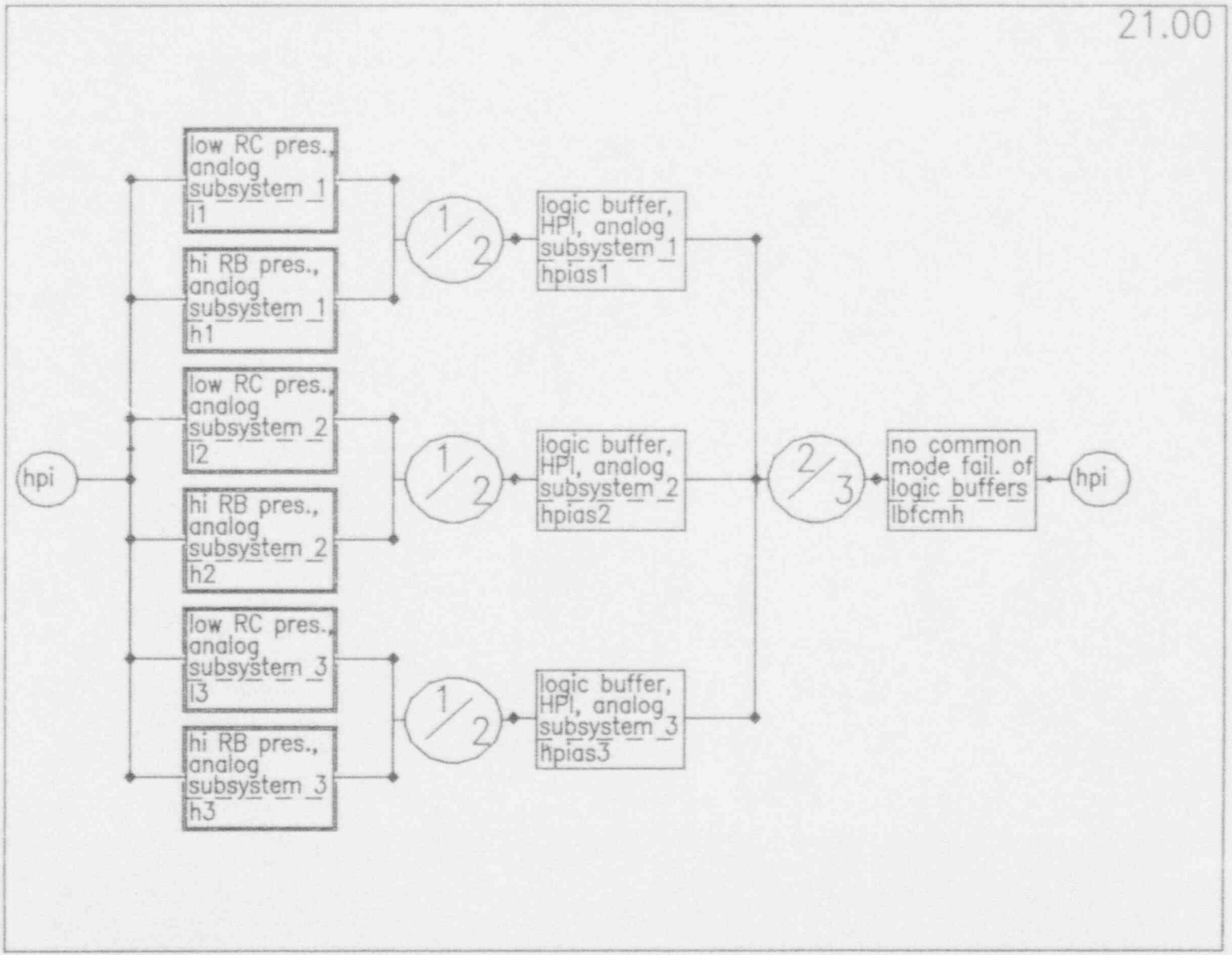
Bailey ESFAS (ANO-1 & Oconee)



NOTE: For ANO, battery is DO7.
For Oconee-1, redundant batteries are 1CA and 2CA. Inverters are Y11 for ANO and 1DIA for Oconee-1.
Oconee-2,3 are similar.

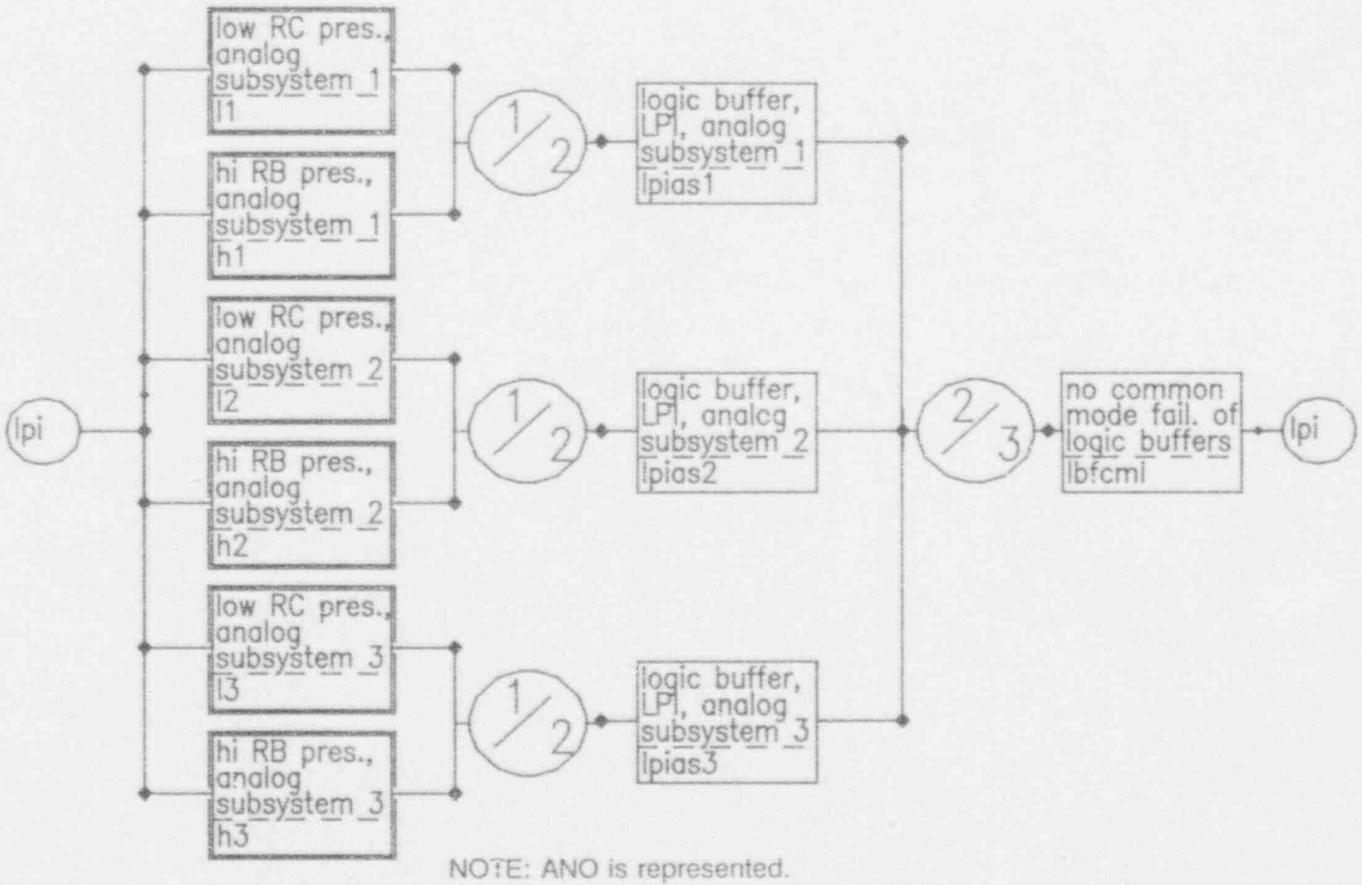


NOTE: For ANO, battery is DO6.
For Oconee-1, redundant batteries are 1CA and 2CB. Inverters are Y22 for ANO and 1DIB for Oconee-1.
Oconee-2,3 are similar.



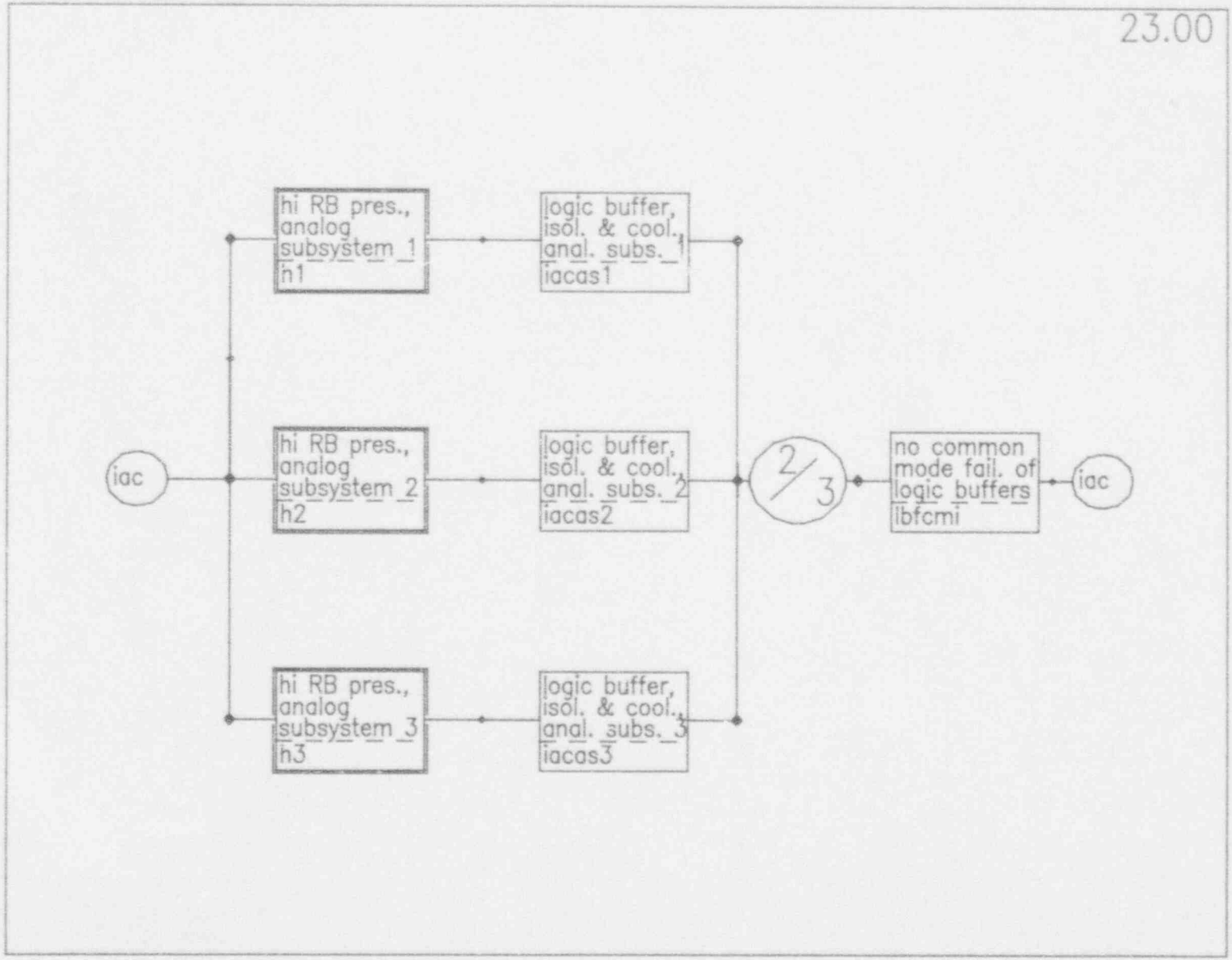
Bailey ESFAS (ANO-1 & Oconee)

22.00

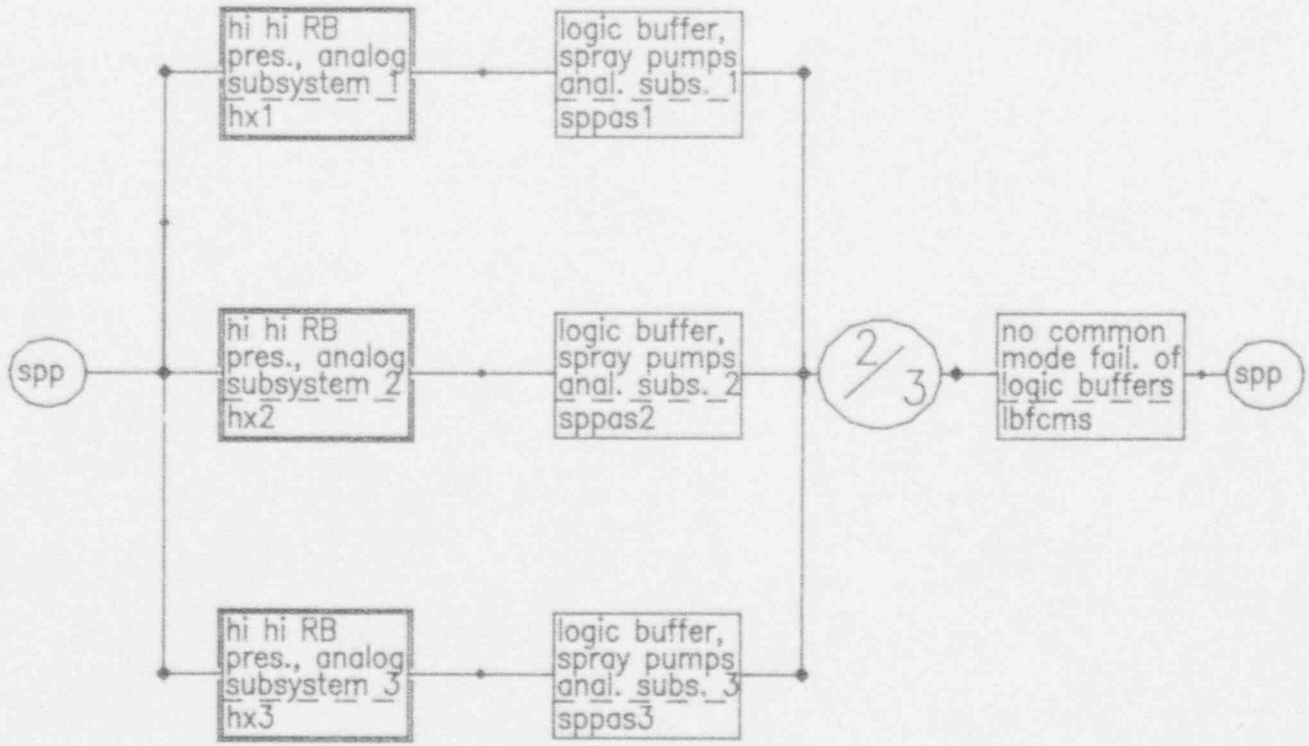


NOTE: ANO is represented.
RC pressure setpoint is low-low for Oconee LPI.

Bailey ESFAS (ANO-1 & Oconee)

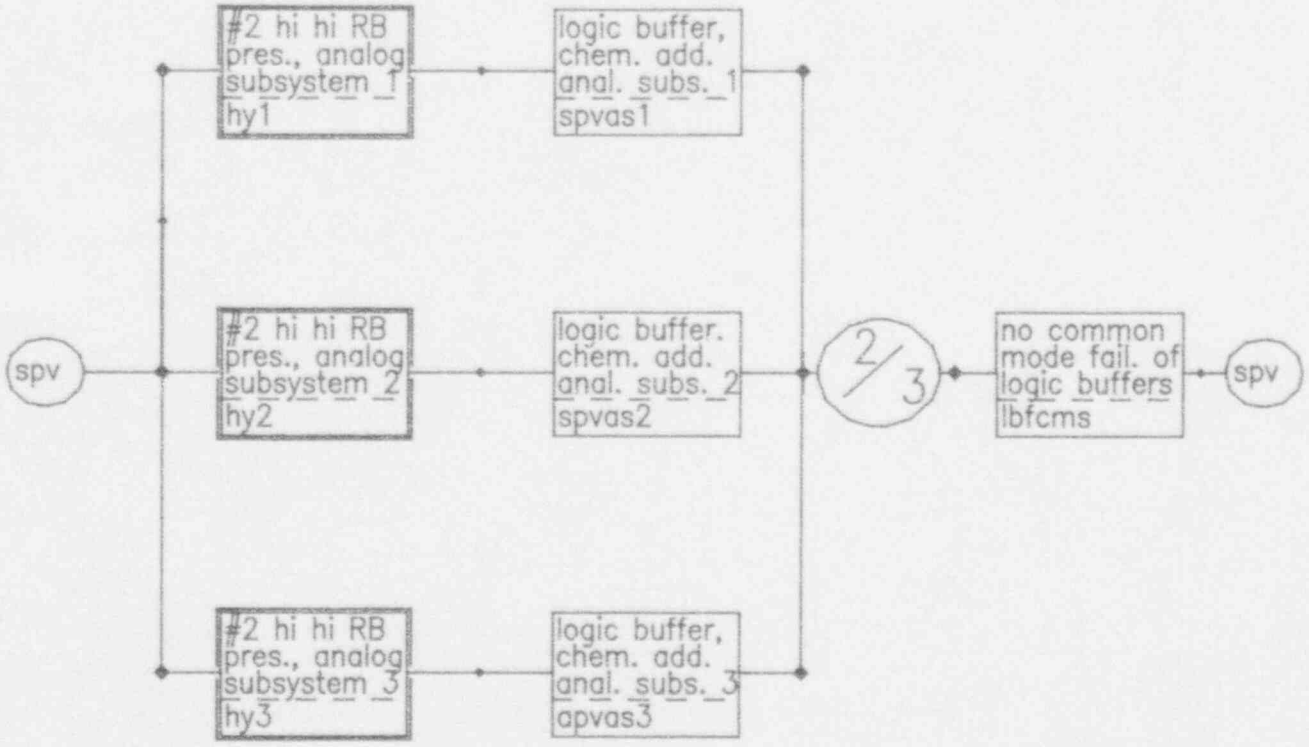


Bailey ESFAS (ANO-1 & Oconee)

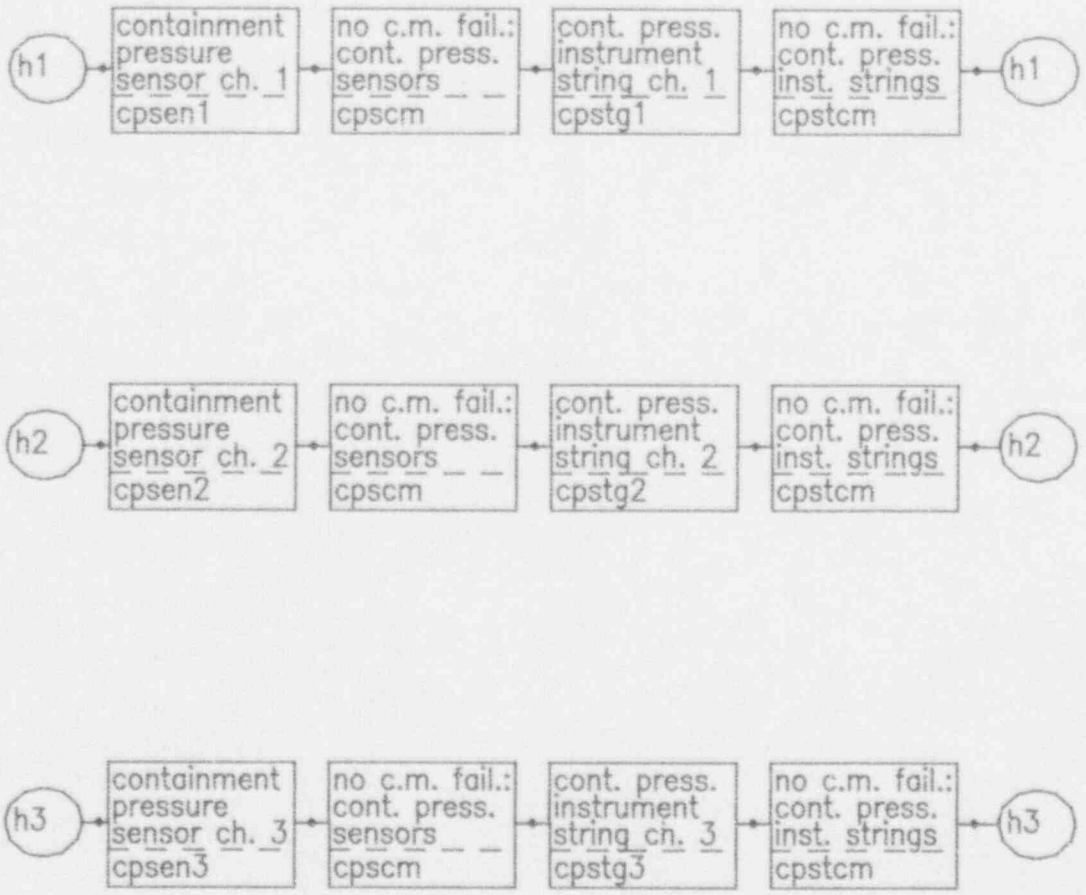


NOTE: ANO is represented. Oconee has contact buffers instead of logic buffers for RB spray actuation channels.

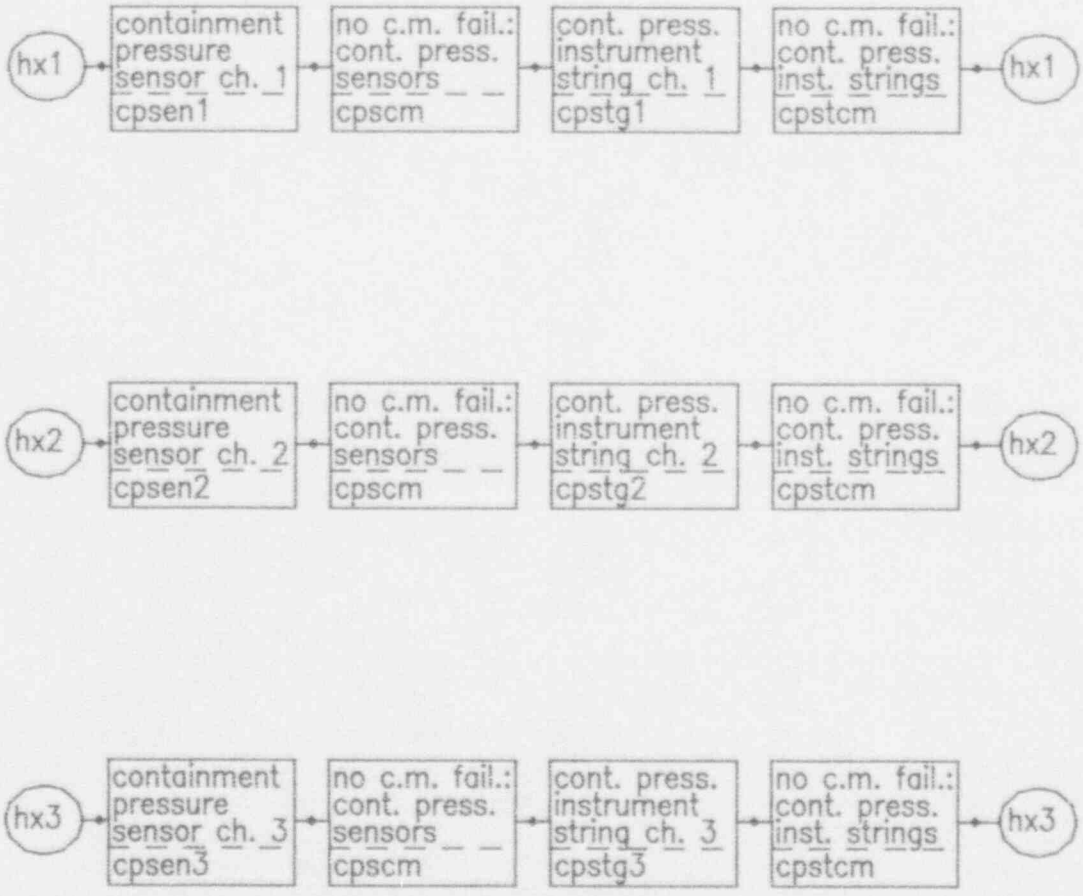
Bailey ESFAS (ANO-1 & Oconee)



Bailey ESFAS (ANO-1 & Oconee)

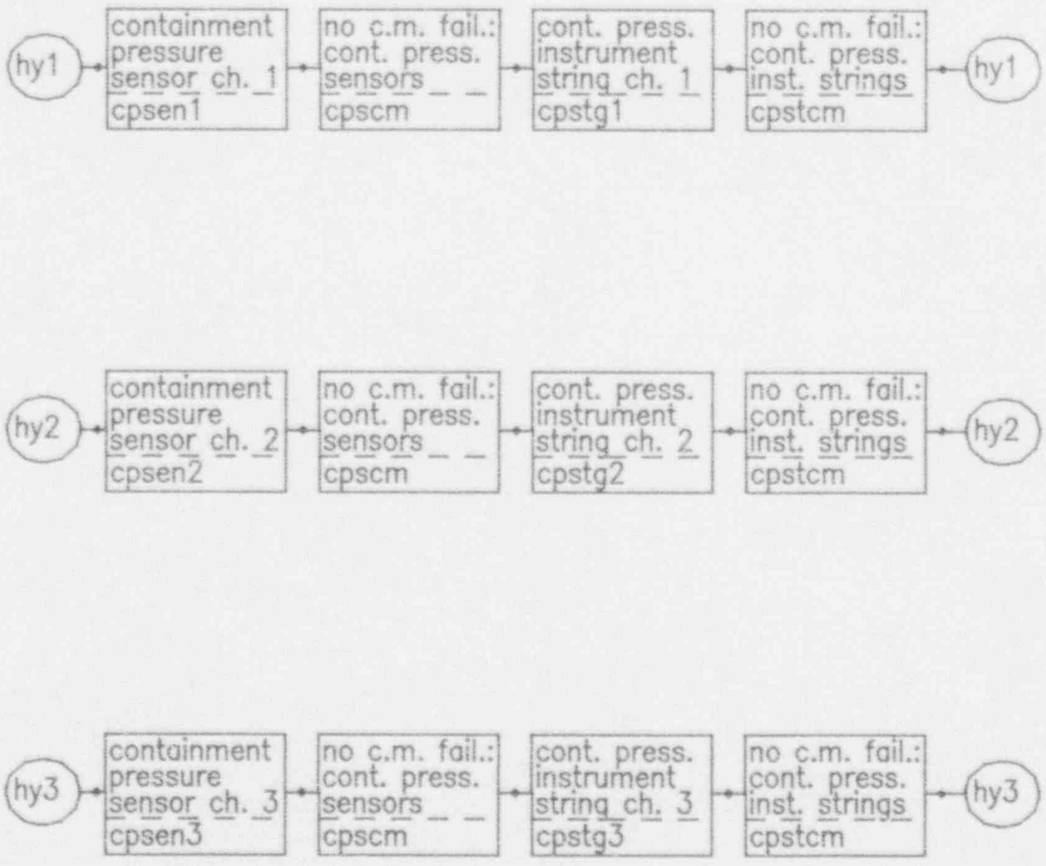


Bailey ESFAS (ANO-1 & Oconee)

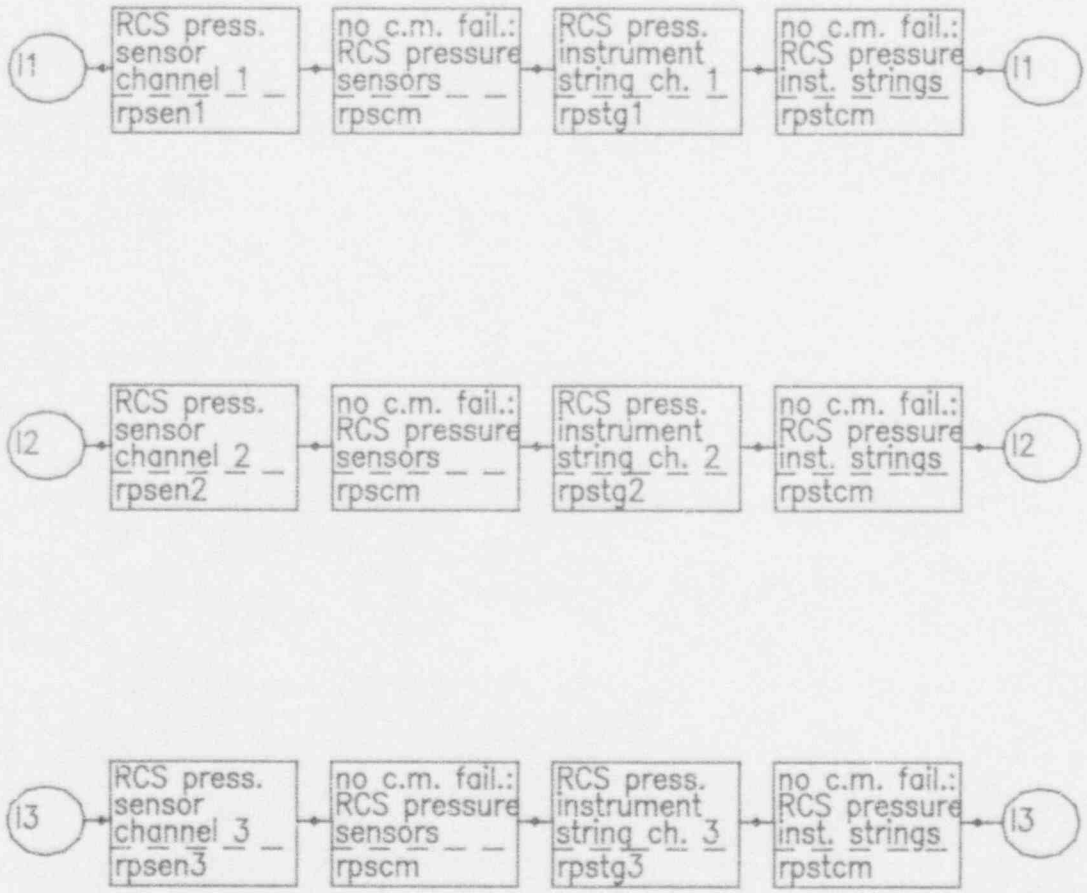


NOTE: Pictured configuration is ANO. For RB spray actuation, Oconee uses digital pressure switches instead of analog sensors.

Bailey ESFAS (ANO-1 & Oconee)



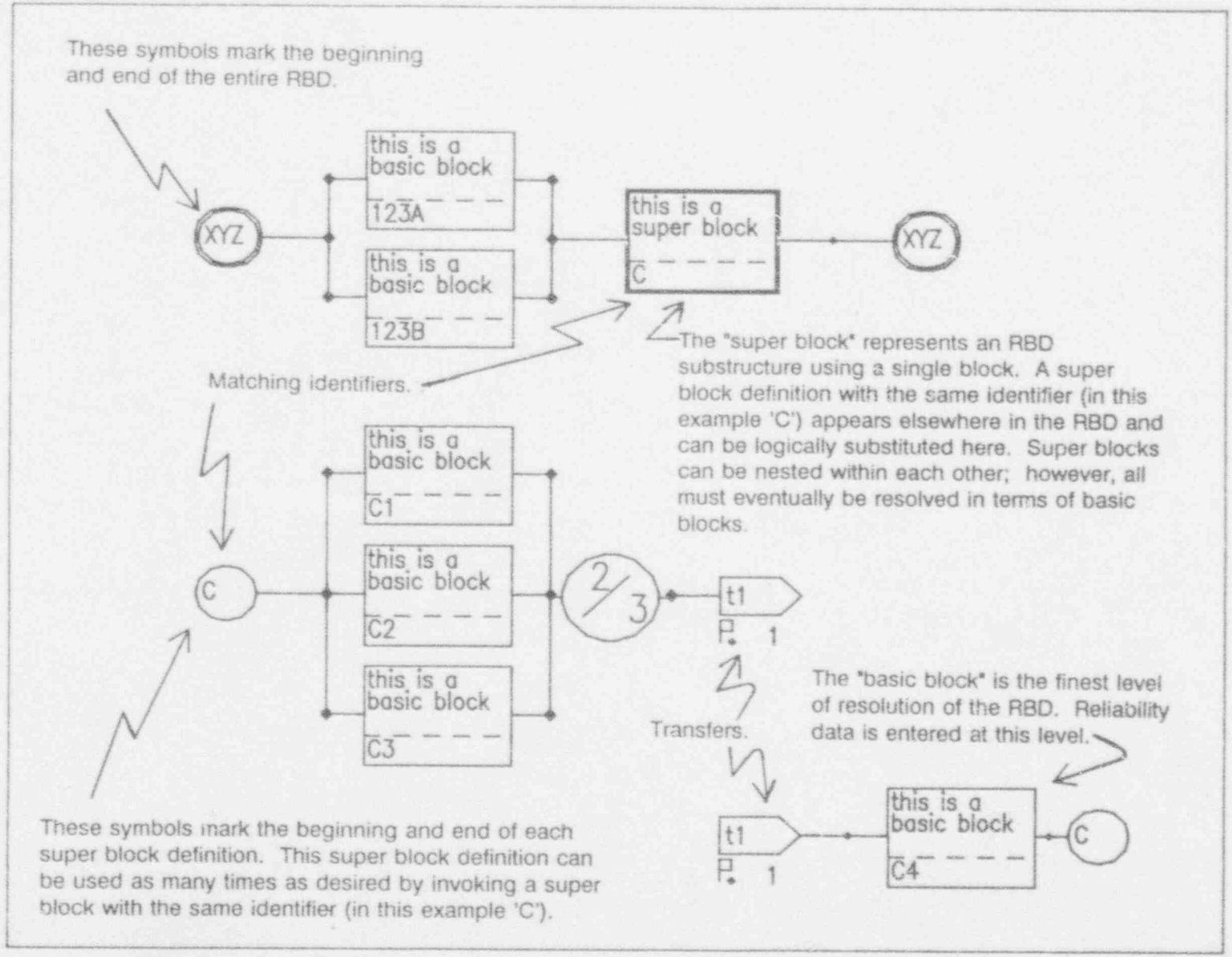
Bailey ESFAS (ANO-1 & Oconee)



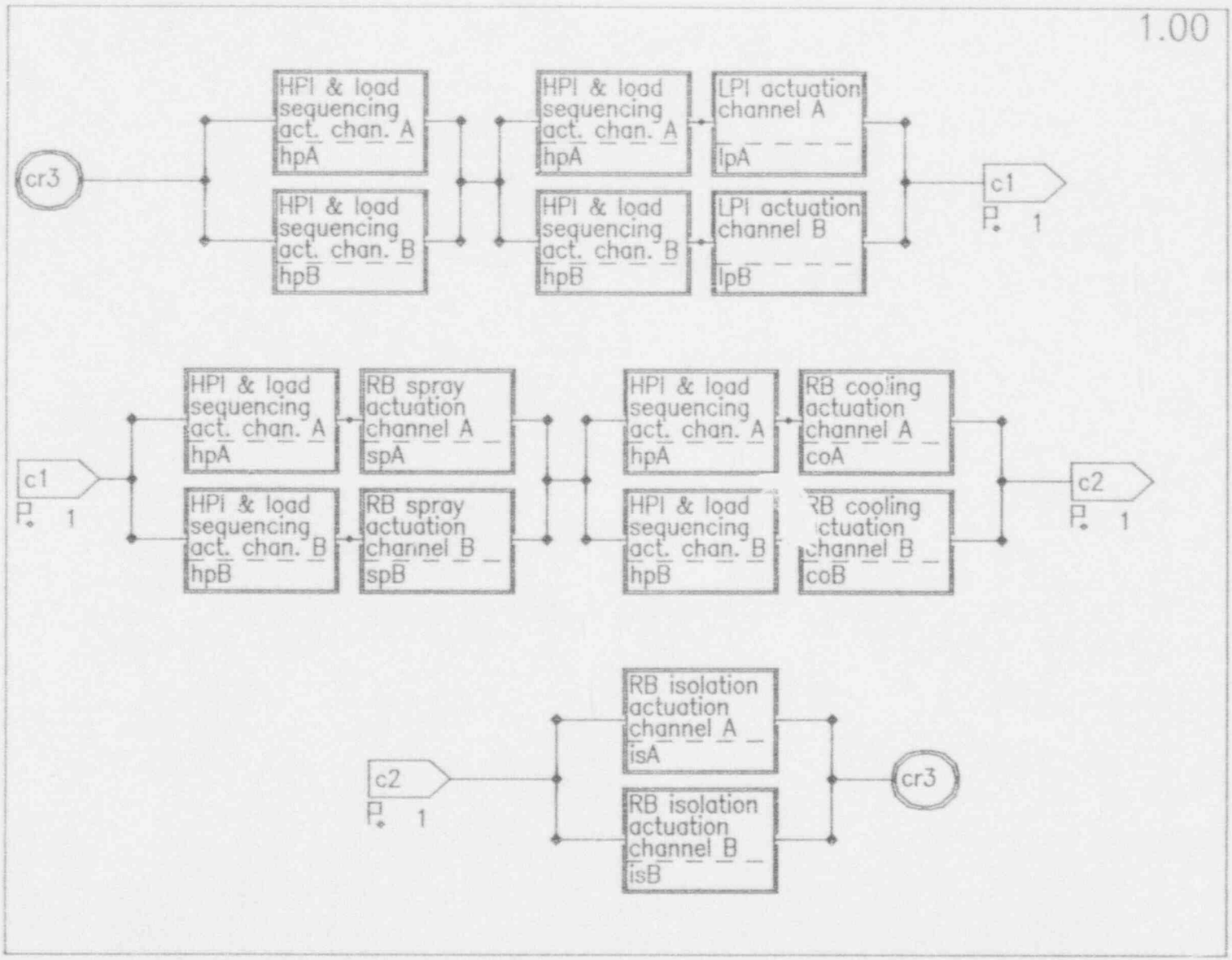
Bailey ESFAS (ANO-1 & Oconee)

APPENDIX B

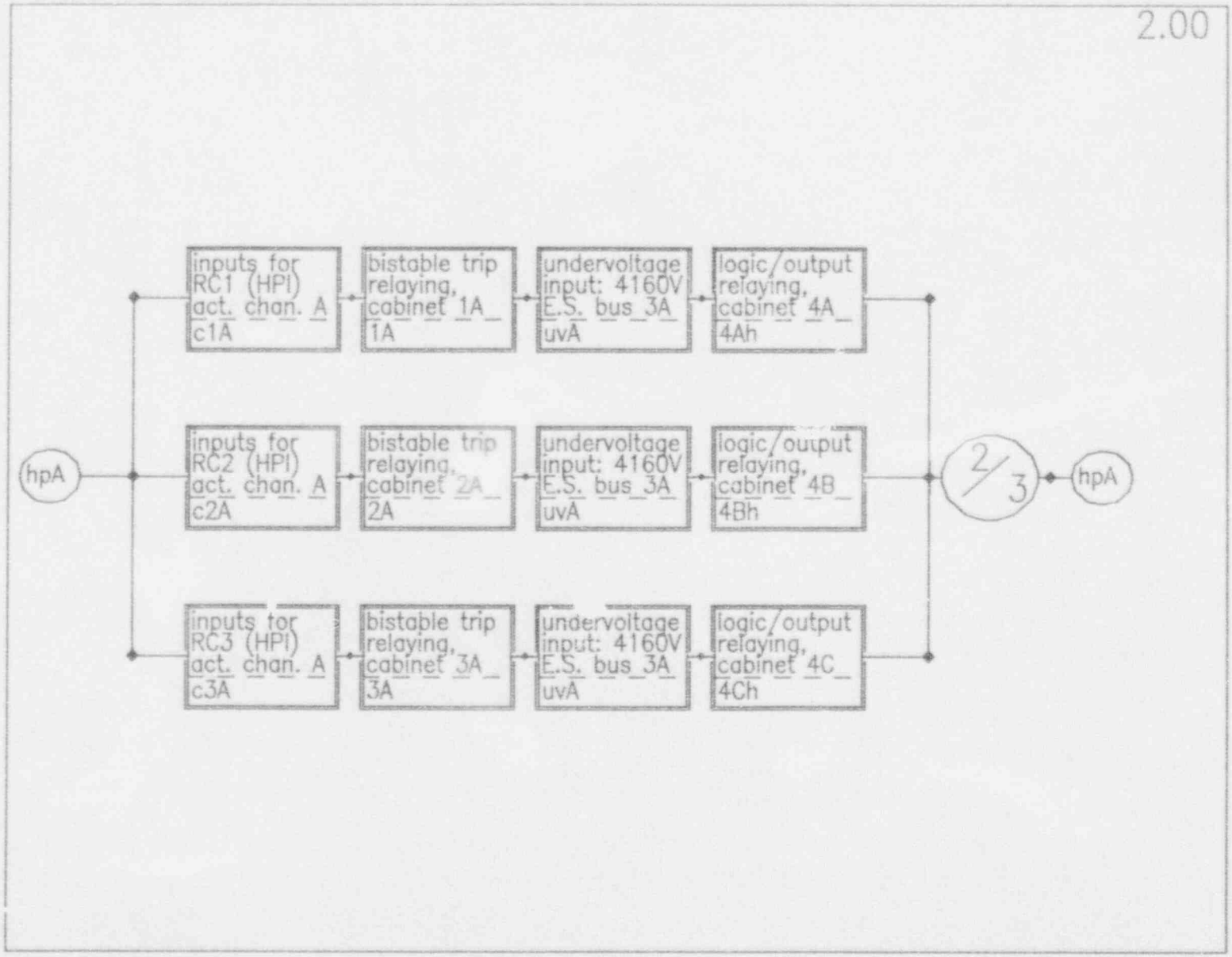
RBD for Gilbert ESFAS (Crystal River-3)



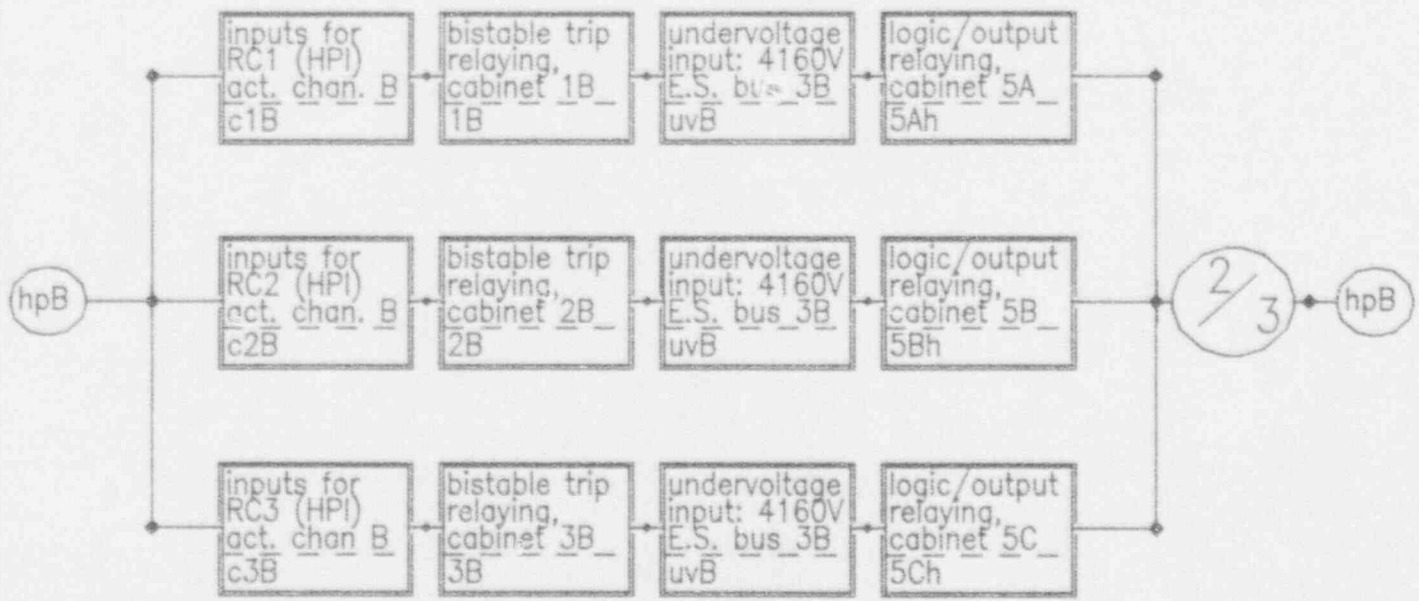
RBD Symbology Description



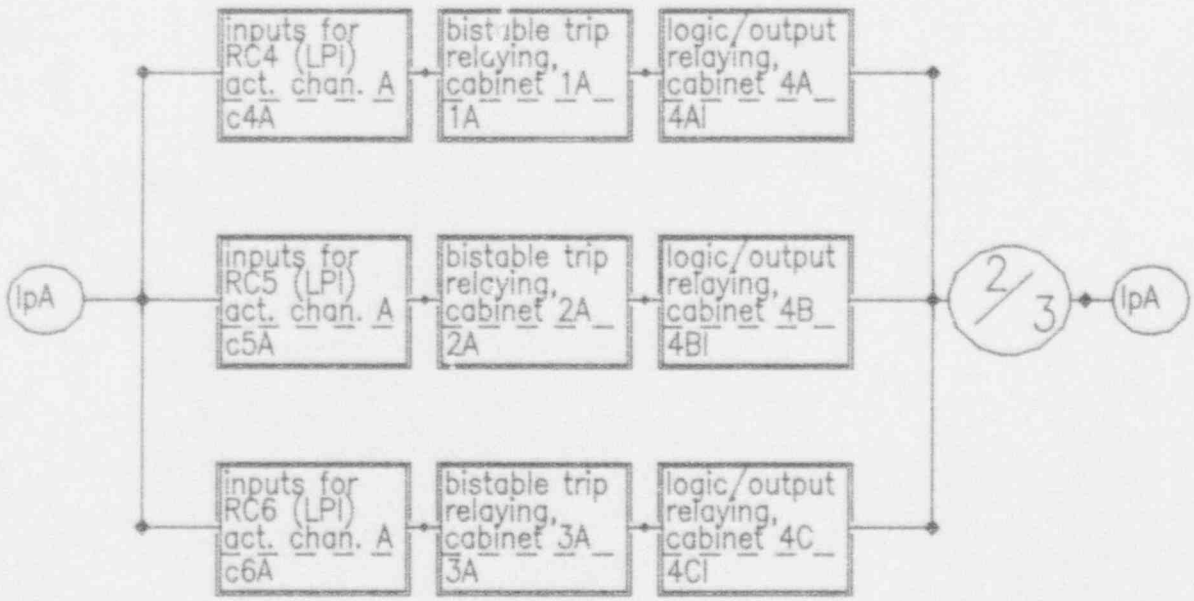
Gilbert ESFAS (Crystal River 3)



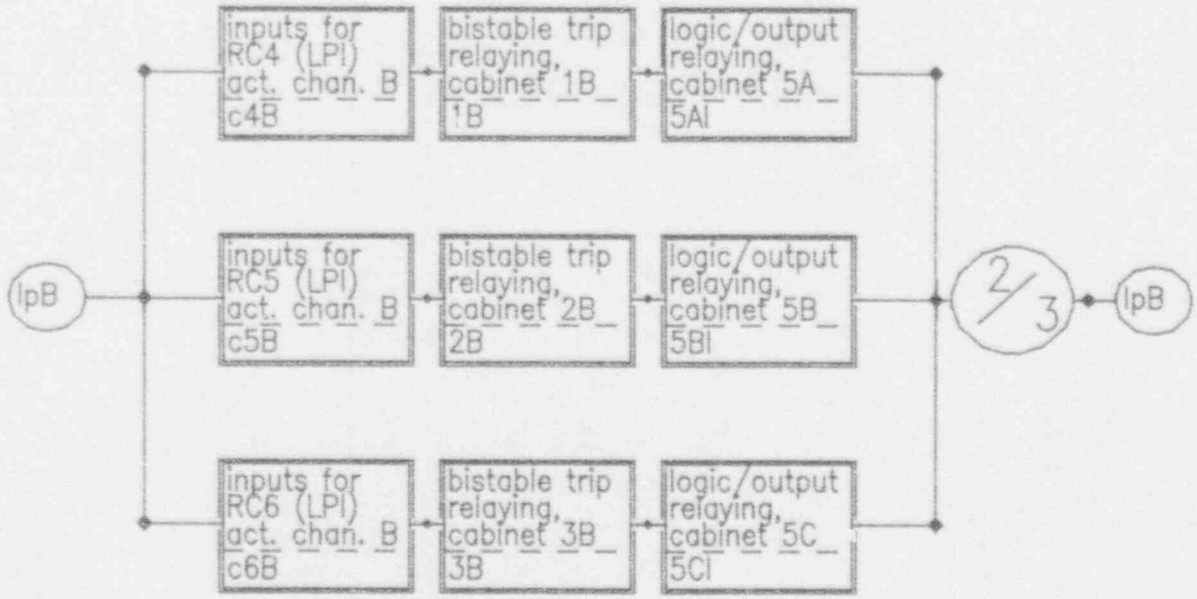
Gilbert ESFAS (Crystal River 3)



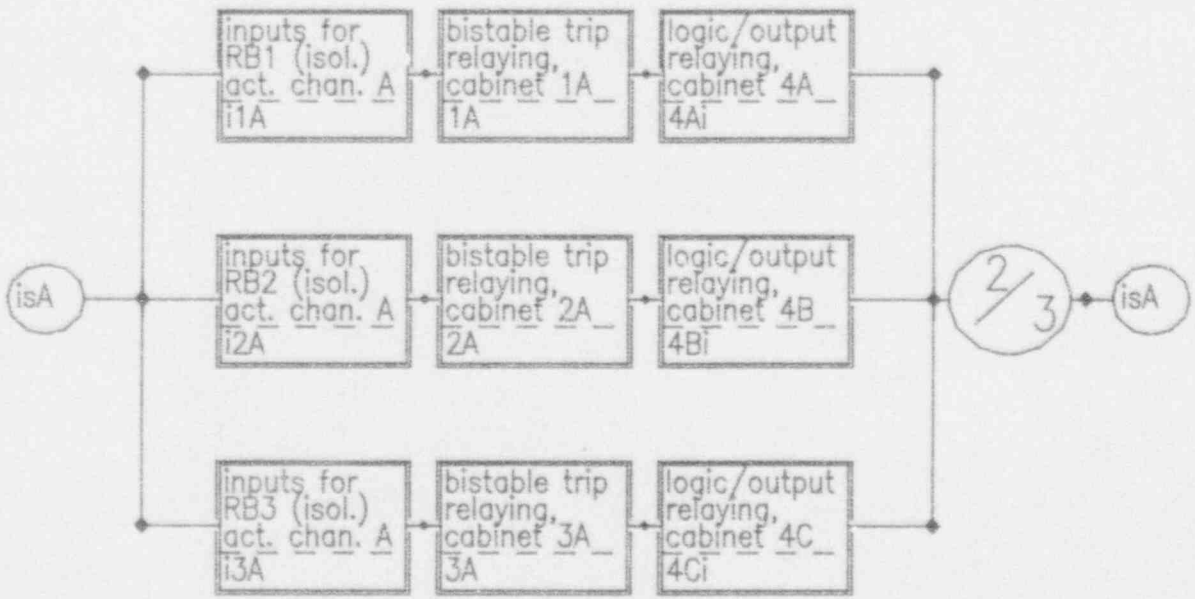
Gilbert ESFAS (Crystal River 3)



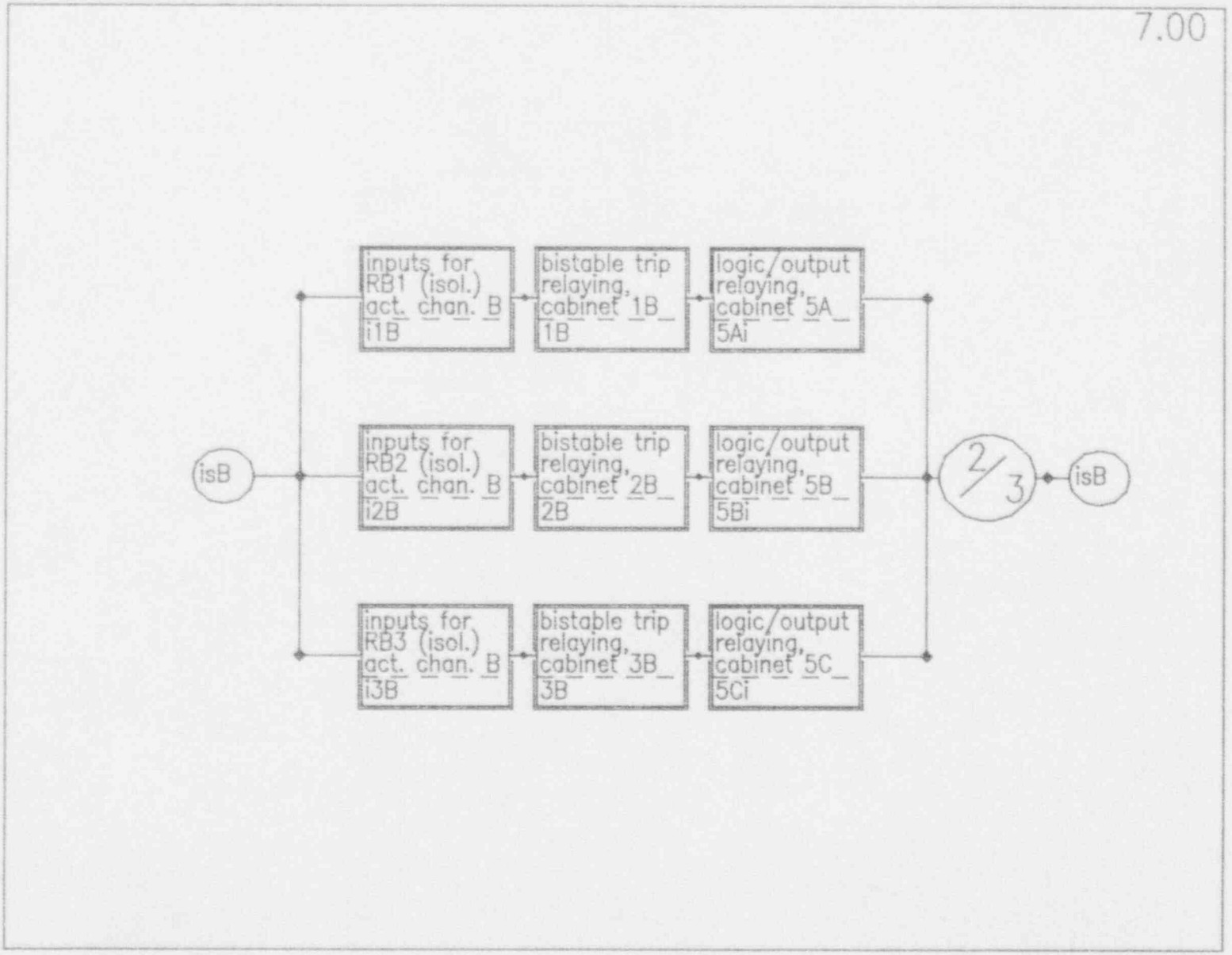
Gilbert ESFAS (Crystal River 3)



Gilbert ESFAS (Crystal River 3)

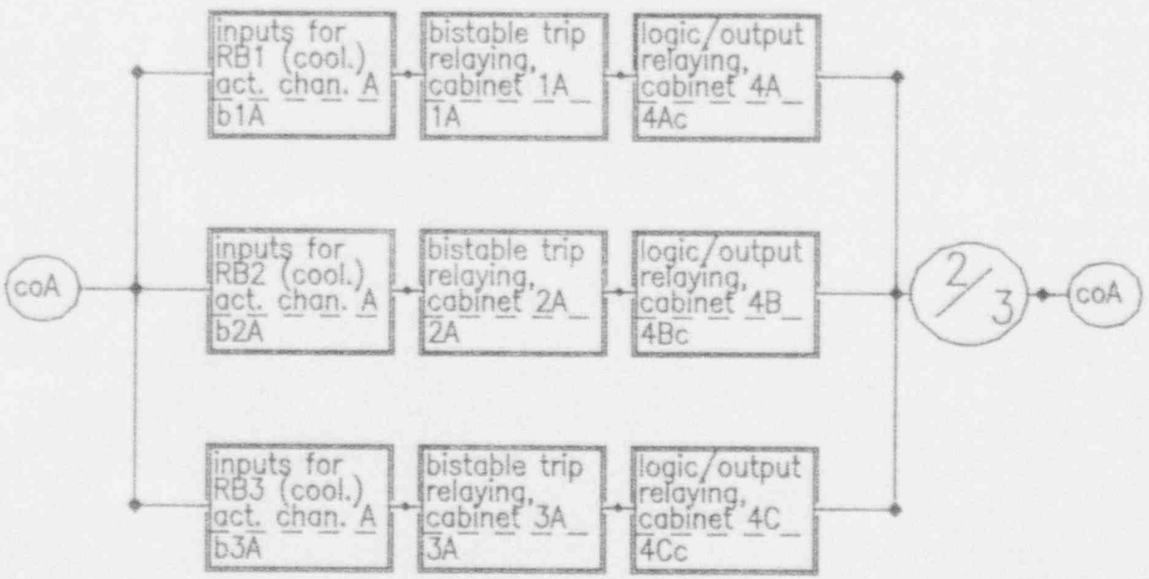


Gilbert ESFAS (Crystal River 3)



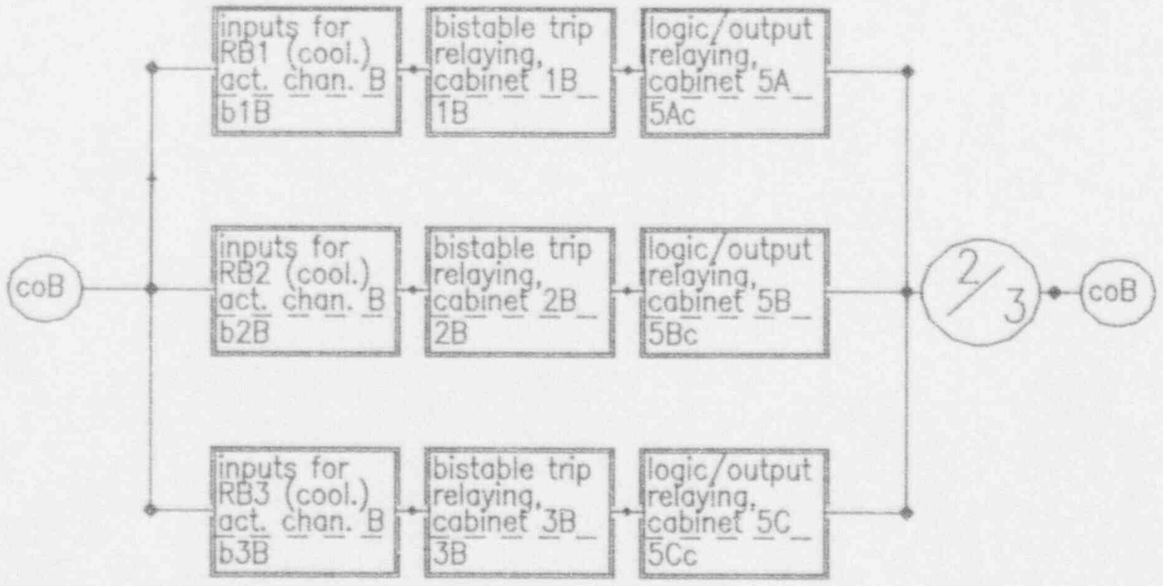
Gilbert ESFAS (Crystal River 3)

8.00

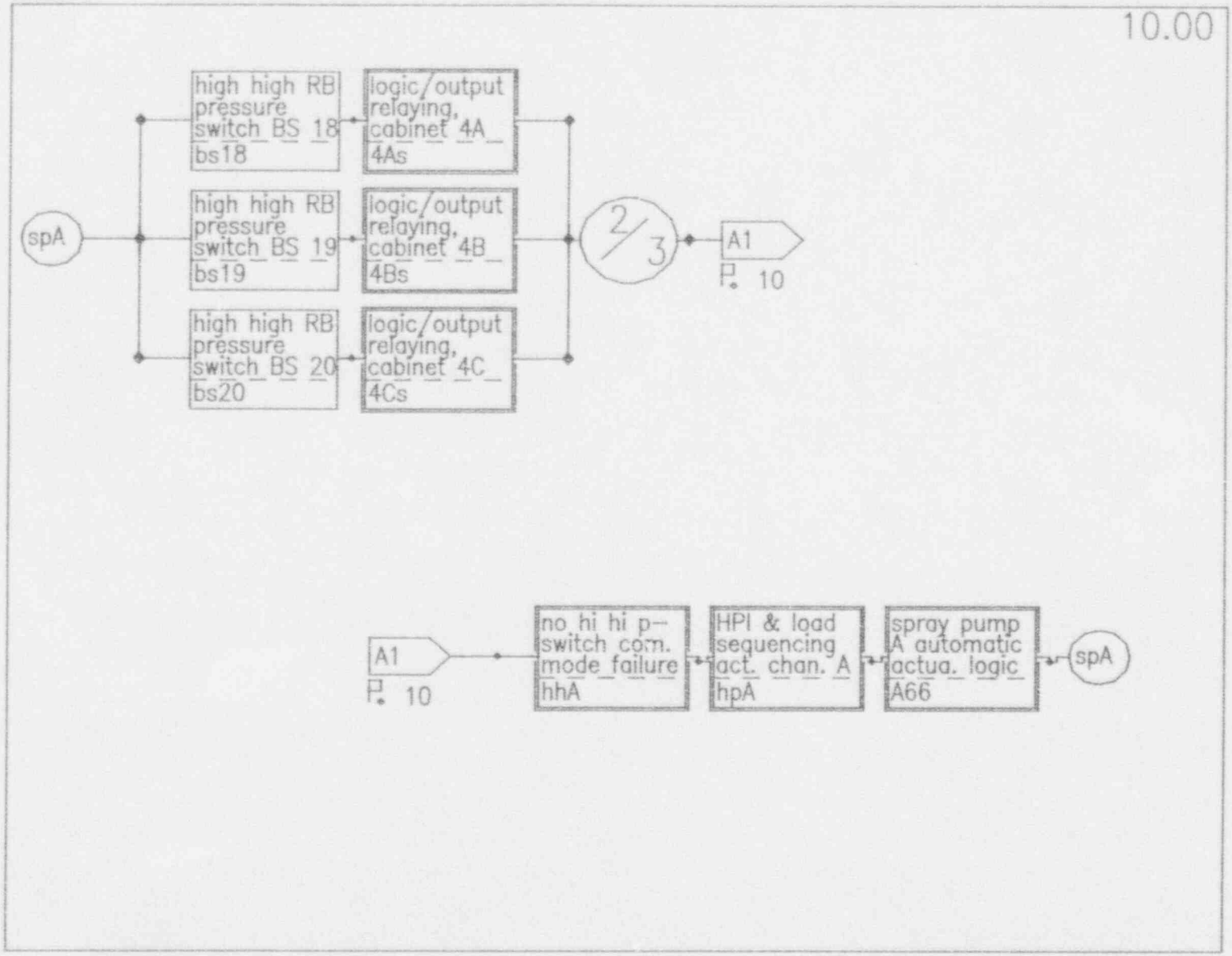


Gilbert ESFAS (Crystal River 3)

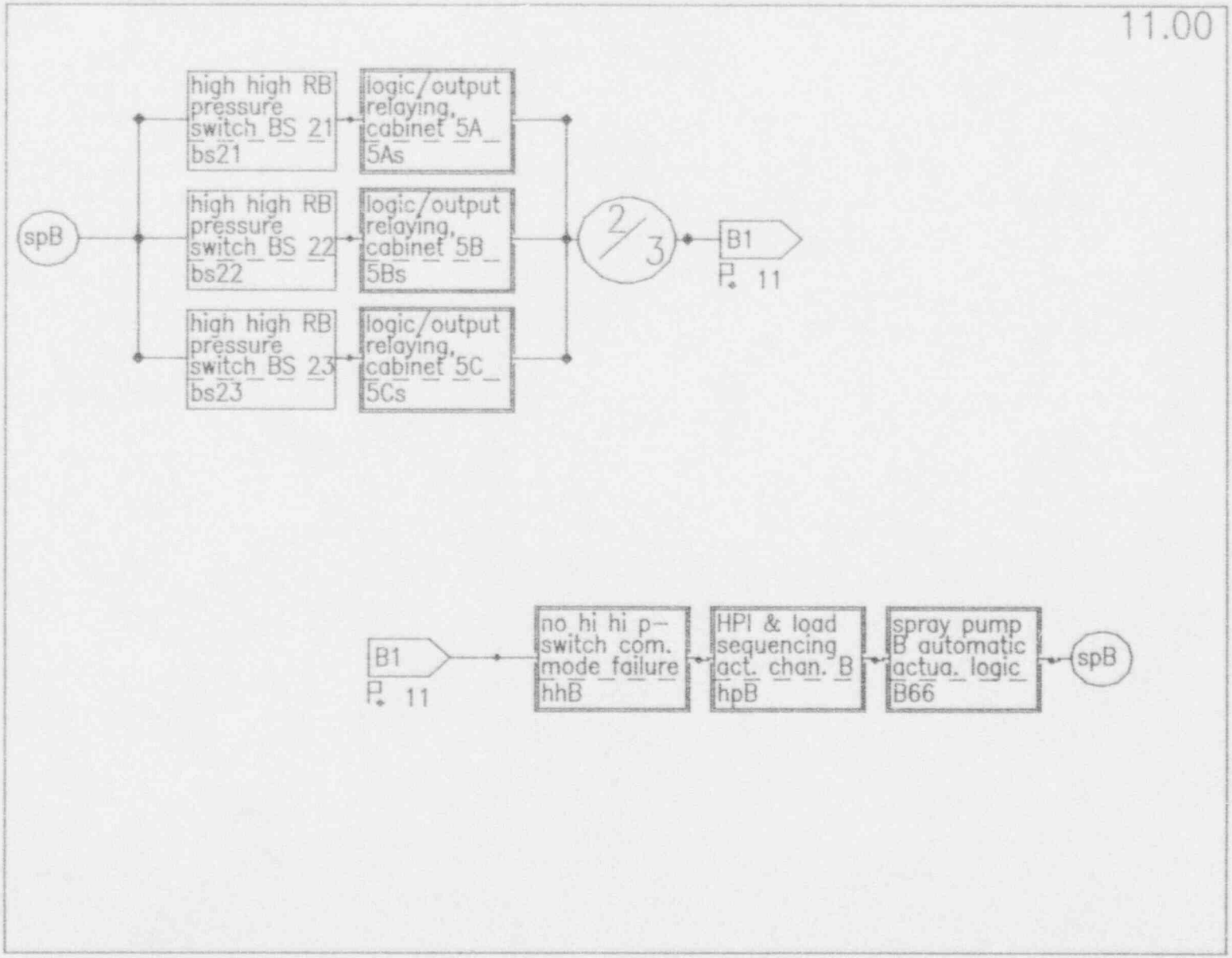
9.00



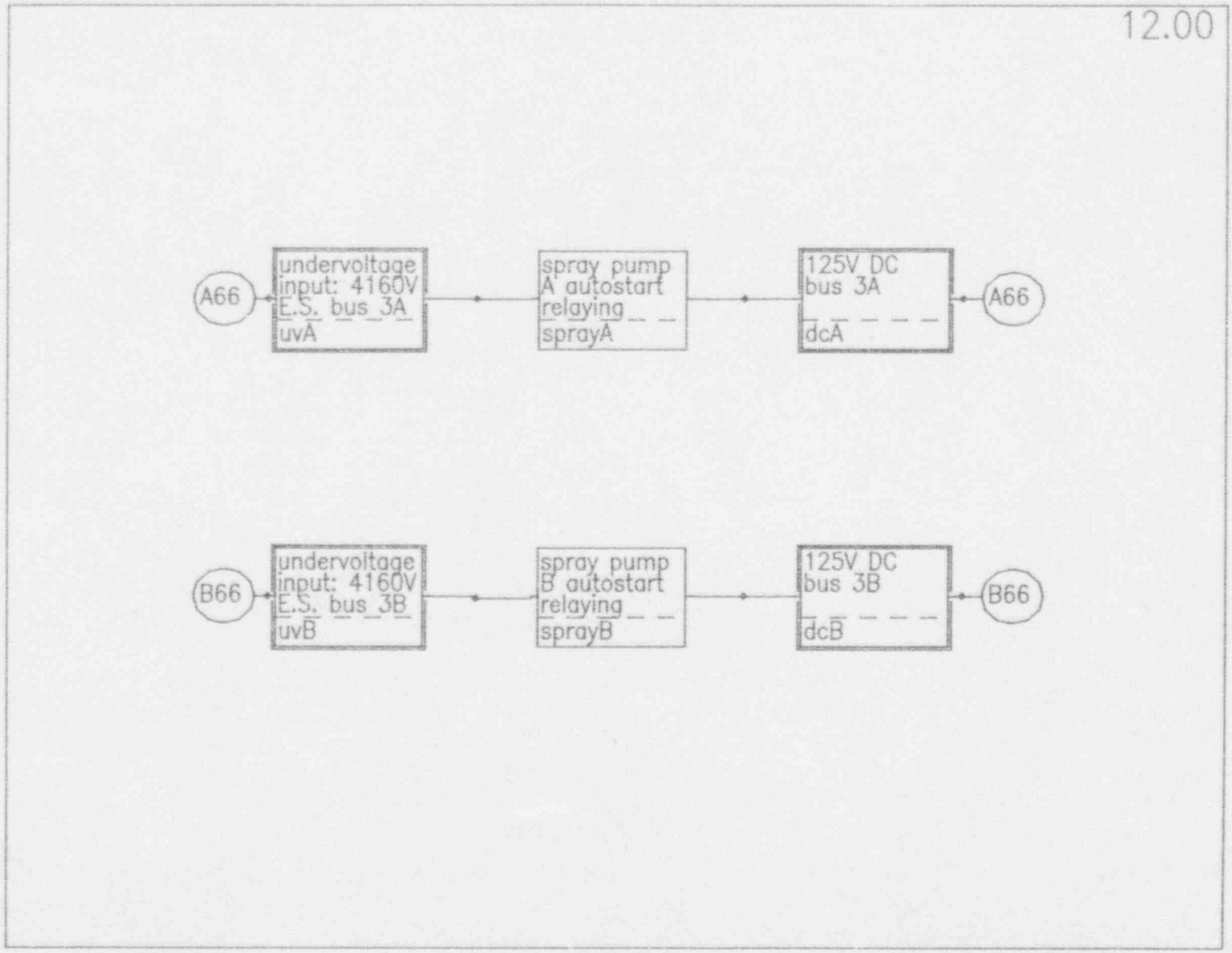
Gilbert ESFAS (Crystal River 3)



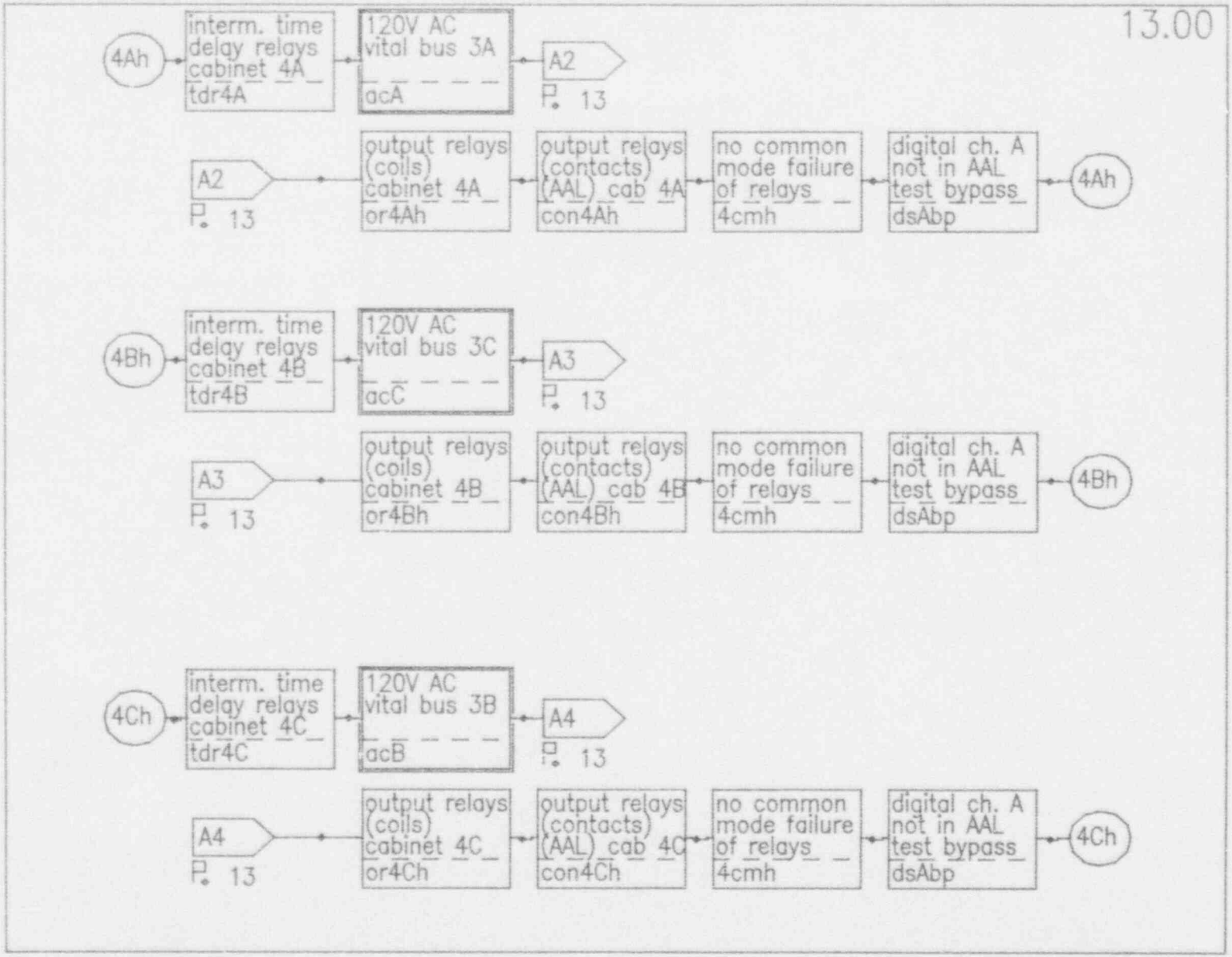
Gilbert ESFAS (Crystal River 3)



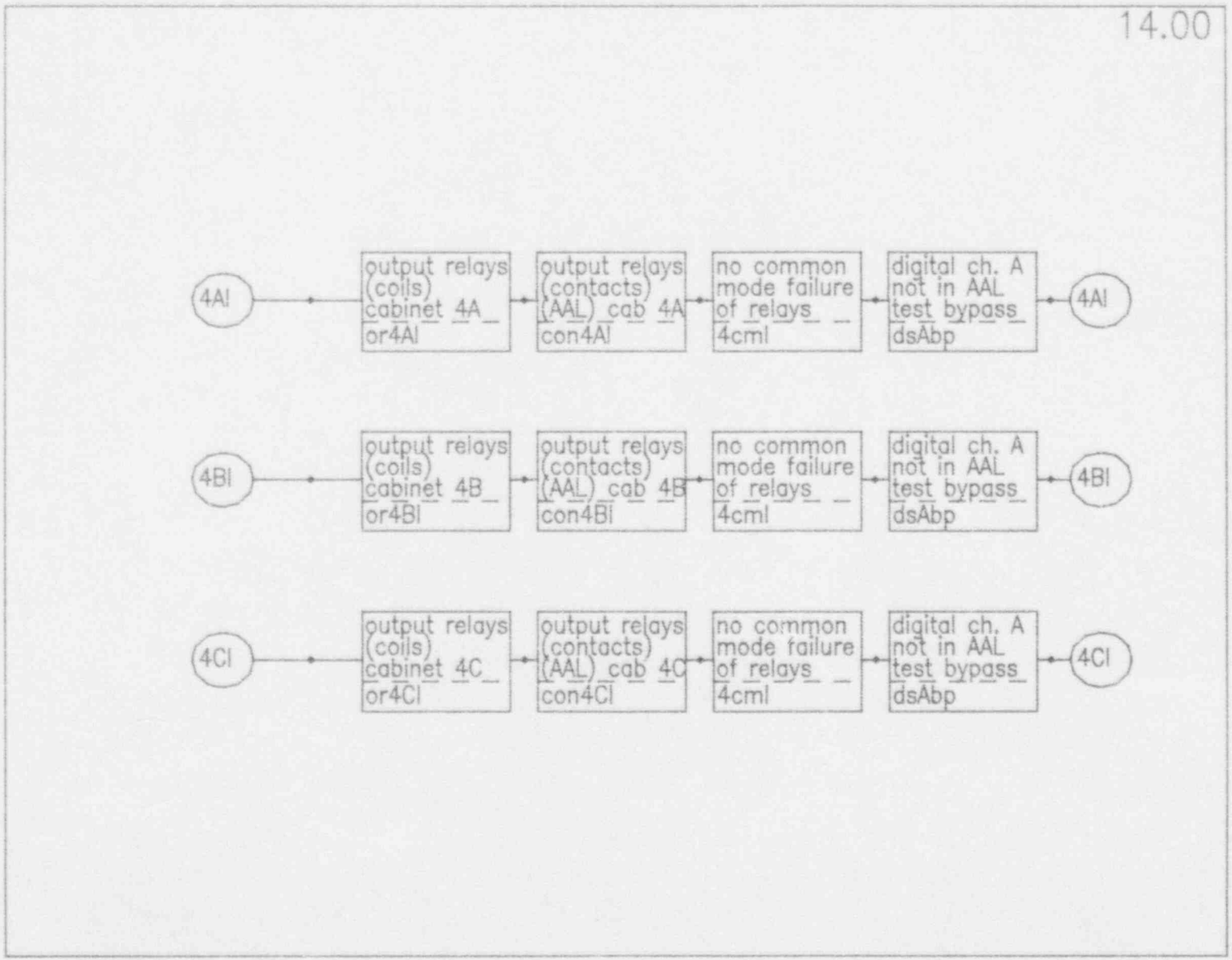
Gilbert ESFAS (Crystal River 3)



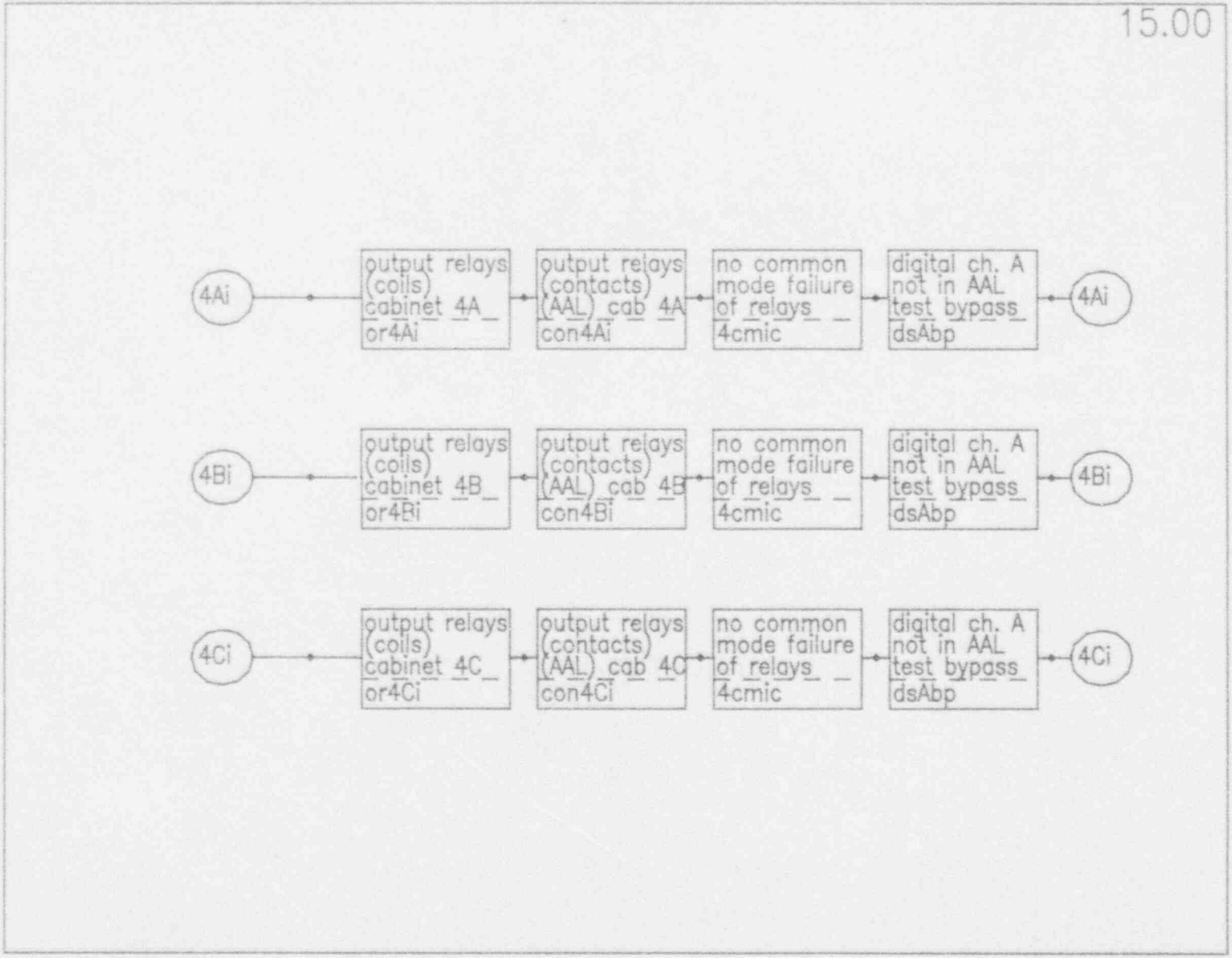
Gilbert ESFAS (Crystal River 3)



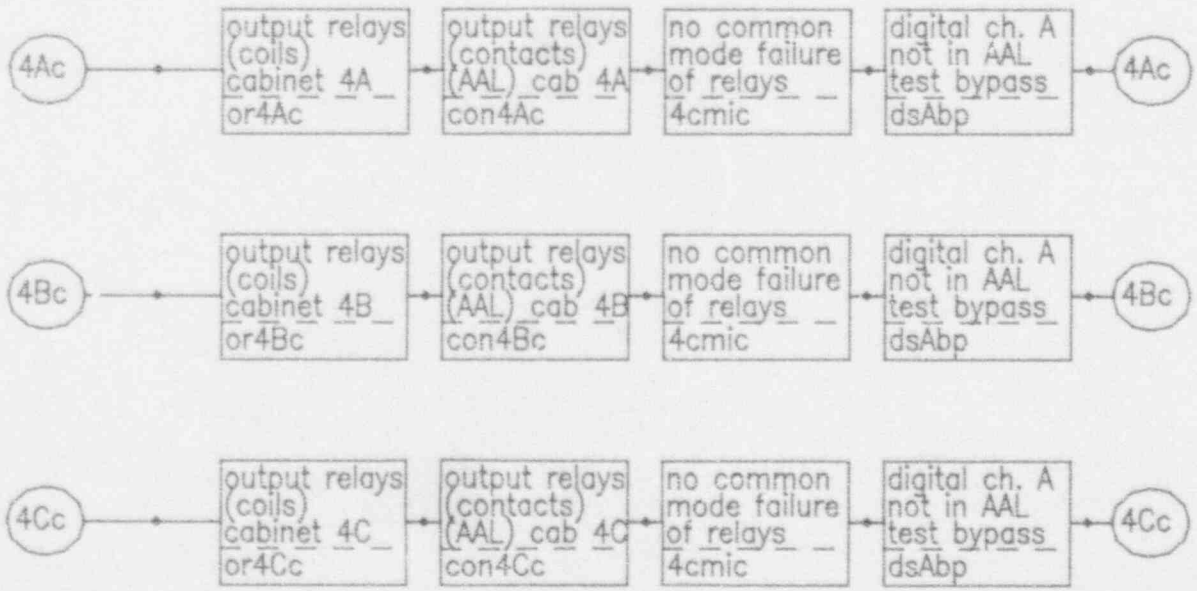
Gilbert ESFAS (Crystal River 3)

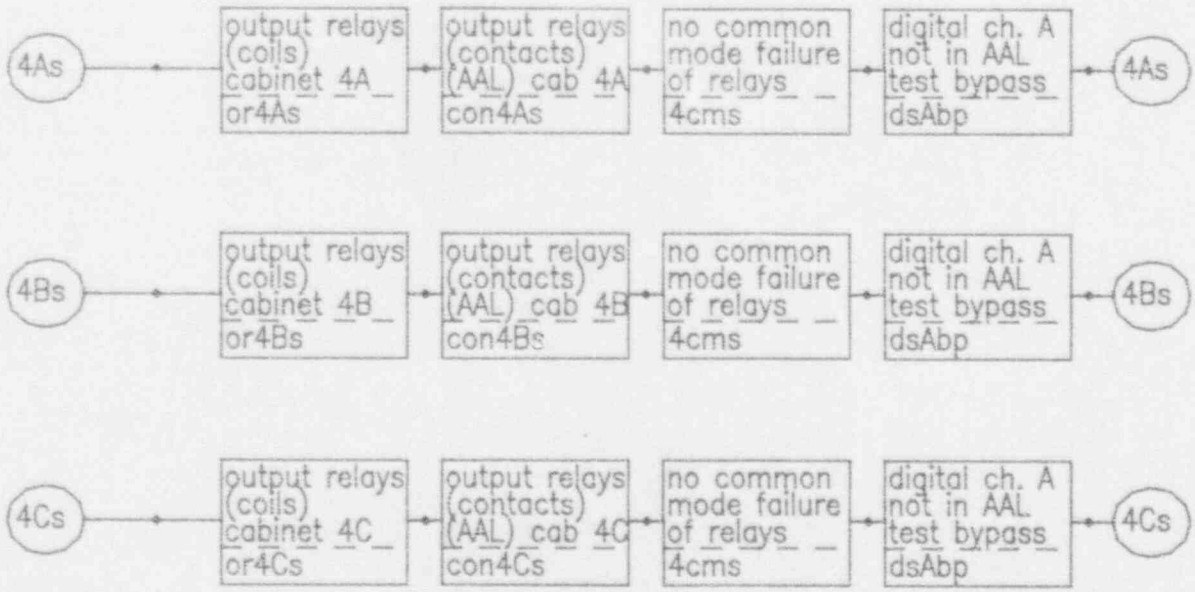


Gilbert ESFAS (Crystal River 3)

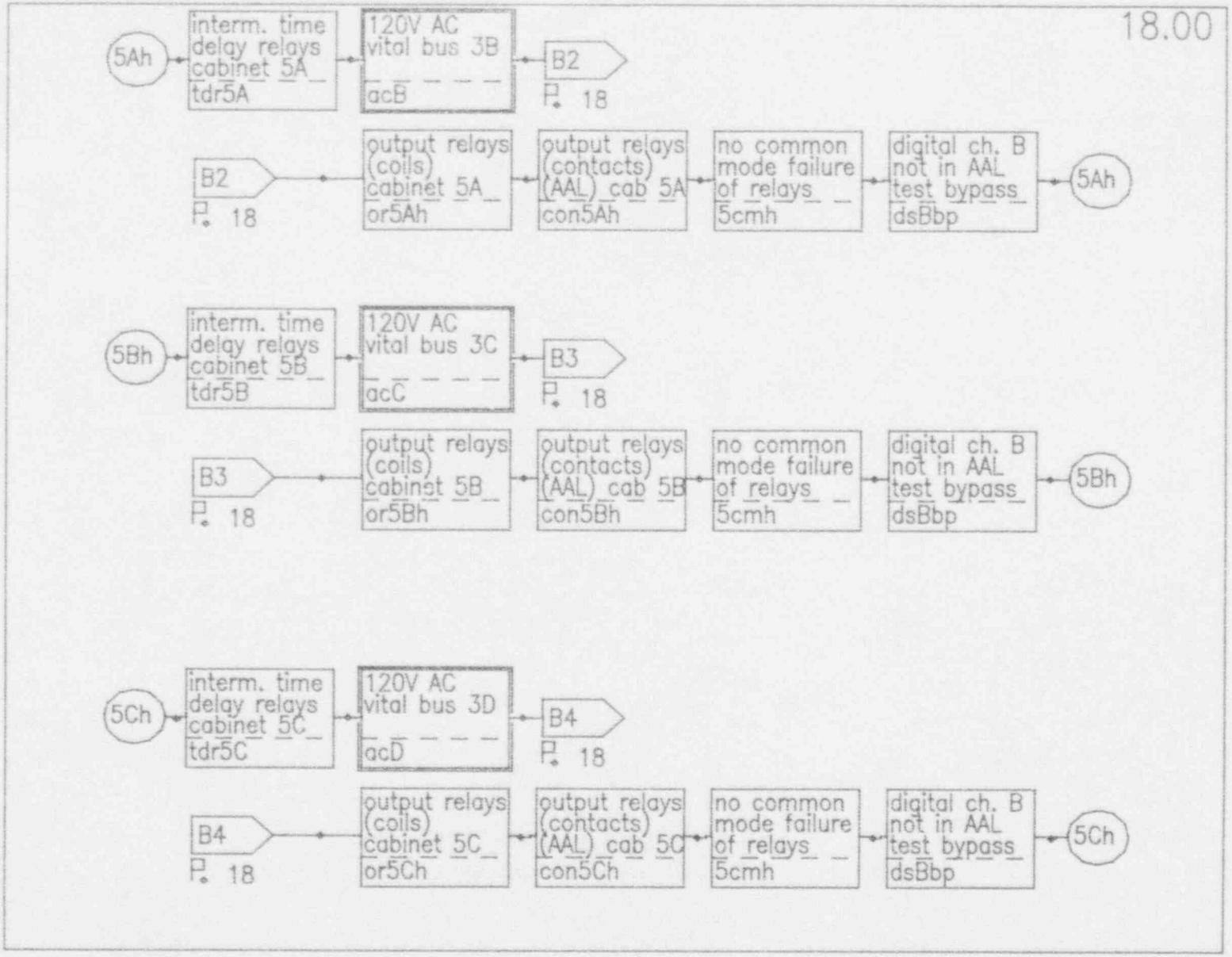


Gilbert ESFAS (Crystal River 3)

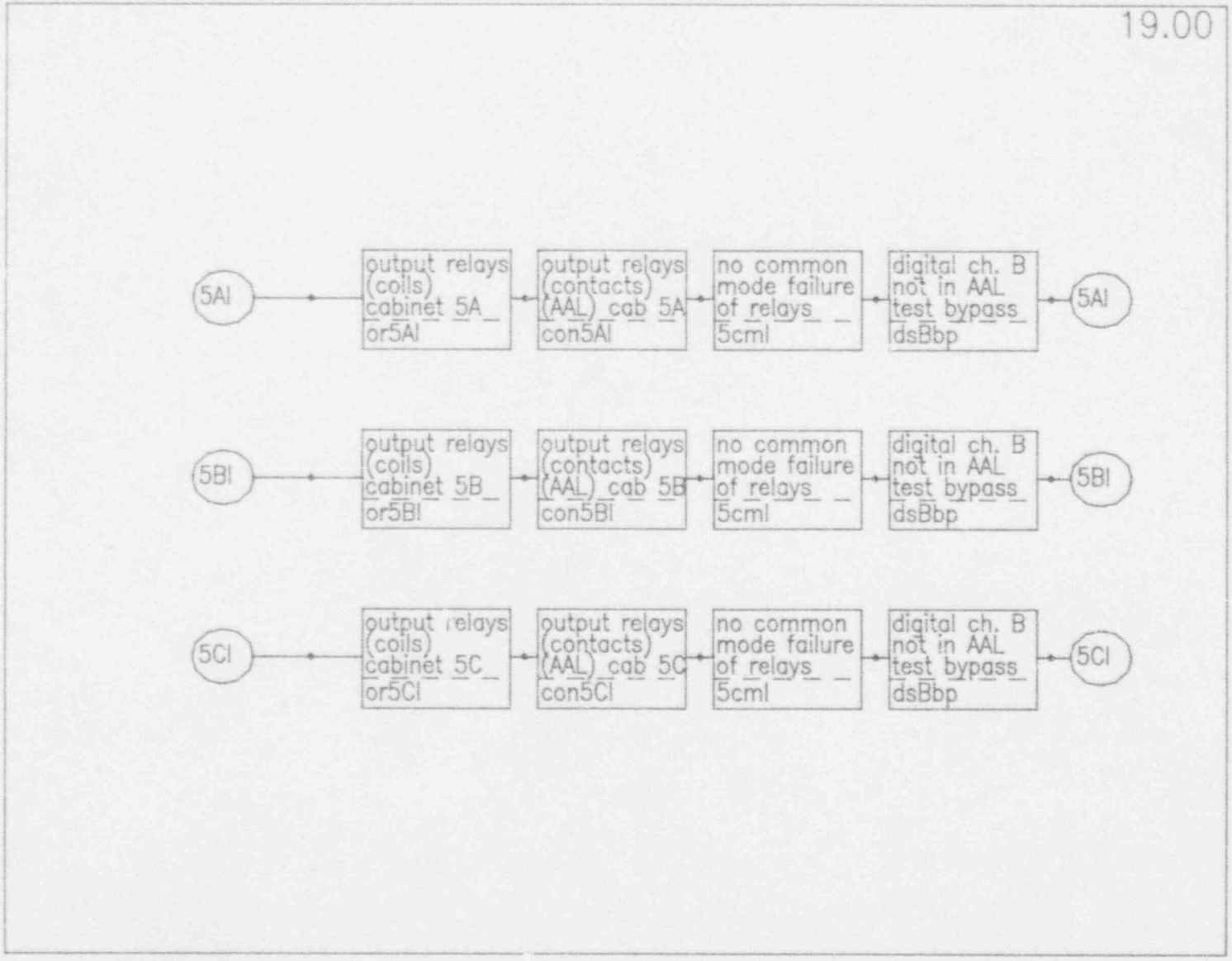

4Ac
output relays (coils) cabinet 4A_ or4Ac
output relays (contacts) (AAL) cab 4A con4Ac
no common mode failure of relays _ 4cmic
digital ch. A not in AAL test bypass dsAbp
4Ac
4Bc
output relays (coils) cabinet 4B_ or4Bc
output relays (contacts) (AAL) cab 4B con4Bc
no common mode failure of relays _ 4cmic
digital ch. A not in AAL test bypass dsAbp
4Bc
4Cc
output relays (coils) cabinet 4C_ or4Cc
output relays (contacts) (AAL) cab 4C con4Cc
no common mode failure of relays _ 4cmic
digital ch. A not in AAL test bypass dsAbp
4Cc



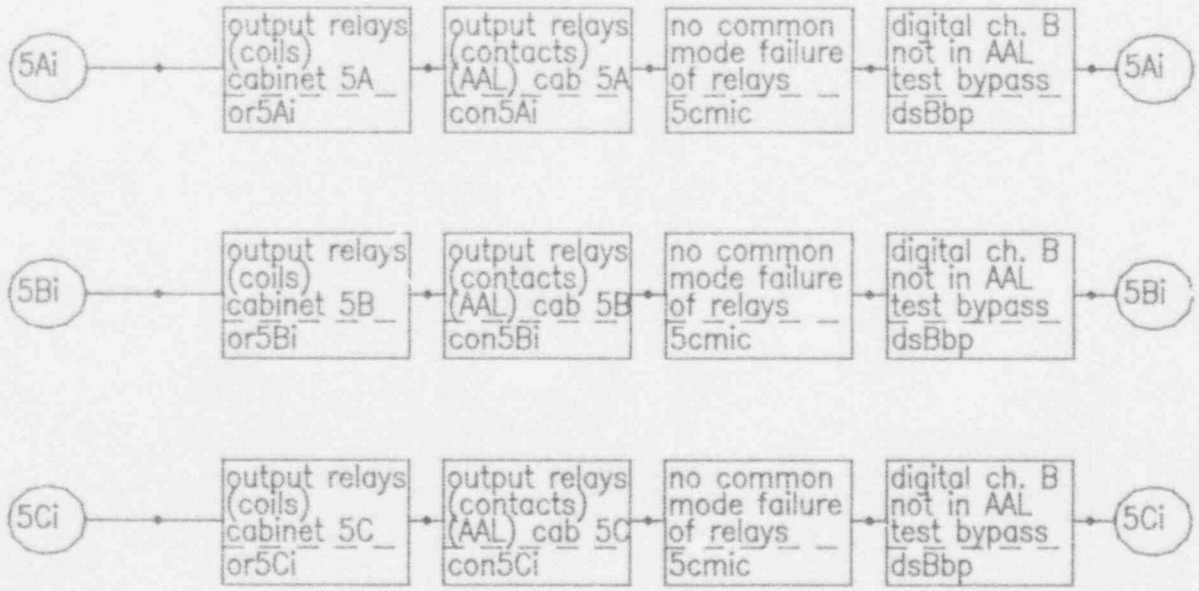
Gilbert ESFAS (Crystal River 3)



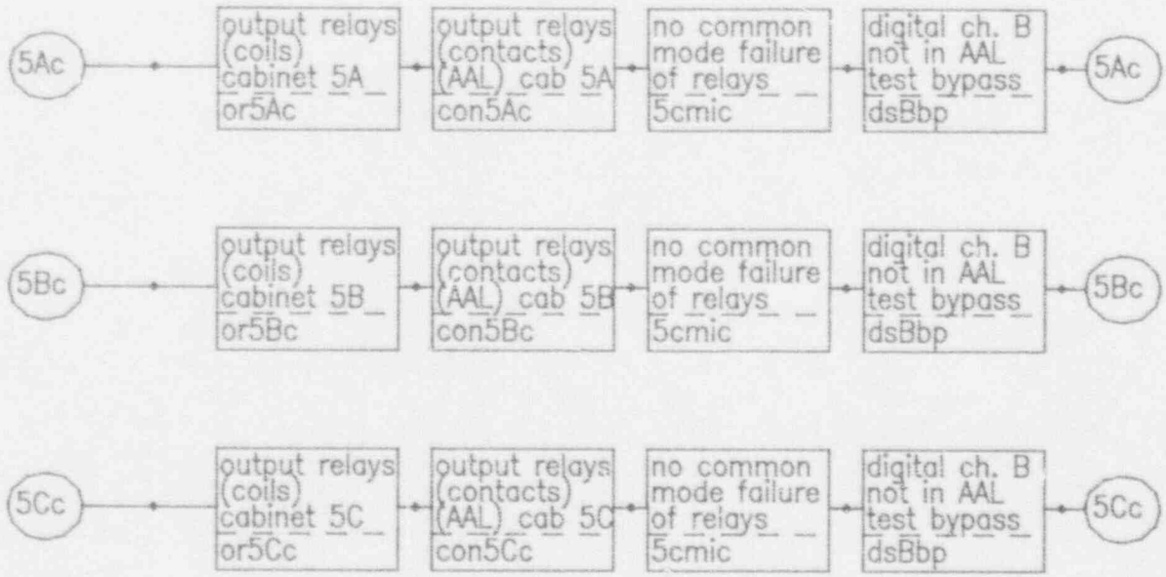
Gilbert ESFAS (Crystal River 3)

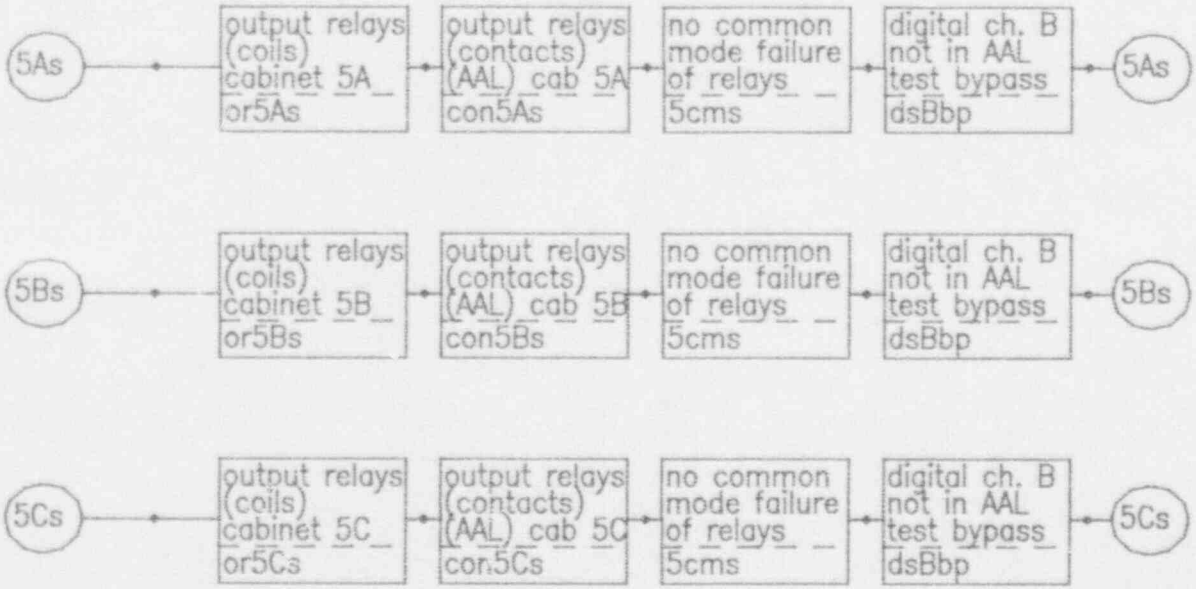


Gilbert ESFAS (Crystal River 3)

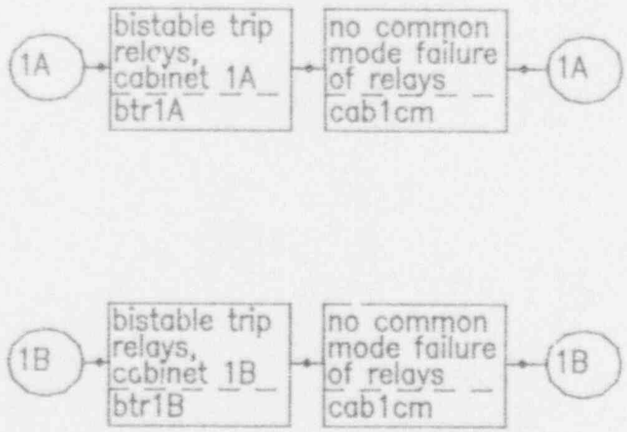


Gilbert ESFAS (Crystal River 3)


5Ac
output relays (coils) cabinet 5A_ or5Ac
output relays (contacts) (AAL) cab 5A con5Ac
no common mode failure of relays_ _ 5cmic
digital ch. B not in AAL test bypass_ dsBbp
5Ac
5Bc
output relays (coils) cabinet 5B_ or5Bc
output relays (contacts) (AAL) cab 5B con5Bc
no common mode failure of relays_ _ 5cmic
digital ch. B not in AAL test bypass_ dsBbp
5Bc
5Cc
output relays (coils) cabinet 5C_ or5Cc
output relays (contacts) (AAL) cab 5C con5Cc
no common mode failure of relays_ _ 5cmic
digital ch. B not in AAL test bypass_ dsBbp
5Cc



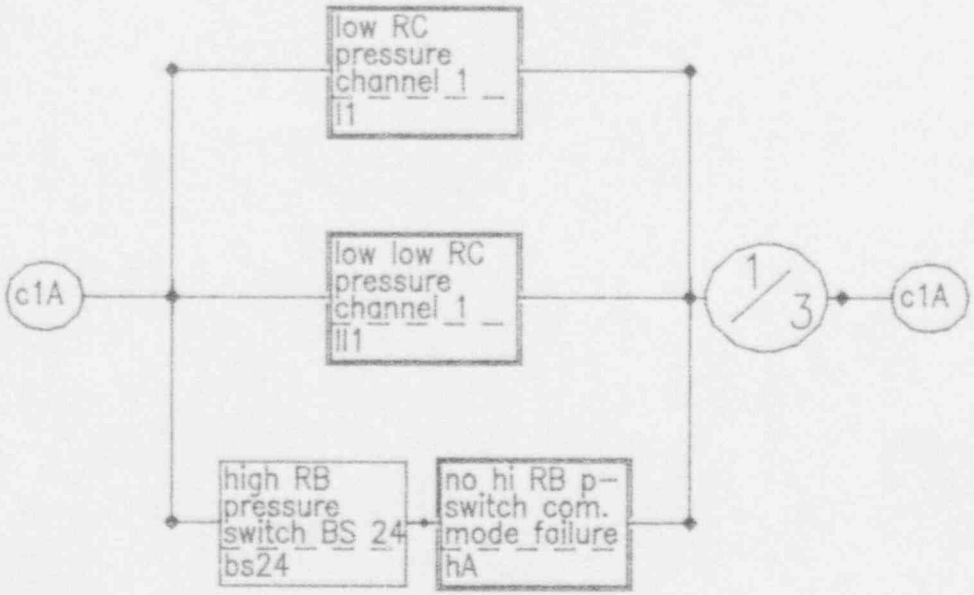
Gilbert ESFAS (Crystal River 3)



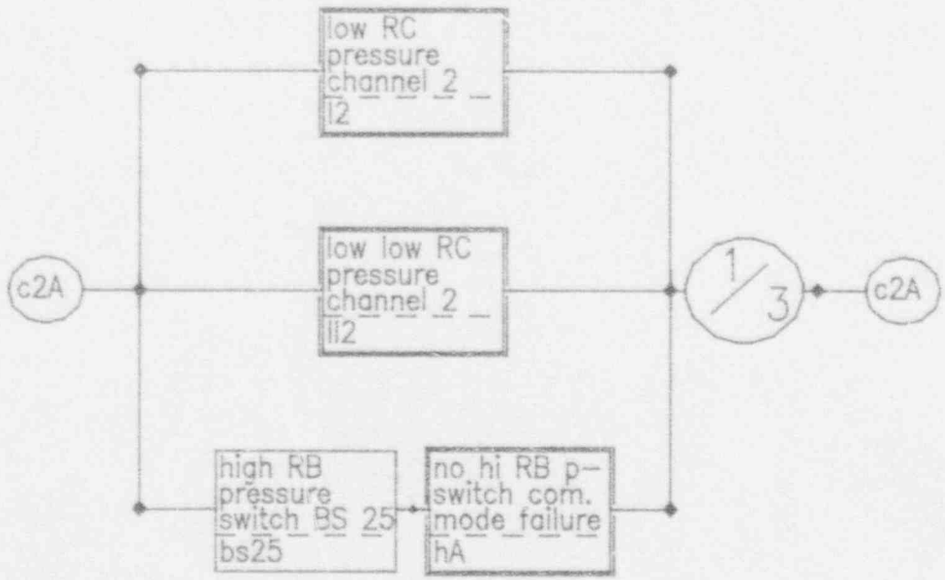
Gilbert ESFAS (Crystal River 3)

Gilbert ESFAS (Crystal River 3)

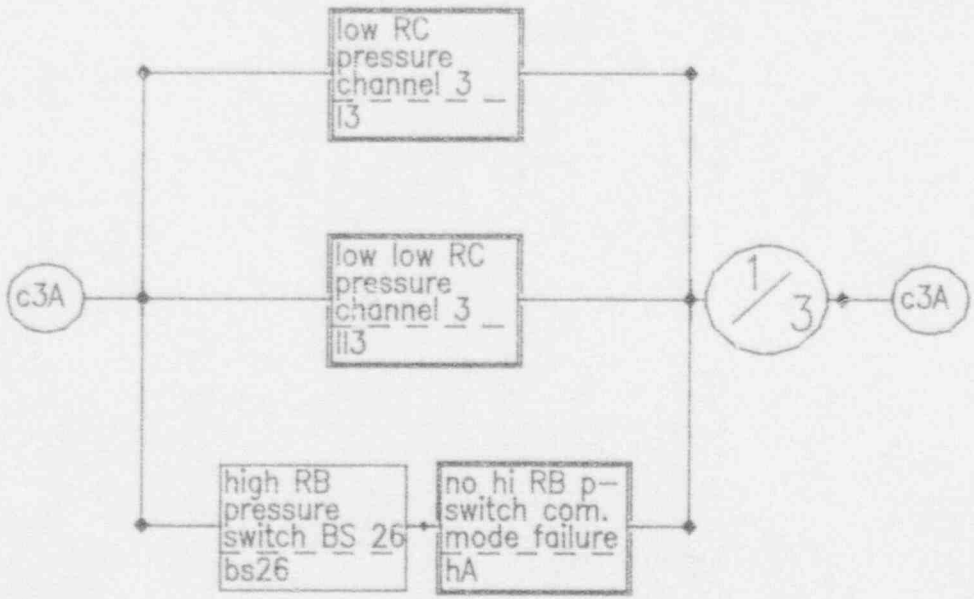
Gilbert ESFAS (Crystal River 3)



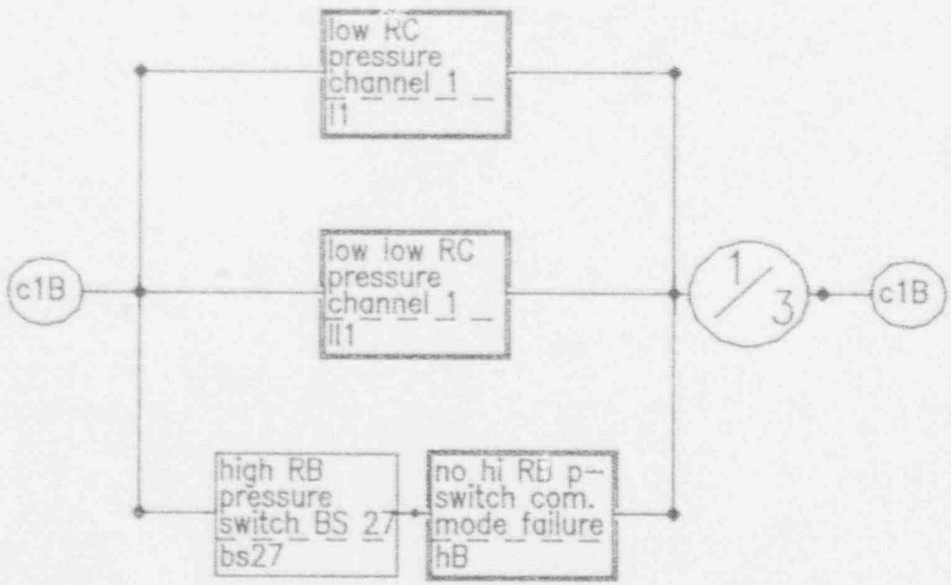
Gilbert ESFAS (Crystal River 3)



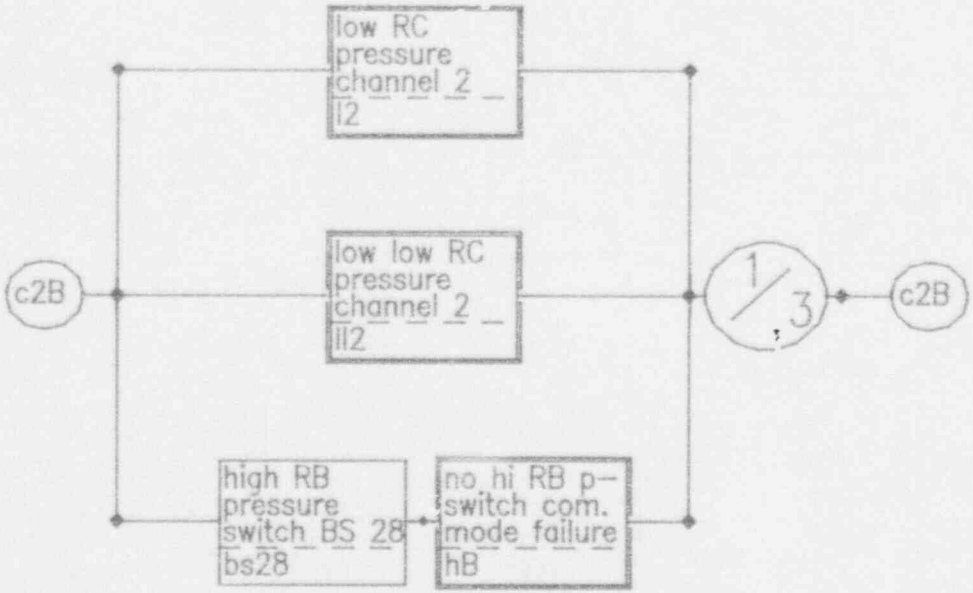
Gilbert ESFAS (Crystal River 3)



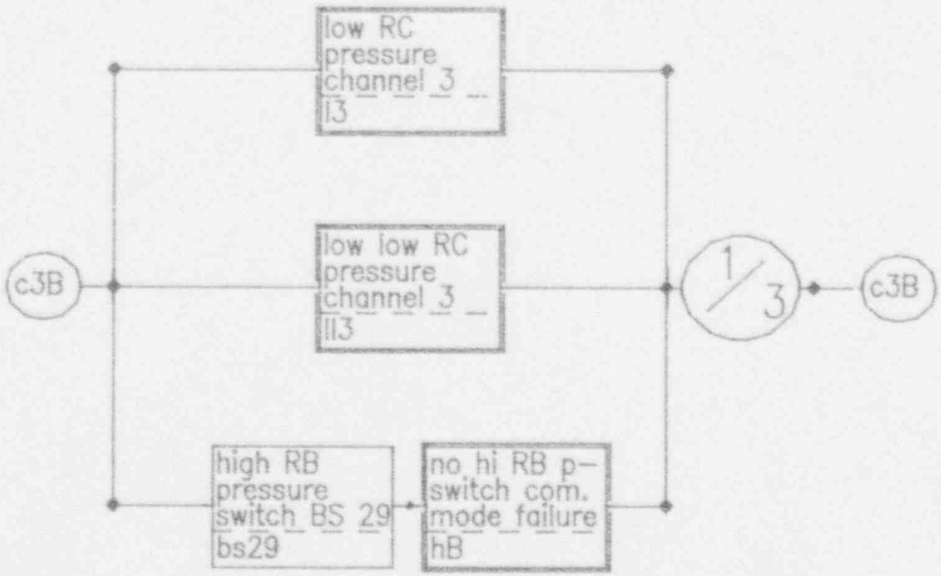
Gilbert ESFAS (Crystal River 3)



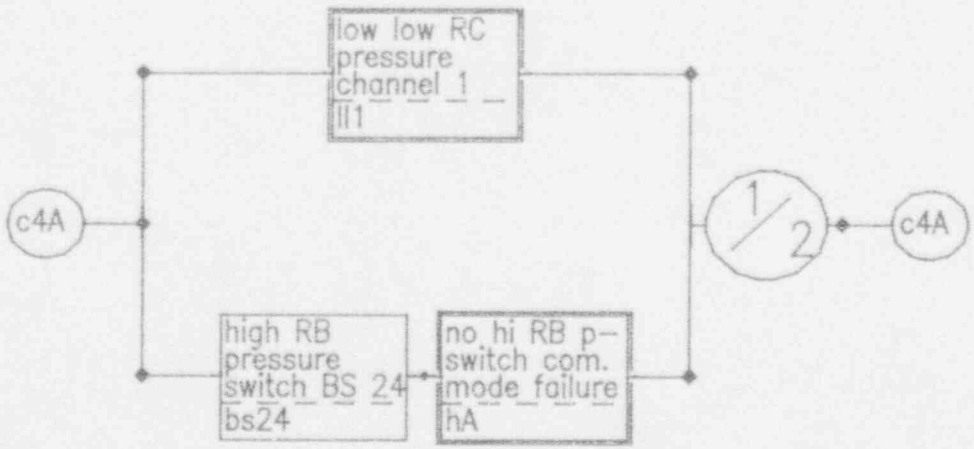
Gilbert ESFAS (Crystal River 3)



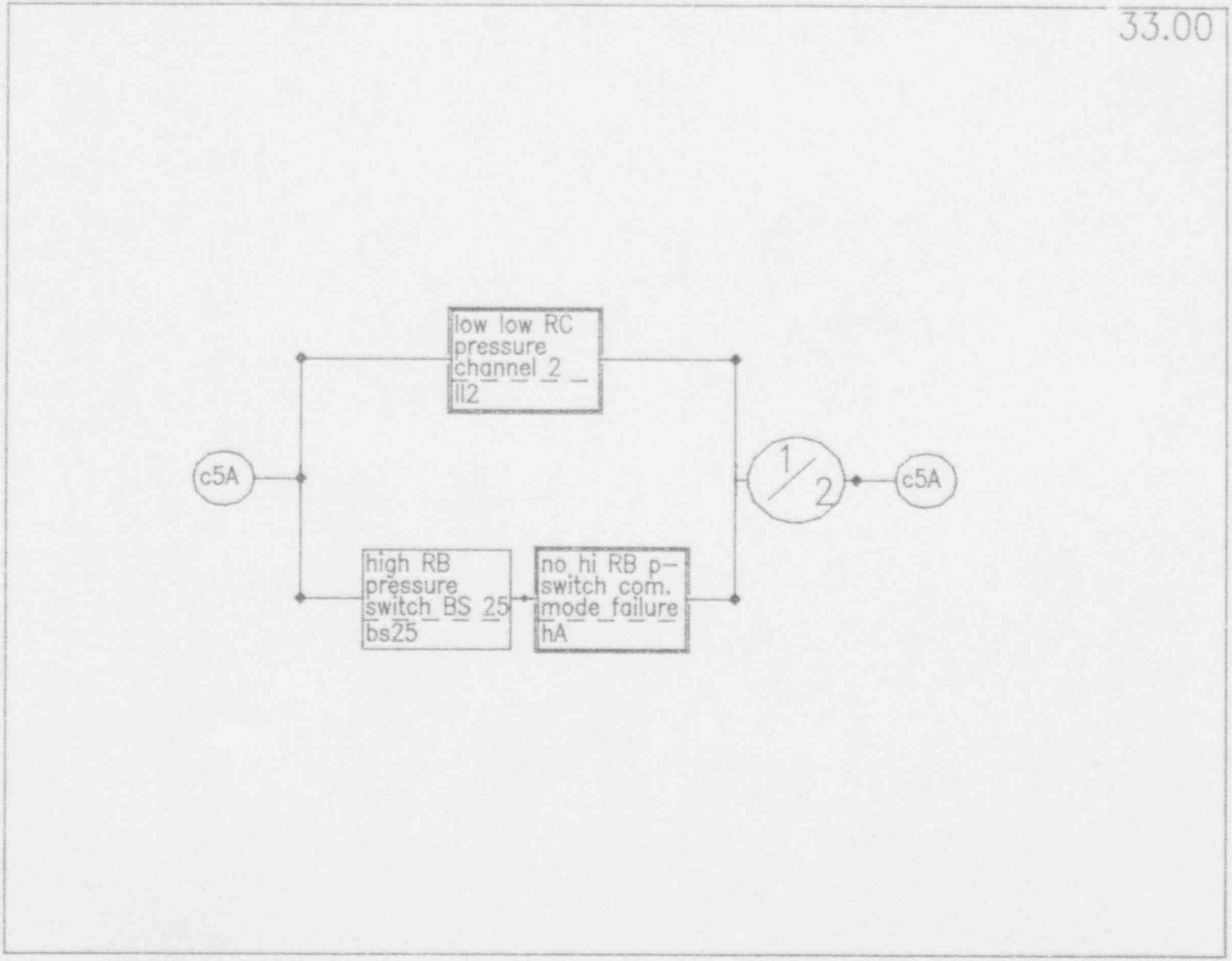
Gilbert ESFAS (Crystal River 3)



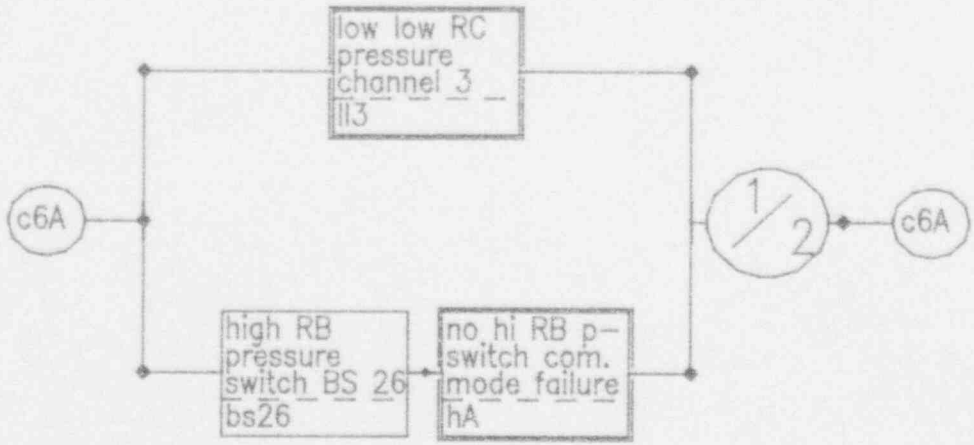
Gilbert ESFAS (Crystal River 3)



Gilbert ESFAS (Crystal River 3)

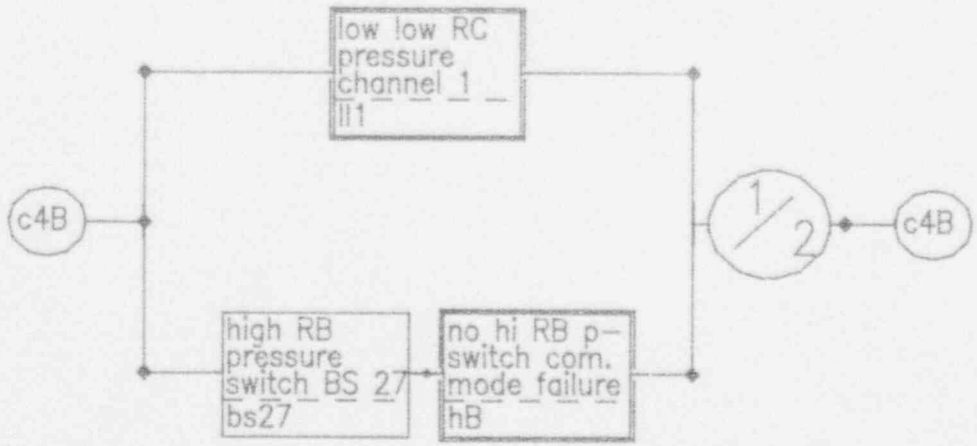


Gilbert ESFAS (Crystal River 3)

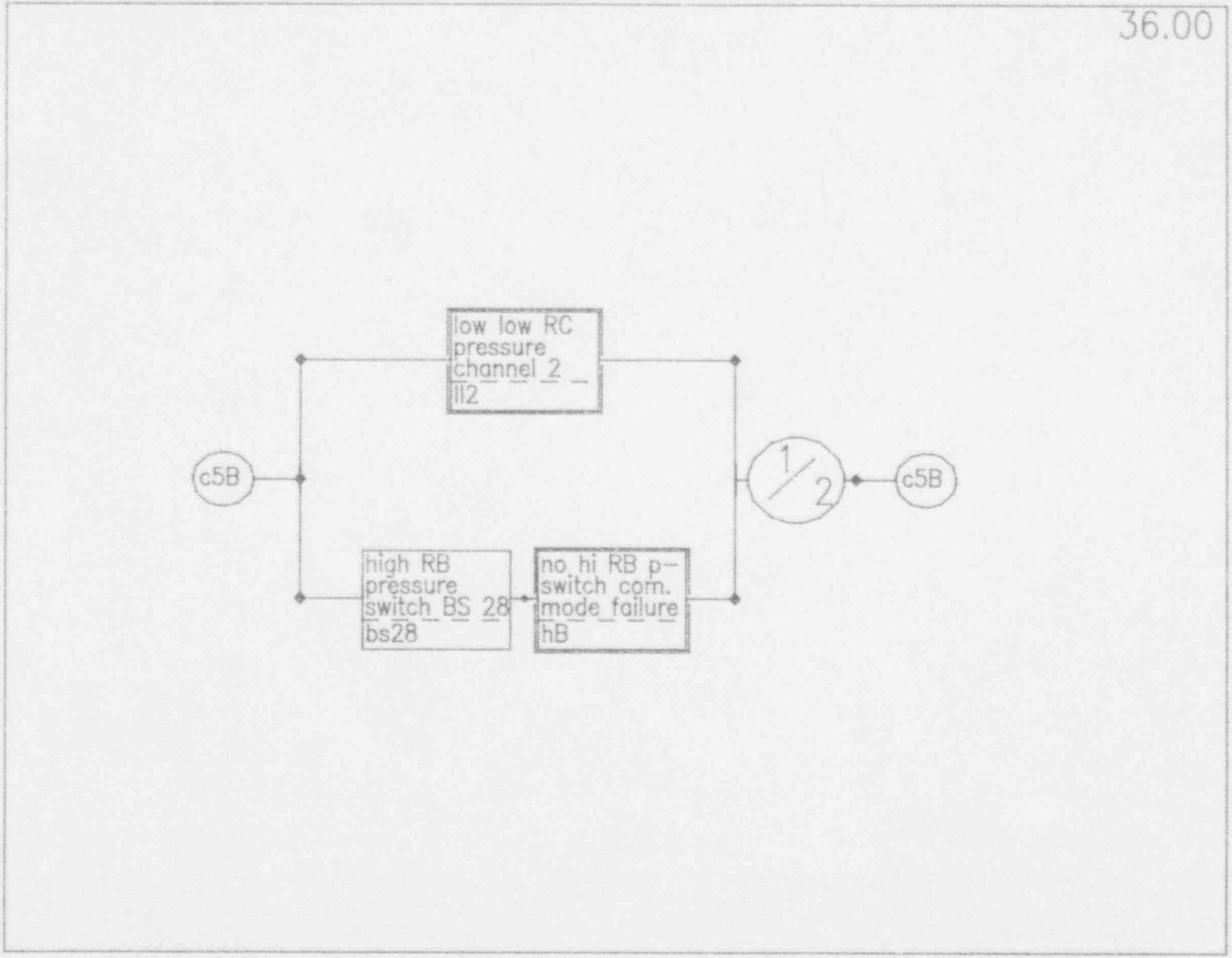


Gilbert ESFAS (Crystal River 3)

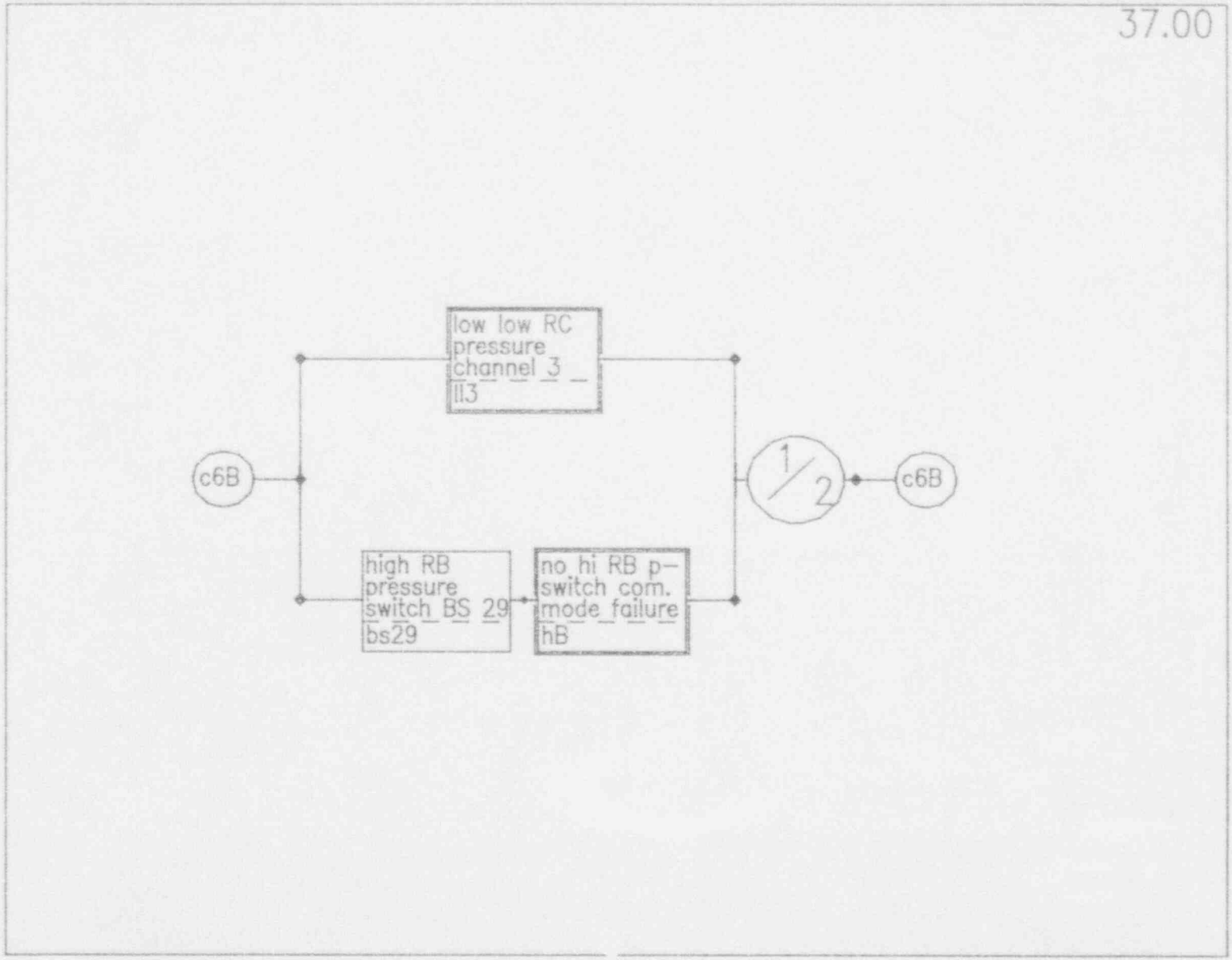
35.00



Gilbert ESFAS (Crystal River 3)

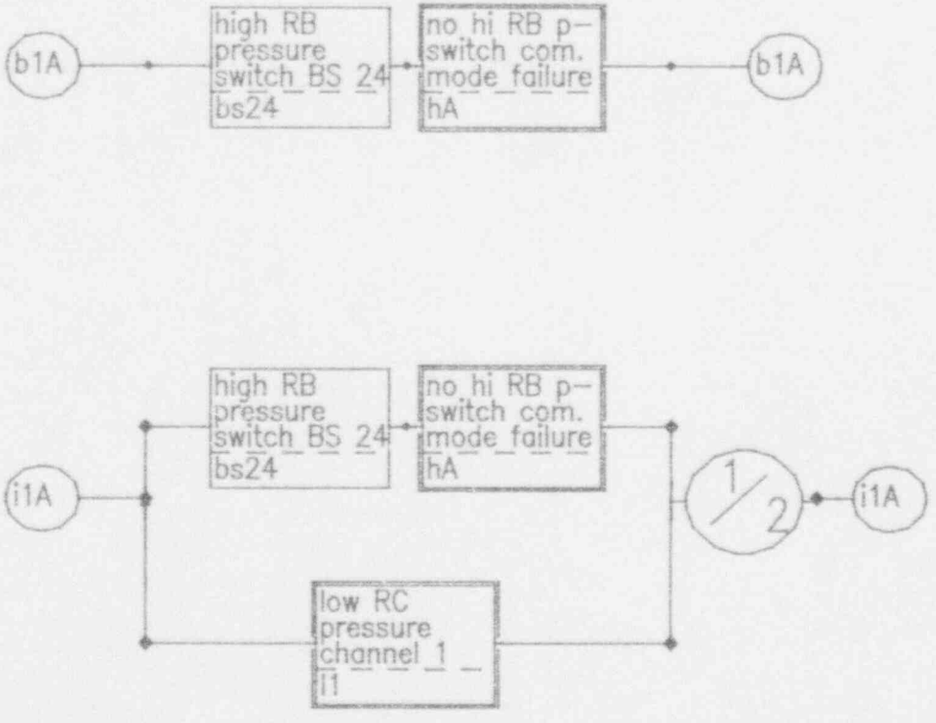


Gilbert ESFAS (Crystal River 3)

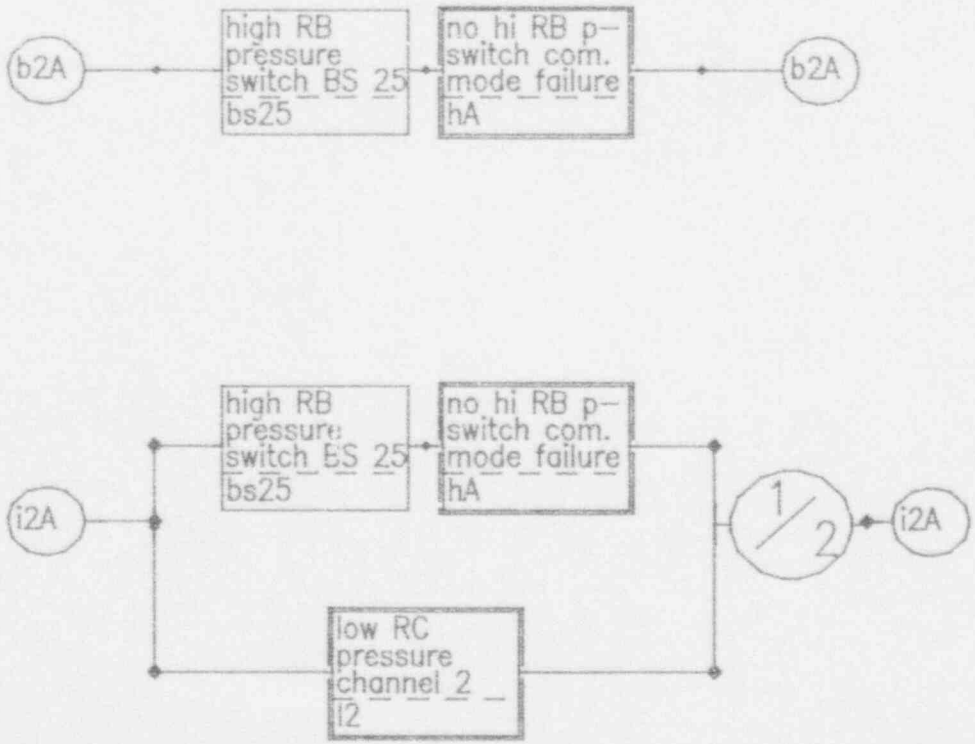


Gilbert ESFAS (Crystal River 3)

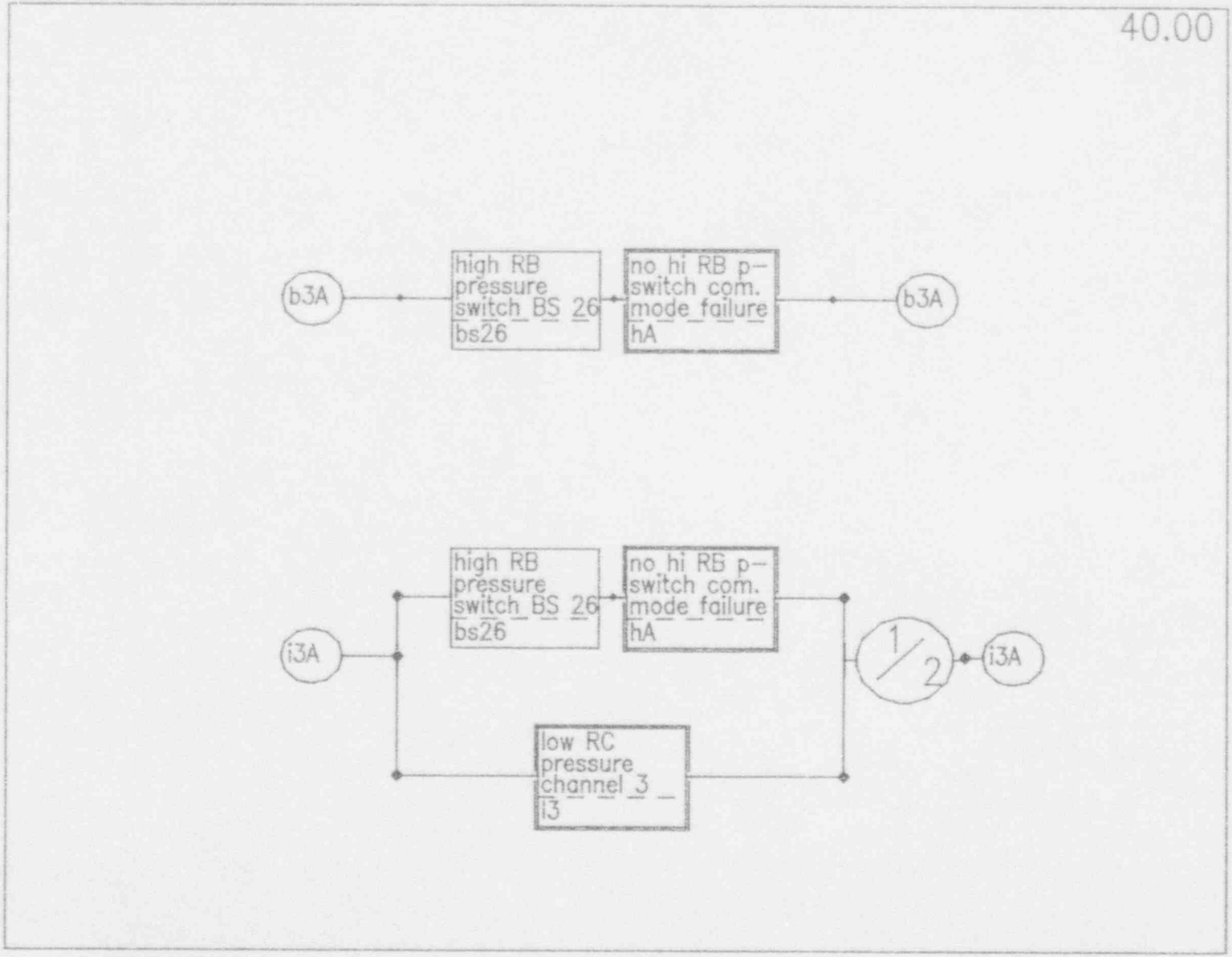
38.00



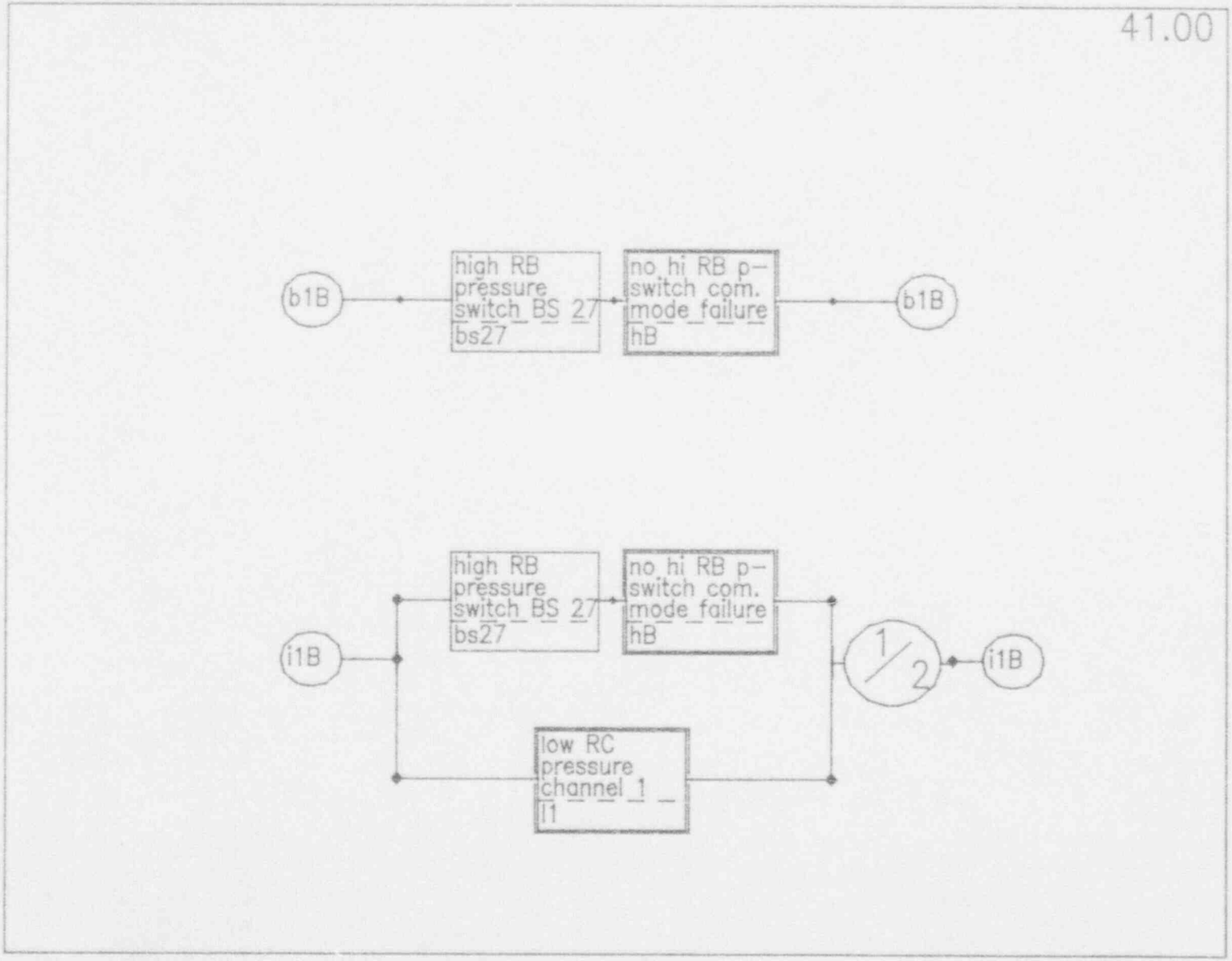
Gilbert ESFAS (Crystal River 3)



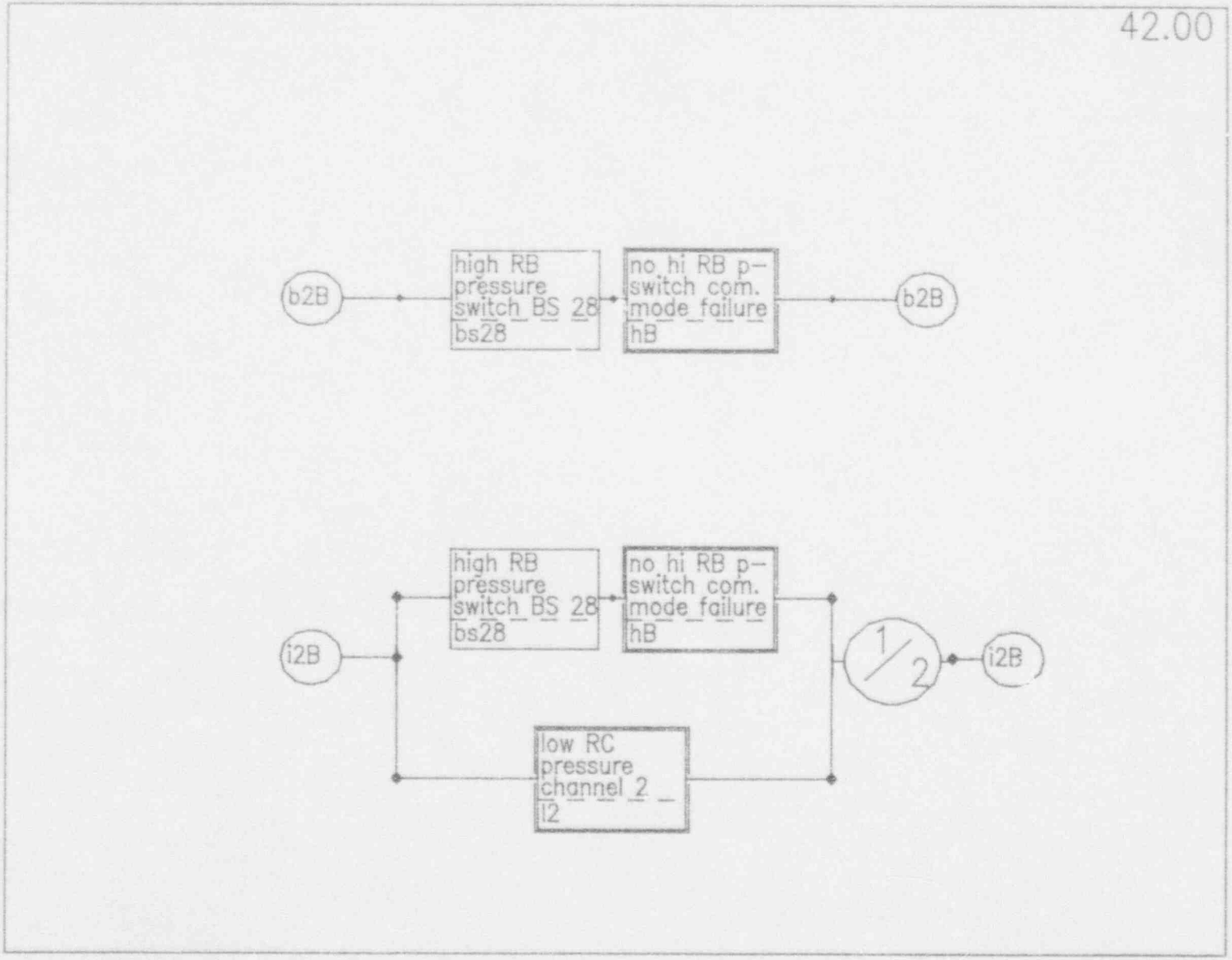
Gilbert ESFAS (Crystal River 3)



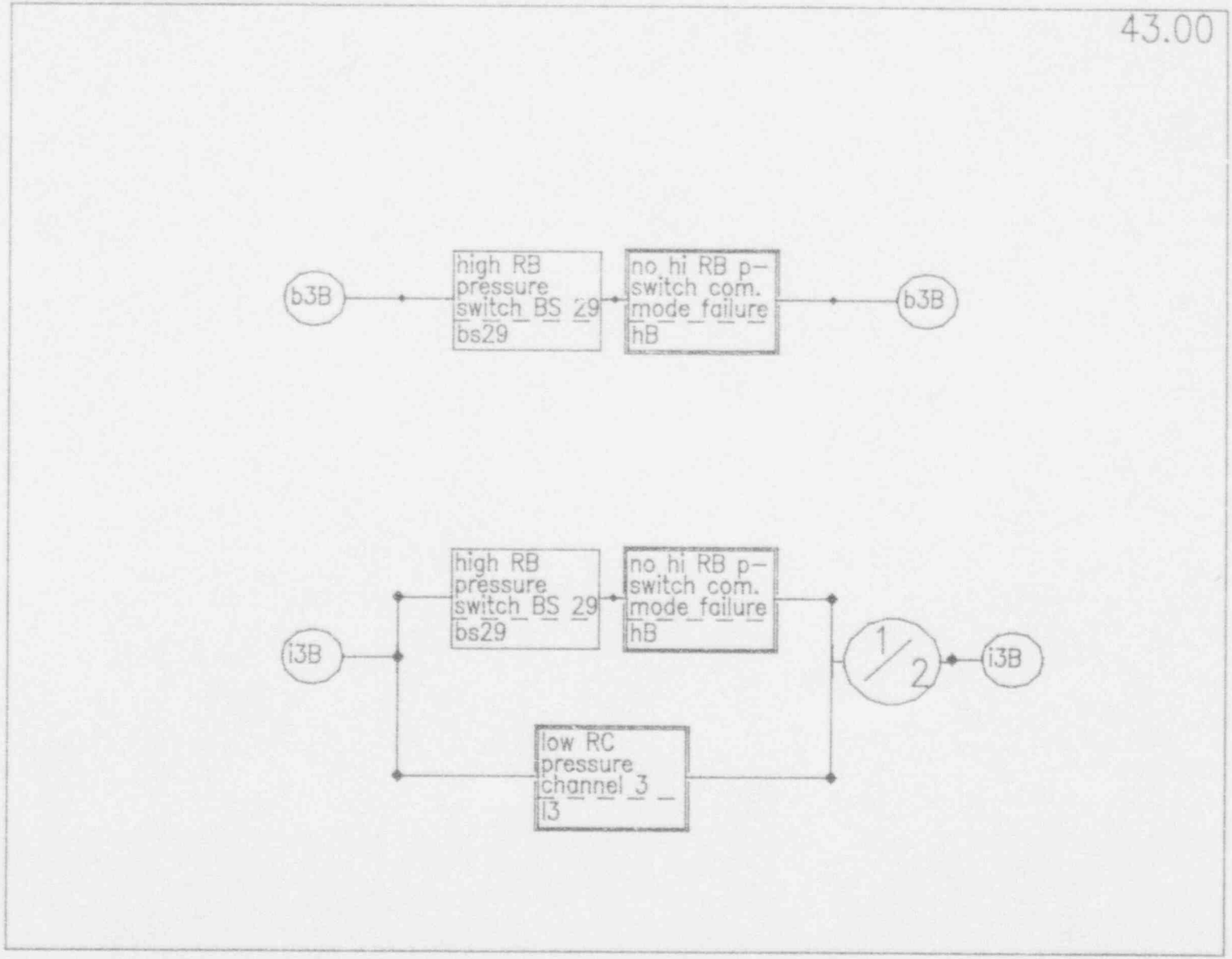
Gilbert ESFAS (Crystal River 3)



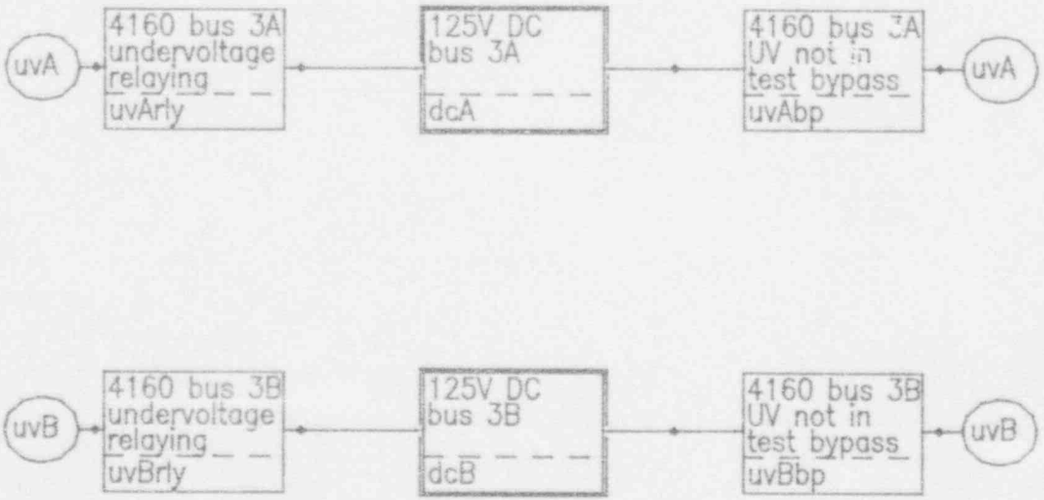
Gilbert ESFAS (Crystal River 3)



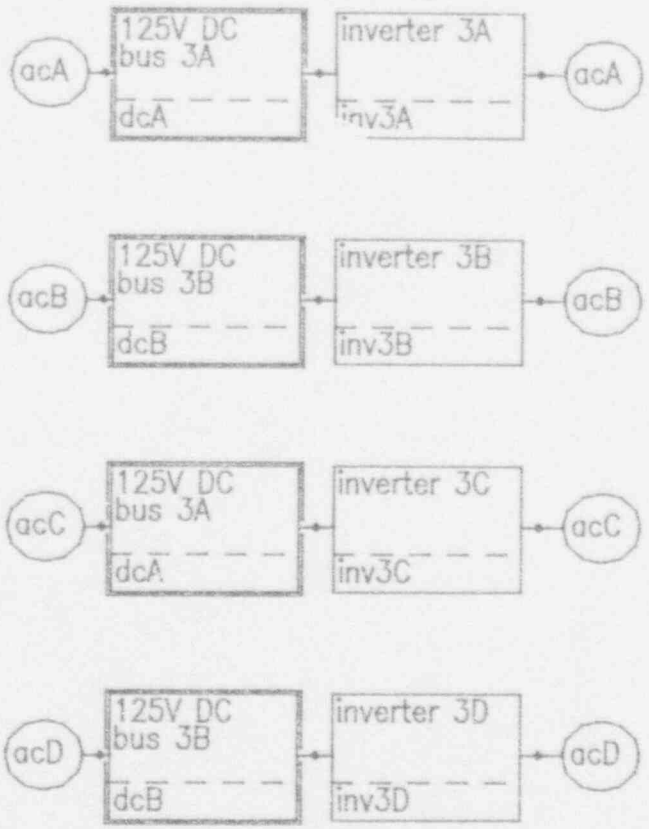
Gilbert ESFAS (Crystal River 3)



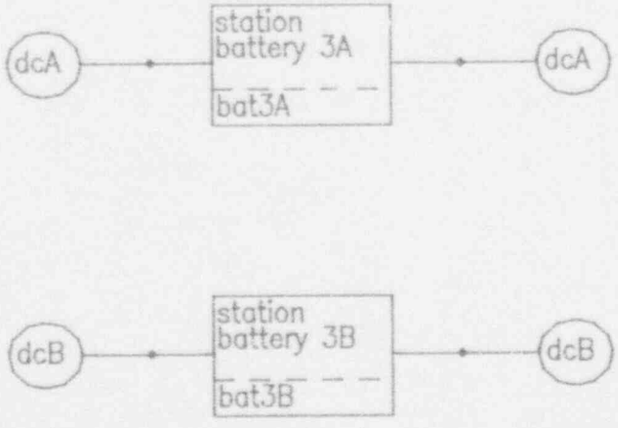
Gilbert ESFAS (Crystal River 3)



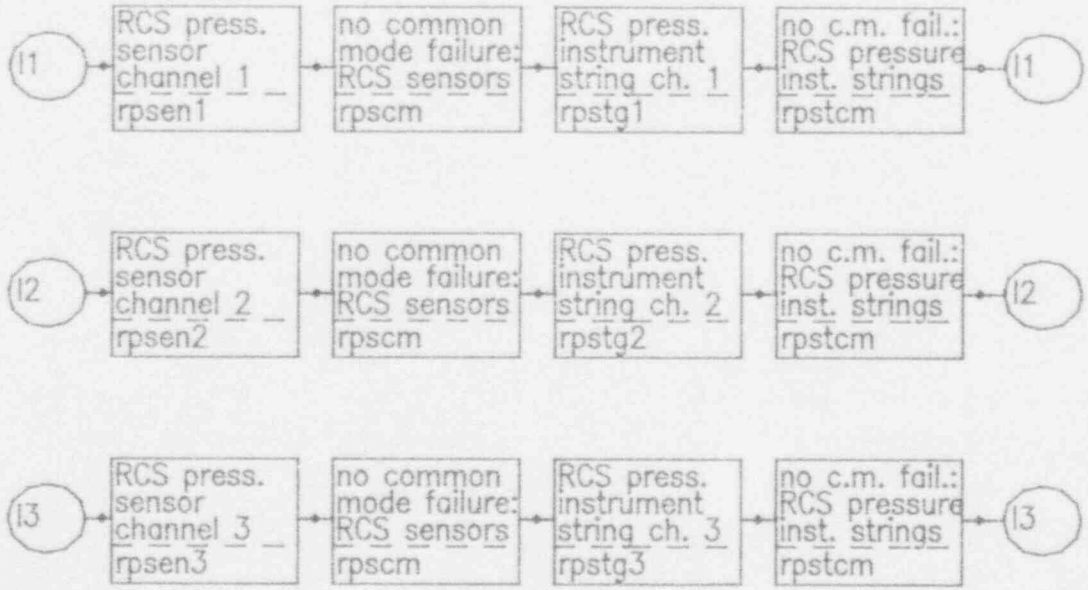
Gilbert ESFAS (Crystal River 3)



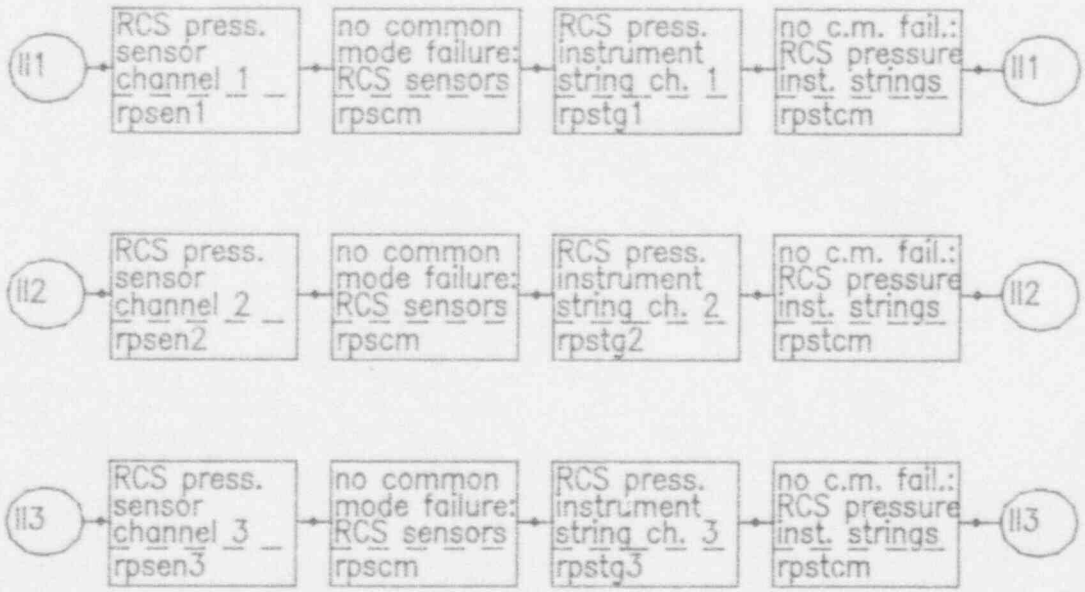
Gilbert ESFAS (Crystal River 3)



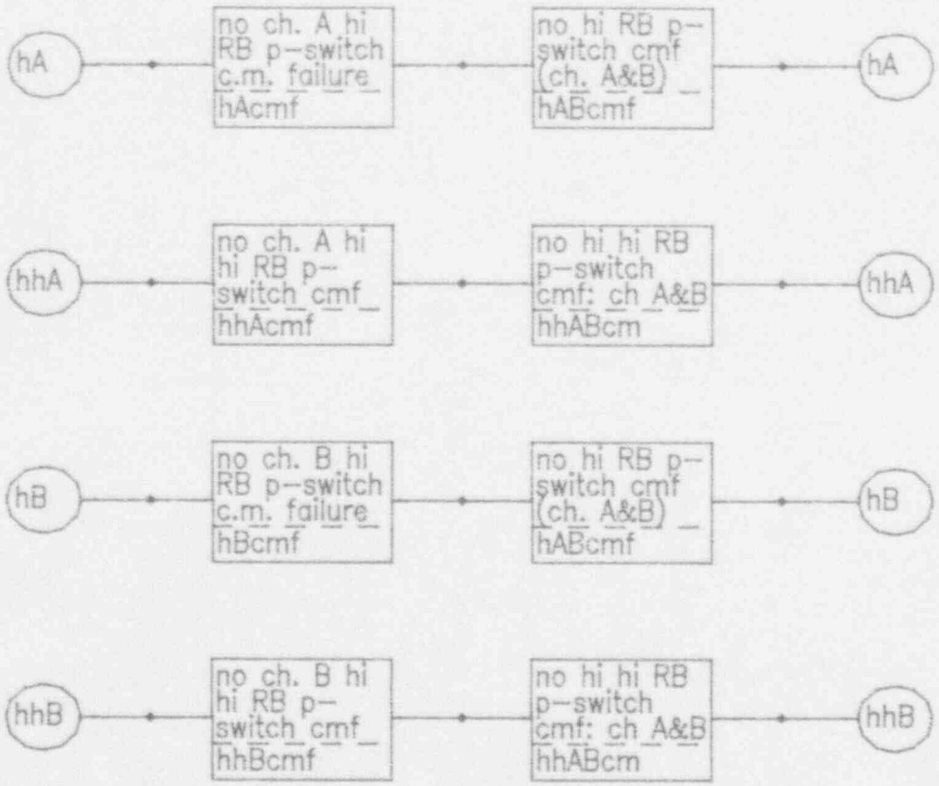
Gilbert ESFAS (Crystal River 3)



Gilbert ESFAS (Crystal River 3)



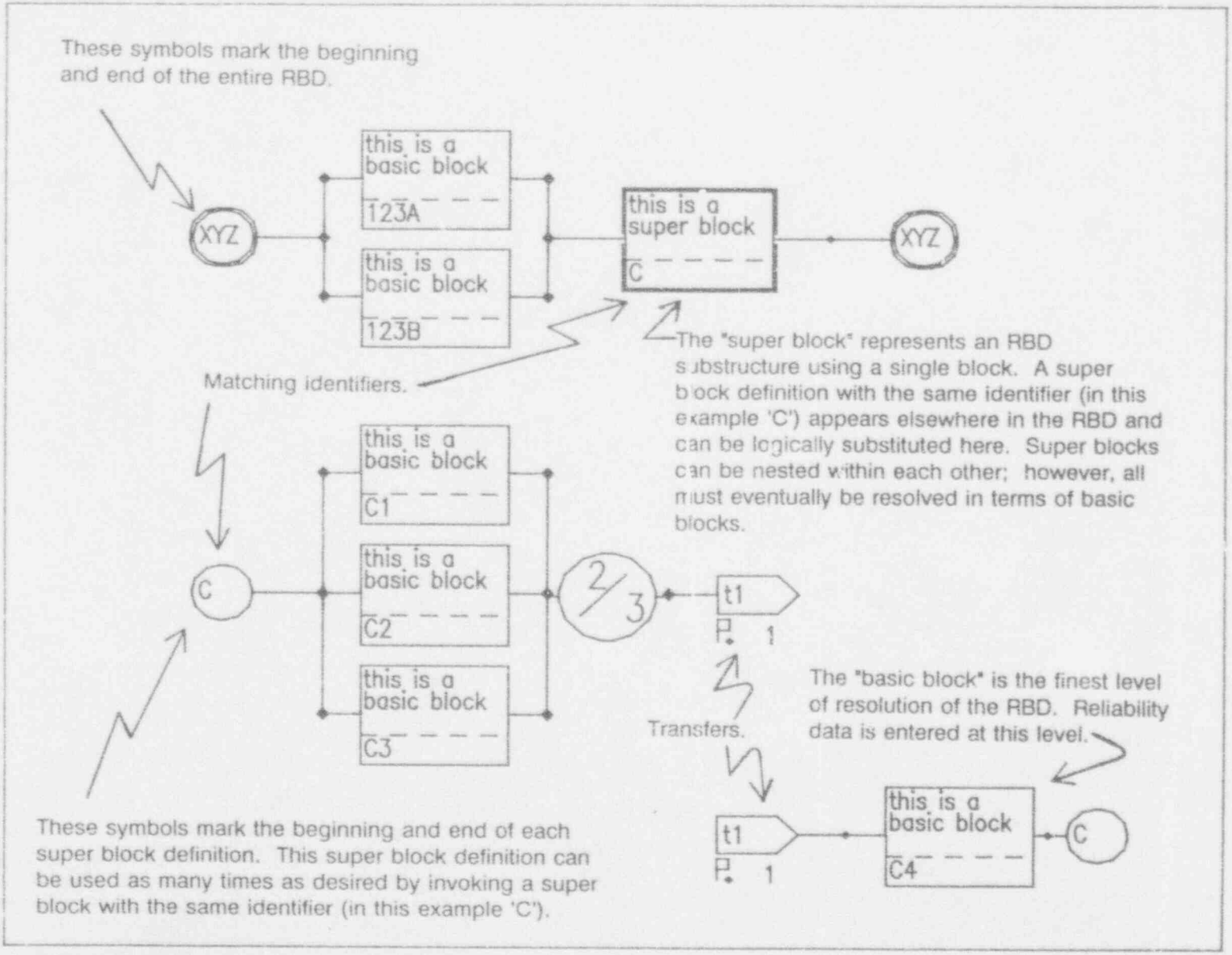
Gilbert ESFAS (Crystal River 3)



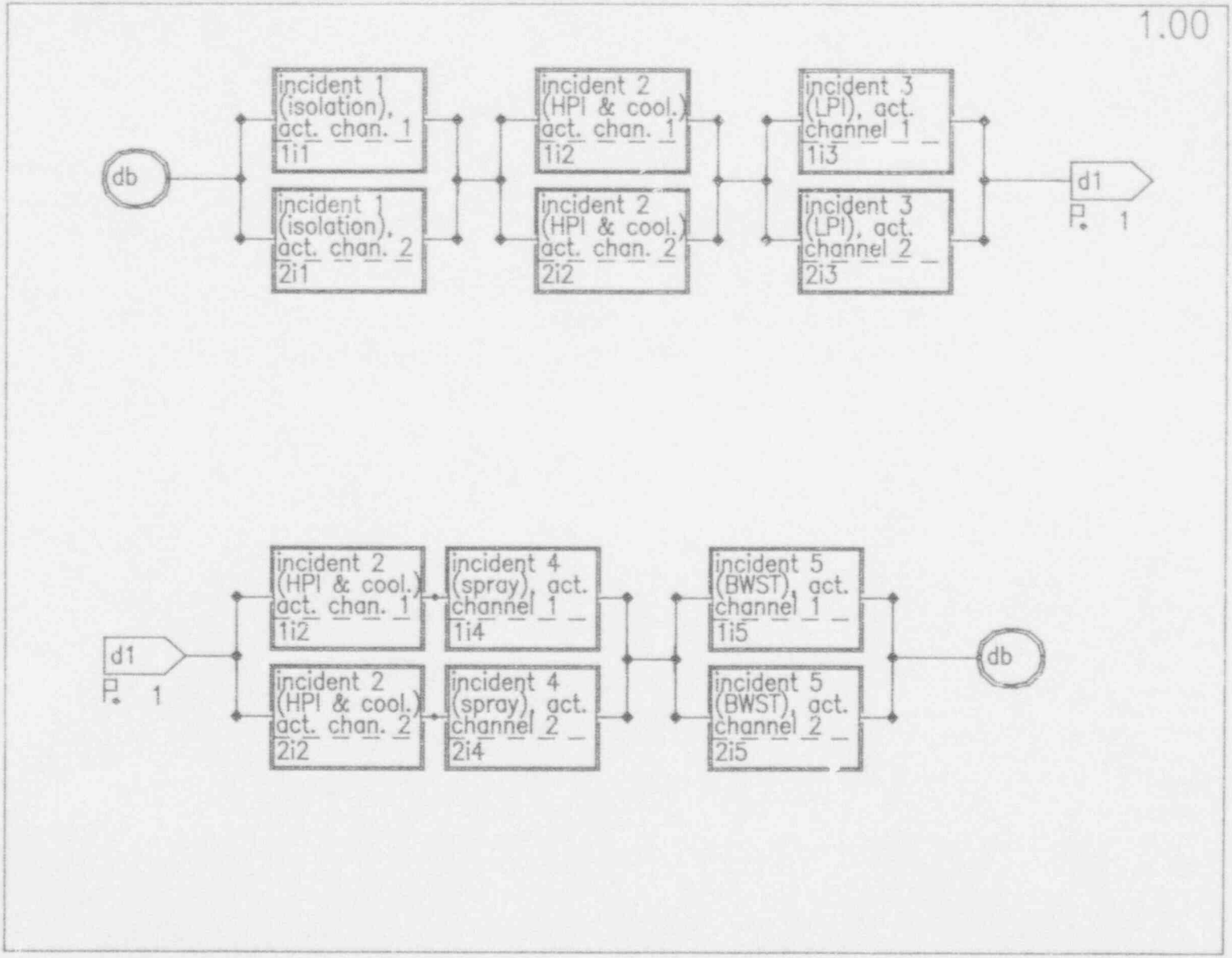
Gilbert ESFAS (Crystal River 3)

APPENDIX C

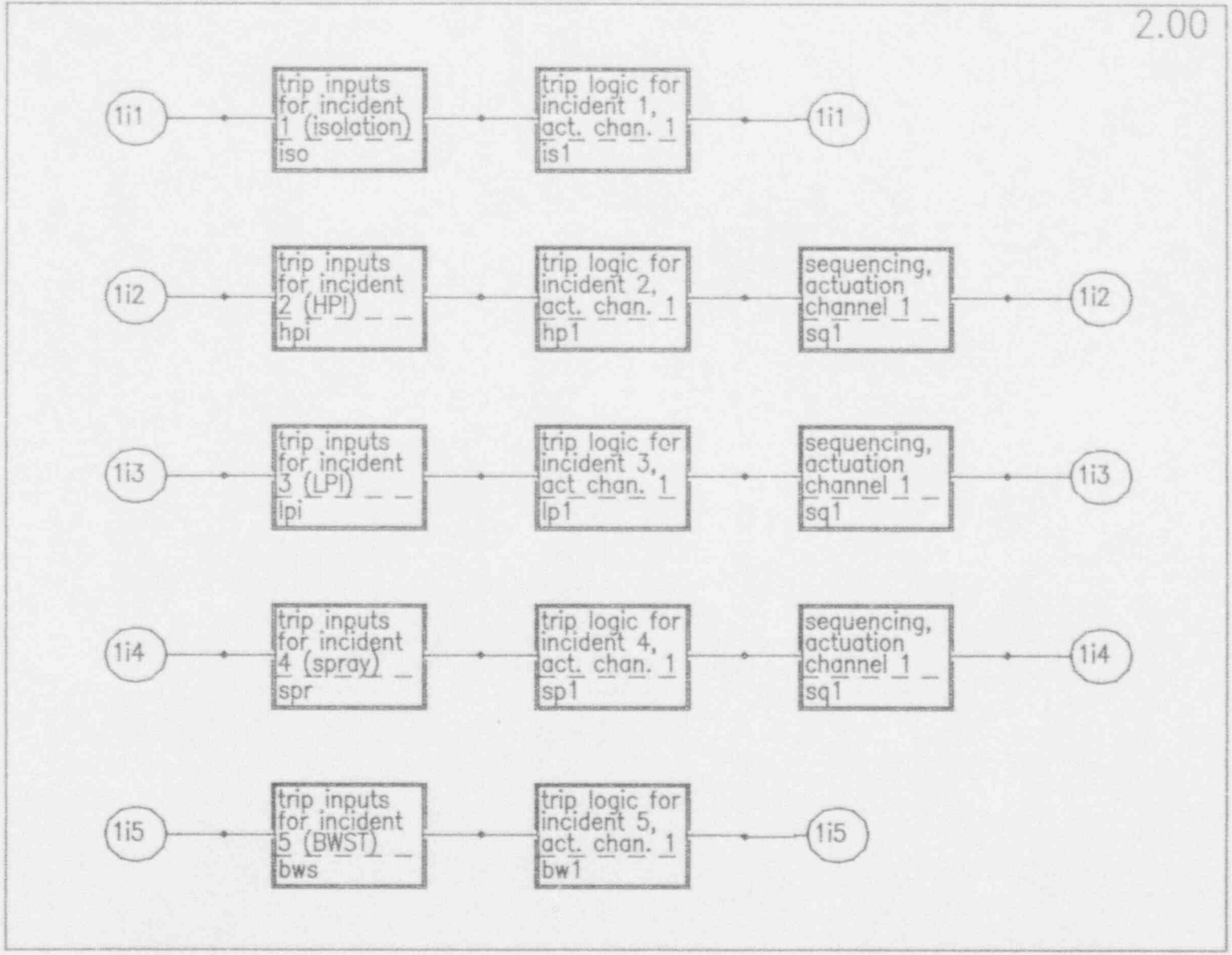
RBD for Bechtel ESFAS (Davis-Besse)



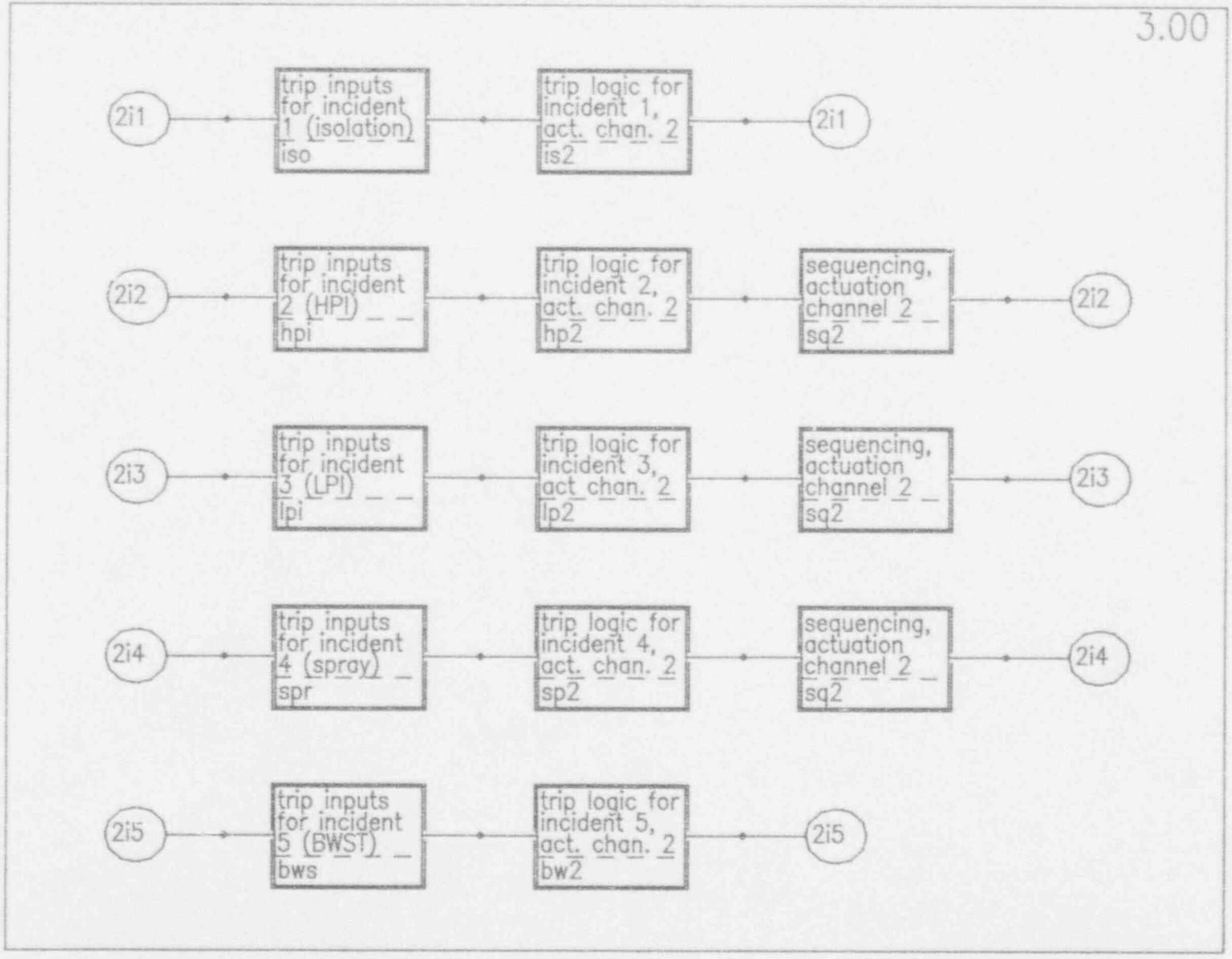
RBD Symbology Description



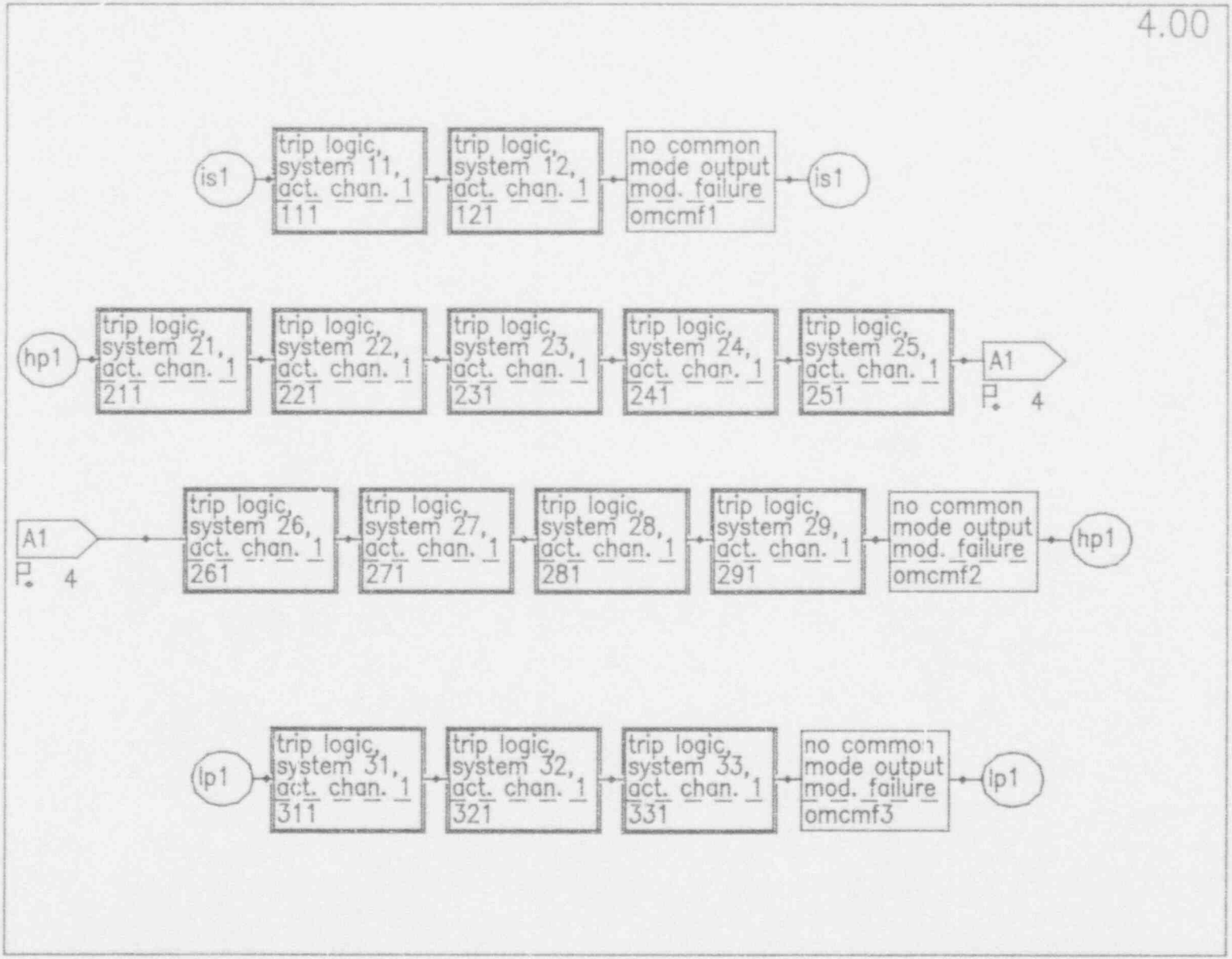
Bechtel ESFAS (Davis-Besse)



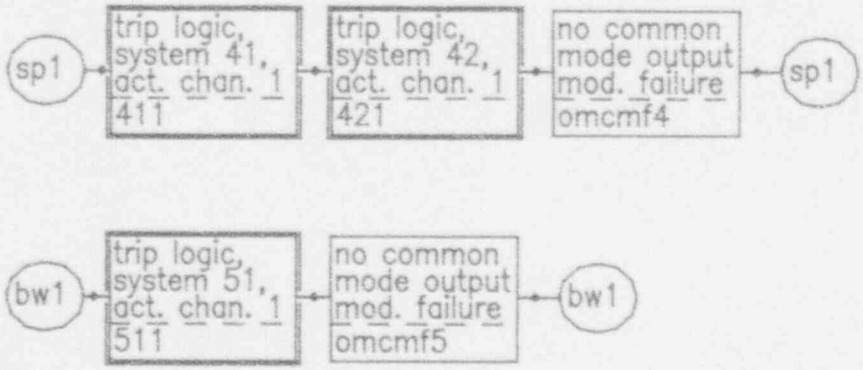
Bechtel ESFAS (Davis-Besse)

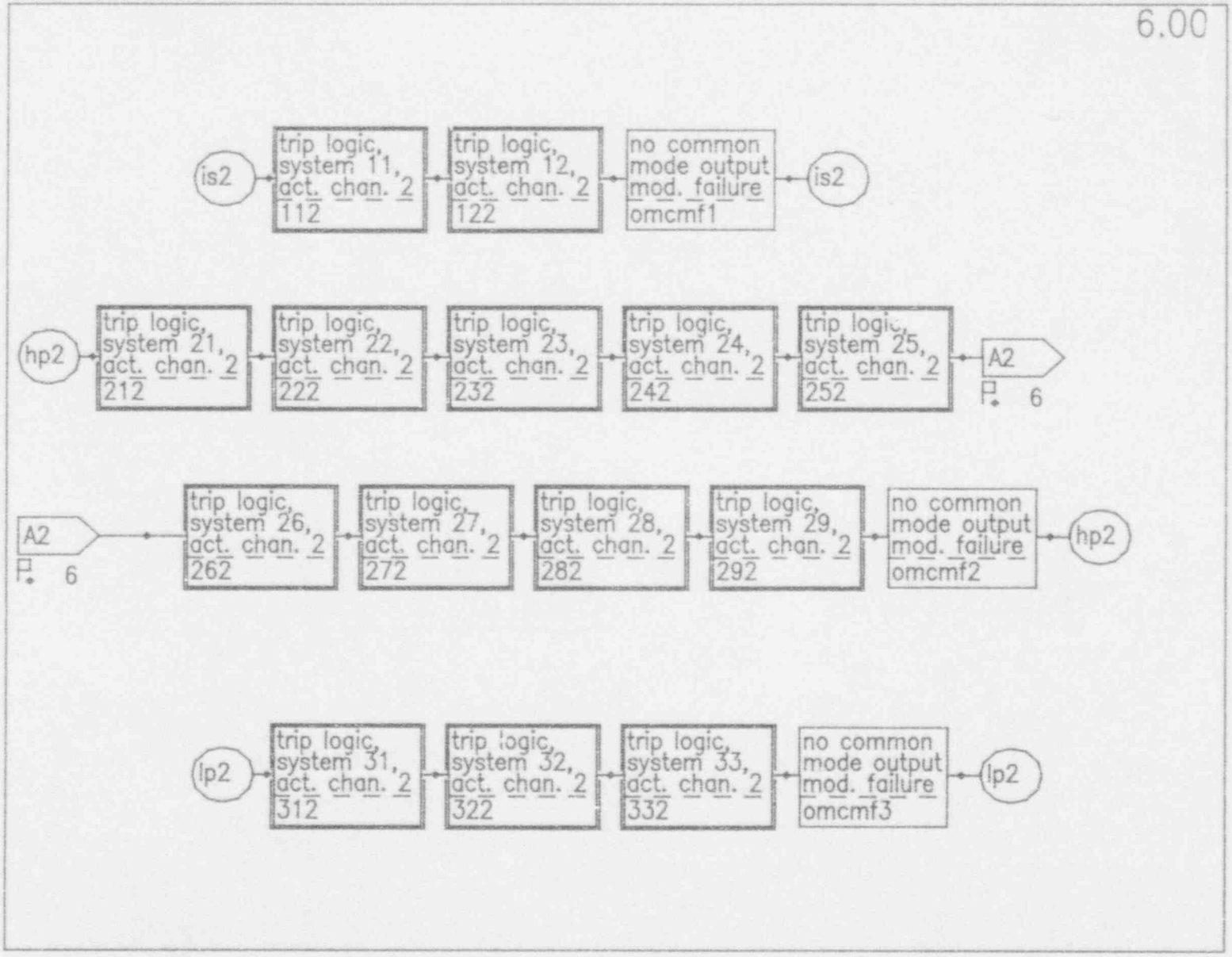


Bechtel ESFAS (Davis–Besse)

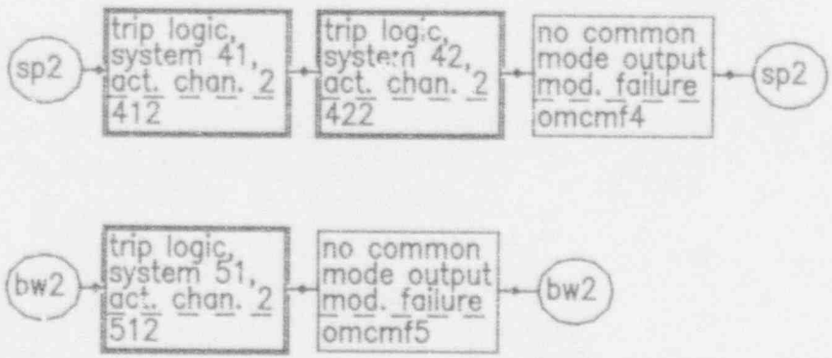


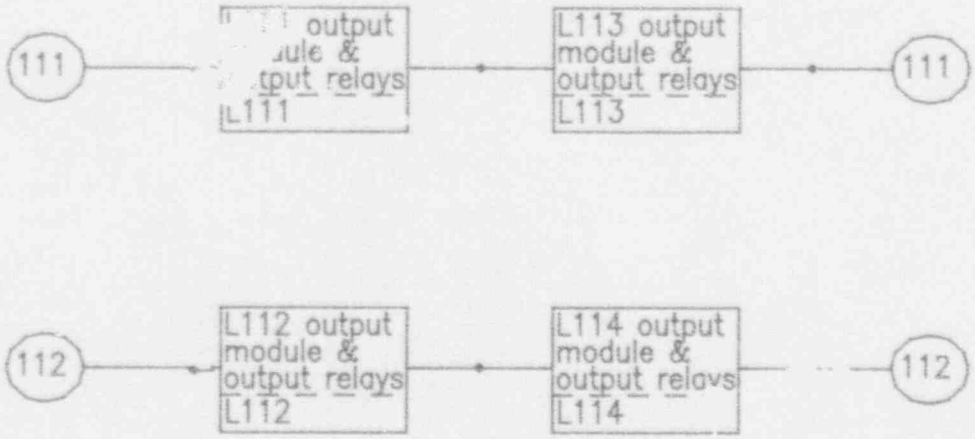
Bechtel ESFAS (Davis–Besse)


sp1
trip logic, system 41, act. chan. 1 411
trip logic, system 42, act. chan. 1 421
no common mode output mod. failure omcmf4
sp1
bw1
trip logic, system 51, act. chan. 1 511
no common mode output mod. failure omcmf5
bw1

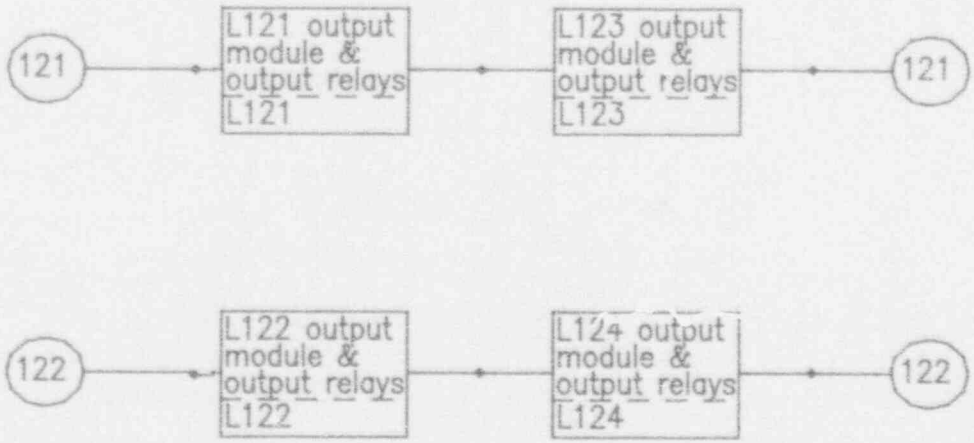


Bechtel ESFAS (Davis–Besse)

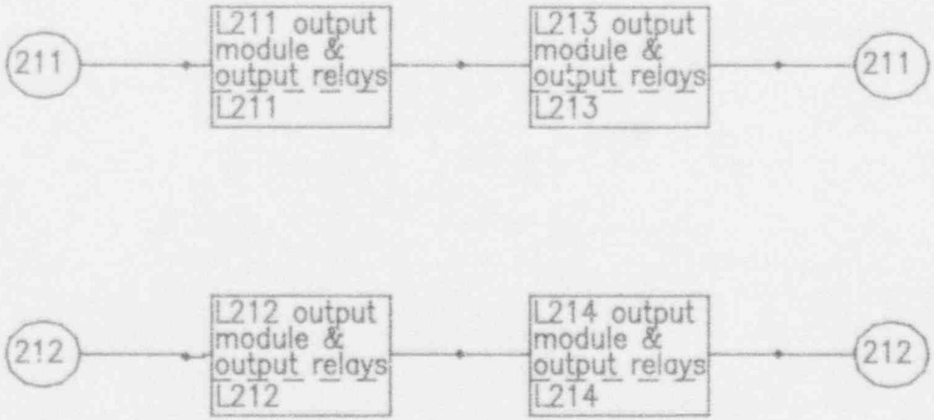

sp2
trip logic, system 41, act. chan. 2
412
trip logic, system 42, act. chan. 2
422
no common mode output mod. failure
omcmf4
sp2
bw2
trip logic, system 51, act. chan. 2
512
no common mode output mod. failure
omcmf5
bw2



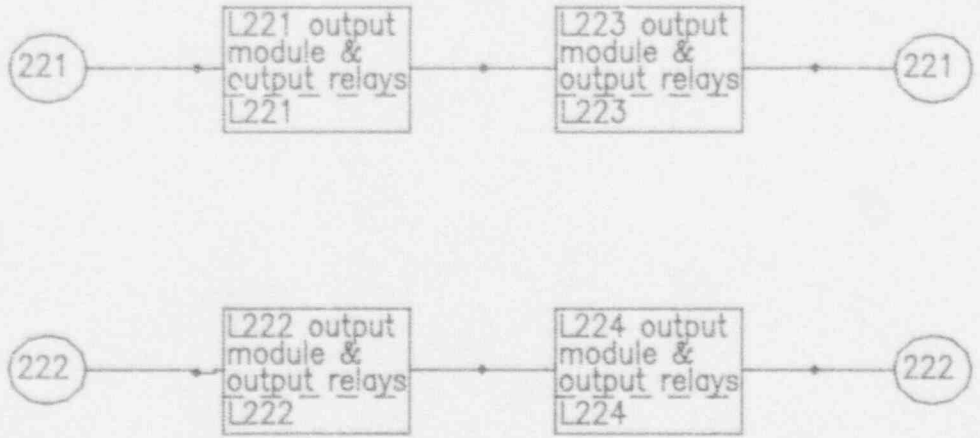
Bechtel ESFAS (Davis-Besse)



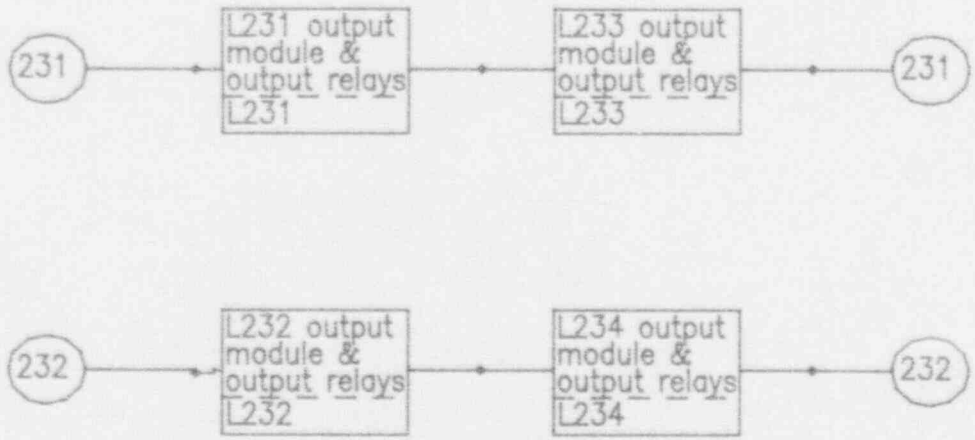
Bechtel ESFAS (Davis-Besse)



Bechtel ESFAS (Davis-Besse)

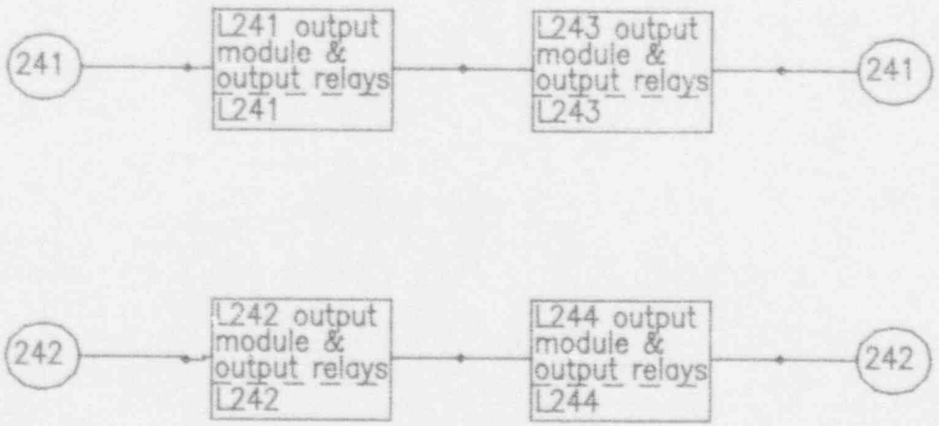


Bechtel ESFAS (Davis-Besse)

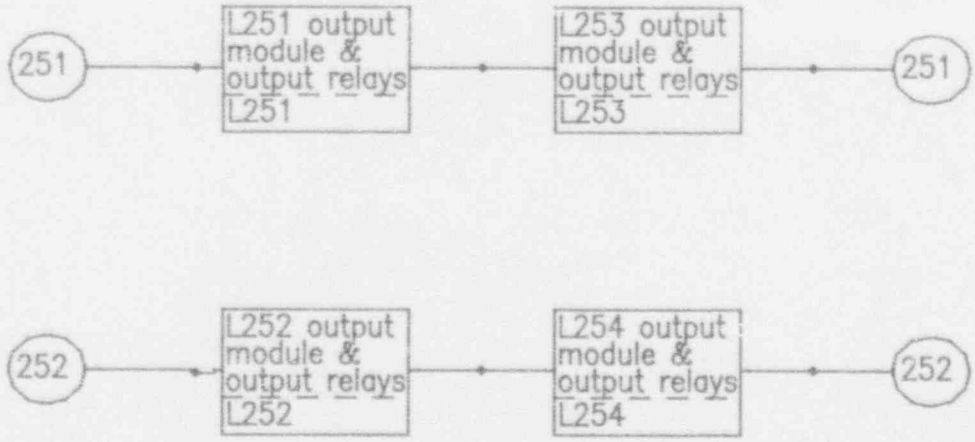


Bechtel ESFAS (Davis-Besse)

13.00

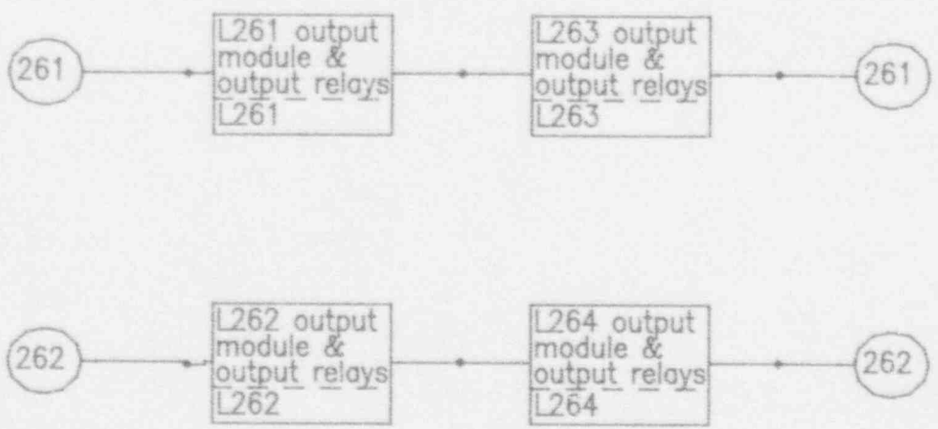


Bechtel ESFAS (Davis–Besse)

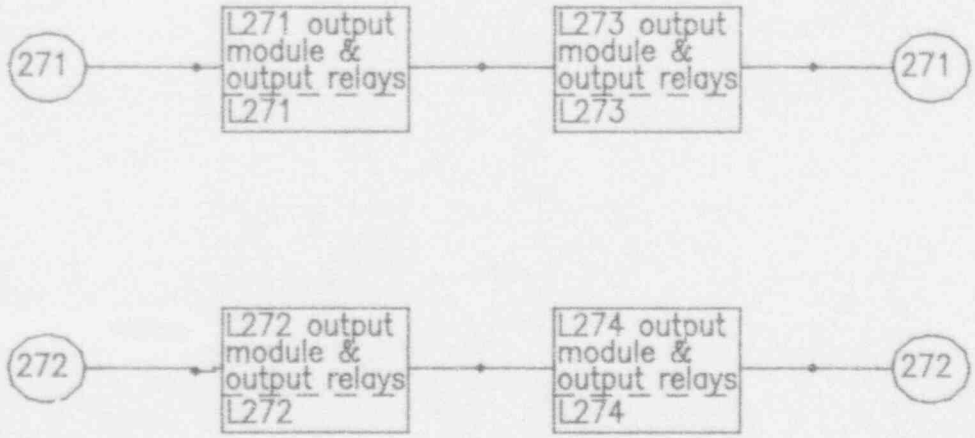


Bechtel ESFAS (Davis-Besse)

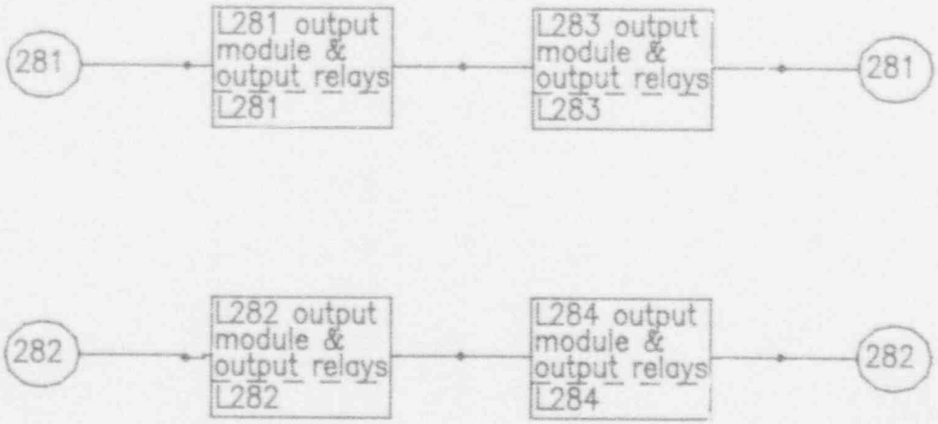
15.00



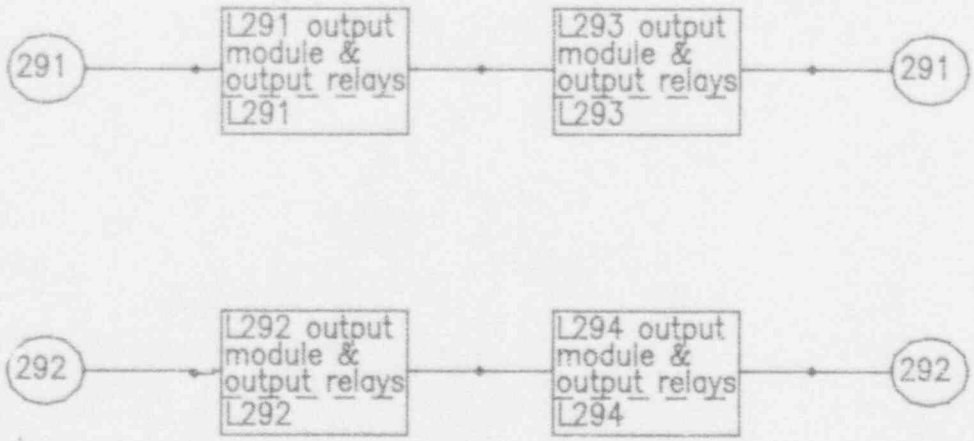
Bechtel ESFAS (Davis-Besse)



Bechtel ESFAS (Davis-Besse)

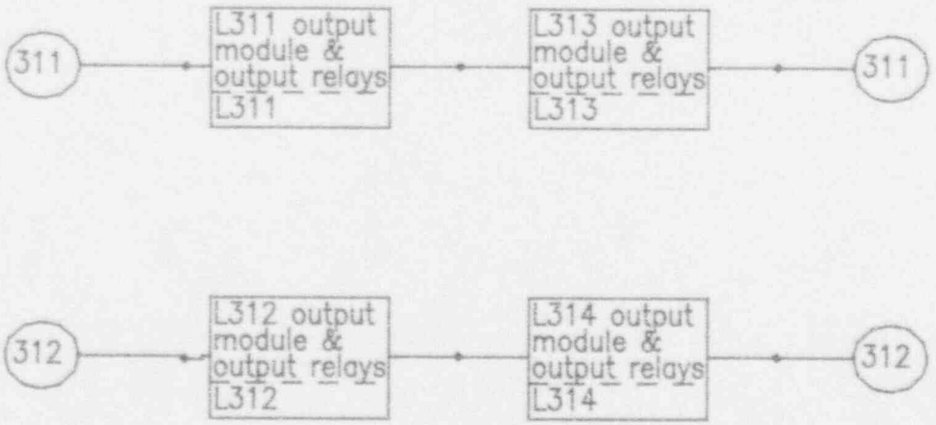


Bechtel ESFAS (Davis-Besse)

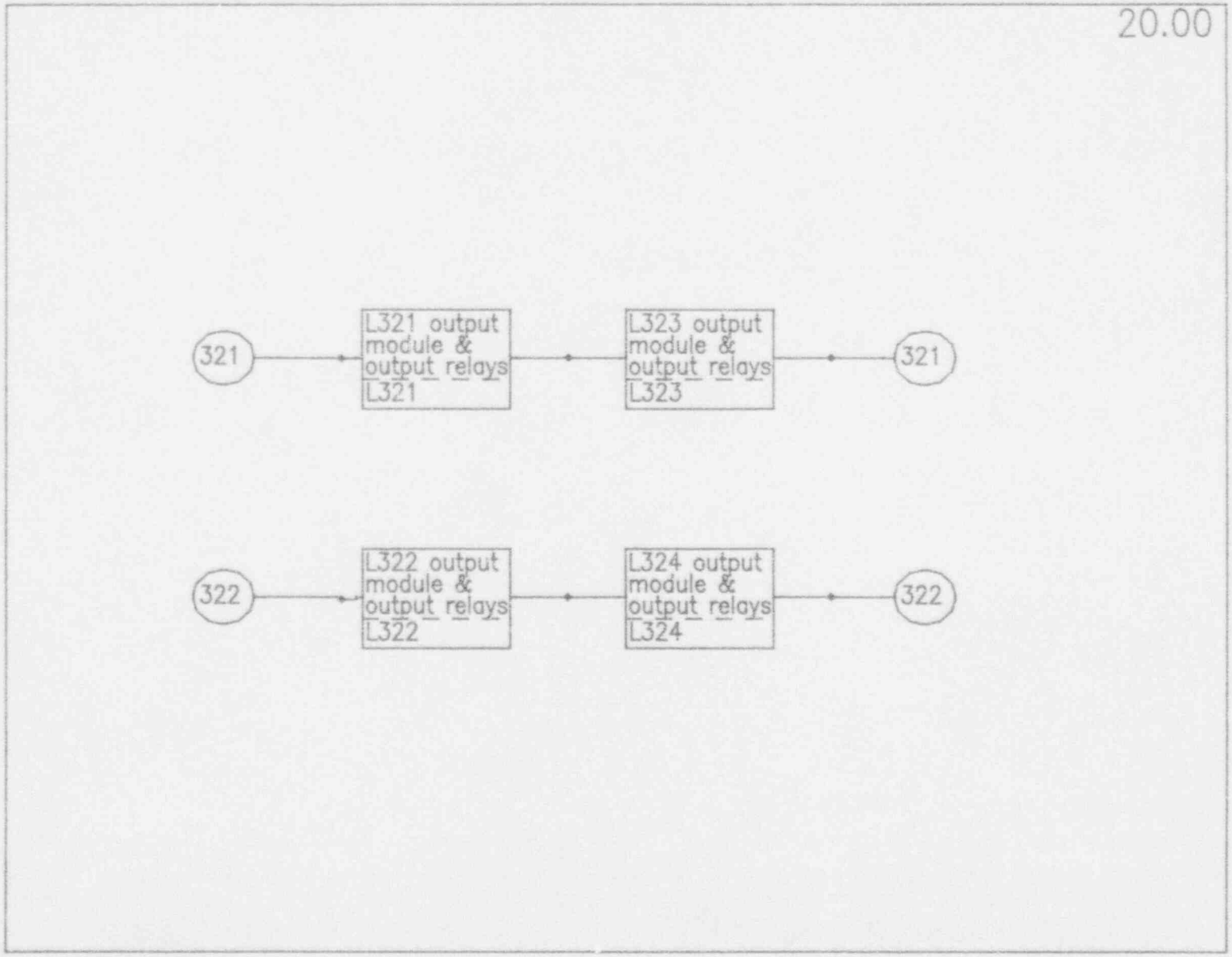


Bechtel ESFAS (Davis-Besse)

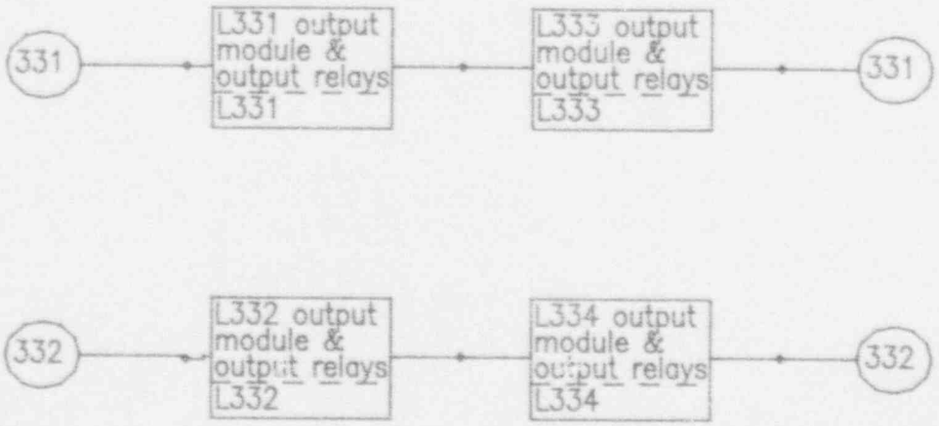
19.00



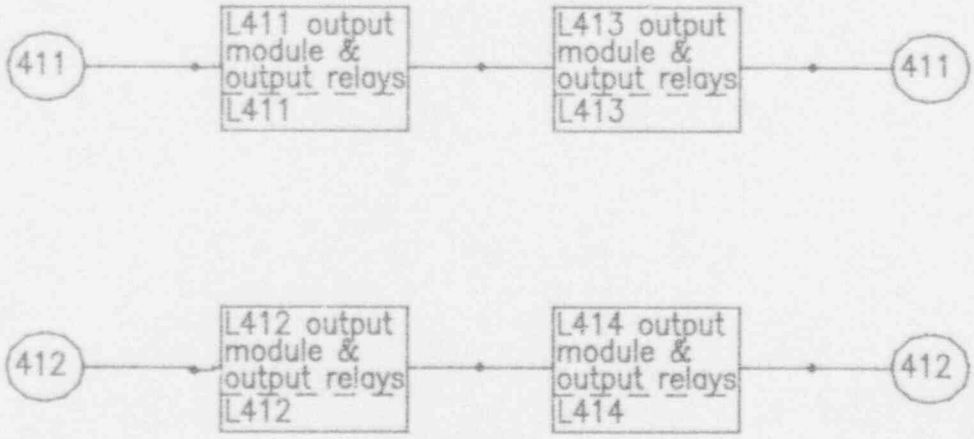
Bechtel ESFAS (Davis-Besse)



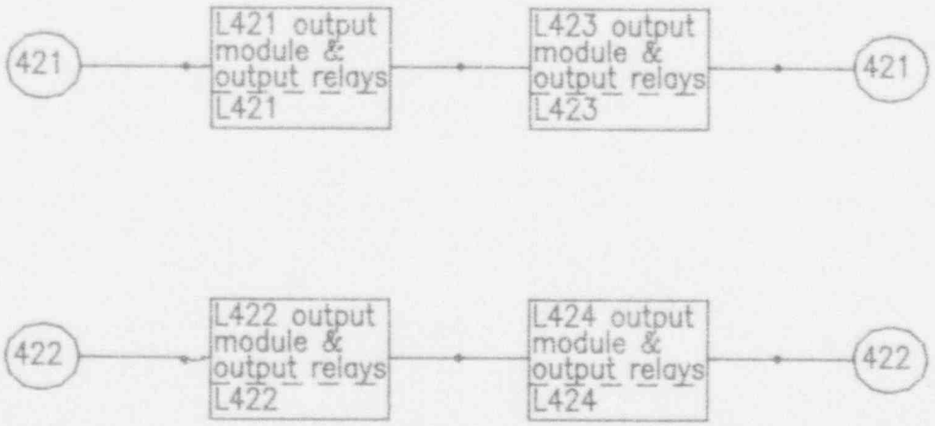
Bechtel ESFAS (Davis-Besse)



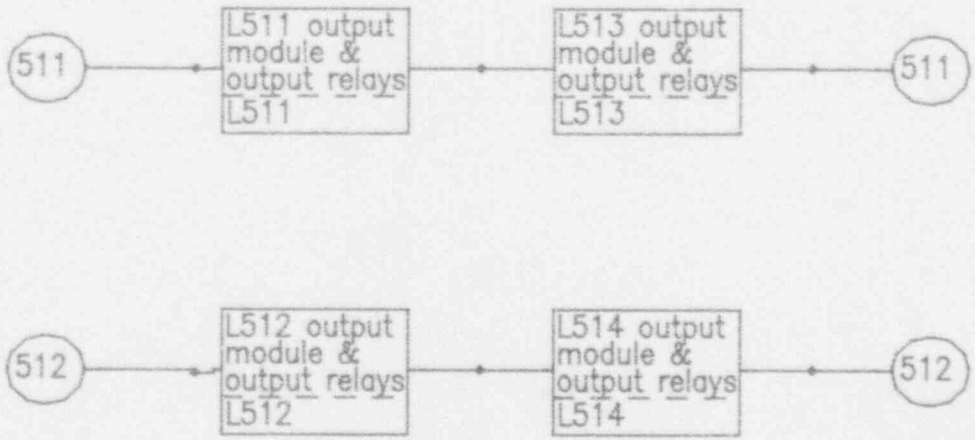
Bechtel ESFAS (Davis-Besse)



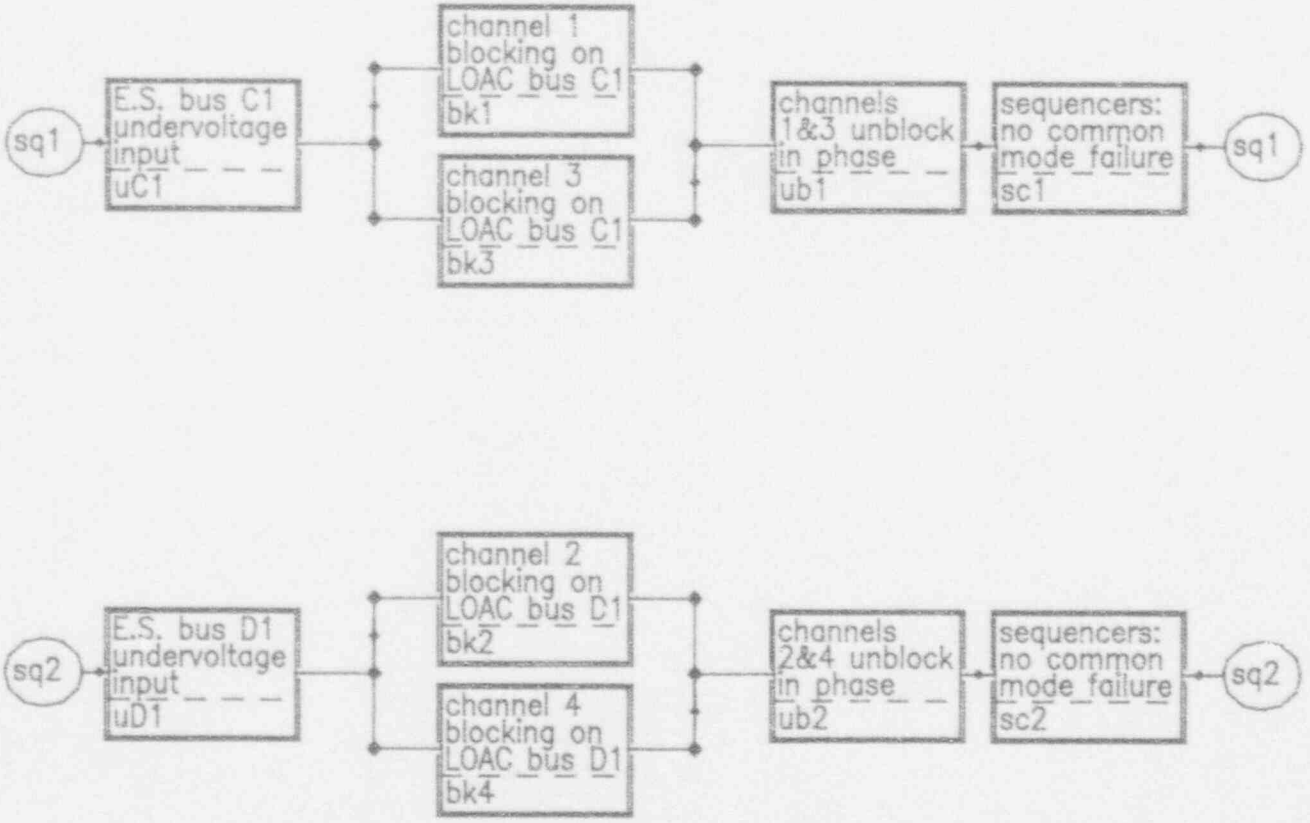
Bechtel ESFAS (Davis-Besse)

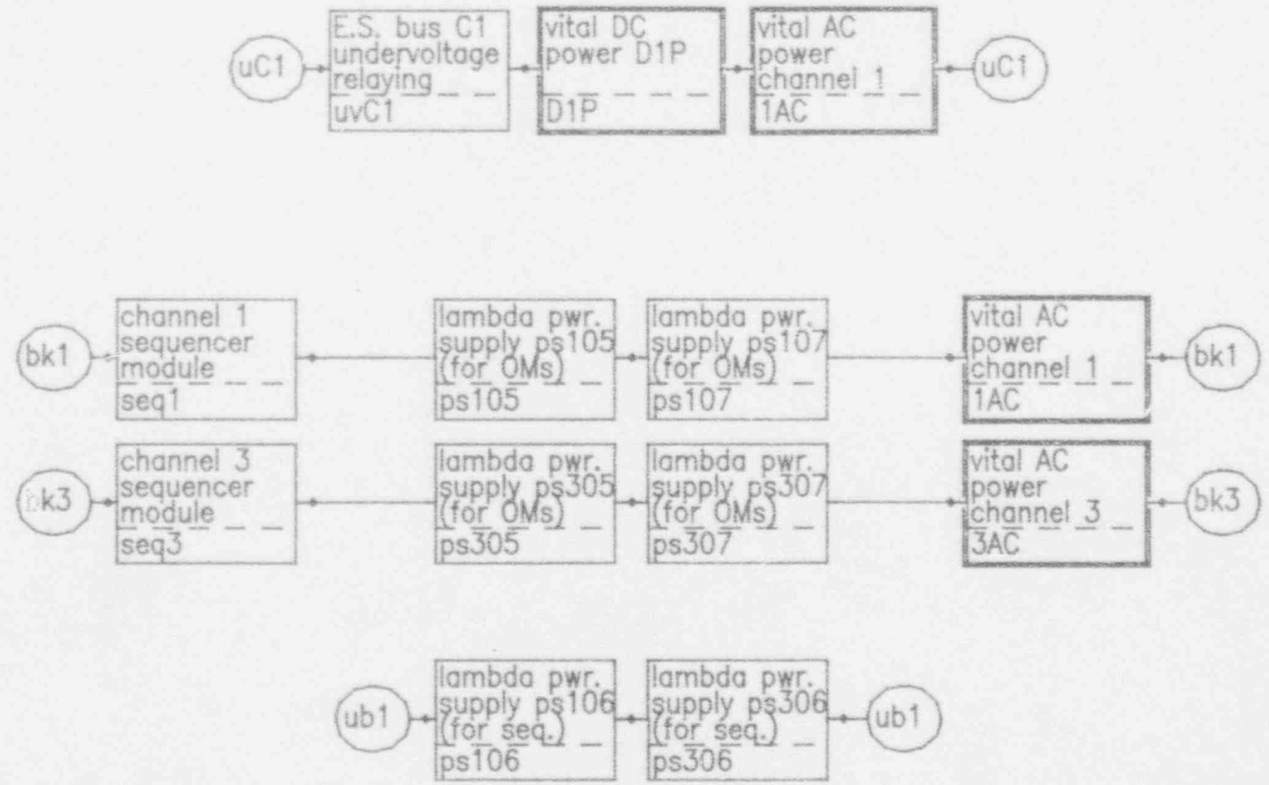


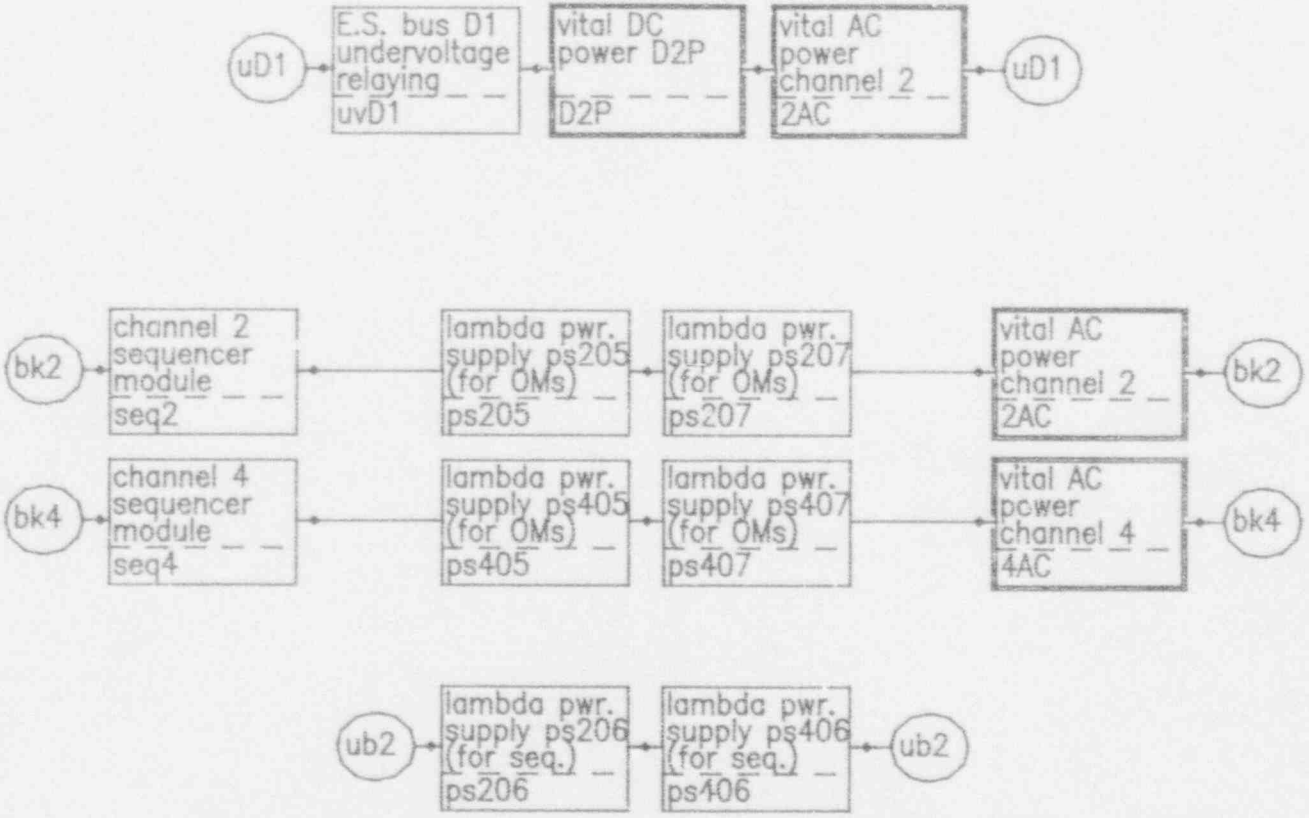
Bechtel ESFAS (Davis–Besse)

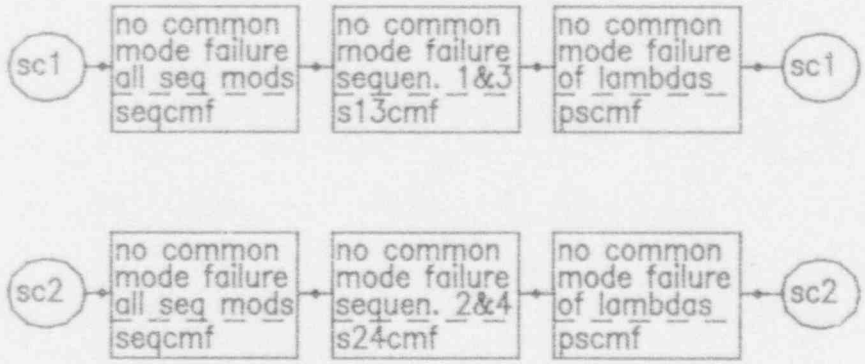


Bechtel ESFAS (Davis-Besse)

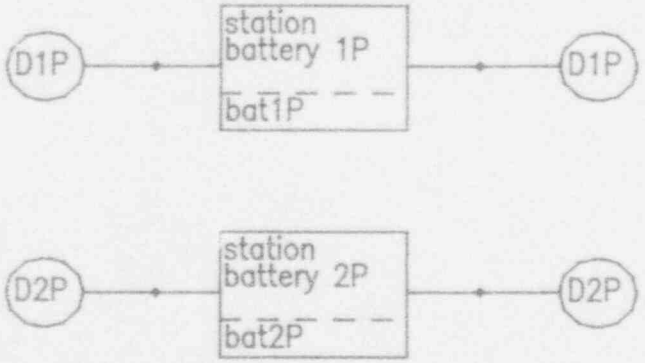

sq1
E.S. bus C1 undervoltage input uC1
channel 1 blocking on LOAC bus C1 bk1
channel 3 blocking on LOAC bus C1 bk3
channels 1&3 unblock in phase ub1
sequencers: no common mode failure sc1
sq1
sq2
E.S. bus D1 undervoltage input uD1
channel 2 blocking on LOAC bus D1 bk2
channel 4 blocking on LOAC bus D1 bk4
channels 2&4 unblock in phase ub2
sequencers: no common mode failure sc2
sq2

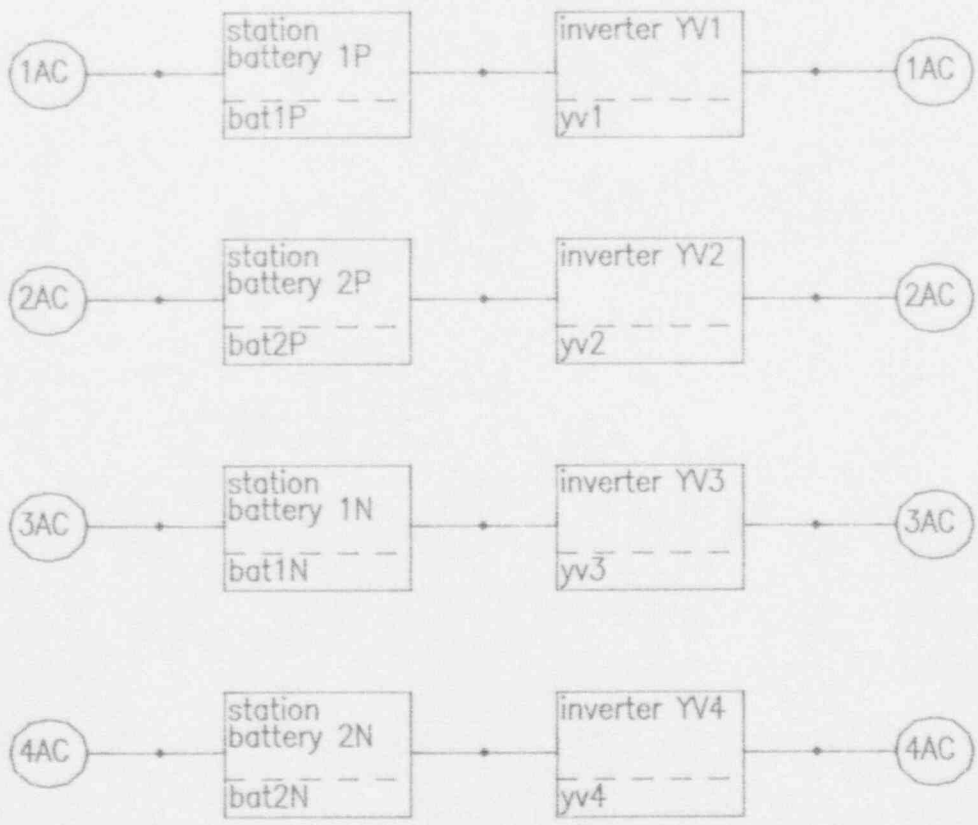

uC1
E.S. bus C1 undervoltage relaying
uvC1
vital DC power D1P
D1P
vital AC power channel 1
1AC
uC1
bk1
channel 1 sequencer module
seq1
lambda pwr. supply ps105 (for OMs)
ps105
lambda pwr. supply ps107 (for OMs)
ps107
vital AC power channel 1
1AC
bk1
bk3
channel 3 sequencer module
seq3
lambda pwr. supply ps305 (for OMs)
ps305
lambda pwr. supply ps307 (for OMs)
ps307
vital AC power channel 3
3AC
bk3
ub1
lambda pwr. supply ps106 (for seq.)
ps106
lambda pwr. supply ps306 (for seq.)
ps306
ub1


uD1
E.S. bus D1 undervoltage relaying
uvD1
vital DC power D2P
D2P
vital AC power channel 2
2AC
uD1
bk2
channel 2 sequencer module
seq2
lambda pwr. supply ps205 (for OMs)
ps205
lambda pwr. supply ps207 (for OMs)
ps207
vital AC power channel 2
2AC
bk2
bk4
channel 4 sequencer module
seq4
lambda pwr. supply ps405 (for OMs)
ps405
lambda pwr. supply ps407 (for OMs)
ps407
vital AC power channel 4
4AC
bk4
ub2
lambda pwr. supply ps206 (for seq.)
ps206
lambda pwr. supply ps406 (for seq.)
ps406
ub2



Bechtel ESFAS (Davis-Besse)


station
battery 1P
bat1P
D1P
D1P
station
battery 2P
bat2P
D2P
D2P



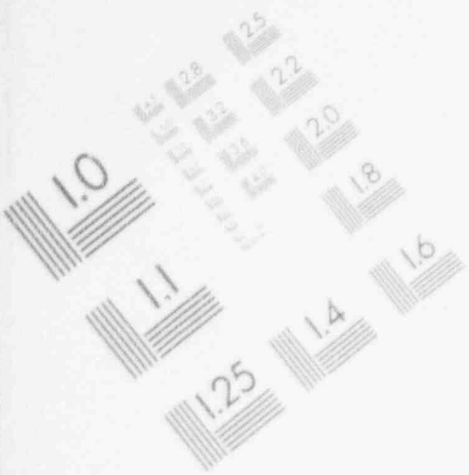
Bechtel ESFAS (Davis-Besse)

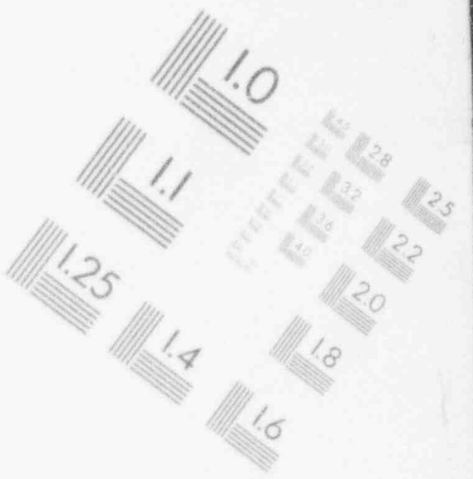
1

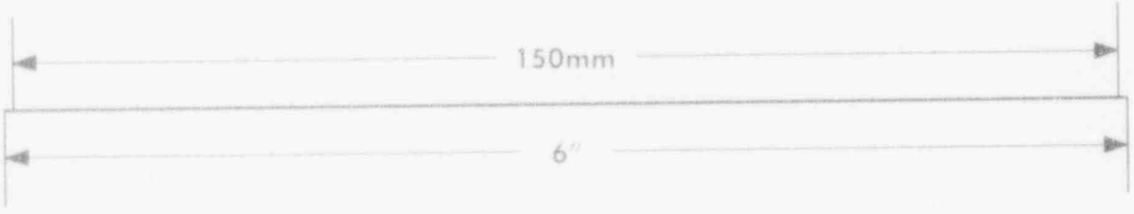
IMAGE EVALUATION TEST TARGET (MT-3)

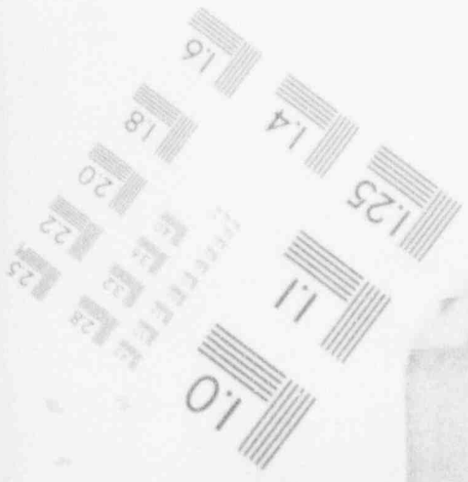
1

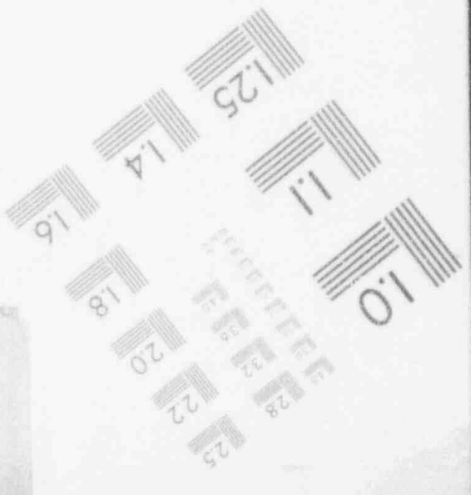
IMAGE EVALUATION TEST TARGET (MT-3)





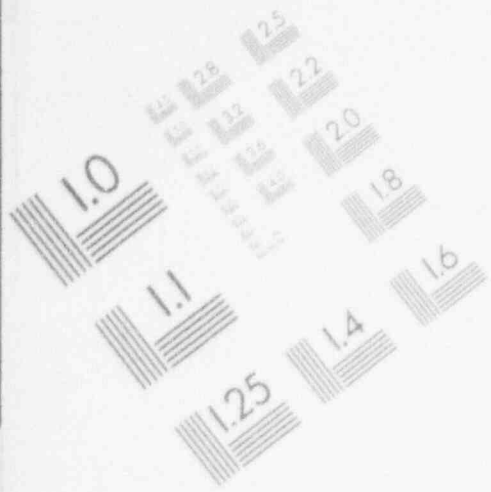


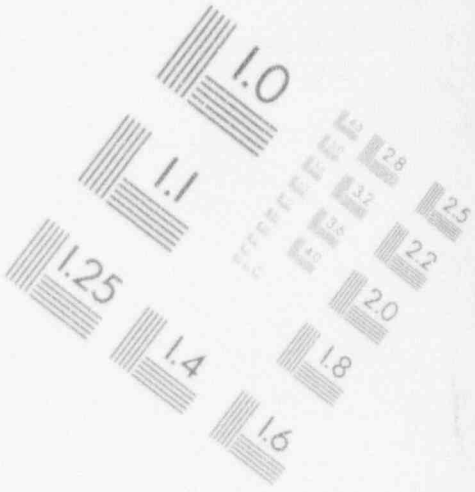


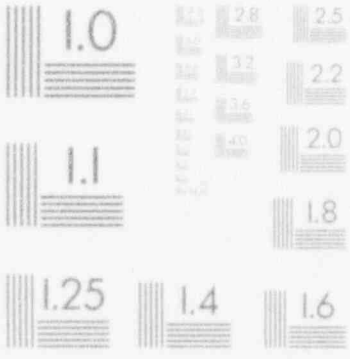


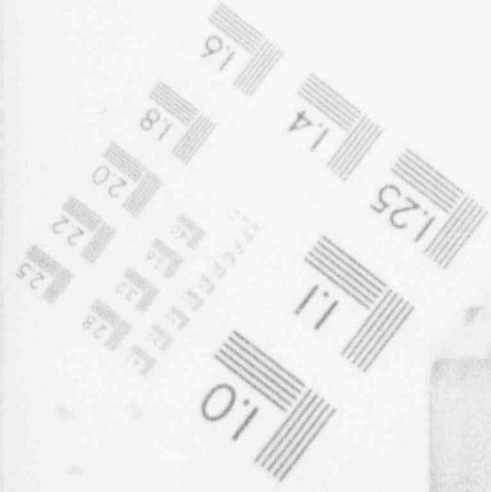
1

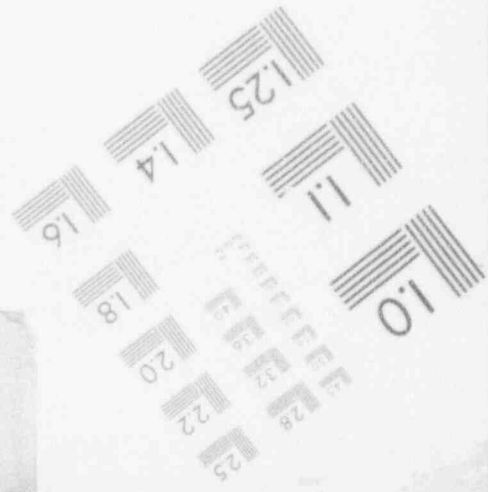
IMAGE EVALUATION TEST TARGET (MT-3)

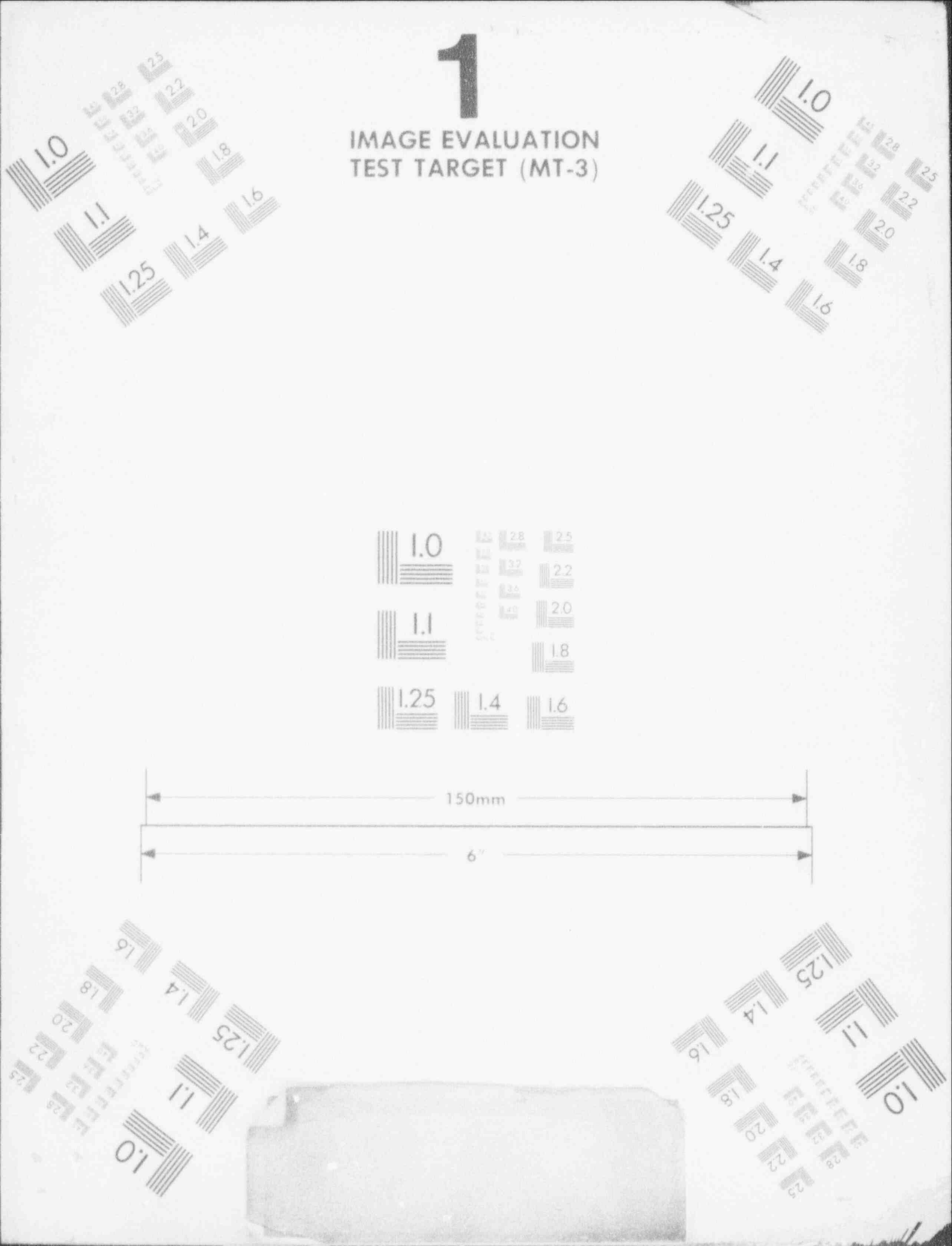


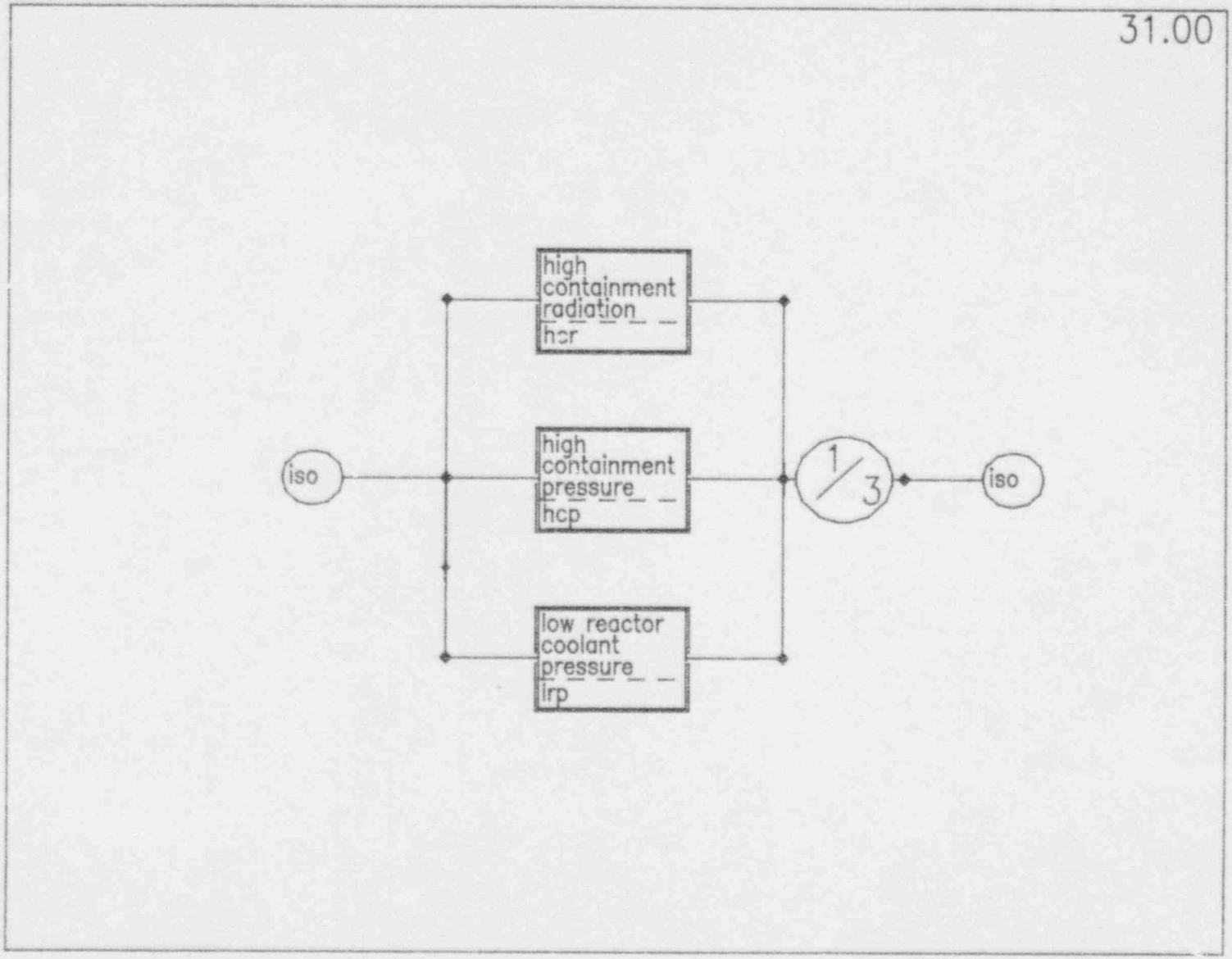




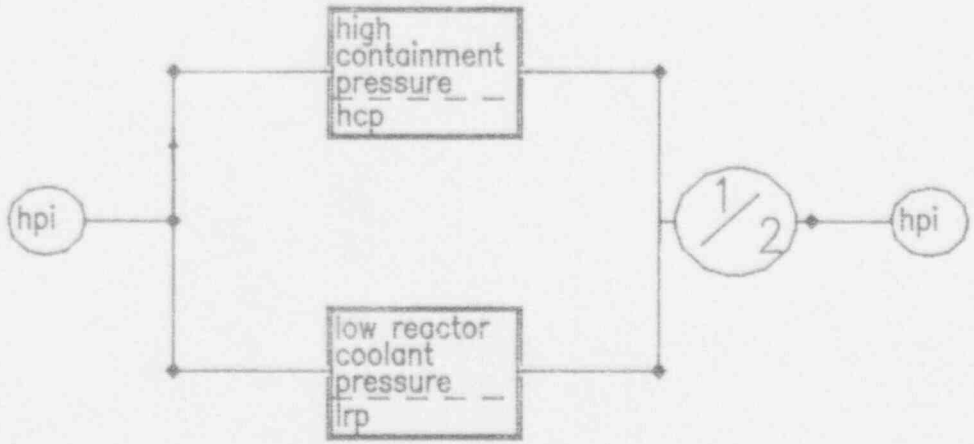





1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

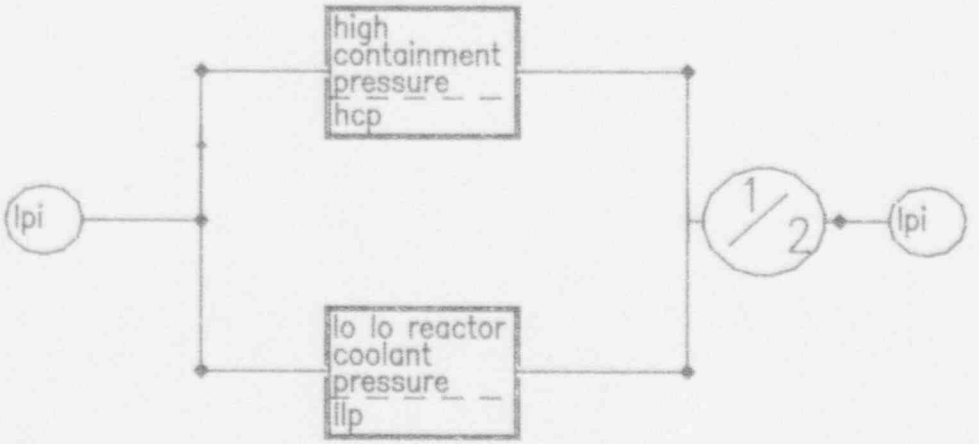


Bechtel ESFAS (Davis–Besse)

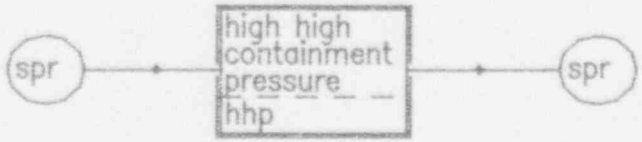


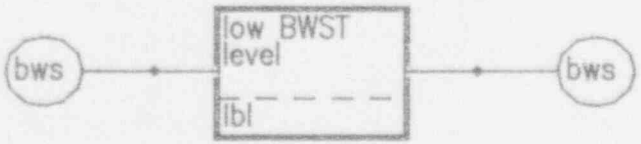
Bechtel ESFAS (Davis–Besse)

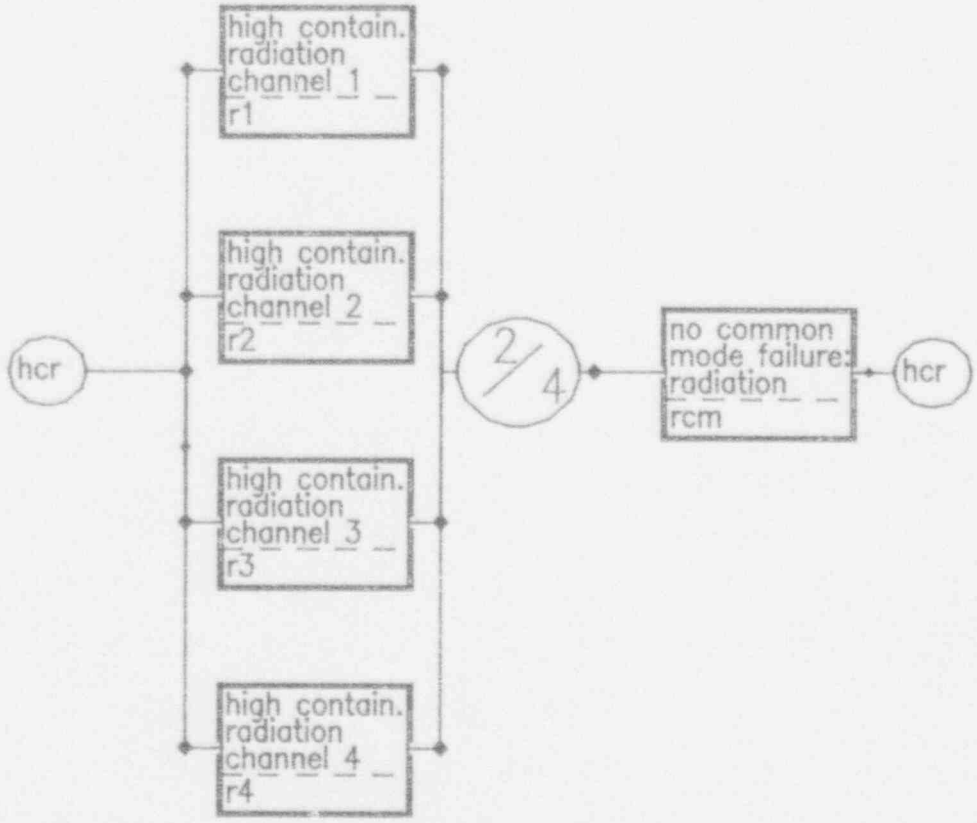
33.00



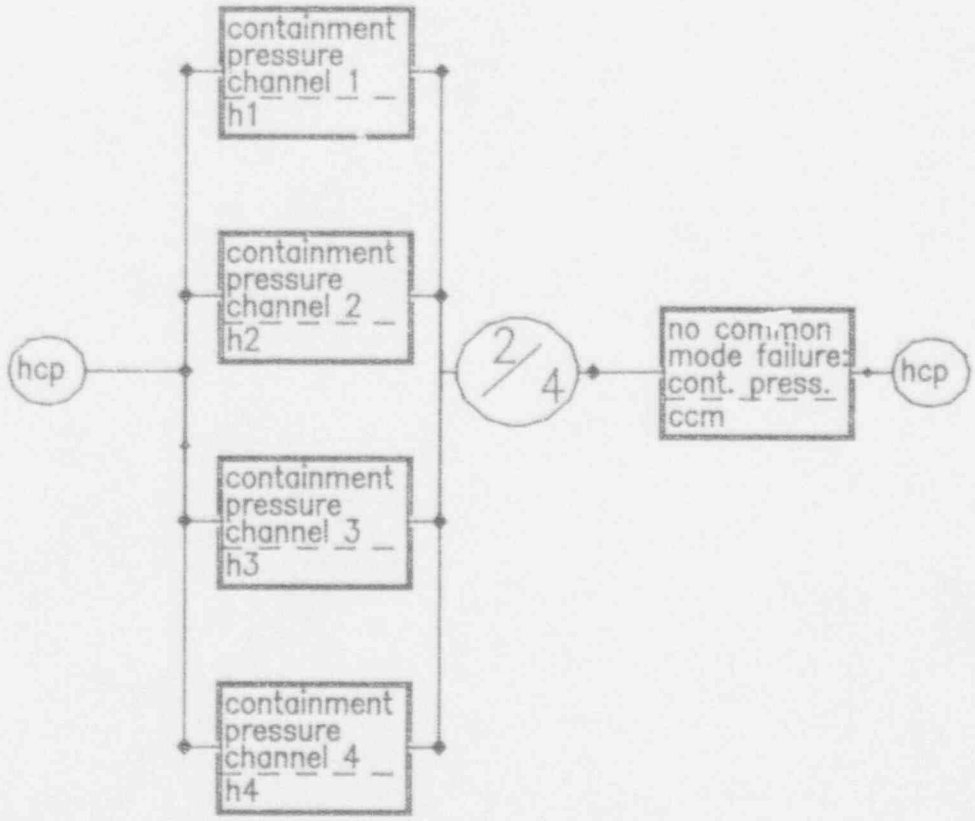
Bechtel ESFAS (Davis–Besse)


high high
containment
pressure
hhp
spr
spr


low BWST
level
lbl
bws
bws

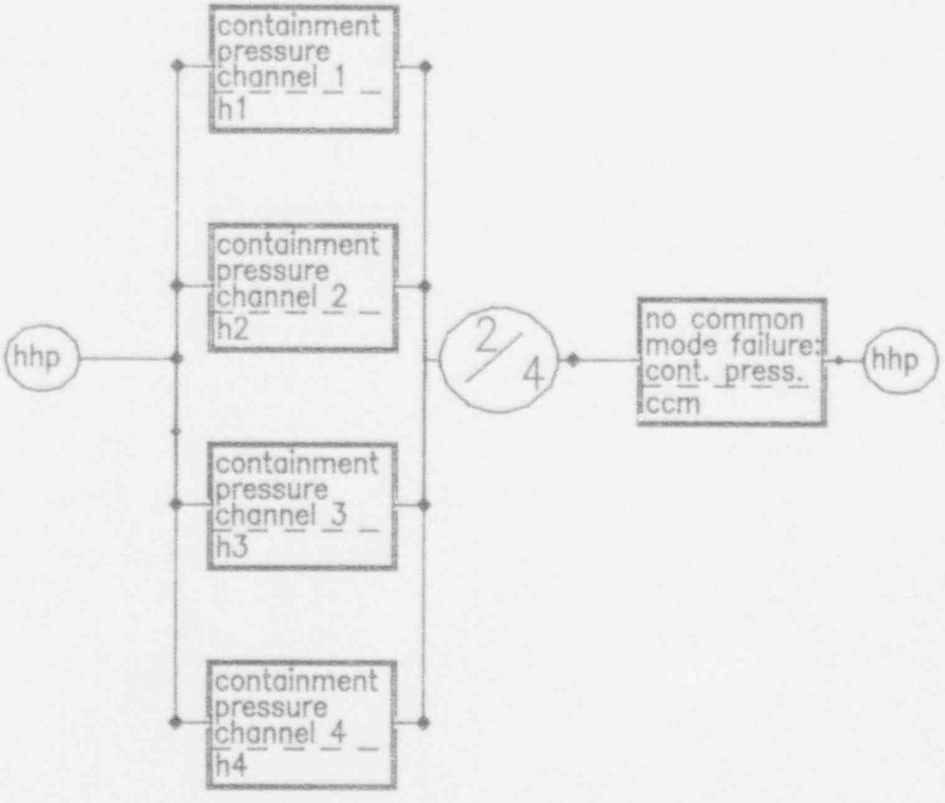


Bechtel ESFAS (Davis-Besse)

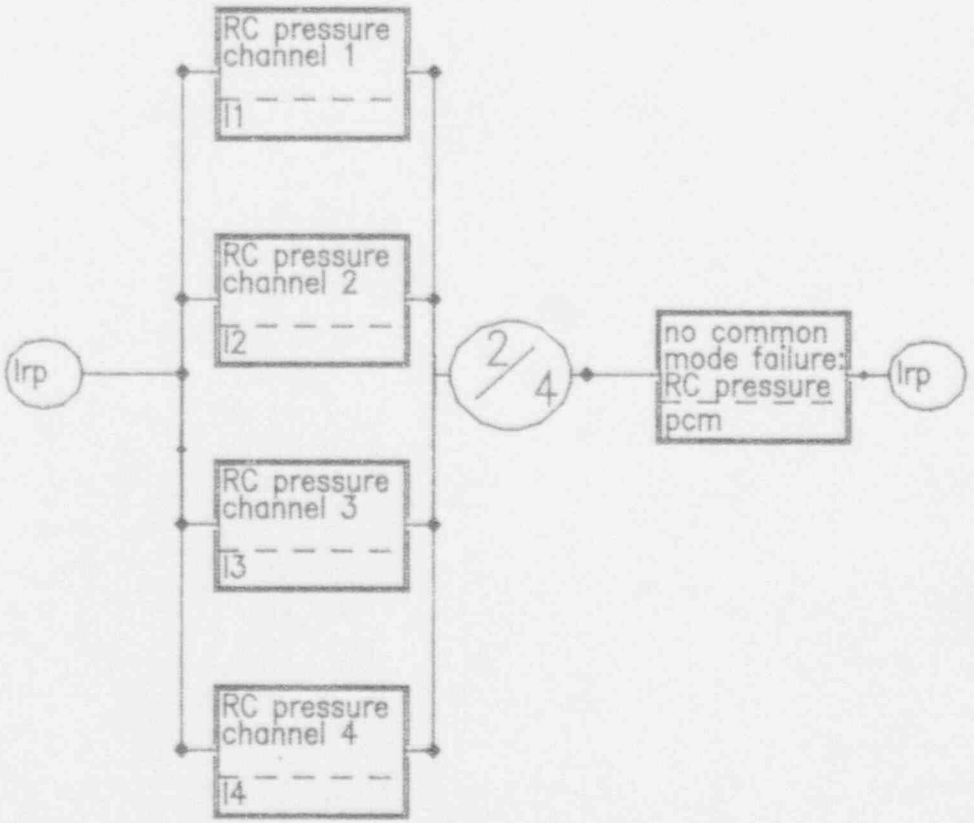


Bechtel ESFAS (Davis-Besse)

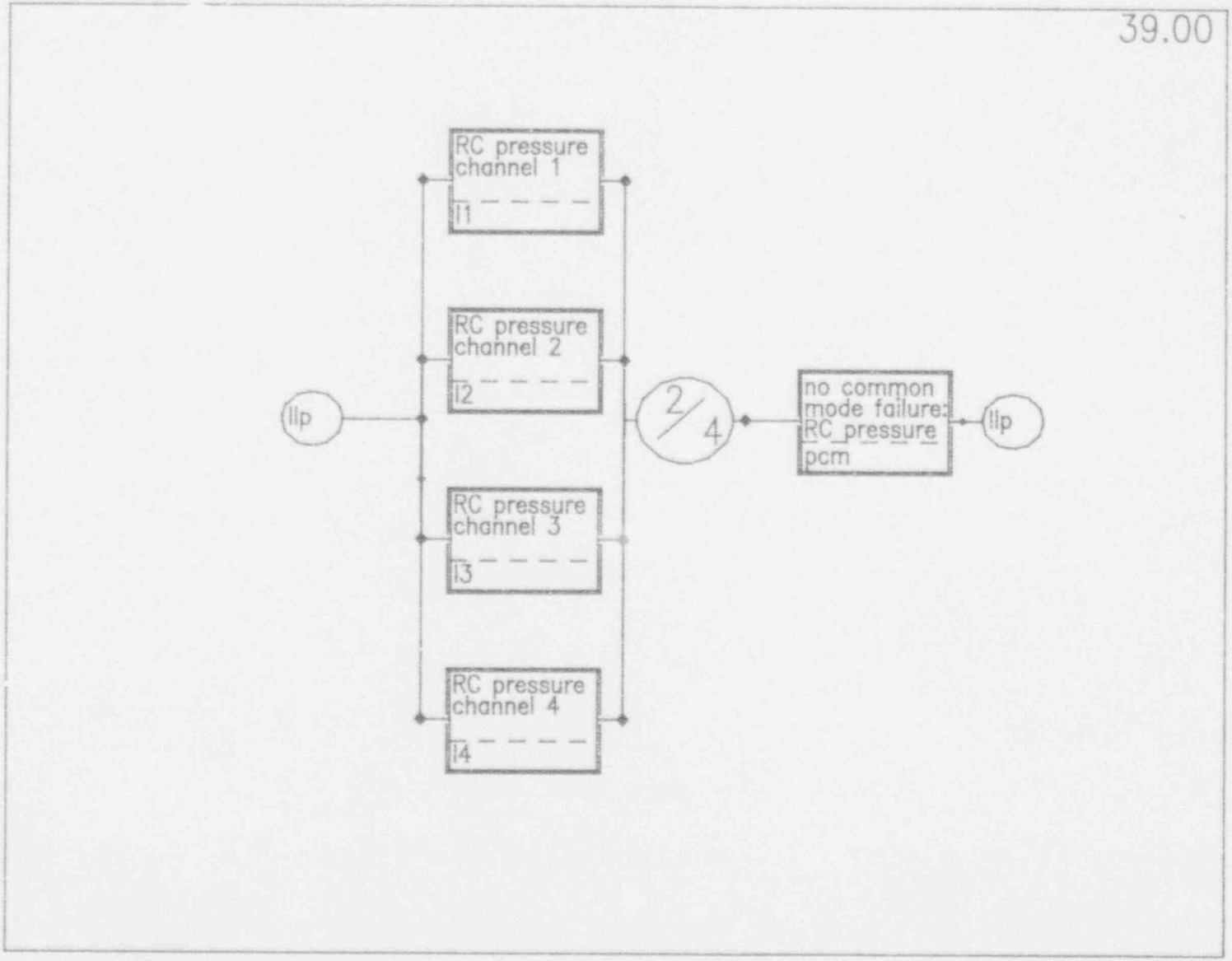
37.00



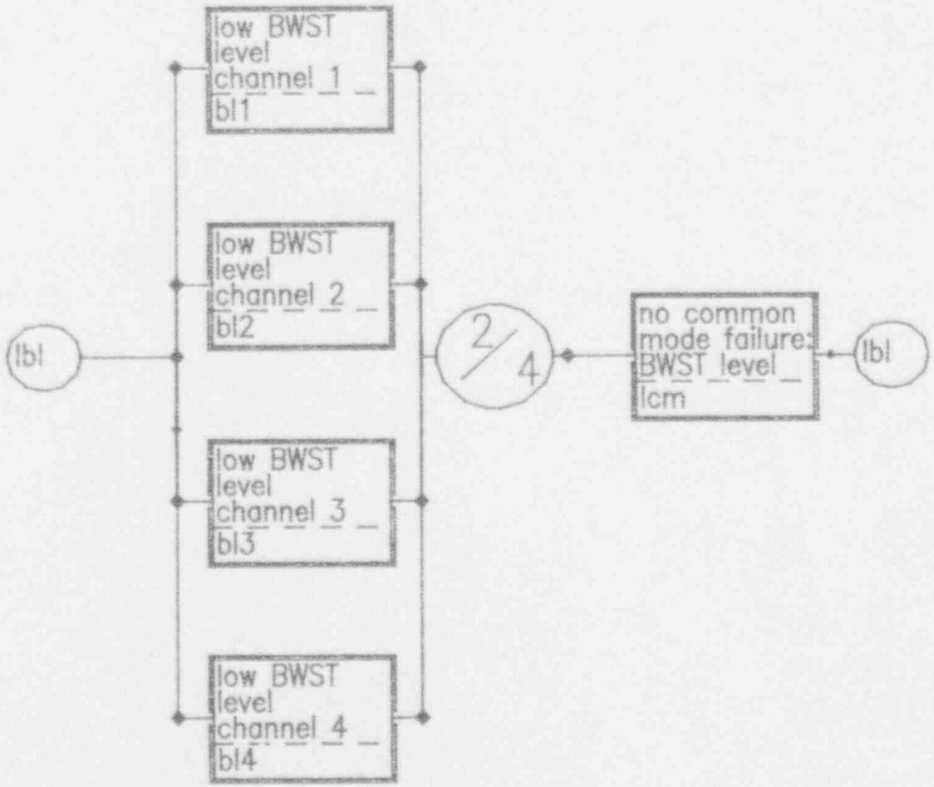
Bechtel ESFAS (Davis–Besse)



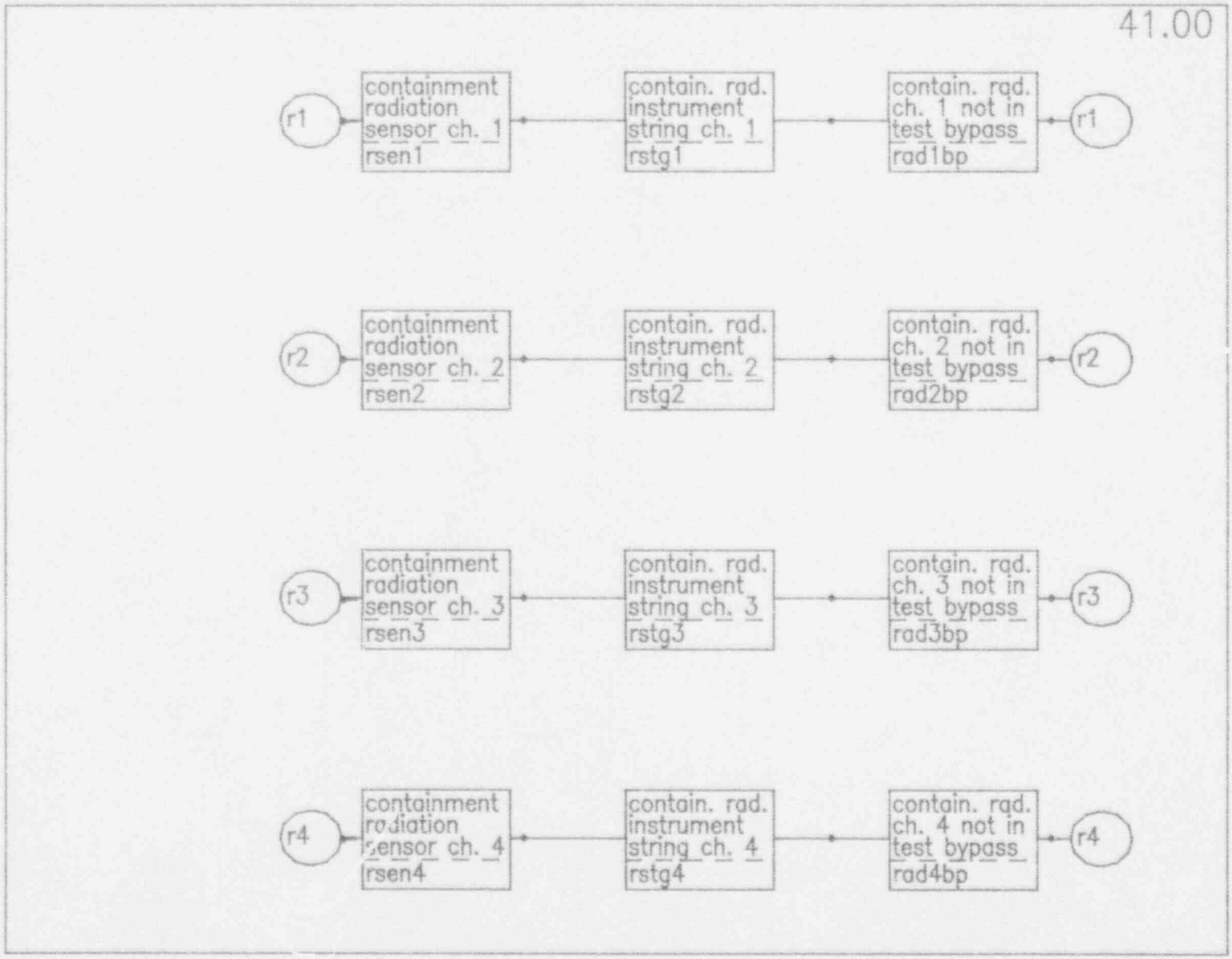
Bechtel ESFAS (Davis–Besse)



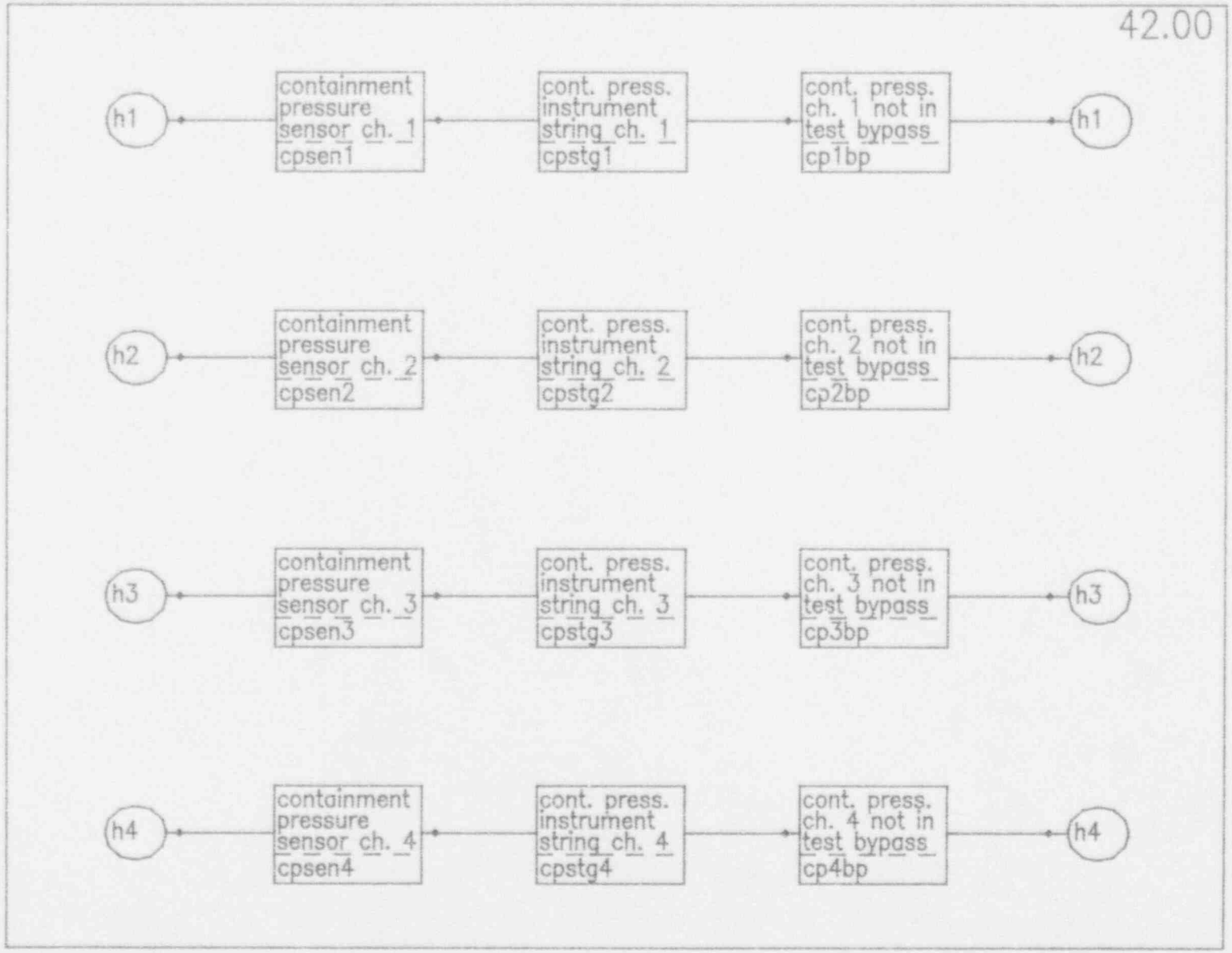
Bechtel ESFAS (Davis–Besse)



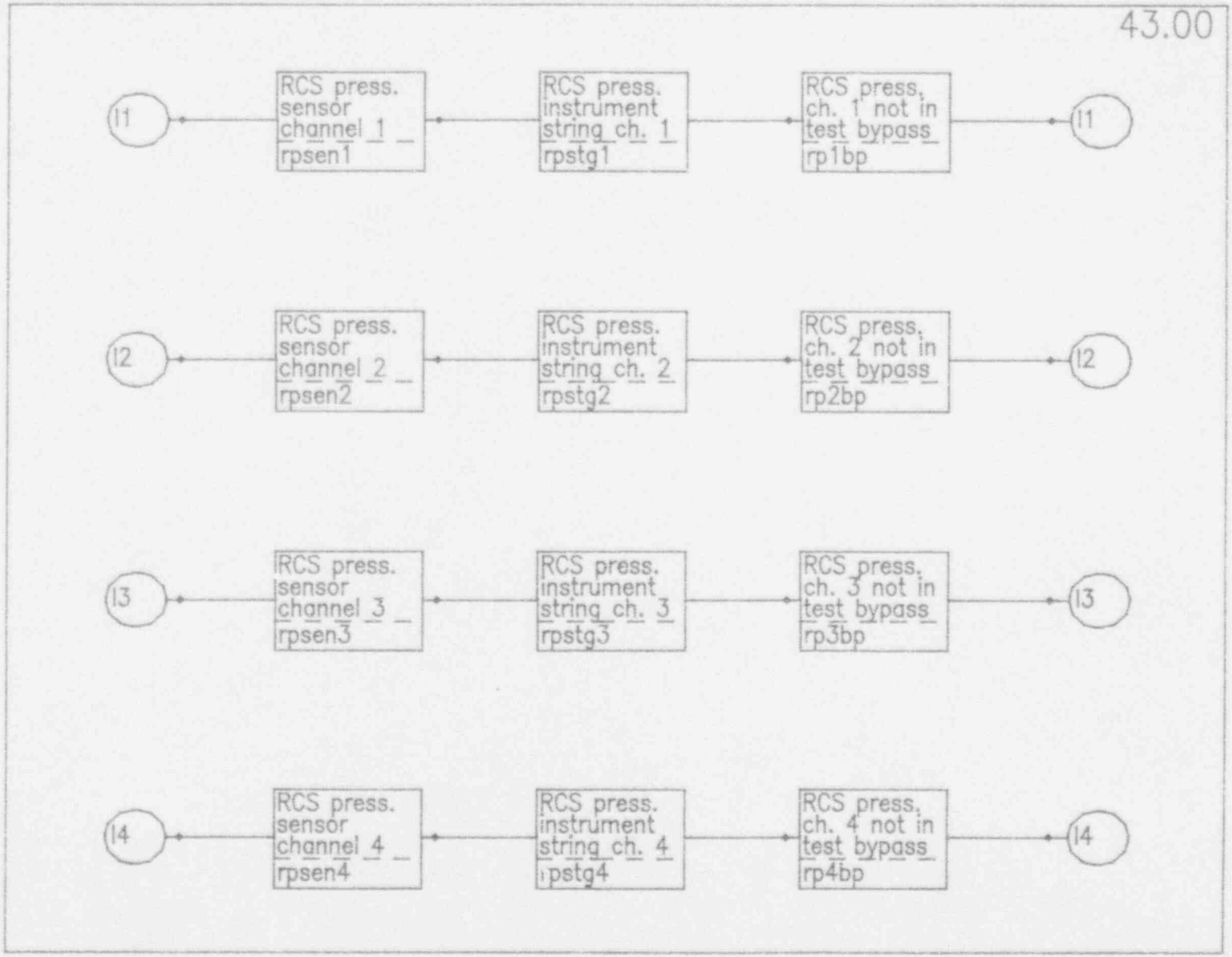
Bechtel ESFAS (Davis-Besse)



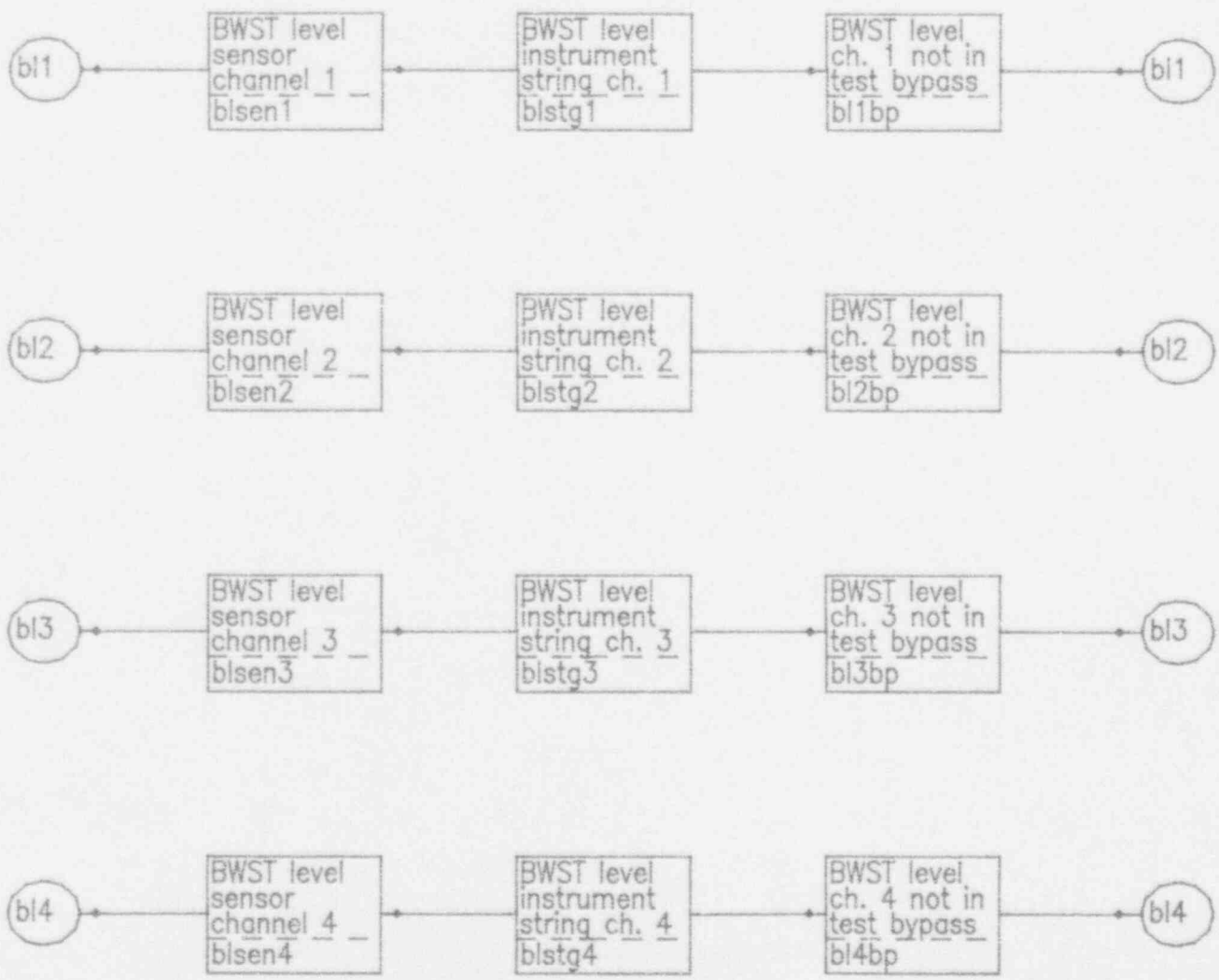
Bechtel ESFAS (Davis–Besse)



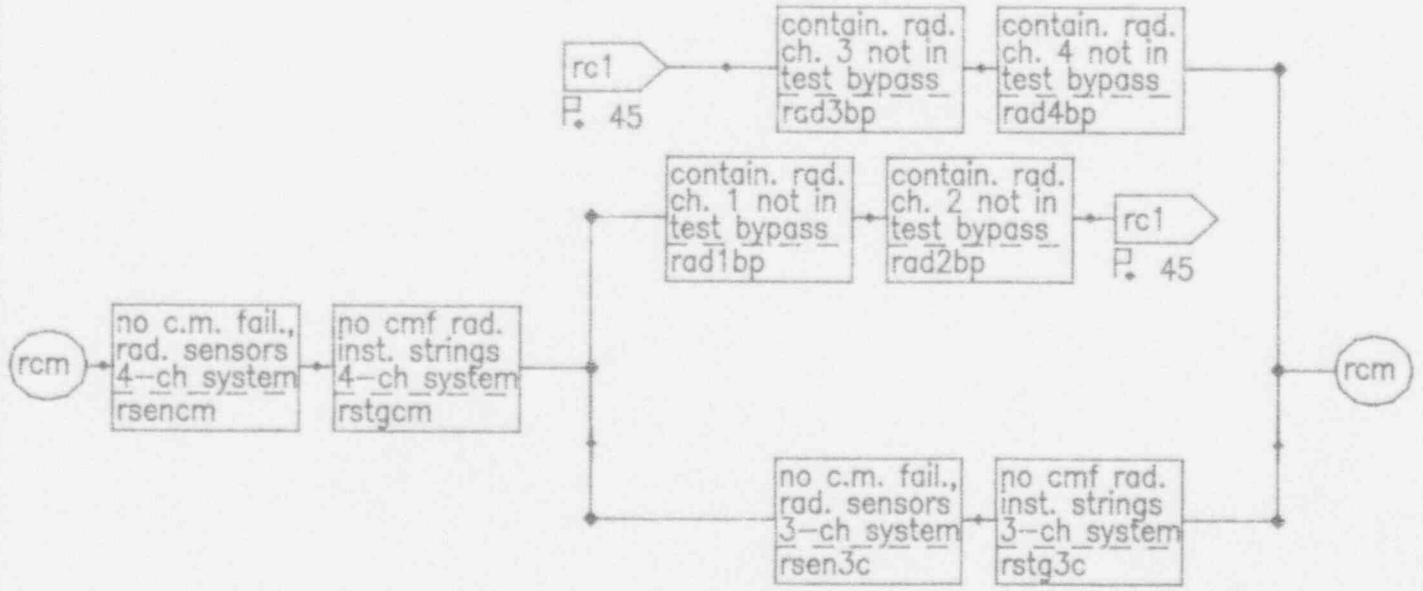
Bechtel ESFAS (Davis–Besse)

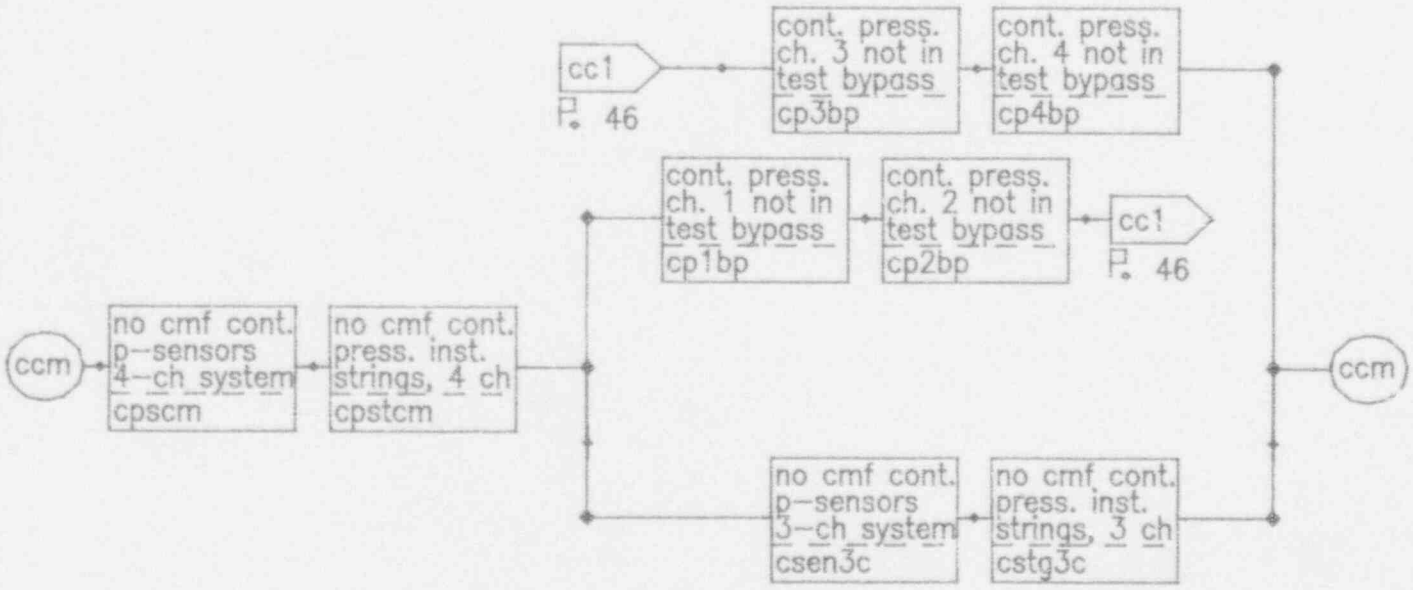


Bechtel ESFAS (Davis–Besse)

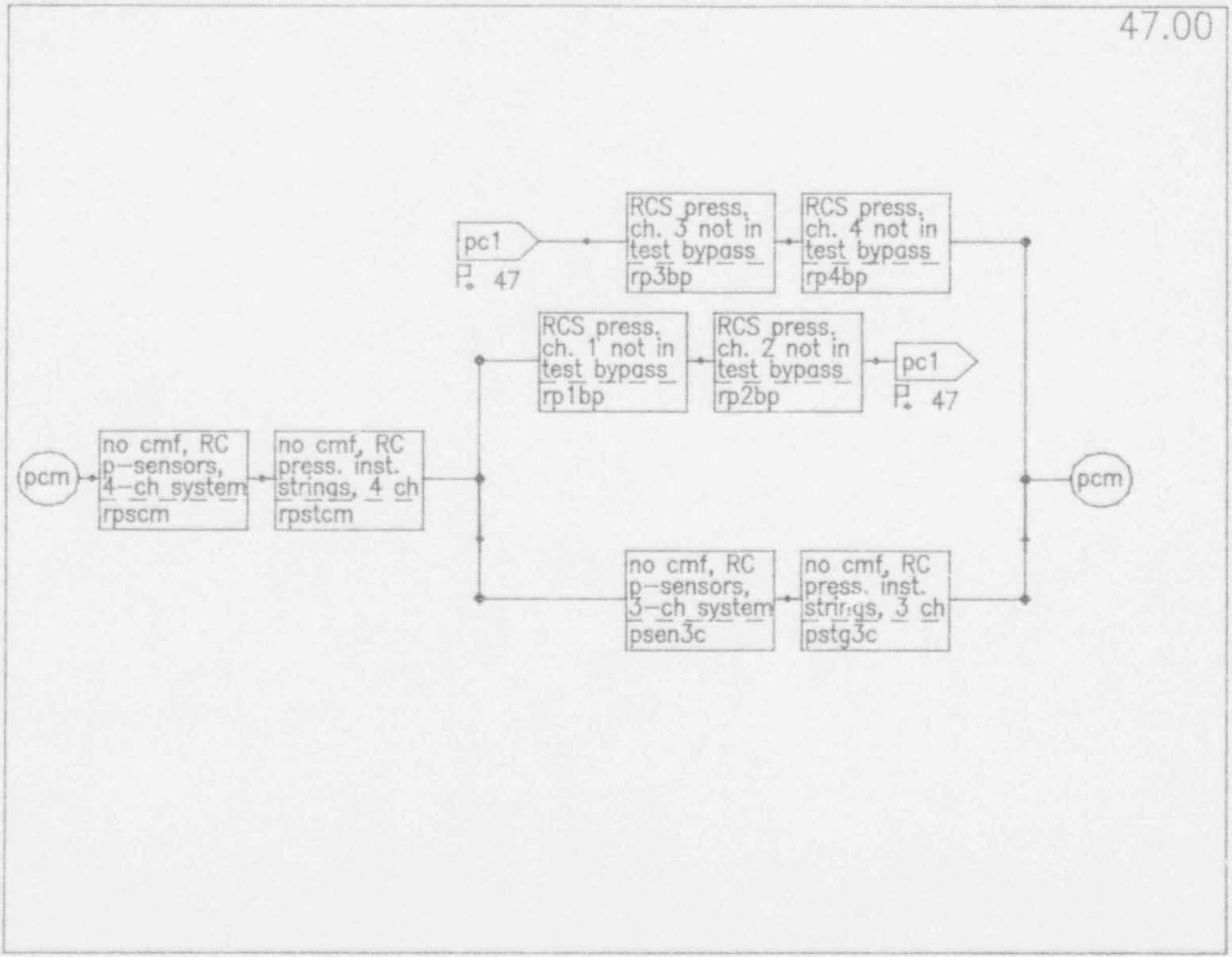


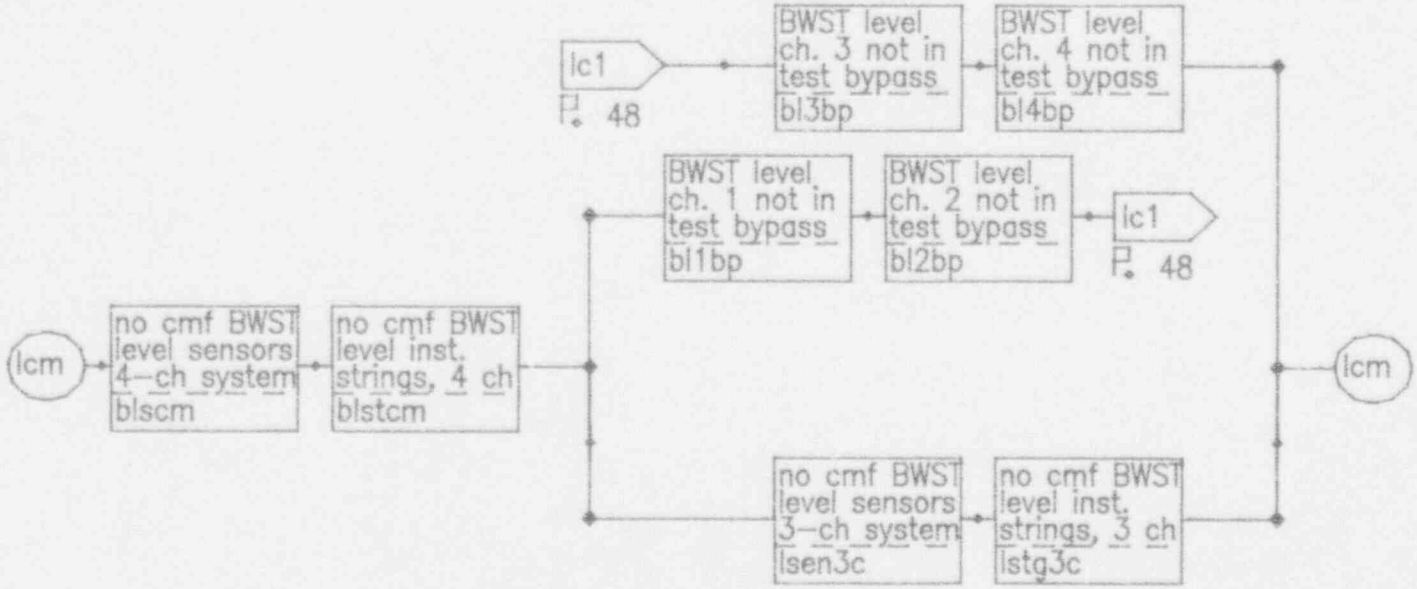
Bechtel ESFAS (Davis-Besse)


rc1
P. 45
contain. rad. ch. 3 not in test bypass
rad3bp
contain. rad. ch. 4 not in test bypass
rad4bp
contain. rad. ch. 1 not in test bypass
rad1bp
contain. rad. ch. 2 not in test bypass
rad2bp
rc1
P. 45
rcm
no c.m. fail., rad. sensors 4-ch system
rsencm
no cmf rad. inst. strings 4-ch system
rstgcm
rcm
no c.m. fail., rad. sensors 3-ch system
rsen3c
no cmf rad. inst. strings 3-ch system
rstg3c



Bechtel ESFAS (Davis-Besse)


pc1
P. 47
RCS press. ch. 3 not in test bypass
rp3bp
RCS press. ch. 4 not in test bypass
rp4bp
RCS press. ch. 1 not in test bypass
rp1bp
RCS press. ch. 2 not in test bypass
rp2bp
pc1
P. 47
pcm
no cmf, RC p-sensors, 4-ch system
rpscm
no cmf, RC press. inst. strings, 4 ch
rpstcm
no cmf, RC p-sensors, 3-ch system
psen3c
no cmf, RC press. inst. strings, 3 ch
pstg3c
pcm


lc1
P. 48
BWST level ch. 3 not in test bypass
bl3bp
BWST level ch. 4 not in test bypass
bl4bp
BWST level ch. 1 not in test bypass
bl1bp
BWST level ch. 2 not in test bypass
bl2bp
lc1
P. 48
lcm
no cmf BWST level sensors 4-ch system
blscm
no cmf BWST level inst. strings, 4 ch
blstcm
lcm
no cmf BWST level sensors 3-ch system
lsen3c
no cmf BWST level inst. strings, 3 ch
lstg3c

APPENDIX D

HUMAN FAILURE PROBABILITY SENSITIVITY ANALYSIS

D.1. Introduction

As discussed in Section 4.7, the time available for human action to avert core damage is an important parameter for determining the risk-impact of ESFAS failure. This time parameter was used in determining the human error probabilities for manual actuation of ES functions that fail to actuate automatically. These probabilities were used in the ESFAS model quantification to determine if the core-melt risk changes significantly when the ESFAS STI is extended. To determine if assumptions of time-to-core-damage have a significant impact on the incremental risk associated with extending the ESFAS STI, a sensitivity analysis was performed.

D.2. Methodology

As discussed in Section 4.7, the probabilities of human error for recovery from ESFAS failure are taken from NUREG/CR-4834 [7] and are based on the time available for the human to react. To perform the sensitivity study, the time available for human reaction was halved, and new human error probabilities were calculated, as shown in Table D-1. Using the perturbed human recovery probabilities in the original models, the core damage risk due to ESFAS failure was recomputed. This was performed for all three ESFAS designs (Bailey, Gilbert, and Bechtel) for both one-month and three-month test intervals (six different cases).

D.3. Results

Table D-2 gives a summary of the contribution to core melt frequency (risk) due to ESFAS failure for the aggregate of all challenging events, for one- and three-month test intervals using the base analysis data and the sensitivity data for human failure probabilities. The delta (or incremental) risk is computed by subtracting the risk of core melt using a one-month test interval from the risk of core melt using a three-month test interval. Thus, the incremental risk represents the increase in core melt frequency from an ESFAS failure due to the changing of the test interval from one month to three months. This is the same procedure that is discussed in Section 5.2. Figure D-1 graphically shows the

results of the sensitivity analysis superimposed on the base analysis results (Figure 5-7). Note that the sensitivity traces are relatively flat, indicating little sensitivity to the ESFAS test interval.

D.4. Conclusions

Although the incremental risk increases (as expected) when the human action times are halved, the increase of the mean incremental core melt frequency associated with the extension of the STI from one to three months is still small as compared to the Commissioner's safety goal. Accordingly, while there may be some sensitivity to the values of human recovery probabilities used in the base analysis, this analysis shows it is not significant and the test interval extension is justified in light of the negligible increase in the overall core melt frequency.

Table D-1

Manual Recovery Probabilities for Sensitivity Analysis
for Determining Risk-Significance of ESFAS Failure Consequences

Manual Recovery Action	Applicable ESFAS Challenging Event	Perturbed Time Available (after ESFAS failure) to Avert Core Melt[a]	Perturbed Probability of Non-Recovery
Initiate Safety Injection	A, B, C	15 minutes	0.044
	D	7½ minutes	0.140
	F	30 minutes	0.013
Initiate RB Long-Term Cooling	A, B, C, F	at least 30 minutes	0.013
	D	at least 15 minutes	0.044
Isolate Interfacing Systems LOCA	E	at least 15 minutes	0.044
Actuate BWST Level permissive (D-B)	A, B, C, F	at least 12½ minutes	0.0615
	D	at least 5 minutes	0.235

[a] These values are one-half of the values that appear in Table 4-4.

Table D-2

Results of the Human Recovery Probability
Sensitivity Analysis

	Core Melt Risk due to ESFAS Failure (/Rx-yr)	
	Base Analysis	Sensitivity Analysis
BAILEY DESIGN (OCONEE and ANO-1)		
One-Month	4.00e-7	1.14e-6
Three Months	5.40e-7	1.55e-6
Delta Risk	1.40e-7	4.10e-7
GILBERT DESIGN (CRYSTAL RIVER 3)		
One-Month	2.11e-8	6.00e-8
Three-Months	4.14e-8	1.20e-7
Delta Risk	2.03e-8	6.00e-8
BECHTEL DESIGN (DAVIS-BESSE)		
One-Month	5.26e-7	1.69e-6
Three-Month	6.10e-7	1.95e-6
Delta Risk	8.35e-8	2.60e-7

Figure D-1: Core Melt Risk due to ESFAS Failure vs. STI
Summary of Base and Sensitivity Analysis