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

AUG 7 1985

MEMORANDUM FOR: Gary M. Holahan, Chief
Operating Reactors Assessment Branch, DL

FROM: J. T. Beard, Reactor Systems Engineer
Operating Reactors Assessment Branch, DL

SUBJECT: DAVIS-BESSE---STEAM AND FEEDWATER RUPTURE CONTROL SYSTEM

Reference: NRC memorandum, Thompson to Denton, "Preliminary Review of the Design and Performance of the Davis-Besse Feedwater and Related Systems", July 2, 1985

The reference memorandum suggests that NRR may review the design of the Steam and Feedwater Rupture Control System (SFRCS) at the Davis-Besse plant. I believe a complete review of the adequacy of this system is essential. While on the NRC Fact Finding Team for the June 9, 1985 event, I developed some information on the SFRCS which should be useful in the NRR review, which is enclosed.

Because of the complexity of the SFRCS design, I had to develop a set of simplified diagrams for my own understanding. These diagrams were discussed with the licensee during transcribed meetings, and the technical accuracy of the diagrams was established. The Team agreed to handle this information separate from the report because the level of detail of both the diagrams and associated text material was not consistent with that desired for the Team's report (NUREG-1154) and the items may not be directly related to the event of June 9, 1985. Furthermore, the scope of the Team effort did not include detail design reviews to search for potential regulatory deficiencies. I believe this to be a proper and reasonable decision.

Three enclosures are provided. The first is a discussion of one design basis accident and the SFRCS as they relate to the single failure criterion. This discussion supplements the discussion in NUREG-1154. The second enclosure is a draft system description for the SFRCS, including the automatic control of equipment actuated by the SFRCS. The third enclosure identifies those areas of the SFRCS where the design is questionable. I did not attempt to review the SFRCS for compliance with any regulatory requirement, but in trying to gain an understanding of the design I found that these areas seemed to jump out. I believe further review is needed to determine if regulatory compliance is deficient in these areas or if any of the apparent descrepancies may be an acceptable deviation.

50-346

This supplementary technical information is being forwarded for three reasons. The NRR review of the SFRCS may benefit from the work that has already been done. If regulatory deficiencies may be present, I feel duty bound to assure that this information receives appropriate attention. This memo should implement the separate handling that the Team agreed to.

/S/

J. T. Beard
Operating Reactors Assessment Branch, DL

Enclosures: As stated

cc w/encl:
A. DeAgazio
F. Rosa
O. Parr
B. Sheron
E. Jordan
W. Rogers
C. Rossi

cc w/o encl:
H. Denton
H. Thompson
F. Miraglia
G. Lainas
D. Crutchfield
B. Bernero
J. Taylor
C. Heltemes

DISTRIBUTION (w/encl.)
PDR (Docket 50-346)
Central Files
R. Kendall
T. Dunning
J. Wermeil
J. T. Beard
R. Wessman

ORAB:DL
JTBeard:cl
8/07/85

This supplementary technical information is being forwarded for three reasons. The NRR review of the SFRCS may benefit from the work that has already been done. If regulatory deficiencies may be present, I feel duty bound to assure that this information receives appropriate attention. This memo should implement the separate handling that the Team agreed to.

/S/

J. T. Beard
Operating Reactors Assessment Branch, DL

Enclosures: As stated

cc w/encl:
A. DeAgazio
F. Rosa
O. Parr
B. Sheron
E. Jordan
W. Rogers
C. Rossi

cc w/o encl:
H. Denton
H. Thompson
F. Miraglia
G. Lainas
D. Crutchfield
B. Bernero
J. Taylor
C. Heltemes

DISTRIBUTION (w/encl.)
PDR (Docket 50-346)
Central Files
R. Kendall
T. Dunning
J. Wermeil
J. T. Beard
R. Wessman

JTB
ORAB:DL
JTBeard:cl
8/07/85

DRAFT
J.T. Beard

10. The delay in recovering the AFW was caused by less-than-adequate hands-on training for the equipment operators.

11. The cause of the PORV failure to close may never be known.

12. Adequate testing of systems and equipment would be expected to have revealed certain major equipment problems prior to an actual demand during a reactor operating event.

It must be recognized that the root cause determination process is critically important and is not yet completed by the licensee. Table 5.1 summarizes the results to date for each equipment problem. The final results could cause the Team to revise its views.

5.3 Steam and Feedwater Rupture Control System (SFRCS)

In order to understand the design and operation of the SFRCS and to determine the extent to which the SFRCS was involved in the June 9, 1985 event, the Team reviewed drawings provided by Toledo Edison and had technical discussions with Toledo Edison. The results of this activity formed the basis for the simplified system description presented in section 4.

Incidental to the Team's review of the SFRCS, the Team found one major design deficiency. Contrary to Updated Safety Analysis Report (USAR) (Section 7.4.2.3), the SFRCS does not satisfy the single failure criterion for all design basis accidents in the plant's licensing basis.

In the event of a postulated break of one main steam line upstream of the MSIV, the overall safety function is to use the unaffected OTSG as the heat sink for the RCS. The overall safety function is divided in time into two parts: first, to isolate the affected OTSG; second, to provide AFW flow to the unaffected OTSG. The SFRCS provides the signals to the equipment involved in executing this safety function. As shown in USAR Accident Analysis Figure 15.4.4-3, the pressure in both steam lines initially falls below the setpoint for SFRCS low pressure at 2-3 seconds after the break. The SFRCS is designed to isolate both

¶ The fact that the licensee had not appreciated that the integrated system response would cause the isolation valves to close and therefore the safety function must include valve re-opening may have contributed to the apparent design oversight of the SFRCS not being identified previously.

OTSGs at this time by producing output signals to close the MSIVs and to close the OTSG/AFW isolation valves, AF-608 and AF-599.

At about 11-12 seconds, the intact OTSG would have repressurized, due to the closure of the MSIVs. The SFRCS is designed to determine which OTSG is intact at this time (i.e., has repressurized), to reopen the OTSG/AFW isolation valve to the intact OTSG, and to align both AFW trains to draw steam only from, and provide feedwater only to, the intact OTSG.

Contrary to USAR (Section 7.4.1.3.3), the SFRCS actuation channels are not redundant in the sense that one channel should be able to perform the functions of the other, in the event of a single failure. Actuation Channel 1 provides output signals primarily to equipment associated with loop #1; Actuation Channel 2, to equipment associated with loop #2. For example, the SFRCS system Actuation Channel 1 outputs (RCS 201,203) cause the OTSG #1/AFW isolation valve (AF-608) to close, and Actuation Channel 2 outputs (RCS 202,204) cause the OTSG #2 AFW isolation valve (AF-599) to close.

If a single failure is postulated to occur in the SFRCS (i.e., system output RCS 301, etc. or the associated upstream logic components), the SFRCS would not provide a signal to reopen the OTSG/AFW isolation valve. Due to the valve arrangement in the AFW design, when the OTSG/AFW isolation valve is not open, neither AFW train can provide flow to the OTSG. Therefore, for the postulated single failure, the SFRCS would fail to accomplish its safety function.

It should also be noted that, independent of the actuation signal from the SFRCS, an electrical or mechanical failure associated with the OTSG/AFW isolation valve itself could also prevent the AFW system from accomplishing the safety function.

The discovery of the potential of the SFRCS not meeting the single failure criterion was brought to the attention of the licensee during a transcribed meeting on July 9, 1985. The licensee was asked to determine if the discovery is technically accurate. The licensee reported later (during a transcribed meeting) that the SFRCS does not meet the single failure criterion.

There were also some other question areas identified by the Team regarding the SFRCS. The areas are of lesser importance and not closely related to the event on June 9, 1985. These areas may be beyond the task assigned to the Team and, therefore, will be handled separately.

ENCLOSURE 2

J.T. BEARD

—DRAFT—

4.6 Steam and Feedwater Rupture Control Systems (SFRCS)

The Steam and Feedwater Rupture Control System (SFRCS, pronounced "S-Farce") is provided in the plant design as an engineered safety features actuation system for postulated transient or accident conditions arising generally from the secondary (steam generation) side of the plant, because the OTSGs serve as the heat sinks for the reactor power. The SFRCS senses loss of main feedwater (MFW) flow, rupture of an MFW line, and rupture of a main steamline. It also senses loss of all forced coolant flow in the primary system.

The safety function of the SFRCS is to provide safety actuation signals to equipment that will: isolate the steam flow from the OTSGs, isolate the MFW flow to the OTSGs, and appropriately start the AFW system. The SFRCS also provides output signals to the turbine trip system and to the Anticipatory Reactor Trip System (ARTS).

In the event of loss of MFW flow, the OTSGs would start to boil dry, and, if action is not initiated promptly, there would be no motive steam available for the turbine-driven AFW system and the OTSGs would be lost as a heat sinks. As soon as the MFW pump discharge pressure falls below the pressure in the OTSG (i.e, reverse differential pressure across a check valve) by a predetermined value, the SFRCS provides safety actuation signals to trip the main steam isolation valves (MSIVs) closed and to start AFW. The SFRCS also receives OTSG low level signals which are diverse from the reverse differential pressure signals.

In the event of a main feedwater line rupture, when the main feedwater pressure is significantly less than the steam pressure, the SFRCS provides safety actuation signals to trip both MSIVs, to trip MFW stop and control valves, and to initiate the AFW system.

In the event of main steamline rupture, when the main steam pressure drops, the SFRCS will trip both MSIVs and trip MFW stop and control valves. The ~~description~~ discussion of the SFRCS in the Updated Safety Analysis Report (USAR) Section 7.4.1.3 does not mention the SFRCS closure (or re-opening) of the OTSG/AFW

isolation valves (AF-608 and AF-599), although the design does include such features. The AFW is also initiated and both AFW trains are aligned to draw steam only from, and to provide feed only to, the unaffected "intact" OTSG.

In the event of loss of all four reactor coolant pumps (RCPs), forced cooling flow of the reactor coolant system would be lost and AFW flow is needed to ~~establish~~ enhance natural circulation flow. Therefore, the SFRCS senses the loss of four RCPs and automatically initiates AFW.

4.6.1 SFRCS Input Signals and Setpoints

Each of the four logic channels of the SFRCS receives the following automatic inputs (actual setpoints):

1. Six pressure switches---two from each of the two steam lines, set at 612 psig decreasing; plus two from one steam line set at 650 psig increasing, for the "operating bypass" feature.

2. Two Feed-Steam dp switches---one across the check valve in MFW line to each OTSG, set at 177 psid, OTSG higher than feedwater, increasing.

3. Four OTSG Hi/Lo level bistables ---two from each of two OTSGs, set at 280 inches, increasing, for Hi level trip, and 26.5 inches, decreasing, for Lo level trip, corresponding to the startup level range.

4. A contact from RCP power sensing circuit ---the contact opens on loss of all four RCPs.

4.6.2 SRFCS Output Actuations

Figure 4.6 depicts the channelizaiton of the SFRCS. There are two Actuation Channels, which each contain two identical logic channels. One logic channel is ac powered and the other logic channel is dc powered, within each Actuation Channel. The field wiring at the actuated equipment is such that generally

both logic channels must "trip" (i.e., a two-out-of-two AND logical arrangement) to actuate most equipment, which is referred to as a "full trip." However, some equipment is actuated by a "half trip" (ie.e, only one logic channel of an actuation channel has tripped.) For example, the atmospheric steam vent valves are closed by "half trips."

Table 1 lists the equipment actuated by each SFRCS actuation channel. It should be noted that the output of each actuation channel of the SFRCS is highly oriented toward equipment related to one of the two main steam lines. For example, Actuation Channel 1 operates MFW stop valve 1, the No. 1 main steam admission valve to AFW turbine No. 1, and the discharge valve for AFW No. 1 to OTSG No. 1.

4.6.3 SFRCS Logics Channels

Each of the two SFRCS Actuation Channels contain two logic channels. Each logic channel receives all four of the automatic input signals listed above.

The actual logic portion of the SFCRS is complex; a complete narrative description would likewise be complex. For the purposes of this description, we have generated greatly simplified logic diagrams from the Bechtel drawing E18, Rev. 14, "SFRCS Logic Diagram." These are intended to cover only the OTSG low level and the steamline low pressure conditions which were involved in the Davis Besse event June 9, 1985.

Figure 4.7 depicts the OTSG level instrumentation associated with the SFRCS. Except for a meter mounted on the Steam Generator Level Instrumentation Cabinet (SGLIC) behind the control room area, these level channels provide no indication or control functions. The level transmitter output signal is monitored by a dual hi/lo bistable. Since the outputs of the bistable are wired in series, the SFRCS input is the same for either a high level or a low level condition.

Table 1: SFRCS EQUIPMENT ACTUATION LIST
(SHEET 1 OF 2)
ACTUATION CHANNEL NO. 1
FULL TRIPS

Steam Line 1 Low Pressure (Over-Riding Action)

Close:

ICS-11B	AVV #1
MS-101-1	MSIV BYPASS #1
MS-394	MS DRAIN #1
MS-611	OTSG DRAIN #1
SP-7A	S/U FW CONT VLV #2
SP-7B	S/U FW CONT VLV #1
FW-612	MFW STOP VLV #1
MS-106	#1 MS to AFPT #1
MS-101	MSIV #1
MS-100	MSIV #2
AF-3870	AFP #1 DISCH to OTSG #1
FW-780	MFW BLK VLV #1
SP-6A	MFW CONT VLV #2
AF-608	AFW DISCH to OTSG #1
AF-3869	AFP #1 DISCH to OTSG #2

Open:

MS-106A	#2 MS to AFPT #1
AF-3869	AFP #1 DISCH to SG #2

Trip:
Main Turbine

Reactor (via ARTS)

OTSG Low/High Level, Reverse FW to OTSG dP, Steam Line 2 Low Press

Close:

ICS-11B	AVV #1
MS-101-1	MSIV BYPASS #1
MS-394	MS DRAIN #1
MS-611	OTSG DRAIN #1
SP-7A	S/U FW CONT VLV #2
SP-7B	S/U FW CONT VLV #1
FW-612	MFW STOP VLV #1
MS-101	MSIV #1
MS-100	MSIV #2
AF-3869	AFP #1 DISCH to SG #2
FW-780	MFW BLK VLV #1
SP-6A	MFW CONT VLV #2
MS-106A	#2 MS to AFPT-1 (only on Steamline 2-Lo Press)

Open:

MS-106	#1 MS to AFPT #1
AF-3870	AFP #1 DISCH to SG #1
AF-608	AFW #1 DISCH to SG #1

Trip:
Main Turbine

Reactor (via ARTS)

Loss of Four RCPs Only

Close:

AF-3869	AFP #1 DISCH to OTSG #2

Open:

AF-608	AFP #1 DISCH to OTSG #1
MS-106	#1 MS to AFPT #1
AF-3870	AFP #1 DISCH to SG #1

HALF TRIPS

Steam Line Low Pressure, OTSG Low/High Level, Reverse FW to OTSG dP

CLose:

ICS-11B	AVV #1
MS-101-1	MSIV BYPASS #1
MS-394	MS DRAIN #1
MS-611	OTSG DRAIN #1

Trip:
Main Turbine

ACTUATION CHANNEL No. 2
FULL TRIPS

Steam Line 2 Low Pressure (Over-Riding Action)

Close:

ICS-11A	AVV #2
MS-100-1	MSIV BYPASS #2
MS-375	MS DRAIN #2
MS-603	OTSG DRAIN #2
SP-7A	S/U FW CONT VLV #2
SP-7B	S/U FW CONT VLV #1
FW-601	MFW STOP VLV #2
MS-107	#2 MS to AFPT #2
MS-101	MSIV #1
MS-100	MSIV #2
AF-3872	AF #2 DISCH to OTSG #2
FW-799	MFW BLK VLV #1
SP-6B	MFW CONT VLV #1
AF-599	AFW DISCH to OTSG #2

Open:

MS-107A	#1 MS to AFPT #2
AF-3871	AFP #2 DISCH #1

Trip:

Main Turbine

REACTOR (via ARTS)

OTSG Low/High Level
Reverse FW to OTSG dP
Steam Line 1 Low Press

Close:

ICS-11A	AVV #2
MS-100-1	MSIV BYPASS #2
MS-375	MS DRAIN #2
MS-603	OTSG DRAIN #2
SP-7A	S/U FW CONT VLV #2
SP-7B	S/U FW CONT VLV #1
FW-601	MFW STOP VLV #2
MS-107A	#1 MS to AFPT #2 (Only on Steamline 2 Low Press)
MS-101	MSIV #1
MS-100	MSIV #2
AF-3871	AFP #2 DISCH to OTSG #1
FW-779	MFW CONT VLV #2
SP-6B	MFW CONT VLV #1

Open:

MS-107	#2 MS to AFPT #2
AF-3872	AFP #2 DISCH to OTSG #2
AF-599	AFW DISCH to OTSG #2

Trip:

Main Turbine

REACTOR (via ARTS)

Loss of Four RCPs Only

Close:

AF-3871	AFP #2 DISCH to SG #1

Open:

AF-599	AFW DISCH to SG #2
MS-107	#2 MS to AFPT #2
AF-3872	AFP #2 DISCH to OTSG #2

HALF TRIPS

Steam Line Low Pressure
OTSG Low/High Level
Reverse FW to OTSG dP

Close:

ICS-11A	AVV #2
MS-100-1	MSIV BYPASS #2
MS-375	MS DRAIN #2
MS-603	OTSG DRAIN #2

Trip:

Main Turbine

Figure 4.8 depicts logic channel 1 of Actuation Channel 1 for OTSG level. Under normal plant conditions, the logic channel receives closed-contact inputs from the steam generator level instrument cabinet. Upon level falling below 26.5 inches (or rising above 280 inches), the contacts open to provide a trip input signal.

If an off-normal OTSG level condition (high or low) is sensed in either OTSG by logic channel #1, four paths of action are initiation. The first path leads to the start of AFW train #1, aligned to draw steam from, and to provide feedwater to, OTSG #1 (i.e. open MS-106, close MS-106A). The second path leads to the isolation of OTSG #1, initiation of a reactor trip input via the ARTS system, and the closure of both MSIVs. The third path leads to the non-safety-related trip of the main turbine. Although not shown on the figure, these paths include OR gates to accept other conditions for which the same end result is appropriate. Also, the AFW #1 start and alignment to OTSG #1 is blocked by an AND gate if OTSG #1 has low pressure.

Figures 4.9 and 4.10 depict the low pressure portion of logic channel #2, which is the ac powered channel within Actuation Channel #2. The basic low pressure actuation logic is shown in Figure 4.9. The "Initiate Bypass and Block" feature associated with the low pressure logic is shown in Figure 4.10. Logic channel #2 was selected for this illustration since it was one of the channels inadvertently actuated by the operator during the June 9, 1985 event. The "Initiate Bypass and Block" feature is included because it was one of the logic features used during the event.

As shown in Figure 4.9, when any one of the four pressure switches (OTST #1 or #2) senses low pressure, its contacts would open and cause four immediate output signals to: (1) both MSIVs, (2) MFW isolation, including closure of the atmospheric vent valves, (3) reactor trip (via the ARTS), and (4) turbine trip systems.

Next in the figure, the low pressure signals are differentiated as to which OTSG is involved. If OTSG #2 has low pressure (at least initially), then AFW train #2 operation on OTSG #2 would be stopped. If OTSG #2 does not have low pressure (or later recovers its pressure) and OTSG #1 does have low pressure, then AFW train #2 would be started so as to draw steam only from, and provide feedwater only to, OTSG #2. Operation of AFW train #2 on OTSG #1 would be stopped. If OTSG #2 does have low pressure and OTSG #1 does not have low pressure (or later recovers its pressure), AFW train #2 would be started so as

to draw steam only from, and provide feedwater only to, OTSG #1. It should be noticed that this Channel does not provide output to AFW train #1.

Figure 4.10 illustrates the "Initiate Bypass and Block" scheme, which is a feature included in the SFRCS as an "operating bypass" to allow normal cooldown without a low pressure actuation. The required safety function is that the block and bypasses be automatically removed as the plant returns to power (i.e., OTSG pressure greater than 650 psig). For an easy understanding of this logic, enter the figure at the point labelled with an "A" inside a diamond, with the presumption that none of the four low pressure switches has tripped (at less than 612 psig). Then, if both of the OTSG pressure switches are below the 650 psig, the "permission to block" (i.e., prevent a trip actuation) red light would come on. Next, when the "block" switch is operated, the following actions would occur:

(1) the "permission to block" light would go off, (2) the "blocked" amber light would come on, (3) a seal-in signal is provided back to point "A", (4) a seal-in signal is provided back to the "block" switch input, and (5) block actuation signals are sent to the low pressure logic and to the high level circuitry. Notice that, when either pressure switch senses a pressure greater than 650 psig, the block logic would be automatically interrupted by an "AND" gate within the seal-in loops.

If, on the other hand, one or more of the low pressure switches (less than 612 psig) have tripped, an additional step is required to bypass the actuation signal (i.e, override, or defeat, an already existing and not cleared trip signal).

If the "initiate bypass" switch is first operated, the same block/bypass signals back to the low pressure and level logics can be actuated (as discussed above), so long as the pressure remains below 650 psig.

¶ Three types of SFRCS-actuated equipment are presented below: (1) operation of the OTSG/AFW isolation valves, (2.) trip of the MSIVs, and (3) start of the AFW trains.

4.6. SFRCS Actuated Equipment

As shown on the SFRCS block diagram (Figure 4.6), each logic channel has a separate output. The field wiring of the controls for each SFRCS-actuated piece of equipment determines what combination of logic channel signals would actuate that equipment. In a few cases (such as the atmospheric vent valves), a single logic channel signal of an Actuation Channel is sufficient (i.e, a "partial trip" condition). For the special case of the MSIVs, both of the logic channel signals ("full trip") are necessary to trip the MSIVs. However, either SFRCS Actuation Channel can trip both MSIVs.

In the more general case, both of the logic channels signals ("full trip") are necessary to actuate the equipment, but only one of the Actuation Channels provides signals to a given piece of equipment. This configuration is equivalent to a two-out-of-two logic for one particular Actuation Channel.

The actuation control scheme for the OTSG #1/AFW isolation valve, AF-608 has been chosen to illustrate the final actuation logic of the SFRCS, as shown in Figure 4.11. The scheme for valve AF-608 illustrates the two-out-of-two logic. Figure 4.11 shows also the bypass contacts around torque switches, which are believed to have cause this valve to fail during the June 9, 1985 event. Further, the figure is a useful reference when considering the vulnerability of the SFRCS to a single failure, as discussed in Section 5.3.

Figure 4.11 is simplified to show only the automatic-open and automatic-close circuitry. Normally, isolation valve AF-608 is open. If the closing torque switch is bypassed, if Actuation Channel #1 is fully tripped (logic channels #1 and #3) due to low pressure being sensed for OTSG #1 , and if the "close inhibit" feature is not actuated, then both closing control relays would be operated and the isolation valve would go closed.

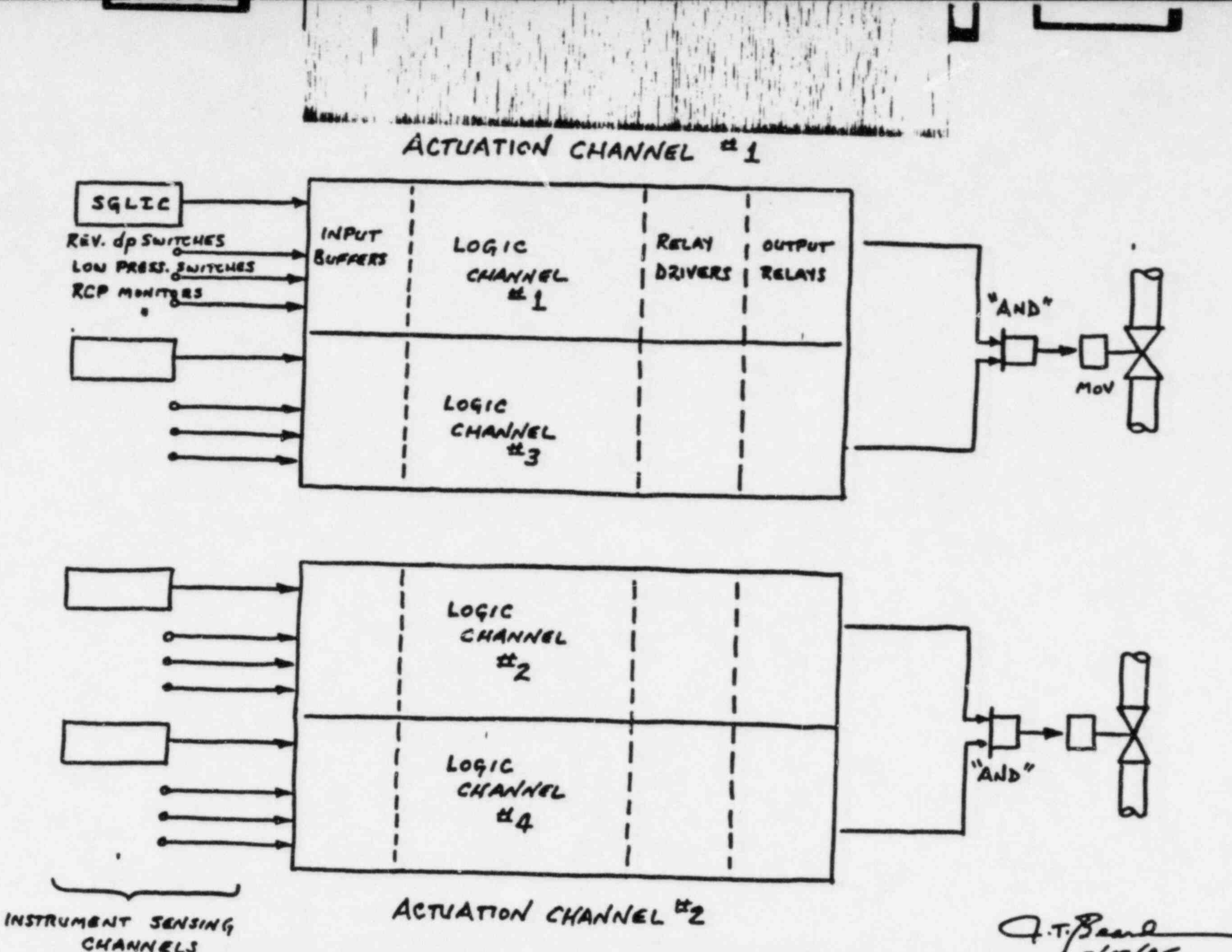
The combination of the low pressure full actuation and the "close inhibit" is logically equivalent to providing a close signal anytime OTSG #1 has low pressure. This results from K301 and K303 remaining untripped (energized, contacts closed) anytime OSTG #1 has low pressure. Conversely, if OTSG #1

never had low pressure, or if the low pressure condition later clears itself (recovers), or if the low pressure logic is bypassed (overridden), then the "close inhibit" function would be operative. However, under this condition, the logical arrangement is such that valve closure is always inhibited, regardless of level in either OTSG and pressure in OTSG #2. The licensee stated that he is currently re-reviewing this logic feature. the "close inhibit" was a modification added by the licensee, himself, and that

The automatic opening (including re-opening)scheme for this isolation valve is much more straightforward. If the valve is not already at the full-open limit switch setting, and if the opening torque switch is bypassed, then a full trip of Actuation Channel #1 (logic channel #1, K301A; and logic channel #3, K303A, tripped) will open the isolation valve. The necessary logic for K301A (and K303A) is that, when OTSG #1 does not have low pressure, one of the OTSGs must have low level or OTSG #2 must have low pressure. During the June 9, 1985 event, when the inadvertent manual low pressure actuation were reset, low level existed for both OTSGs. Therefore, the OTSGs/AFW isolation valve, AF-608 should have re-opened automatically, but it did not.

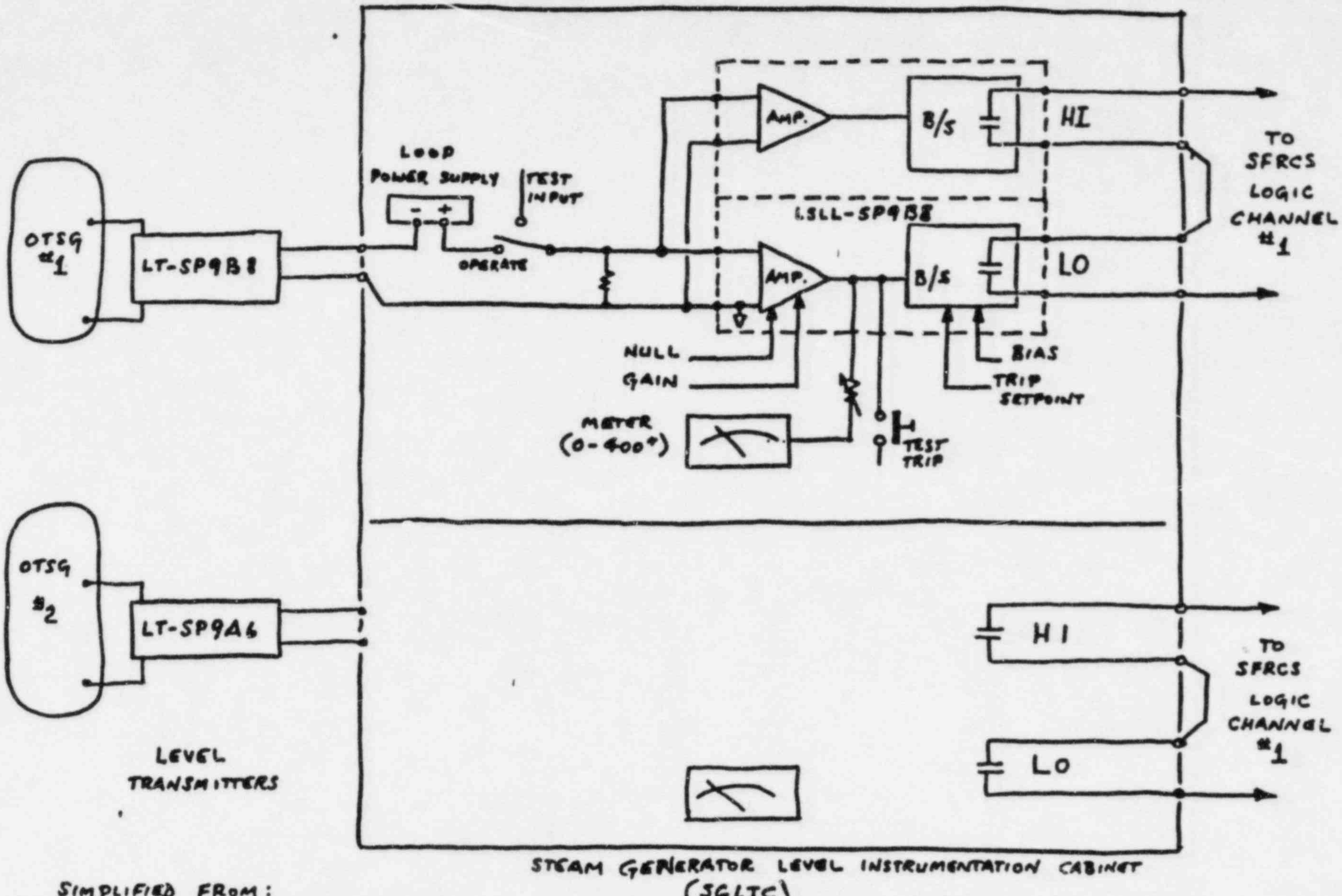
¶ The logic and actuation features for the MSIVs is shown in Figures ______ and ______. It should be noted that both MSIVs can be tripped by the SFAS or by either Actuation Channel of the SFRCS.

¶ An AFW train is actuated by simply opening the steam supply valve to the turbine. A simplification of the control scheme for MS-107, the steam supply valve from OTSG #1 to AFW train #1, is shown in Figures ______ and ______. The turbine governor is pre-set to the full-speed stop. AFW flow is controlled by varying the speed of the turbine via the governor with manual controls in the main control room.



J.T. Beard
7/17/85

FIGURE 4.6 SFRCS BLOCK DIAGRAM



SIMPLIFIED FROM:
BECHTEL DWG E18, REV. 14
CCC DWG KAD 7316
CONDEC/CCC DWG 6N88-3

Q.T. Board
7/17/85

FIGURE 4.7 SFRCS LEVEL INSTRUMENTATION

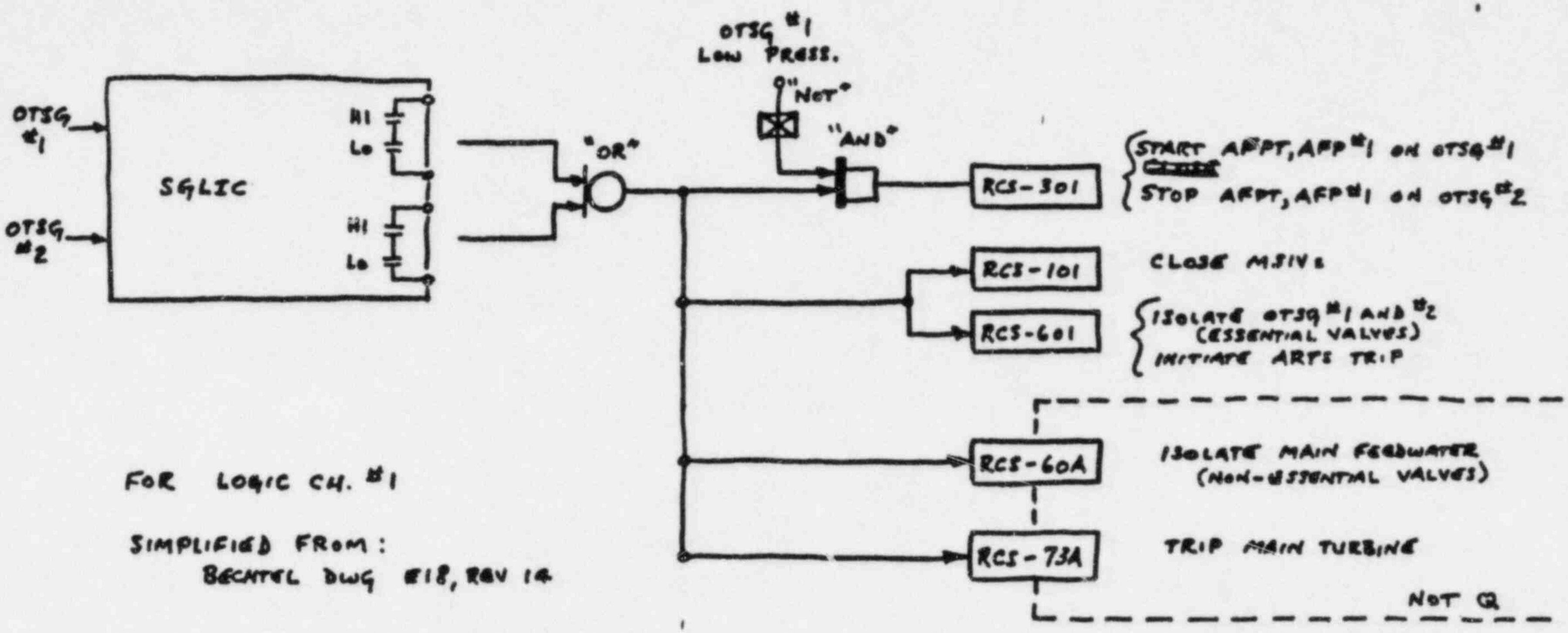


FIGURE 4.8 SFRCS OTSG LEVEL LOGIC

J. T. Beard
7/17/85

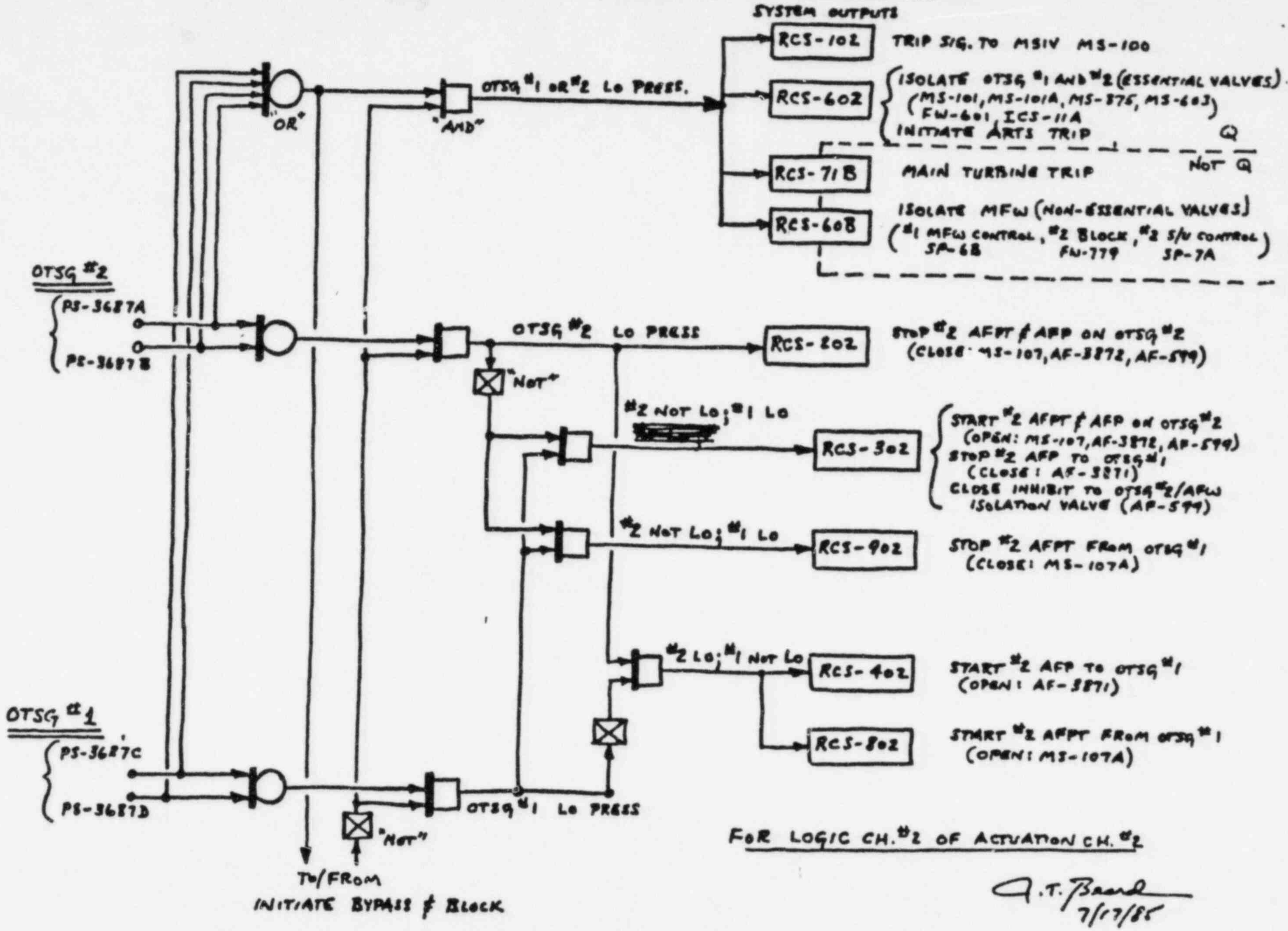


FIGURE 4.9 SFRCS OTSG LOW PRESSURE LOGIC

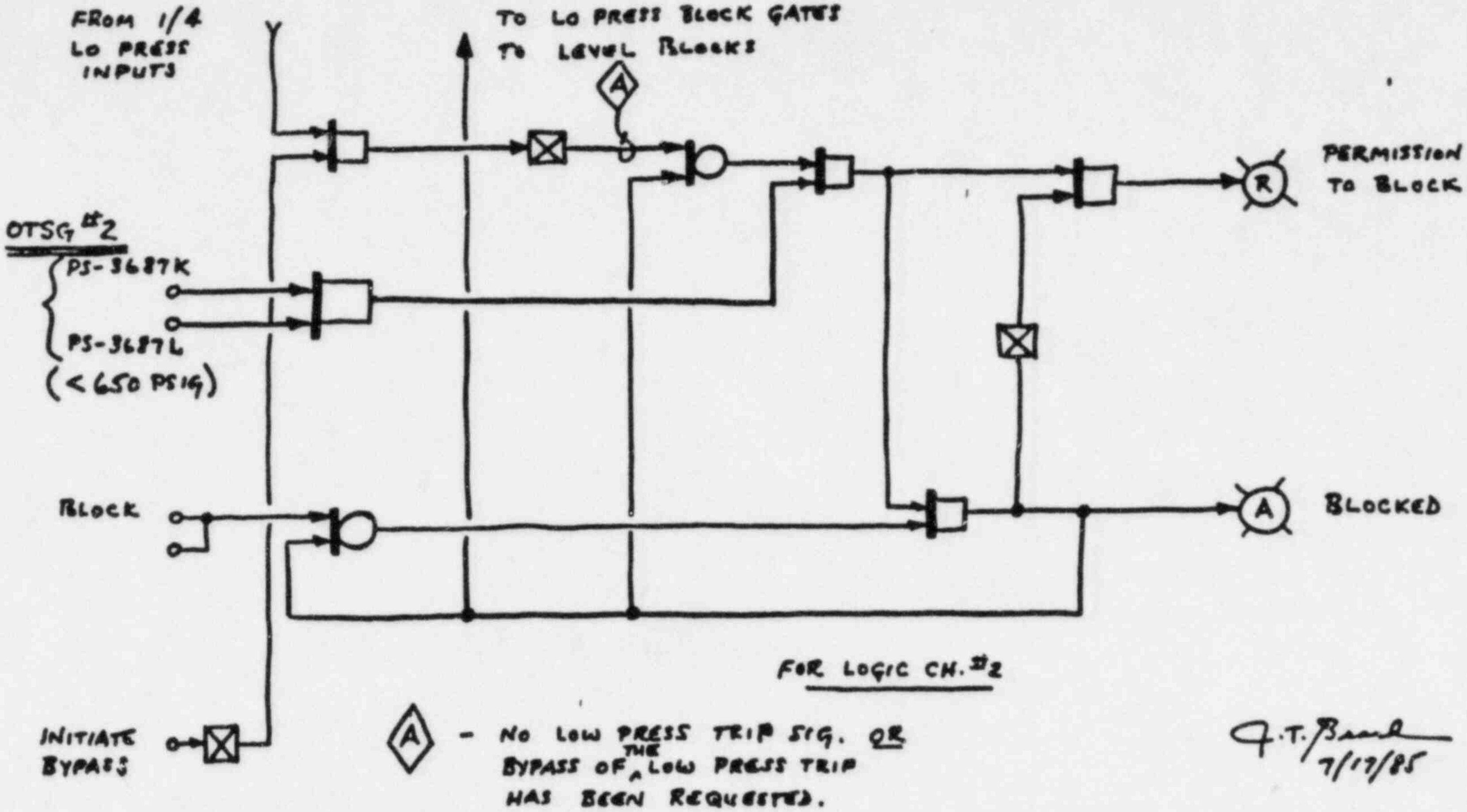
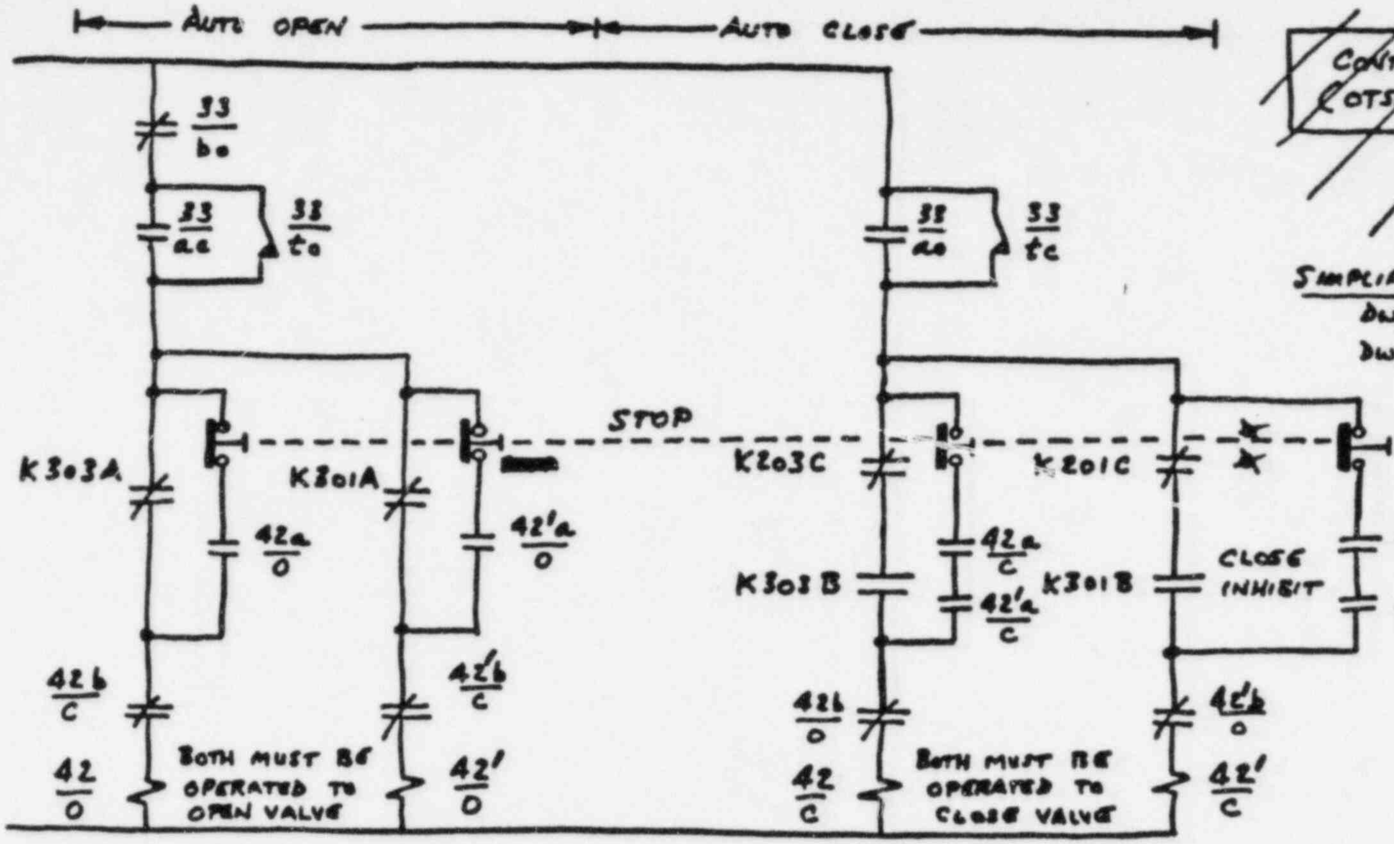


FIGURE 4.10 SFRCS "INITIATE BYPASS AND BLOCK" LOGIC



~~CONTROL SCHEME FOR AF-608 (OTSG #1/AFW ISO VALVE)~~

A. T. Baard 7/09/85

SIMPLIFIED FROM:
DWG E-44B SH-2C REV 10
DWG E-18 REV. 14

K303 (ACT. CH. #1, LOGIC #3)

[OTSG #1 NOT LOW PRESS] AND

[LOW LEVEL (EITHER OTSG) OR OTSG #2 LOW PRESS]

K301 (ACT. CH. #1, LOGIC #1)

[OTSG #1 NOT LOW PRESS] AND

[LOW LEVEL (EITHER OTSG) OR OTSG #2 LOW PRESS.]

K203 (ACT. CH. #1, LOGIC #3)

OTSG #1 LOW PRESS.

K201 (ACT. CH #1, LOGIC #1)

OTSG #1 LOW PRESS.

~~VALVE CLOSURE - K203 [illegible] AND K303B~~

ALL CONTACTS SHOWN DE-ENERGIZED (AND SFRCS TRIPPED)

A. T. Baard 7/18/85

FIGURE 4.11 ACTUATION SCHEME FOR VALVE AF-608

(OTSG #1/AFW ISOLATION VALVE)

MSIV SIMPLIFIED ELECTRICAL LOGIC

J.T. BEARD

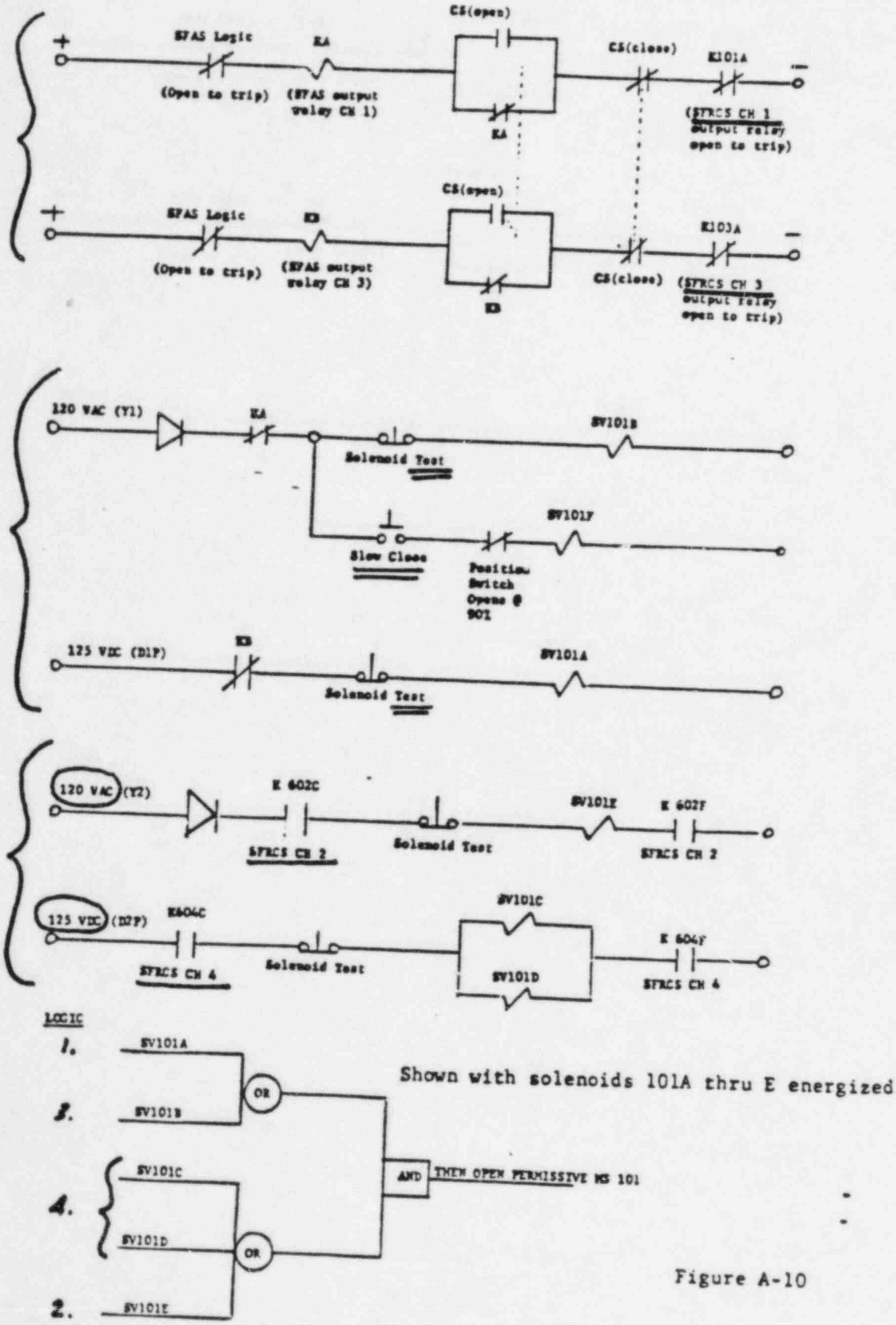
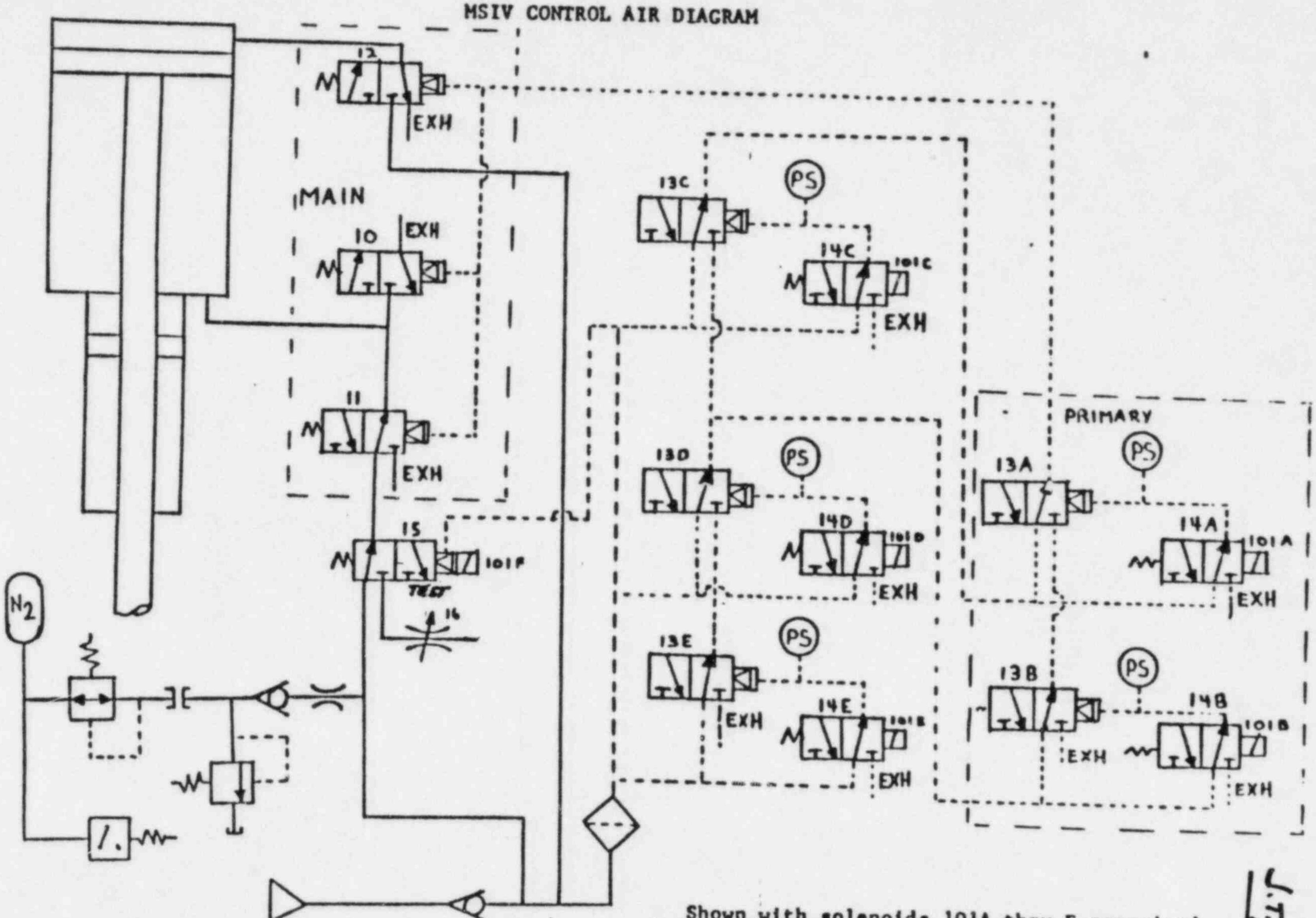


Figure A-10

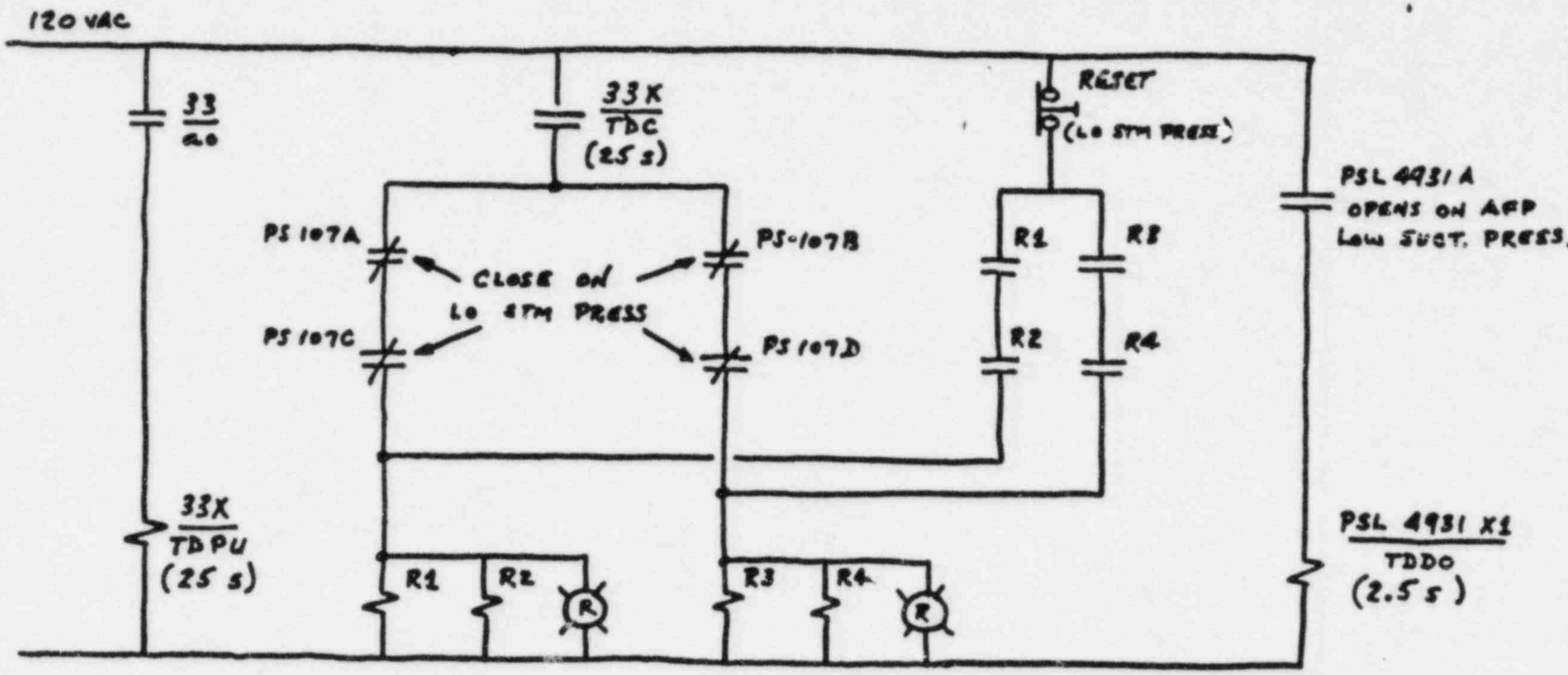
MSIV CONTROL AIR DIAGRAM



Shown with solenoids 101A thru E energized and MSIV open

Figure A-9

J.T. Beard

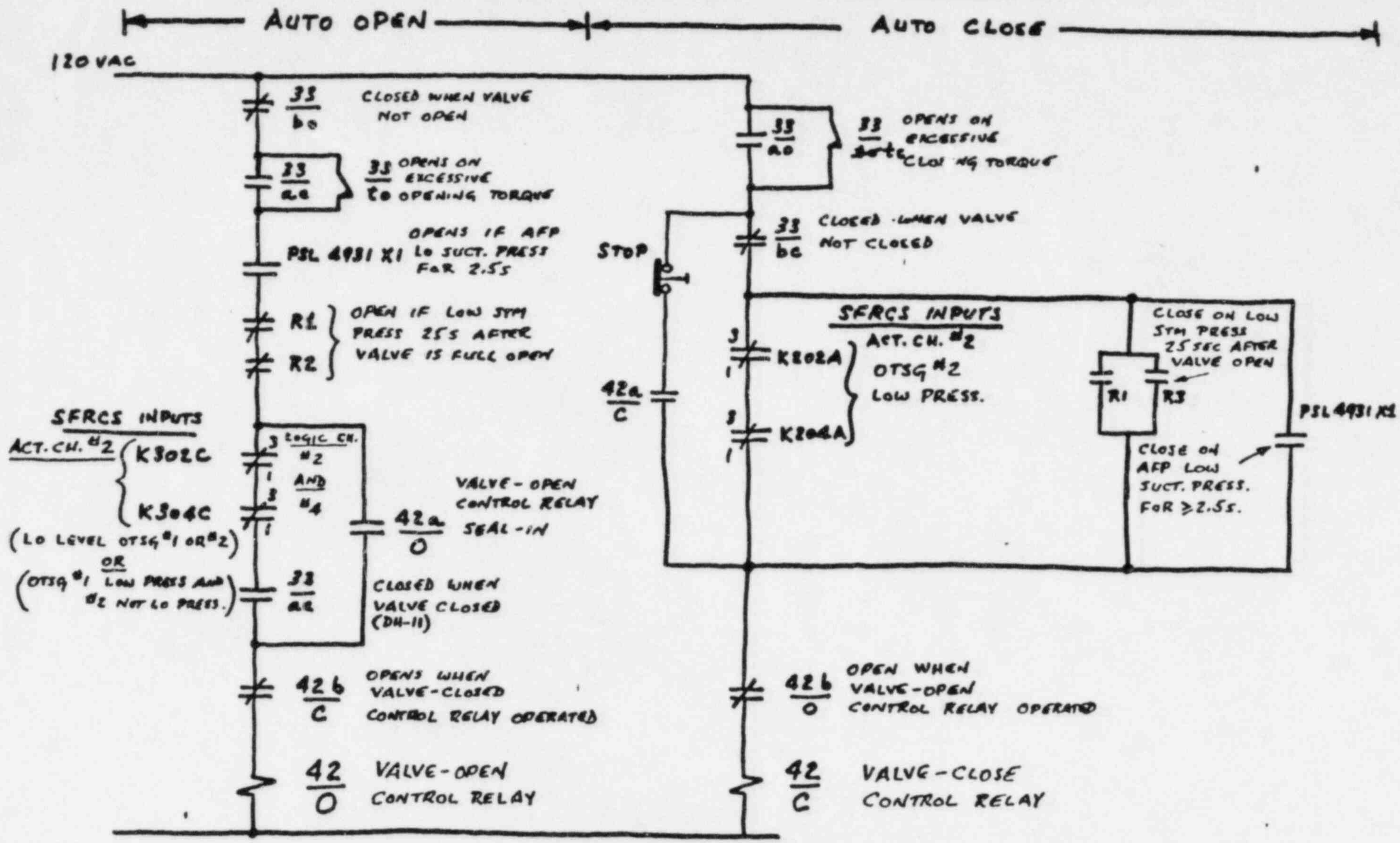


SIMPLIFIED FROM:
DWG. E-44B SH-4A,B REV.10

CONTROL SCHEME FOR VALVE MS-107
(MAIN STM ISO VALVE TO AFPT #2)

PAGE 1 OF 2

J.T. Beard
7/09/85



CONTROL SCHEME FOR VALVE MS-107
(MAIN STM ISO VALVE TO AFPT #2)

PAGE 2 OF 2

J. T. Beard
7/09/85

ENCLOSURE 3

-DRAFT-

6.3.2 SFRCS Question Items

6.3.2.1 The licensee stated that the spurious trip of the SFRCS Actuation Channel #2 on OTSG low level that caused the MSIVs to close could have been caused, at least in part, by the replacement of certain B&W/Bailey OTSG level transmitters with Rosemont transmitters, because these transmitters share the same instrument taps and impulse sensing lines with the level transmitters that provide the input signals to the SFRCS. In looking at the matter of the transmitter change, we noted that, while the technical manuals for the level transmitters (both Bailey and Rosemont) specify that the slope of the impulse lines should be a minimum of one inch per foot, the as-built drawings indicate a slope of only a quarter inch per foot. The significance of this apparent discrepancy was not assessed by the team.

6.3.2.2 The licensee stated that the low level bistables of the SFRCS level instrument channels were replaced with dual hi/low bistables and the hi/low output contacts were wired in series to provide a single output (i.e. single input to the SFRCS). The licensee stated that the SFRCS design was further modified to provide a block of the high level trip upon actuation of the "operating bypass" on low pressure. The acceptability of bypassing a level signal with a pressure bypass and the possible affect on the low level SFRCS are uncertain. The loss of automatic AFW actuation on OTSG low level would appear to be a reduction in the safety margin.

6.3.2.3 During the early phase of the June 9, 1985 event, when the SFRS actuated apparently spuriously on OTSG low level, some of the equipment to be actuated by the SFRCS did not go to completion (become fully actuated). The SFRCS itself is designed for automatic reset of its output signals as soon as the input signals return to acceptable values. Even though the SFRCS output actuation signals appears to have persisted for over 3 seconds, the lack of seal-in circuits appears to have allowed only partial actuation of some equipment.

6.3.2.4 The actuation of the SFRCS discussed above was difficult for the reactor operators to recognize because the combination of the SFRCS and the control room annuciator system did not provide timely and accurate status information regarding the SFRCS.

6.3.2.5 Certain safety system actuations can have a significantly adverse affect on plant safety if they should occur spuriously. During the June 9, 1985, the spurious actuation of the SFRCS apparently caused all the MSIVs to close and thereby cause a complete loss of main feedwater. This complication of a transient might not have occurred if the SFRCS had been required to satisfy the single failure criterion with regard to spurious actions that have significantly adverse effects (Reference IEEE Standard 379). If the licensee's hypothesis is correct, any turbine trip could be compounded into a complete loss of main feedwater event.

6.3.2.6 The SFRCS is designed for automatic reset as soon as the plant variable returns to within the trip setpoint value. The review of the control scheme for the actuated equipment (e.g. MS-107) indicates that, if the reactor operator (willfully or inadvertantly) uses the normal controls to request that the actuated equipment go to the non-safety state (e.g. close MS-107 after it has opened), the equipment will in fact go to the non-safety state (e.g. MS-107 will close), whether the SFRCS actuation signal is still present or has reset itself. Paragraph 7.4.2.3.1 of the USAR states that: "The actuated Class 1E equipment once initiated by the SFRCS will remain in its actuated stated until deliberately and individually reset by operator action." This type of statement normally refers to a separate reset action to be taken to make the normal controls available for operator use (i.e. a two-step process is provided to position the equipment out of its safety-state). The SFRCS-actuated equipment does not appear to have inhibit features that would preclude re-positioning until the reset is operated. The significance of this apparent discrepancy has not be evaluated.