Consumers Power Company

Stephen H. Howell
Senior Vice President

General Offices: 1945 West Parnall Road, Jackson, Michigan 49201 • (517) 788-0453

April 1, 1980
Howe 69-80

US Nuclear Regulatory Commission
Att Mr Harold R Denton
Office of Nuclear Reactor Regulation
Washington, DC 20555

MIDLAND PROJECT
DOCKET NO 50-329, 50-330
RESPONSE TO 10 CFR 50.54 REQUEST
ON DESIGN ADEQUACY OF B&W SYSTEMS
FILE: 0485.19 SERIAL: 8563

Enclosed are ten (10) copies of Consumers Power Company's response to your supplemental 10 CFR 50.54(f) request dated March 7, 1980 regarding B&W System Sensitivity.

Our conclusions with regard to continued construction contained in our original response to your 10 CFR 50.54(f) request have not changed either as a result of additional analyses performed and included as Revision 2 to that document or due to the effort expended in developing the attached response. Changes to the Midland Plant expected to result from identified design evaluations and reviews will be mainly in the instrumentation and controls areas and can be accommodated within the current construction schedule. Therefore, we feel that sufficient information has been provided to support a decision to allow continued construction and that future exchanges on this issue should be conducted as part of the normal licensing review process.

The majority of your additional requests do not appear central to the 10 CFR 50.54(f) issue regarding potential construction stoppage since they do not seek information which we feel is supportive of determining the advisability of continued construction. The nature of these requests is mostly in the area of design review and verification more appropriately issued as part of the normal FSAR licensing review. The Midland operating license application has been docketed for this purpose and we encourage your reinstitution of this process. Consumers Power Company is prepared and available to interact with your staff and restart the detailed review of the Midland application.

Consumers Power Company

Dated: April 1, 1980

By Stephen H Howell
Stephen H Howell, Senior Vice President

Sworn and subscribed to before me on this 1st day of April 1980.

Betty L Bishop
Notary Public, Jackson County, Michigan
My commission expires September 21, 1982

8004080431

Question F.1

Your discussion in Appendix F of the pre-TMI-2 changes for Midland states that newer control systems hardware (non-nuclear instrumentation [NNI]/ integrated control system [ICS]) using dual auctioneered power supplies for logic modules rather than individual power supplies are being used.

a. For this modification, provide the logic and/or your failure mode and effects analysis that shows how systems will respond to failure in the power supply and input parameters. Also provide your design criteria for the ICS with respect to these types of failures. Information in the FSAR may be referenced or supplemented as appropriate for this response.

b. Operating events at several plants with B&W NSSS designs (including Rancho Seco in March 1978; Oconee Power Station, Unit 3 on November 10, 1979; and the Crystal River Station on February 26, 1980) have occurred which resulted in loss of power to the ICS and/or NNI system. The loss of power resulted in control system malfunctions, feedwater perturbations, and significant loss of or confused information to the Operator. NUREG-0500 also discussed LER 78-021-03L on Three Mile Island, Unit 2 whereby the RCS depressurized and safety injection occurred on loss of a vital bus due to inverter failure. Discuss the extent to which these events would have been mitigated or precluded by the changes incorporated into the Midland design. Include a response to action items 1 to 3 required of near-term licensees in IE Bulletin 79-27 and identify corrective actions you consider appropriate as a result of the Crystal River event.

Response

a. A failure modes and effects analysis (FMEA) was performed as one of the long-term actions directed by the NRC in its order of May 7, 1979. The integrated control systems (ICS) FMEA determined the expected effects upon the Babcock & Wilcox (B&W) nuclear steam system from single failures of ICS input, output, and internal modules. The Rancho Seco plant, specifically, was chosen as a representative design for all the B&W units for the analysis; however, because of the close functional similarity between plants, the results of the study are applicable to all 177-FA B&W plants including Midland.

The analysis was complemented with an evaluation of field data from all B&W operating plants, and a computer simulation to confirm the effects of various ICS failures on associated equipment. The overall conclusion of the FMEA was that the reactor core remains protected throughout all of the ICS failures studied. For those postulated ICS failures that could cause reactor trip, the safety systems operate independently of the ICS malfunction. The overall conclusion from the operating experience evaluation was that ICS hardware performance has not led to a significant number of reactor trips. The ICS has prevented more re ctor trips than it has caused and thus its net effect has been a reduction in the number of challenges to the reactor protection system.

b. The FMEA of the ICS described in the response to Part a, above, discusses the reliability of the 820 control system design. The nonnuclear instrumentation (NNI) utilizes the same design concept as the ICS; therefore, reliability of the NNI hardware is expected to be equivalent to that of the ICS. This reliability is expected to minimize the frequency of ICS/NNI internal component failures which could result in plant transients. The arrangement of the external power sources to the NNI and ICS is shown in Figure F.1.a-1 and is described in FSAR Subsections 8.3.1.1.6 and 8.3.2.1. As shown, the ICS is supplied by two separate 120 V ac battery-backed power sources. These sources power individual 24 V dc power supplies whose output is auctioneered. Also supplied is a 120 V ac bus within the ICS cabinet which is equipped with an automatic bus transfer switch that provides access to both external battery-backed 120 V ac sources. This is an extremely reliable power supply arrangement in that loss of either external power source will not result in a loss of ICS power.

NNI-X channel cabinets are supplied power in a manner similar to the ICS with the exception that the 120 V ac bus within the NNI-X cabinets is not equipped with an automatic bus transfer for access to both external battery-backed 120 V ac sources. Within the NNI-X cabinets, the 120 V ac bus is used to power resistance temperature detectors (RTDs), (E/P) converters and for monitoring field contacts. Consumers Power Company (CPCo) is evaluating incorporation of an automatic bus transfer, similar to that utilized in the ICS, to improve the reliability of the NNI-X channel.

NNI-Y channel cabinets are supplied power from a single external battery-backed power source. Loss of this supply would, therefore, result in a complete loss of the NNI-Y channel. In light of the recent event at Crystal River, CPCo is reviewing the functions and interrelationships which exist between the NNI-X and NNI-Y channels. Based on the results of this review, appropriate measures will be taken to improve the overall reliability of the NNI system.

In the unlikely event that a loss of power to the NNIs should occur, the consequences would be mitigated by design features including those listed below:

a. Upgrading of PORV control circuit to Class 1E status and removal of control from the NNI

b. Upgrading of selected pressurizer heater controls to Class 1E status and removal of control from the NNI

c. Class 1E indication of pressurizer level and pressurizer pressure independent of the NNI

d. Psat/Tsat subcooling meter independent of the NNI

e. Safety-grade auxiliary feedwater (AFW) actuation, control, and indication independent of the NNI/ICS.

These additional features result in providing the operator key information required to control the plant until NNI power is restored. In addition to the modifications described above, CPCO is currently evaluating the need for upgrading other control room indications. Necessary modifications or design changes based on the results of this evaluation will be implemented upon completion of this study.

CPCo evaluations of the design of the ICS, NNI, and associated power supplies will consider events at Rancho Seco, Oconee, Crystal River, and Three Mile Island. Changes resulting from these studies would make any immediate response to IE Bulletin 79-27 premature and therefore inappropriate at this time.

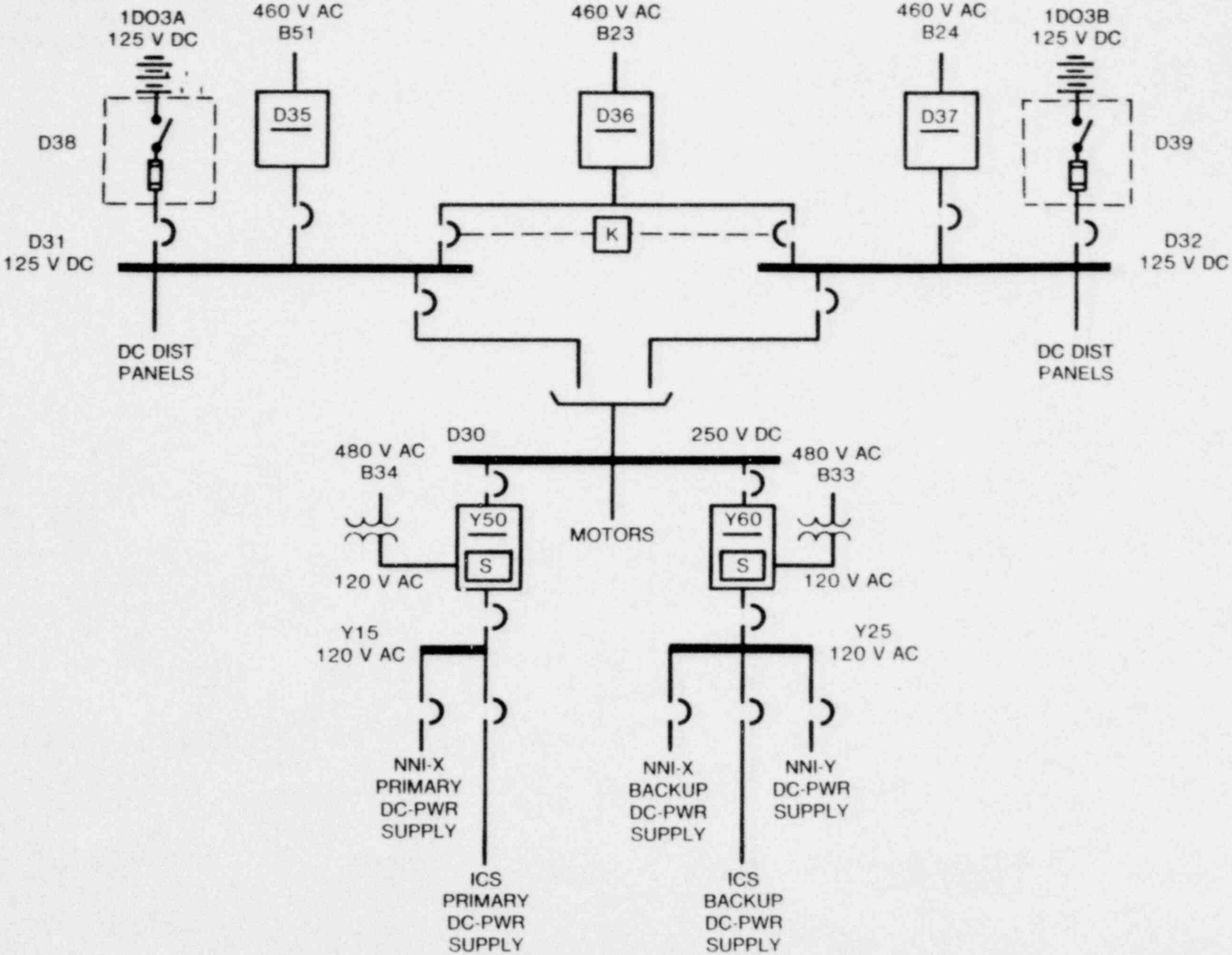


FIGURE F.1-1

NNI AND ICS 120 V AC PREFERRED POWER SUPPLY

G-1019-52

Question F.2

We are concerned that an instability in the ICS could lead to transients initiating with plant parameters more severe than those assumed for the safety analysis or significantly increase the number of challenges to the protection system during early plant life. In this regard:

a. The Midland ICS includes a significant difference from ICS designs of other plants in its evaporator steam development. Describe all studies and tests which have been and will be conducted to establish stability and reliability of the Midland ICS design.

b. Operating experience at the Crystal River plant has indicated a control instability for the integrated control system when bringing the plant up to power with pump out of service. Specify your criteria and describe Midland design features to preclude this type of instability.

c. Describe your design criteria, features, and operational requirements for the ICS and its supporting systems to preclude instabilities when: (1) switching from manual to automatic control and vice versa or (2) switching from one operating mode for process steam to another mode.

Response

This question expresses a concern that the integrated control system (ICS) may cause nuclear steam supply system (NSSS) instabilities that significantly increase the number of challenges to the protection system. This concern is unwarranted as can be readily ascertained by examination of the data tabulated below:

		B&W	Combustible Engineering	Westinghouse
1976	Number of automatic trips	25	46	147
	Number of plants	6	5.1	19.13
	Trips/plant/year	4.17	9.02	7.68
1977	Number of automatic trips	30	31	174
	Number of plants	6.85	6.67	21.6
	Trips/plant/year	4.38	4.65	8.06

		B&W	Combustible Engineering	Westinghouse
1978	Number of automatic trips	43	41	150
	Number of plants	8	7	23.4
	Trips/plant/year	5.38	5.86	6.41
Three-year average (trips/plant/year)		4.64	6.51	7.38

This information was extracted from the NRC Gray Book (NUREG-0020, Operating Units Status Report) for the years indicated. Because Babcock & Wilcox (B&W) plants are not subject to excessive transients that challenge the protective systems [when compared to other pressurized water reactor (PWR) vendors], the concern that the ICS causes a significant increase in protective system challenges does not appear warranted. On the contrary, operating experience at B&W plants has demonstrated that the ICS is a reliable system that tends to mitigate NSSS upsets rather than initiate them.

a. The Midland ICS design is not significantly different than designs at other B&W plants; rather, it is essentially the same. The differences that exist are in the evaporator steam demand development described in FSAR Subsection 7.7.1.2.7. This uniqueness has been scrutinized during the normal design review process. Additionally, proper operation will be verified during ICS startup testing. There are extensive preoperational (prefuel load) tests designed to determine system response and to identify and correct system instabilities. Coupled with ICS tuning at power, the results of these tests will lead, where necessary, to the identification and correction of any potential operational difficulties.

b. This question expresses a concern that operation of the ICS in a three reactor coolant (RC) pump mode is suspect, due to the problem experienced at Crystal River in mid-1979. The difficulties encountered during this incident were due to both operator unfamiliarity with this type startup and reduced operating margins resulting from the reduction in the high RC pressure trip setpoint. At Midland, this trip setpoint will retain its original value, thus providing an increased operating margin over that existing at Crystal River. The procedures were revised following the Crystal River event and the operators given further instruction in the proper execution of three RC pump startup. The ICS is fully capable of providing adequate NSSS control during three RC pump startup and it is not expected to reoccur as a problem.

c. The ICS and evaporator steam demand development (ESDD) system are described in FSAR Section 7.7. Operating procedures for plant startup and shutdown as well as procedures for switching process steam operating modes will be written. These procedures will be utilized by the operators during these evolutions and will contain guidelines for transfer of control from automatic to manual and from manual to automatic.

In summary, the B&W ICS that will be used at Midland is designed and has been proven to regulate feedwater flow and other parameters automatically to maintain the plant in a stable condition during both steady-state and transient power operation. A failure modes and effects analysis has been completed and shows that no ICS failure can prevent proper safety system functioning. This analysis and operating experience also demonstrates that the ICS is a reliable system with respect to preventing plant upsets.

Question F.3

Experience at operating B&W plants have indicated that the dynamics associated with main feedwater termination and steam generator pressure control following a reactor trip can lead to overcooling of the primary system. Discuss your criteria and the adequacy of your existing and proposed design features and changes to preclude this overcooling situation.

Response

The dynamics associated with main feedwater (MFW) termination and steam generator pressure control following a reactor trip do not normally lead to overcooling of the primary system. Following a reactor trip, the integrated control system (ICS) is designed to close the MFW control valves to terminate MFW and to open the turbine bypass valves to control steam pressure at approximately 1,000 psi. The startup feedwater valve then controls MFW to the steam generator to provide for decay heat removal following the reactor trip.

Figure F.3-1 illustrates reactor coolant (RC) temperature and pressure following a reactor trip with proper feedwater flow and steam pressure control. The rapid decrease in reactor power causes RC temperature to decrease; the resultant RC contraction causes a decrease in RC liquid volume and pressure. The RC cold leg temperature reaches an equilibrium value equal to the saturation temperature of the secondary side steam pressure (546F at 1,000 psig), and the RC pressure is restored to 2,155 psig due to the normal makeup flow which accommodates the RC contraction that occurs as the average RC temperature drops from 579F to 546F.

Overcooling of the primary system can occur if excessive MFW is added to the steam generator (due to improper feedwater valve control), or steam pressure falls significantly below 1,000 psig (due to improper steam relief valve operation). Experience at a Babcock & Wilcox (B&W) operating plant has demonstrated that such overcooling is a moderate frequency event which is safely mitigated by the action of the high-pressure injection (HPI) system. The operating data shows that there have been 24 reactor trip events followed by an overcooling which caused the RC pressure to fall below 1,600 psig and/or caused the RC temperature to exceed a 100F in 1 hour cooldown rate. The 1,600 psig value of RC pressure approximates the setpoint for automatic initiaton of the HPI system (1,500 psig for Midland), and should be avoided for anticipated transients to minimize challenge to the safety systems. The 100F in 1 hour cooldown is a Technical Specification limit based upon the reactor coolant system (RCS) design analysis. Table F.3-1 summarizes the B&W operating experience for such events and identifies the minimum values of RC temperature and pressure. The 24 overcooling events which caused pressure to decrease to 1,600 psig or caused an average RC temperature cooldown in excess of 100F in 1 hour have occurred in over 40 reactor years of operation, which is an acceptable moderate frequency of 0.6 events/year. These 24 overcooling events compare to the 346 total number of reactor trips on B&W reactors.

Therefore, the basic design goal for overcooling is to minimize the frequency of automatic actuation of the HPI system and excessive cooldown rates due to improper steam generator pressure and feedwater flow control following a reactor trip. Even though the actuation of HPI will maintain the plant in a safe condition for overcooling events (based on operating experience and the overcooling analysis presented in Reference F.3-1), the Midland design includes several additional features to further preclude such overcooling events caused by the dynamics associated with MFW termination and steam generator pressure control following a reactor trip. These include:

a. Upgrade of required pressurizer heaters and controls to safety classification to enhance RCS pressure control following reactor trip

b. Addition of a two-channel, Class 1E auxiliary feedwater (AFW) control system to reliably establish a preset steam generator level and preclude overcooling due to AFW overfeeding

c. Adoption of newer control systems hardware [nonnuclear instrumentation (NNI)/integrated control system (ICS)] which uses dual auctioneered power supplies for the logic modules rather than individual power supplies for each logic module

d. Adoption of an increased pressurizer level range of 400 inches

In addition, Appendix F of Reference F.3-1 identifies proposed hardware and procedural changes related to the need for and methods for damping the primary system sensitivity to perturbations in the once-through steam generator (OTSG). Several of these features are specifically included to preclude overcooling events caused by improper steam generation pressure or feedwater flow control following a reactor trip. These changes are:

a. Restore the original B&W design features of turbine bypass, ICS runback, and power-operated relief valve (PORV) actuation to keep the reactor online, thereby minimizing the reactor trip frequency and the probability of subsequent overcooling. Changes to accomplish this goal include the following features:

   1) Original B&W 177-FA PORV and high RCS pressure setpoints (2,255 psig and 2,355 psig, respectively)

   2) Safety-grade anticipatory reactor trip on total loss-of-MFW

   3) Fully qualified safety-grade PORV

   4) Reliable safety-grade indication of PORV position

   5) Dual safety-grade PORV isolating block valves actuated by low RCS pressure engineered safety features actuation system (ESFAS) signal

   6) Test program to demonstrate PORV operability (EPRI)

b. Upgrade the two-channel, Class 1E AFW control system to limit the rate of primary system cooldown by limiting the rate of steam generator level increase following a reactor trip where AFW is initiated (i.e., limiting AFW flowrates).

c. Evaluate the recommendations contained in the B&W ICS Failure Modes and Effects Analysis and implement appropriate modifications to ensure improved steam generator pressure and feedwater flow control following reactor trip.

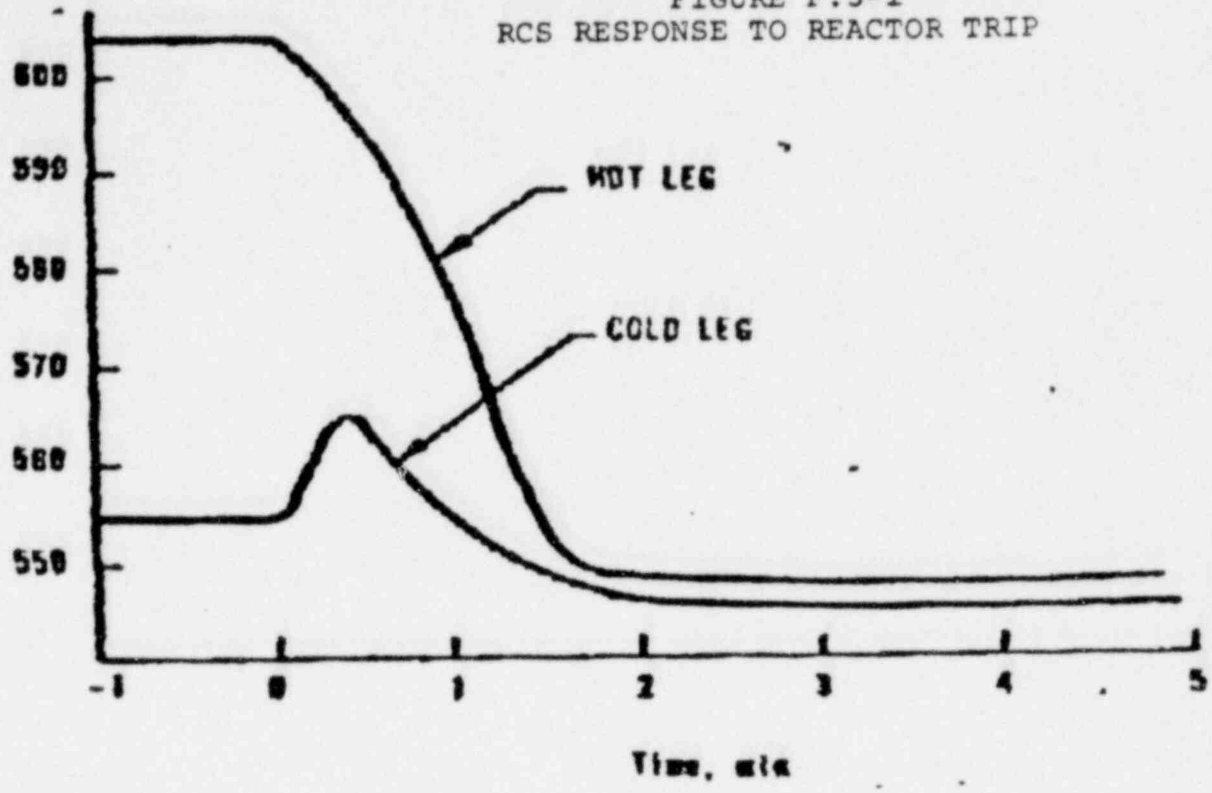
d. Review the current Midland MFW system design to identify changes which would significantly decrease the frequency of feedwater upsets which might cause reactor trip, thereby minimizing the probability of subsequent overcooling.

e. Install an MFW overfill limiter to preclude feedwater overfill above a preset steam generator level, thereby minimizing overcooling due to failures in the MFW flow control system following reactor trip.

These existing and proposed design features will reduce the frequency of reactor trips during minor feedwater flow and steam pressure upsets while the reactor is at power, and minimize the probability of subsequent overcooling. In addition, several of the features provide more reliable and accurate feedwater flow and steam pressure control following a reactor trip.

In summary, the experience at B&W operating plants has demonstrated that overcooling is a moderate-frequency event which is safely mitigated by the actuation of the HPI system. The combination of existing and proposed design features at the Midland plant will serve to further reduce the frequency of overcooling due to improper steam generator pressure and feedwater flow control following reactor trip.

FIGURE F.3-1
RCS RESPONSE TO REACTOR TRIP



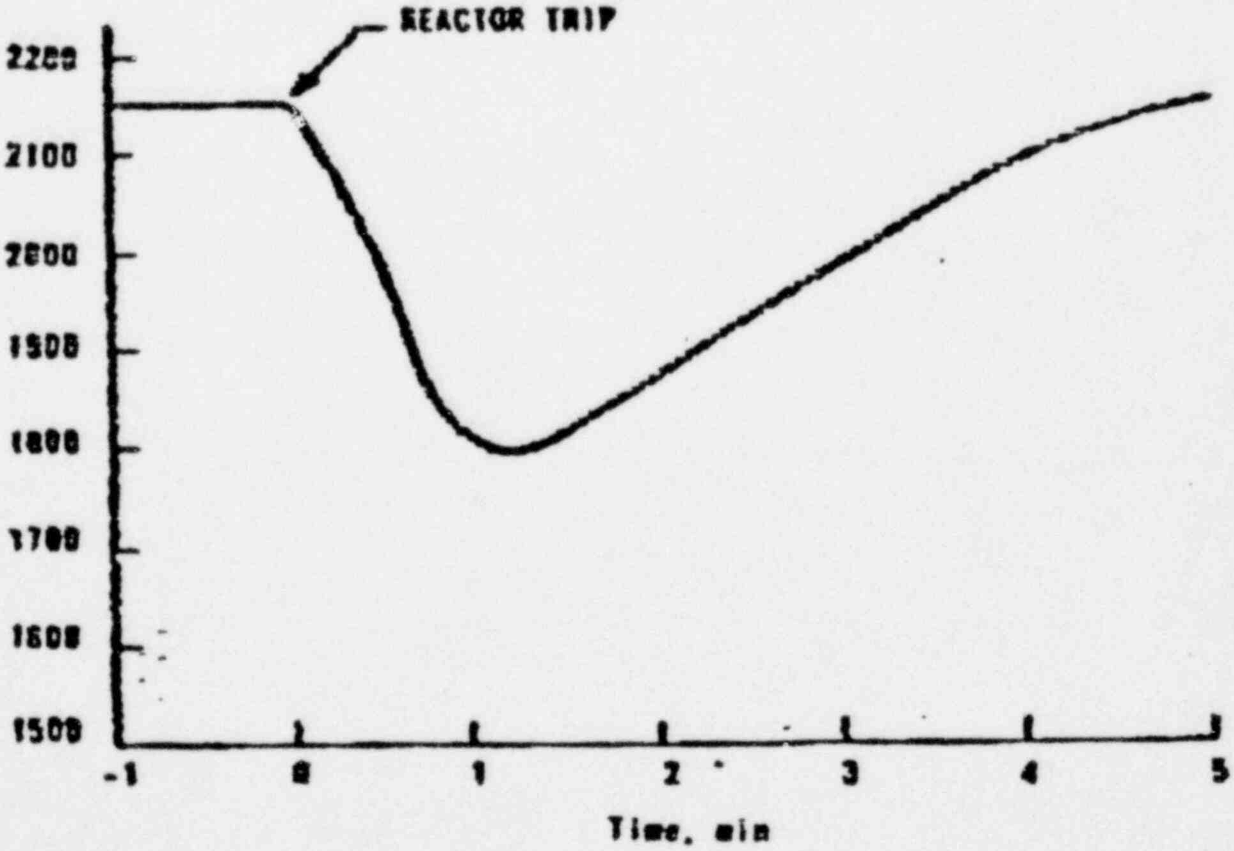


TABLE F.3-1

OVERCOOLING EVENTS AT B&W REACTORS

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
6/13/75	Reactor trip on low pressure from 19% FP due to pressurizer PORV opening. Five and one-half minutes into the transient HPI initiated when RC pressure reached 1,500 psig; RC pressure bottomed out at 720 psig when the PORV block valve was closed 28 minutes into the transient.	429	720
5/5/73	The reactor was manually tripped from 18% FP after an instrument technician inadvertently opened a valve and caused a loss of MFW. Approximately 4 minutes after the initial loss of FW, FW flow to both OTSGs was re-established at a high flowrate causing a rapid cooling of the RCS.	520	1,330
11/10/79	Reactor trip from 99% FP on RC due to OTSG feeding. Approximately 20 seconds after the reactor trip, all power to the ICS was lost and caused OTSG overfeeding due to the opening of FW valves.	420	1,650
4/23/78	Reactor trip from 30% FP due to noise spike on power range neutron detector. Five main steam safety valves failed to reseat at the correct pressure and the OTSGs blew down to 550-600 psig before the valves reseated. The operator reduced FW demand but failed to recognize that feed pump speed was in manual and did not run back feed pump speed causing overfeeding of the OTSGs.	464	

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
3/2/77	Reactor trip from 40% FP due to loss of power to the control rods and the ICS. Subsequent OTSG overfilling caused RCS cooldown.	410	1,800
7/11/74	The reactor tripped on low RC pressure following loss of the ICS auto power. An instrument supervisor knocked out the 2KI-22 circuit breaker which supplies ICS auto power. ICS power was restored in 30 to 45 seconds. The reactor tripped from 80% on low RCS pressure. The overcooling apparently was the result of improper FW control while the ICS auto power was out.	528	1,450
10/23/77	The reactor tripped on low RCS pressure following OTSG overfeeding by AFW. The transient started when a "half-trip" of the steam and FW rupture control system closed the startup FW valve to OTSG 2 followed by a low OTSG level trip of the turbine, OTSG isolation, and AFW initiation. A rapid cooling of the RCS resulted due to AFW overfill.	520	1,575
9/24/77	Manual reactor trip from 9% power when OTSG undercooling resulted in high pressurizer level (290 inches) and pressure. The pressurizer PORV cycled nine times and stuck open, discharging to the quench tank. PORV remained open and pressure decreased tripping ESFAS and starting HPI pumps at 1,600 psig.	505	875

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
	Pressure continued to decrease until the PORV block valve was closed at 20 minutes.		
11/29/77	Reactor trip on high flux at 50% FP due to improper jumper in test equipment which caused the ICS to increase FW and pull control rods to increase power from 40% to the high flux trip setpoint at 62% FP. Subsequent overcooling was caused by OTSG overfill with AFW.	512	1,600
11/7/78	The reactor was in a power runback from 92% FP when it tripped on the variable temperature pressure trip due to loss of one MFW pump. The ICS began a power runback to 55% FP, but because of the initially elevated Tave, the reactor tripped at 64% FP; subsequent overcooling was apparently caused by a leaking or stuck open turbine bypass valve.	528	1,550
1/30/77	Reactor trip on low RC pressure from 15% FP following manual turbine trip. Following turbine trip, the OTSGs were underfed causing RCS heatup. Operator action to regain FW caused overfeeding and a subsequent low pressure reactor trip.	NA	1,540
2/26/80	The reactor tripped on high RCS pressure at 2,300 psig during an MFW upset initiated by loss of NNI power. Due to the loss of NNI power, the ICS ran FW down and tried to increase	514	1,325

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
	reactor power resulting in the reactor trip. The pressurizer PORV opened and stayed open due to the power failure. RCS pressure decreased to 1,500 psig where HPI was automatically initiated and the four RCS pumps were turned off in accordance with procedure. The PORV isolation valve was manually closed by the operator.		
3/28/79	Reactor trip on high RC pressure from MFW. 100% power due to loss of MFW. The pressurizer PORV stuck open and remained open, and RC pressure decreased below 1,600 psig to ∿600 psig.	~280	~600
12/14/78	The reactor tripped from 98% FP on pressure/temperature trip after an electrical short caused the ICS to pull rods to raise Tave. Both main feed pumps tripped on high discharge pressure; emergency feed pumps started and then stopped when MFW was reestablished. MFW did not control properly, and level in "B" OTSG went to zero. Emergency FW reestablished to "B" OTSG and caused overcooling which initiated HPI.	NA	1,440
6/18/74	The reactor was tripped manually from 7% FP following about 10 minutes of oscillatory behavior of the primary and secondary systems. A loss of instrument air caused the turbine bypass valves to close and the FW valve to partially open. The undercooling caused the RC temperature and	~530	~1,610

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
	pressure to increase followed by several minutes of oscillation before the reactor was tripped. The OTSGs were boiled dry and were dry for 7-8 minutes before level was restored to normal.		
11/20/73	The reactor tripped on low RC pressure from 57% FP due to a stuck-open pressurizer spray valve. The RC pressure started decreasing and the oeprator was successful in attempts to close the pressurizer spray valve and block valve. The spray line block valve was finally closed after reactor trip when an electrician entered the containment and jumpered the torque overload circuit.	NA	~1,600
3/29/78	Reactor trip on the pumps/power trip during hot zero power testing caused by a loss of vital bus power to the reactor protection system. The loss of vital power caused a partial loss of NNI and caused the pressurizer PORV to open and remain open. RCS pressure decreased from 2,200 psig to 1,173 psig in 4-1/2 minutes before the vital bus power was restored and the PORV closed. HPI started automatically at 1,600 psig, 2 minutes and 15 seconds after the reactor trip, and restored RCS pressure.	530	1,173
4/16/77	Manual reactor trip from 15% FP in accordance with the test procedure for shutdown from outside the control room. Subsequent OTSG overfeeding was due	~474	1,810

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
	to the FW pump in manual and the startup FW valves sticking partially open. Both OTSGs were fed to a point in excess of 100% on the operating range.		
1/6/79	Turbine trip from 71% FP with an FW block valve stuck in an open or partially open position. The operator then closed the MFW cross-connect valve and tripped one feed pump causing underfeeding. The operator tripped the reactor and started the emergency feed pump which then overfed the OTSGs.	521	1,600
12/2/78	Reactor trip from 22% FP on low RCS pressure while switching from the startup to the MFW control valves. Prior to the trip, the MFW control valves were full open by manual handwheel with the instrument air isolated. When the operator increased FW pump speed during the switching process, the OTSGs were overfed and the reactor tripped on low RCS pressure; subsequent overcooling was caused by overfeeding the OTSGs.	515	1,600
3/20/78	Reactor trip on high RC pressure from 70% power due to LOMFW caused by faulty input signals to ICS. Subsequent OTSG overfeed from both MFW and AFW overcooled primary system and overfilled the OTSGs.	285	1,490

TABLE F.3-2 (Continued)

Date	Event Description	Minimum RC Temperature (°F)	Minimum Rc Pressure (psig)
1/15/79	Reactor trip on high RC pressure from 100% power due to OTSG under-feeding caused by loss of power to ICS. MFW was not terminated. AFW was started and both MFW and AFW overcooled the primary system by overfilling the OTSGs.	430	1,183
8/16/79	Reactor trip on high RC pressure from 45% power due to OTSG under-feeding caused by faulty FW pump speed control. The "A" MFW valve remained open and subsequent OTSG overfeed caused primary system overcooling.	500	1,550
10/7/74	Manual reactor trip from 15% power to prevent RCS heatup caused by LOMFW due to loss of condenser vacuum. Secondary steam leaks to auxiliary loads (MFW pumps, air ejectors, etc) caused excessive steam relief, loss of steam pressure, and primary system cooling.	408	1,810

Question F.4

Your response states that you intend to bring together information from B&W and your own evaluations of B&W operating plant experience coupled with the ICS-FMEA and a B&W review of overcooling transients to identify the changes which may significantly decrease the frequency of upsets to feedwater. State when this review and analysis of the MFW system will be performed and how the recommendations and studies proposed in your response are likely to be affected by your results.

Response

The review of the Midland feedwater system will be performed during 1980 and the results of this study will be factored into the Midland design. As stated in our original response, the potential changes to the design which have been identified to date are related to plant control and instrumentation. We do not expect that the final results of this study will affect these conclusions.

Question F.5

Other applicants responding to our October 25, 1979 requests have considered the following additional items to further decrease undesirable perturbation in the once-through steam generator:

a. Increased demineralized water makeup capacity to the condenser hotwell during runback following a turbine trip.

b. Increased bypass capability around the condensate polishers with fast acting valves.

Discuss these and like considerations which you have given to the Midland design and their effectiveness.

Response

The items identified in this question have been evaluated for their applicability to the Midland plant. As discussed below, unique features of the Midland design eliminate the need for or benefit of these changes.

a. Increased Demineralized Water Makeup Capacity to the Condenser Hotwell During Runback Following a Turbine Trip

The Midland design does not include the large atmospheric dump capability which may exist in other plants. As a result, the water lost from the Midland cycle, which must be made up from the condensate storage tank, will be less. Also, the Midland design includes a deaerator with a fairly large storage capacity. During a transient, the deaerator and the condenser provide a large surge volume which, balanced with the size of the line from the condensate storage tank to the condenser, provide adequate makeup capability. During the normal course of design, the adequacy of the makeup line has been verified.

b. Increased Bypass Capability Around the Condensate Polishers with Fast Acting Valves

This design modification is more applicable to plant designs which do not include a deaerator in the cycle. A fast bypass capability is not necessary for Midland since a surge volume for the feedwater and booster pump suction is provided by the deaerator storage tank. This feature would be more important when the condensate pumps provide a direct discharge into the feedwater pump suction and disturbances in the condensate system are immediately reflected at the feedwater pump.

Other considerations which are applicable to the feedwater system are under review and are included in the main feedwater design study. The items in this study include, but are not limited to, assuring a stable delta P signal for control of main feedwater, assuring smooth transients from startup to the main feedwater valve control, and investigating the role of the integrated control system runbacks on secondary system disturbances.

Question F.6

Discuss the advantages and disadvantages, if any, of a control independent of the ICS to terminate main feedwater flow following a reactor trip.

Response

The routine termination of main feedwater (MFW) following a reactor trip would constitute an overreaction to the potential for low probability (overfill) or low risk (overfeed) events. These two events are sometimes confused. Temporary overfeed occasionally occurs following reactor trip. While this constitutes a departure from ideal post-trip performance, it is not a serious concern. The resulting shrinkage can be easily accommodated within the indicated range of the pressurizer. The most frequent causes of this event are equipment malfunction or improper tuning of control systems. At Midland, careful tuning of the integrated control system should reduce the probability of this occurrence. Once-through steam generator (OTSG) overfill is definitely an undesirable event which, as previous analysis demonstrates, can result in reactor coolant system overcooling. It is, however, a low probability event and certainly does not routinely occur following reactor trip. At Midland, the design of the MFW control system will include the capability to prevent OTSG overfill.

The routine termination of MFW (the preferred source of water for the steam generator) following reactor trip would unnecessarily exercise the auxiliary feedwater system, complicate the control room operators' duties following a trip, and superimpose an additional transient upon the steam generators. Furthermore, this action would place the entire nuclear steam supply system in a degraded condition by deliberately defeating the primary means of removing heat from the reactor coolant system, main feedwater.

Question F.7

Specify the extent to which control limitations such as valve and pump speed responses effect main feedwater stability, particularly:

a. during startup from the manual to the automatic operational mode or

b. during automatic switchover from one process steam mode to another.

Response

a. The response of the main feedwater system during the startup phase at low power is a critical item in both the once-through steam generator (OTSG) and recirculating steam generator startups. At low power levels during both manual and automatic control, the response of the system should be as smooth as possible and the system should be designed to eliminate any perturbations which could cause rapid changes in system parameters. To accomplish this, the feedwater pump speed when in manual control should be adjusted to maintain an approximately 35 psi differential pressure across the control valve. In this way, changes in feedwater valve positions during manual control will result in a slow change of flow. Also, since the automatic control maintains an approximately 35 psi differential across the control valve, the transfer from manual to automatic will not result in changes to the pump speed which could perturb the system. The flow control valve characteristics at low flows are also an important factor in obtaining smooth control. A 35 psi pressure drop across the control valve permits the valve to operate in its normal control range resulting in smoother control. In addition to these operating guidelines, design features have been incorporated in the Midland plant to eliminate unwanted perturbations of the system. One such feature is the Midland feedwater pump recirculation valve which is a modulating valve and eliminates any changes caused by an on/off valve controller. Even considering the above, manual control of feedwater is highly dependent on the operator. Operator capability to control the flow at low powers increases with experience and training.

b. The process steam transfer system will be modified so that all mode changes except Mode 1 to 2 will be initiated by the operator and will be executed at rates of load change which are well within the response capabilities of the integrated control system (ICS), reactor, turbine-generator, and feedwater system.

A Mode 1 to 2 transfer (Unit 1 extraction supply to Unit 1 main steam supply) can be initiated manually or automatically. When manually initiated, the Mode 1 to 2 transfer will be conducted in a controlled manner to minimize perturbations in Unit 1 reactor power, MWe load, and feedwater flow. When automatically initiated, such as following a turbine trip, our intent is to execute the Mode 1 to 2 transfer as quickly as possible to reduce the magnitude of the steam and feedwater flow transients.

Question F.8

State the design objectives of the revised auxiliary feedwater control system. Also indicate whether it will:

a. Initiate for all loss of MFW events, either total or partial, and at what lower limit;

b. Initiate on SIAS;

c. Initiate on loss of offsite power;

d. Preclude overcooling or undercooling of the primary system even with a single failure in the system (e.g., failures in input, power, valves); and

e. Interact in any adverse fashion with the Feed-Only-Good-Generator interlock.

Also, describe how you will demonstrate that the dynamic response has been achieved.

Response

I. GENERAL

The design objectives of the auxiliary feedwater (AFW) control system are as follows.

a. Redundant and independent initiation and control circuits will be provided for each AFW train such that the capability to initiate and control at least one AFW train, when required, is maintained even when degraded by a single random failure. Redundancy and independence will be provided from the sensors through the actuated devices.

b. The redundant portions of the AFW control system will be powered by separate Class 1E vital battery-backed buses such that the objective of Item I.a can be accomplished with the loss of a single vital bus or with the loss of all ac power except that derived from inverters.

c. The system will provide automatic initiation of AFW for all required conditions including emergency core cooling system actuation.

d. The AFW system and its controls will be designed such that AFW flow will be injected within 40 seconds after an initiation signal. This time limit includes the time required for diesel startup and generator loading.

e. Two level setpoints will be provided. The low steam generator level setpoint (approximately 2 feet) provides adequate inventory for decay heat removal with forced primary circulation. The high steam generator level setpoint (approximately 20 feet) provides adequate inventory for decay heat removal with natural circulation of primary coolant. The control system will automatically select the appropriate setpoint based on reactor coolant (RC) pump status.

f. The injection of full AFW flow can, under certain conditions (high level setpoint, low decay heat), result in considerable cooling of the primary system. Therefore, the control system will be designed to limit AFW flow based on a predetermined rate of steam generator level increase. The rate limit will be selected such that overcooling is minimized at low decay heat levels and adequate cooling is provided at maximum decay heat levels. The minimum level rate will be established based on providing adequate cooling with maximum decay heat. This rate limit will then be assessed with respect to minimization of overcooling at low decay heat conditions. Calculations have shown that under worst case overcooling conditions (high level setpoint, zero decay heat, no makeup flow), level rate control will provide at least 10 minutes of automatic control before operator action is required to prevent loss of pressurizer level indication. However, performance verification of level rate control and final setpoint (rate limit) determination will be accomplished by preoperational testing.

g. Primary system cooldown during AFW operation will be controlled to less than 100F in any 1 hour time period.

h. The system shall not include control of secondary system pressure. Existing control of steam generator pressure by the integrated control system utilizing both turbine bypass valves and steam safety relief valves shall be retained.

i. The system will include necessary bypass features of the automatic initiation for plant startups and shutdowns.

II. RESPONSES TO QUESTION F.8.a THROUGH F.8.e

a. See response to Question F.9.

b. See response to Question F.9.

c. See response to Question F.9.

d. The entire AFW system, including controls, is designed to provide decay heat removal assuming a single failure. The level rate control feature of the AFW control system is not intended to be designed to single failure requirements, i.e., a single failure can result in full AFW flow with resultant potential for overcooling. AFW flow to the steam generator caused by such an event would be terminated automatically when a high once-through steam generator level was reached or more probably by manual operator action. Designing level rate control to prevent overcooling in the event of a single failure, if indeed achievable, would result in a reliability degradation in meeting the safety function of the AFW system (decay heat removal).

e. See response to Question F.12.

As stated in Item I.f, preoperational tests to verify the adequacy of the AFW level control system will be conducted. This program will require that a test of the system be performed both before and after fuel load.

Question F.9

For your intended revision to the AFW initiation logic, identify the signals (e.g., generator level, no feedwater flow, loss of pump suction pressure, SIAS, and loss of steam flow to pumps) that will be used to initiate AFW and justify their use. Also, update your response to our request 031.51 to identify the type and characteristics of the revised transmitters selected for the reverse feedwater flow monitoring system.

Response

Automatic initiation of the auxiliary feedwater (AFW) system is based on the need for AFW flow to accomplish the following:

a. Maintain continuity in reactor coolant system (RCS) flow during the transition from forced to natural circulation when RC pumps are tripped

b. Prevent the boil-off of the entire inventory of water immediately following a loss-of-main feedwater (MFW) occurrence and anticipatory trip of the reactor

c. Provide a conservative margin to prevent overpressurization of the RCS due to potential undercooling following a loss-of-MFW event

The individual parameters selected to initiate AFW and the specific justification for each are as follows:

a. Loss of both MFW pumps: The AFW system provides a backup source of feedwater sufficient to remove decay heat and pump heat should the primary source (MFW) be lost. Low control oil pressure is sensed because this condition will exist whenever an MFW pump turbine is tripped.

b. Low steam generator level: Low level in either once-through steam generator (OTSG) is indicative of insufficient feedwater flow and provides a backup for initiation on loss of MFW.

c. Emergency core cooling actuation system (ECCAS): ECCAS actuation results in initiation of the main steam line isolation system (MSLIS) which isolates main steam and MFW to both OTSGs. Therefore, AFW is required to remove decay heat. FOGG logic will prevent AFW flow to a ruptured steam generator and acts independently of the AFW actuation system.

d. Loss of RC pumps: Loss of forced RC flow will result in a reactor trip and integrated control system (ICS) runback of MFW. AFW is initiated to raise the OTSG level to approximately 20 feet to facilitate establishing and maintaining natural circulation of primary coolant.

e. Low steam pressure: Low steam pressure will initiate the MSLIS and isolate main steam and MFW to both OTSGs. Therefore, AFW is required to remove decay heat. FOGG logic will prevent AFW flow to a ruptured steam generator. (See the response to Question F.12 for a discussion of the FOGG logic).

f. Loss of offsite power: Undervoltage on either of the Class 1E 4160 V buses is sensed to indicate a loss of offsite power. A loss of normal ac station power will result in the loss of MFW and all four RC pumps. This signal provides diverse initiation for both a loss of MFW and a loss of forced RCS flow.

The necessity for and configuration of the reverse feedwater flow monitoring system are currently being reevaluated. Therefore, additional information is not available at this time.

Question F.10

You state that changes to the Midland auxiliary feedwater configuration since the TMI-2 accident will include:

a. Modification of the AFW pump suction piping from one interconnected system for both Midland units to two systems operating independently to supply AFW to each unit, and

b. The addition of redundant flowpaths from the discharge of each AFW pump to each steam generator.

Provide a simplified diagram illustrating the previous and revised configurations. Include a table denoting valve positions during normal and abnormal operating conditions. Specify your schedule for completion of the details of the revised Midland AFW design.

Response

Figures F.10-1 and F.10-2 illustrate the previous (current) design and planned revised design, respectively, for both the suction piping and the discharge piping. The detailed control design and analysis is incomplete at this time; however, Figure F.10-2 indicates the control parameters planned to be used in the design.

Table F.10-1 summarizes the position of valves under five selected operating conditions. For simplicity of presentation, we elected to assume no single failures. The positions tabulated represent the alignment of the valves upon receipt of the actuation signal.

Detailed design of the revised auxiliary feedwater system is expected to be essentially complete by August 1980. FSAR updating is anticipated at that time.

TABLE F.10-1

AFW SYSTEM VALVE POSITIONS - REVISED SYSTEM

Valve Number	Normal Cooldown to DHR Initiation (Deaerator Suction)	AFWAS Actuation (CST Suction)	AFWAS and Low AFW Pump Suction Pressure (SWS Suction)	Steam Generator A Main-Steam Break (CST Suction)	Station Blackout Operation (CST Suction)
Train A					
2MO3993A1	Close	Close	Open	Close	Close
2MO3993A2	Close	Close	Open	Close	Close
2MO3968A	Open	Open	Close	Open	Open
2LV3975A1	Modulate	Modulate	Modulate	Close	Modulate(3)
2LV3975A2	Modulate	Modulate	Modulate	Modulate(2)	Modulate(3)
2XV3989(1)	Close	Close	Close	Close	Close
2MO3965A	Open(2)	Open	Open	Close	Open
2MO3970B	Close(2)	Open	Open	Close	Close
Train B					
2MO3993B1	Close	Close	Open	Close	Close
2MO3993B2	Close	Close	Open	Close	Close
2MO3968B	Open/Close	Open	Close	Open	Open
2LV3975B1	Close	Modulate	Modulate	Modulate	Modulate
2LV3975B2	Close	Modulate	Modulate	Close	Modulate
2MO3965B	Open(2)	Open	Open	Open	Open
2MO3970A	Close(2)	Open	Open	Open	Close
Common					
2MO3956	Close	Open	Open	Open	Open
2MO3940A	Open	Close	Close	Close	Close
2MO3940B	Close	Close	Close	Close	Close
2MO3936	Close	Close	Close	Close	Close

(1) Valve 2XV3989 is only open when the AFW system is used for plant startup or cooldown via the main feedwater system.

(2) At least one of the two valves to each steam generator will be open.

(3) Valves will modulate, but since motor-operated pump is not operating, there will be no flow through these valves.

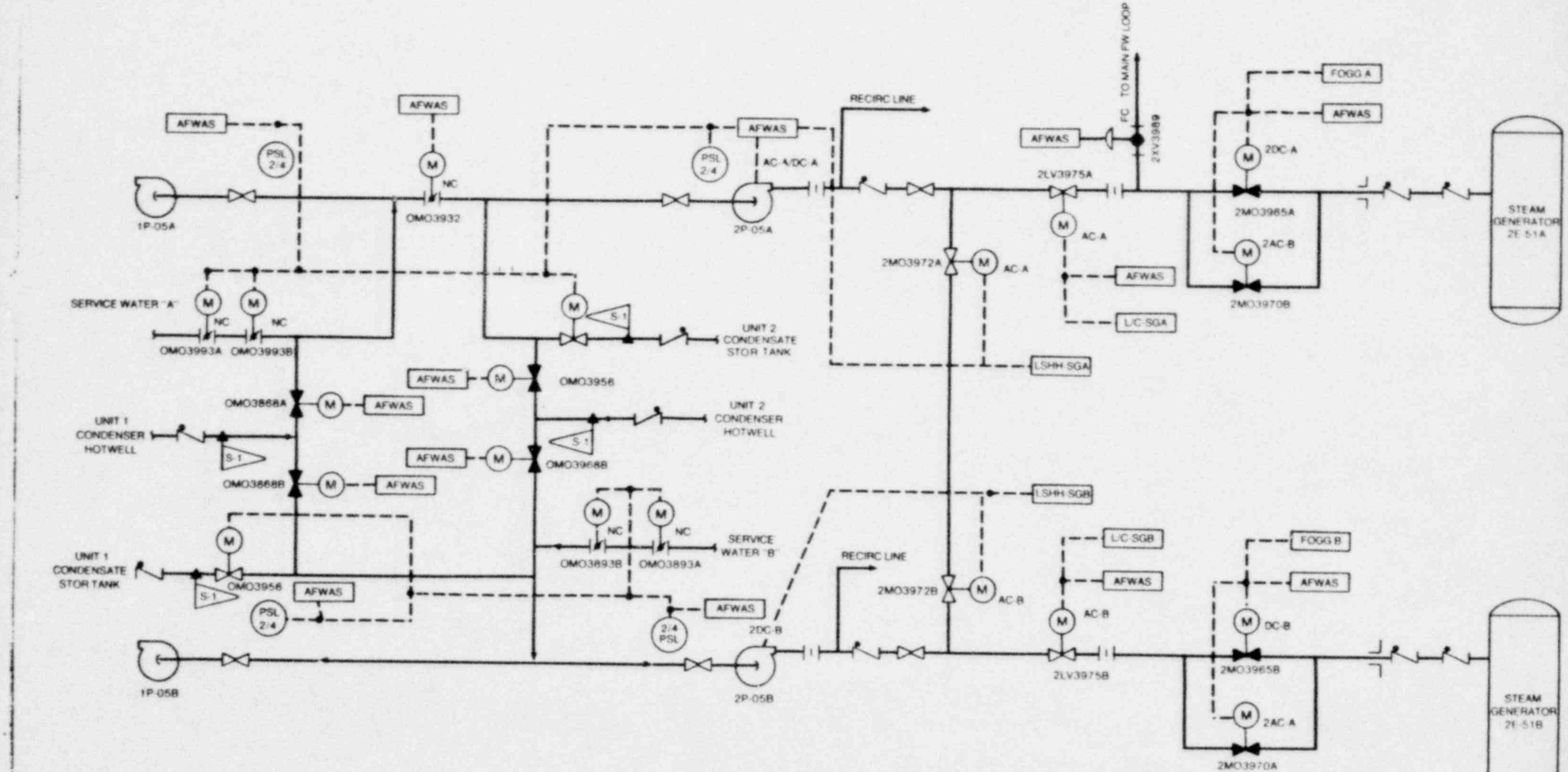


FIGURE F 10-1
SIMPLIFIED DIAGRAM
MIDLAND PLANT UNITS 1 AND 2
AUXILIARY FEEDWATER SYSTEM
CURRENT DESIGN

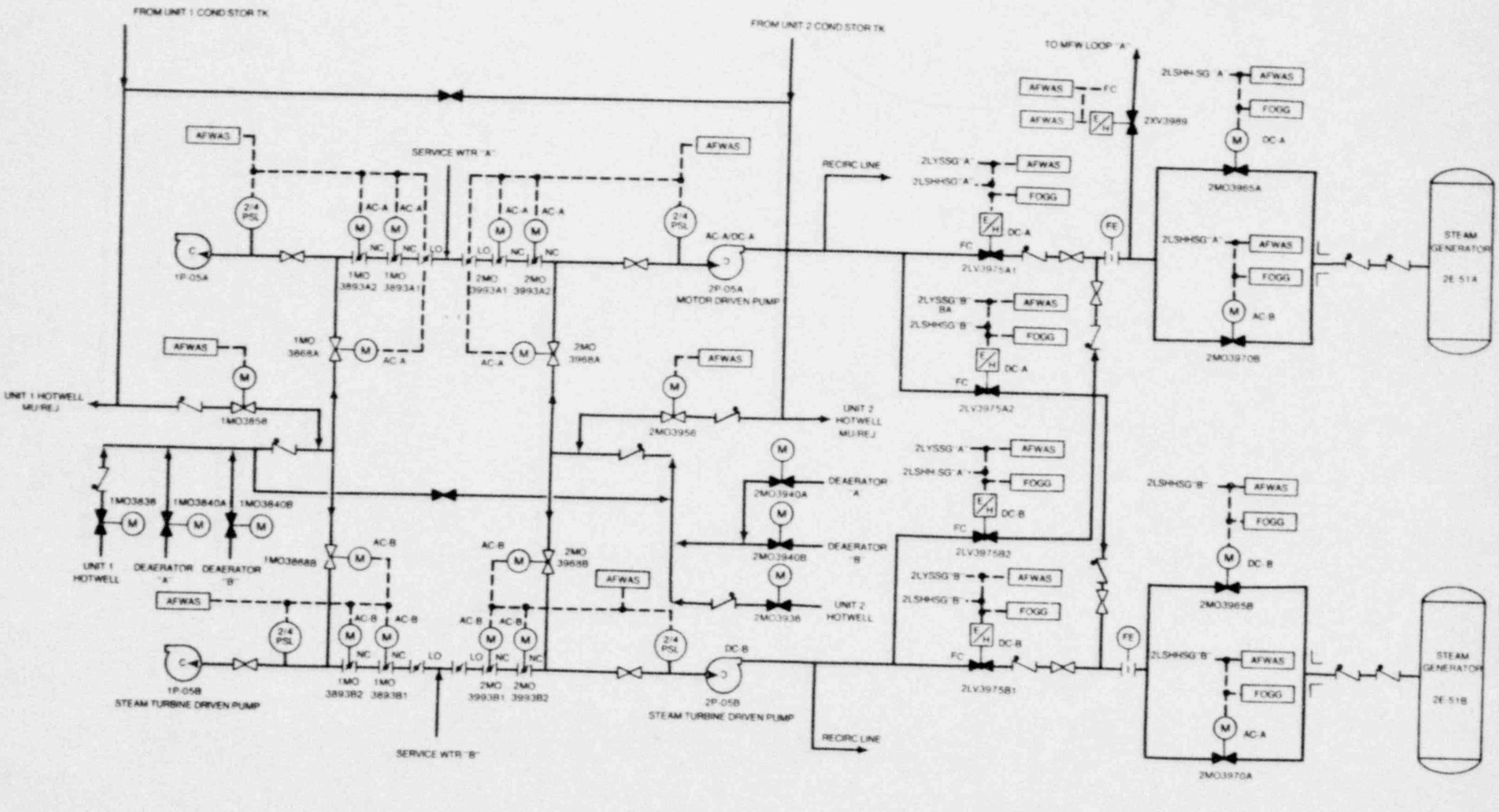


FIGURE F.10-2

SIMPLIFIED DIAGRAM
MIDLAND PLANT UNITS 1 AND 2
AUXILIARY FEEDWATER SYSTEM
PRELIMINARY REVISED DESIGN

G-1067-01

Question F.11

In the event of a steam line break upstream of the MSIVs accompanied by failure of a MSIV in the intact line, reliance is placed upon reliable but non-safety grade circuits and downstream valves to isolate steam flow except for residual flows associated with turbine gland sealing, etc. Describe the behavior of the revised FOGG interlock during this accident scenario, including the significance, if any, of the residual steam flow limits on the FOGG system.

Response

An analysis of worst-case single failures following a main steam line break has been performed and is discussed in the FSAR in the response to NRC Question 211.185. This analysis shows that the maximum blowdown of the unaffected steam generator occurs if the atmospheric dump valve on that steam generator fails open. Blowdown from the unaffected steam generator through the atmospheric dump valve exceeds the blowdowns through available residual flowpaths if the main steam isolation valve fails to shut and therefore provides a worst-case scenario for evaluation of the revised FOGG logic. The results of this analysis will be reviewed as described in the response to Question F.12 to ensure proper operation of the FOGG interlock.

Question F.12

In addition to the FMEA for the revised FOGG interlock to be provided as part of your revised AFW evaluations, identify those events and combinations of events which have been and will be evaluated to assure that no confused or inadvertent inputs (such as from a previously unrecognized event or event combination) can lead to a malfunction or undesirable operation of the FOGG system. Also describe any studies and tests performed to assure proper integration and interaction of the FOGG interlock with other systems.

Response

Failure modes of the FOGG interlock will be evaluated during the normal process of system design to ensure the design meets single failure criteria. No formal failure modes and effects analysis of the FOGG interlock is being prepared.

Babcock & Wilcox is currently reviewing the steam line break spectrum studies submitted in the Midland FSAR. This review is to assure the revised FOGG logic does not invalidate any of the submitted results, will respond properly for all break sizes, and does not interfere with normal operational transients. The output from this review will be appropriate setpoints for FOGG action.

Question F.13

Describe the results of your design evaluation studies for the several process steam operating modes performed to determine whether any unique opportunities for operator or equipment errors (such as improper system alignments, including misalignments between circuitry and hardware) or adverse interactions unique to a given mode exist which could lead to overcooling or overpressurization transients or accidents more severe than those for which the protection systems have been analyzed and designed. Identify the maximum potential contribution of the process steam to the sensitivity of overcooling events for the Midland plant, whether as a result of heat extraction through the tertiary heat exchangers or via any control system change influenced by the Dow use of steam.

Response

Operating at its full design capacity, the Midland process steam system (PSS) will consume about 40% of the steam flow from the nuclear steam supply system (NSSS) from which it is supplied. Actual load projections indicate that the system will operate at 50% or less of its design capacity for several years following initial operation. The potential contribution of the PSS to cause undercooling transients is limited by the fraction of NSSS output which is dedicated to process steam production. Unique operator errors or equipment malfunctions could produce a step decrease in NSSS steam load of 40% (loss of the PSS). This load rejection is obviously well within the capability of the reactor protection systems, which are designed for 100% load rejections. The maximum potential PSS load increase leading to reactor overcooling is represented by a rupture of the 36-inch main steam supply line to the PSS. Analyses of such steam line breaks of varying size and location are presented in Appendix 15D of the Midland FSAR. No unacceptable overcooling conditions were found.

Although the worst case transients originating from the PSS are well within the design capabilities of plant protection systems, the impact of less severe PSS operational transients is of concern. In response, reevaluation of the design and operation of the PSS is being conducted with the objective of reducing the frequency and severity of operational transients within the PSS while maximizing system availability. Additionally, post-fuel load testing of the PSS will be conducted to verify that normal mode transfers and load changes are within the response capabilities of the plant control systems.

Question F.14

You state that you are currently investigating modifications to the AFW level control system to limit primary cooldown rate following AFW actuation. Describe how the control modifications under consideration would provide the capability to distinguish in a positive manner between transients and accidents with regard to SG level setpoint control. Also describe how two-phase level during swell from depressurization affects level detection and how this is treated in the analyses.

Response

The auxiliary feedwater (AFW) control system will have two once-through steam generator (OTSG) level setpoints that are automatically selected based on reactor coolant (RC) pump status. This method of selection ensures the appropriate level setpoint will be in effect for all transients and accidents requiring AFW. The high level setpoint (20 feet) will be selected automatically when the RC pumps are tripped. For transients and accidents where the RC pumps remain operational, the low level setpoint is adequate for heat removal. For accidents where the RC pumps are lost, either intentionally as in a small break loss-of-coolant accident or due to a loss of offsite power, the level setpoint will automatically be raised to the high level. During the initial phase of a small primary system break (approximately 20 minutes to 1 hour depending on power level at time of trip), the control system will automatically raise steam generator levels to the high setpoint. The operator will then manually control AFW flow to raise OTSG levels to the level specified in the small break operating guidelines.

Preliminary evaluations indicate that level rate control provides adequate AFW flowrates for all accidents requiring AFW. This will be verified by a detailed evaluation of Chapter 15 events. In the unlikely event that level rate control provides insufficient AFW flow for certain accidents, the control system will provide for bypass of the level rate limiting function under those conditions and allow full AFW flow up to the OTSG level setpoint.

Errors in level detection can occur from several phenomena, most notably ambient temperature effects on reference legs and level sensors. Of these phenomena, errors due to two-phase level during swell from depressurization are considered to be relatively minor and of short duration. However, this effect and other error mechanisms are presently under evaluation and will be accounted for in the overall design either by analytical input assumptions, changes in level setpoints, or operating guidelines.

Question F.15

The modifications, recommendations, and studies you present to reduce sensitivity are in the direction of additional automation of the plants. While this approach leaves the operator free to verify system performance and should improve the control of transients, we are concerned that potential system interaction effects might result. Therefore, a complete and integrated review of the primary and secondary system should be performed to assure that no significant adverse interactions result from the modifications that are ultimately made. Describe your plans and schedules with regards to performing such a comprehensive, integrated evaluation of these changes, based upon conservative and realistic analyses and simulator comparisons as appropriate.

Response

The modifications proposed in our response to your 10 CFR 50.54(f) request are based upon sound engineering judgment of their benefit to both system operation and overall plant safety. A comprehensive integrated evaluation of these changes will be provided through various methods previously discussed. These include safety sequence analysis work by EDS Nuclear, construction of event trees as part of the abnormal transient operating guidelines (ATOG) program, reliability analysis of the Midland auxiliary feedwater system being conducted by Pickard, Lowe, and Garrick, Inc., and overall plant response testing to be conducted prior to commercial operation. Additionally, extensive analysis has been conducted by Babcock and Wilcox on the overall plant impact of overcooling type accidents and transients. This work is presented in our revised 10 CFR 50.54(f) response (Revision 2, April 1980).

Question F.16

Provide the following analyses:

a. Overcooling event initiated by steam pressure regulator malfunction resulting in increased steam flow.

b. Overcooling event initiated by feedwater system malfunctions that result in decreased feedwater temperature.

For these analyses, assume no beneficial operator action before 10 minutes. Also, only qualified safety systems should be assumed for mitigation. Identify which safety and nonsafety grade systems are considered to operate during this transient and specify the part each of these systems take in the transients. Identify the signals acting upon these systems during the transients.

The analyses should be performed for a period of at least 10 minutes after transient initiation. If existing analyses which are presented for a shorter duration are utilized for this response, then confirm that during the time not shown out to 10 minutes:

(1) No operator action is required or assumed.

(2) No changes in operating systems are required.

(3) No significant changes result out to 10 minutes, such that extrapolation from the results presented is considered valid.

Response

a. The steam pressure regulator malfunction event has been analyzed and is included in our 10 CFR 50.54(f) response, Revision 2, April 1980.

b. The overcooling event initiated by feedwater system malfunctions that results in decreased feedwater temperature was analyzed in the FSAR, Section 15.1.1. The overcooling effect is less severe than the steam generator overfill and steam pressure regulator malfunction events previously analyzed and therefore is not included as part of the 10 CFR 50.54(f) response.

The existing FSAR analysis is carried out for 60 seconds. If this analysis was continued for a full 10 minutes operator action would not be necessary, operating systems would continue to perform in their normal, post-trip mode, and plant parameters would trend from their 60-second value as expected after a reactor trip.

Question F.17

You have stated during related meetings with NRC and with ACRS subcommittees that the analyses presented in your current 50.54(f) response were not necessarily selected to represent the worst case. Provide your recommendations as to what criteria, assumptions, and experience should be recognized in defining the worst case for design purposes.

Response

From those events considered to be of moderate frequency, a full spectrum of overcooling events has been presented in the Midland response to 10 CFR 50.54(f), Revision 2 (April 1980). The results have varied from no voiding in the reactor coolant system to the formation of large steam voids. In all cases, however, adequate core cooling has been maintained. The referenced statements were meant to indicate that additional analyses were to be performed. These analyses have been completed and are included in the revised 10 CFR 50.54(f) response.

Question F.18

Regarding your proposed changes to the pressurizer level indication, specify the new location of the instrumentation taps and revise FSAR Figure 3.8-73 accordingly. Also provide or reference the relationship between "indicated" and "actual" level for the revised Midland design.

Response

The Midland pressurizers will be modified to increase the indicated level range from 0-320 inches to 0-400 inches. Figures F.18.1 and F.18.2 show the azimuthal and elevation locations, repsectively, of the three new high level sensing nozzles and the three new low level nozzles. Table F.18.1 is to be used in conjunction with Figure F.18.2 to define the location of each nozzle. Table F.18.2 provides the relationship between "indicated" pressurizer level and the "actual" water volume.

FSAR Figure 3.8-73 will be revised when field modification is completed.

RESPONSE TO 10 CFR 50.54(F)
SUPPLEMENT 1

TABLE F.18.1

NOZZLE LOCATION MATRIX(1)

Nozzle No.	Angular Location	Dimension	Move From Present Location
1	W to X 14°±1°	A	32.375±0.125 up
2	Y to Z 74°±1°	A	32.375±0.125 up
3	Z to W 44°±1°	A	32.344±0.125 up
4	W to X 14°±1°	B	40.344±0.125 down
5	Y to Z 74°±1°	B	40.25±0.125 down
6	Z to W 44°±1°	B	40.3125±0.125 down

(1) The new level nozzles locations are to be established based on the existing as-built nozzle locations as a datum. Appropriate locating dimensions and directions are given above.

4/80

RESPONSE TO 10 CFR 50.54(F)
SUPPLEMENT 1

TABLE F.18.2

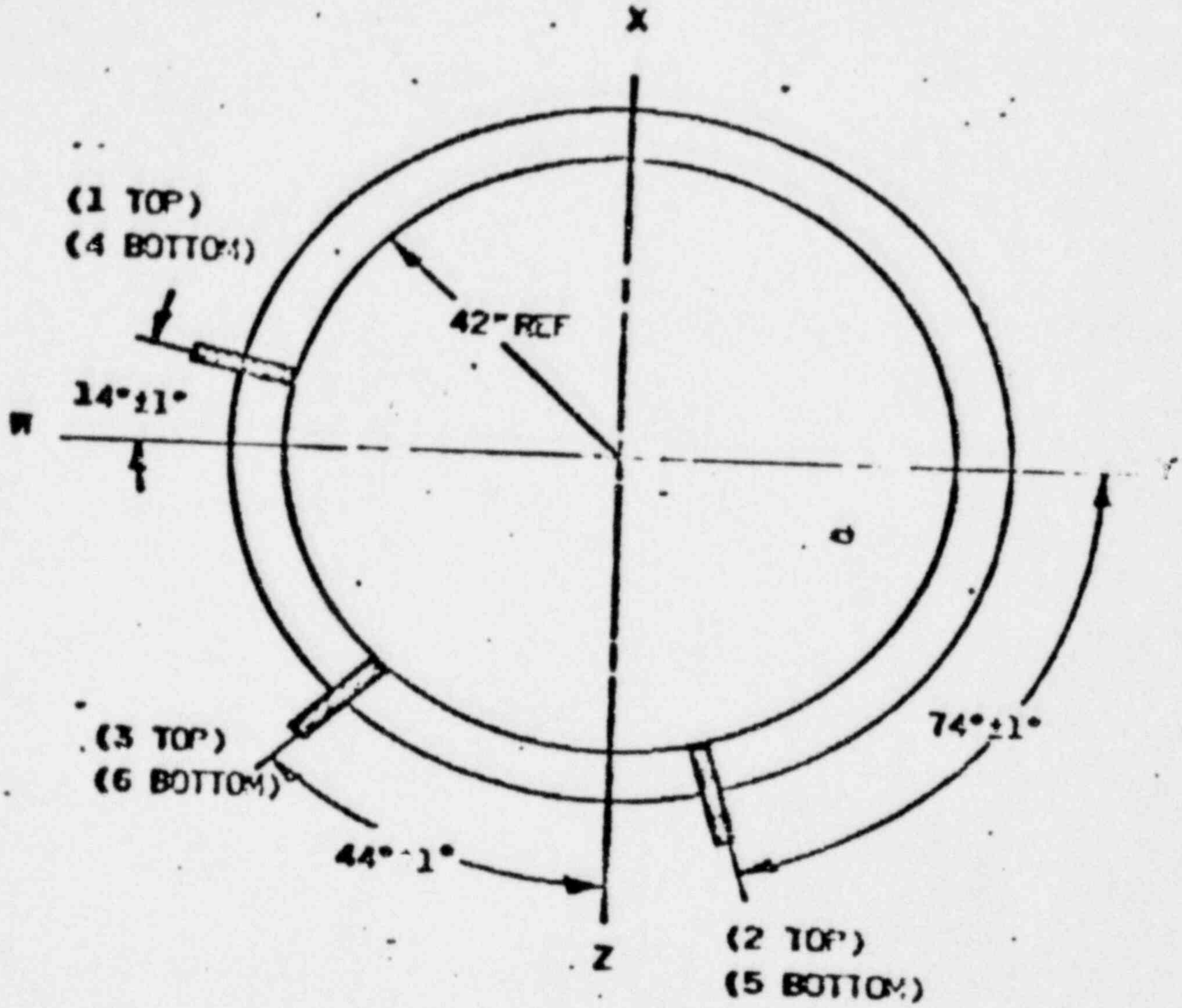
ACTUAL PRESSURIZER WATER VOLUME

VERSUS

INDICATED PRESSURIZER LEVEL

Indicated Level (in)	0-320 Inches Range (cu ft)	0-400 Inches Range (cu ft)
0	239	112
Maximum level	1,281	1,384

Note: Values are based on nominal pressurizer dimensions.



AZIMUTHAL LOCATION OF NEW NOZZLES

Three required at upper level and three required at lower level

FIGURE F.18-1

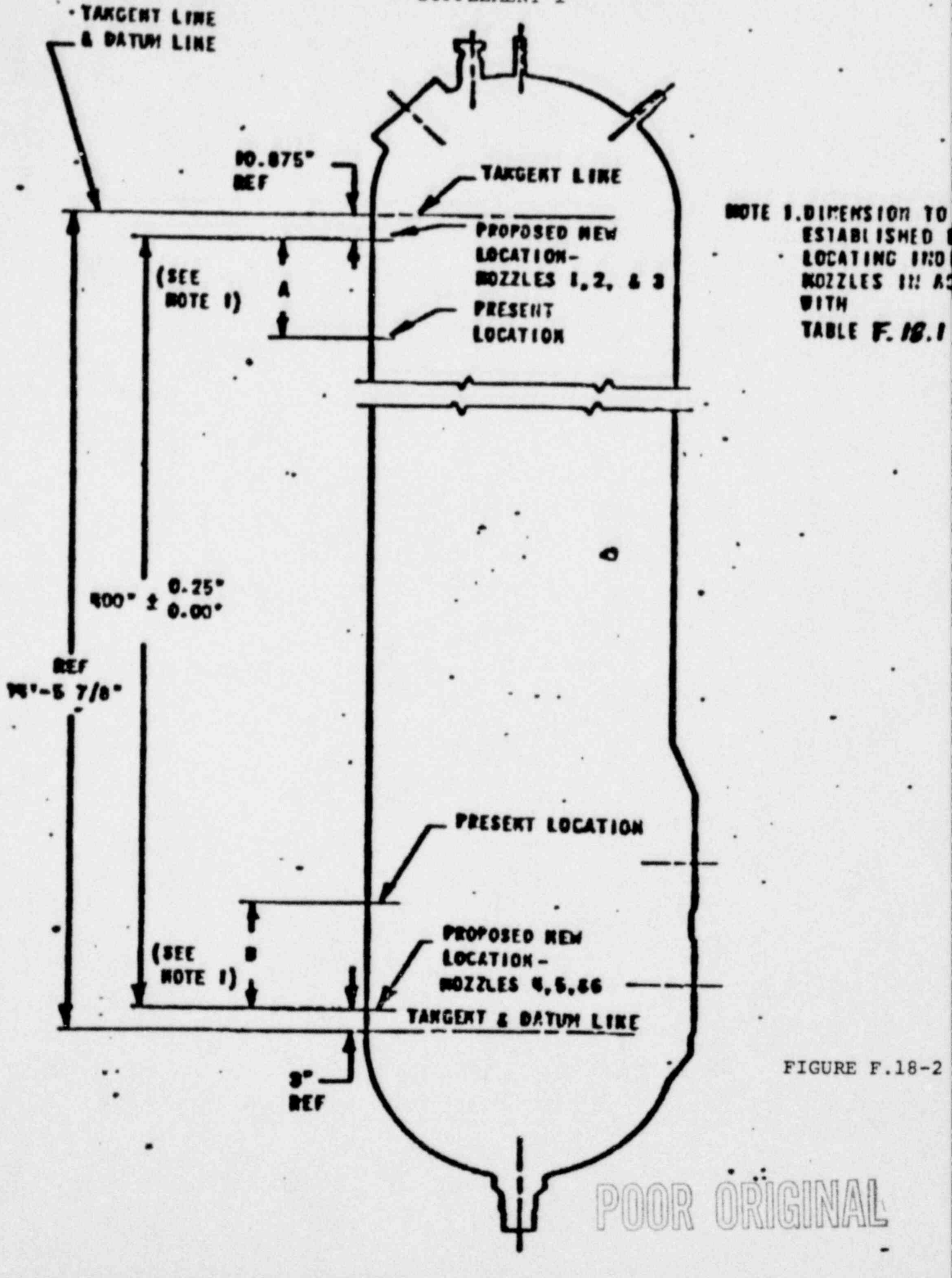

TANGENT LINE
& DATUM LINE
10.875"
REF
TANGENT LINE
PROPOSED NEW
LOCATION-
NOZZLES 1, 2, & 3
(SEE
NOTE 1)
A
PRESENT
LOCATION
NOTE 1. DIMENSION TO
ESTABLISHED
LOCATING
NOZZLES IN
WITH
TABLE F.18.1
400" ± 0.25"
0.00"
REF
56'-5 7/8"
PRESENT LOCATION
(SEE
NOTE 1)
B
PROPOSED NEW
LOCATION-
NOZZLES 4, 5, & 6
TANGENT & DATUM LINE
3"
REF

FIGURE F.18-2

Question F.19

Provide additional detail regarding the safety sequence analyses to be performed by your contractor, EDS Nuclear. Identify the 16 safety and operational sequence diagrams and the 15 auxiliary system diagrams to be used as the vehicle for this review. Describe the end product of this study and describe how these results will be factored into the A103 program.

Response

The safety sequence analysis being performed by EDS Nuclear uses the methodology previously described in Appendix F of the Midland response to 10 CFR 50.54(f) request. Attached is a reference paper authored by EDS Nuclear which more fully discusses this methodology.

The following diagrams are being developed by EDS Nuclear for Midland as part of our design review:

a. Operational sequence diagrams

1) Shutdown and cooldown to cold shutdown

2) Power operation

3) Startup

4) Refueling

b. Safety sequence diagrams

1) Loss-of-coolant accident*

2) Loss of normal feedwater*

3) Loss of nonemergency ac power*

4) Failures resulting in increased steam flow

5) Loss of external load and/or turbine trip

6) Complete loss of forced reactor coolant flow

7) Steam generator tube rupture

8) Accidental depressurization of the reactor coolant system

9) Radwaste system leak/failure

10) Loss of seal injection component cooling water

11) Excessive feedwater*

12) Small steam line break*

c. Safety sequence auxiliary diagrams

1) Turbine control (electro-hydraulic)*

2) Turbine bypass

3) Emergency core cooling*

4) Decay heat removal*

5) Auxiliary feedwater*

6) Makeup and purification*

7) Low-pressure injection*

8) Pressurizer pressure control*

9) Containment heat removal*

10) Reactor building isolation*

11) Reactor protection system

12) Engineered safety features actuation system

13) Safeguard chilled water

14) Combustible gas control system

15) Miscellaneous safety-related heating, ventilating, and air conditioning

The above diagrams represent the output from EDS Nuclear safety sequence analysis work. The diagrams noted with an asterisk (*) will serve as design input for the event trees to be developed for Midland by Babcock & Wilcox (B&W) as part of the ATOG program. This process was explained to NRC personnel at B&W Owners Group meetings on October 15, 1979 and again on February 22, 1980.

SAFETY FUNCTION AND PROTECTION SEQUENCE ANALYSIS

Authored by

R. A. Fortney
J. T. Snedeker

of
EDS Nuclear

and

J. E. Howard
W. W. Larson

of
Boston Edison Company

presented at
American Nuclear Society
Winter Meeting
November 11-16, 1973
San Francisco, California

Safety Function and Protection Sequence Analysis

Abstract

Today's complex nuclear plant safety requirements demand a planned and systematic engineering approach to identify the functional design requirements of the nuclear plant systems. This systems engineering concept is required to ensure that the nuclear plant design satisfies the various federal regulations and industry standards. The Safety Function and Protection Sequence Analysis provides such a systematic design verification process. The plant safety functions essential to achieving acceptable consequences following postulated accidents and transients are first carefully identified, and then the sequence of prime system responses that form redundant success paths to the safety functions are diagrammed as Safety Sequence Diagrams (SSD). Systems that act as essential auxiliaries in supporting the prime safety systems are functionally diagrammed on Safety Systems Auxiliary Diagrams (SSAD). When complete, the SSD's and SSAD's form the basis for comprehensive design review of all safety related systems. Because the full range of plant conditions is considered in evaluating each postulated event, the true design criteria and requirements are easily derived and documented for each safety related system, structure and component; the Quality Assured Items List is established; and redundancy and separation criteria are set. The SSD's and SSAD's also facilitate the identification of Seismic Category I equipment and structures. Systematic criteria are established for protection against pipe whip, jet impingement, fire and flooding. The information on the SSD's and SSAD's also forms the basis for the development of operating technical specifications. The concentrated effort required to perform the Safety Function and Protection Sequence Analysis is repaid many times over through the resulting benefits the analysis brings to today's nuclear project.

Introduction

Developments over the past decade in nuclear plant safety technology have given birth to numerous technically complex nuclear plant design and operational requirements. The proper application of the AEC requirements and industry codes and standards offers a significant challenge to nuclear plant engineers, managers and operators alike. The overall effect of the Safety Function and Protection Sequence Analysis is to systematize the identification of the functional design requirements to the nuclear power plant design. Developed as a systematic approach to the nuclear safety aspects of the Pilgrim Unit 2 design, the Safety Function and Protection Sequence Analysis (SFPSA) identifies the necessary and sufficient functional design requirements of the nuclear power station to insure protection of the public health and safety.

The SFPSA provides the following specific benefits for a nuclear project:

1. A complete response to Section 15.1 of the AEC's *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.*

2. A systematic and consistent identification of all systems, structures and components that must be on the Quality Assured Items List and subjected to a Quality Assurance Program satisfying the requirements of 10CFR50, Appendix B.

3. A systems level design verification process satisfying, in part, the design control requirements of 10CFR50, Appendix B.

4. A systems level failure modes and effects analysis which assists in the identification of the necessary inputs for the development of functional, physical and electrical separation criteria.
5. A systems level, single failure analysis as required by IEEE-279, IEEE-379 and Regulatory Guide 1.53.
6. A documented basis for establishing operating plant technical specifications for inclusion in Chapter 16.0 of the Safety Analysis Report.
7. A documented basis for the preparation and review of those plant operating procedures which address abnormal and accident conditions.
8. A learning and training aid for engineers and operators to facilitate understanding of the integrated plant response to various plant abnormal and accident conditions.

TABLE I

EVENTS CLASSIFICATION FOR PILGRIM 2

SFPSA EVENT CATEGORY	EVENT FREQUENCY	10CFR50, APP. A EVENT CATEGORY	10CFR50, APP. I EVENT CATEGORY	ANSI 18.2 EVENT CATEGORY
Planned Operation	Routine	Normal Operation	Normal Reactor Operation	Condition I; Normal Operation
Expected Operational Occurrences	≥ 1/year	Anticipated Operational Occurrences	Expected Operational Occurrences	Condition II; Incidents of Moderate Frequency
Infrequent Operational Occurrences	1/40 yrs ≤ f < 1/yrs	Anticipated Operational Occurrences	Expected Operational Occurrences	Condition III; Infrequent Incident
Accident	< 1/40 yrs	———	———	Condition IV; Limiting Faults

Development of the Safety Function and Protection Sequence Analysis

The fundamental objective of the nuclear plant design is to develop the functional requirements of the plant's safety systems to prevent the occurrence of specified unacceptable results during a postulated event. To achieve this proper plant design, a consistent systems engineering analysis must be developed. The Safety Function and Protection Sequence Analysis, the development of which is described in the following paragraphs, is an example of this required systems engineering analysis.

Event Classification and the Unacceptable Results

The first task in the analysis is to categorize the postulated events and to select the unacceptable results for each event category. The postulated events are grouped into event categories based upon some common event initiating characteristic, such as expected frequency of occurrence or the event initiating mechanism (e.g., pipe breaks). Event categories are not based upon event consequences because such categorization would involve circular reasoning. The event consequences are dependent upon the plant safety systems for which the design requirements are sought. Consideration is given to the various event classifications set forth in such regulatory and industry literature as 10CFR50 and its appendices and ANSI N18.2. Table I lists the event categories used in the Boston Edison Pilgrim 2 SFPSA and compares them to the event classifications used in other industry publications. Expected frequency of occurrence was used as the basic event classification characteristic.

After classifying the events into categories, the specific unacceptable results applicable to each category are defined. To define the unacceptable results the specific design limits associated with the proposed nuclear plant are identified. For the Boston Edison Pilgrim 2 analysis these limits were selected from the design criteria for the plant and included consideration of the AEC's Federal Regulation, Safety and Regulatory Guides, Interim Acceptance Criteria and Interim Policy Statement on Emergency Core Cooling; and the ASME codes and IEEE standards. Because the unacceptable results must be specific and measurable to be useful in the SFPSA, certain key plant variables or parameters are associated with the specific design limits of the plant, and thus with the unacceptable results. Examples of these plant parameters are fuel centerline temperature, site boundary dose, and containment structure stress. The unacceptable results are developed from the design limits using these key plant variables. Table II lists the unacceptable results used in the Pilgrim 2 analysis.

Safety Functions

Having defined the unacceptable results for each event category, the plant safety functions must be identified and developed. These safety functions are the functional means whereby the important plant variables are controlled or limited following a postulated event to avoid the unacceptable results. The development of the safety function is one of the major steps in the SFPSA. As a safety function is developed, the initial functional design requirements of the nuclear plant systems are established. For example, the safety function "Trip Reactivity Control" establishes the functional requirement for the rapid insertion of negative reactivity into the reactor core to prevent a certain plant parameter, DNBR, from exceeding its design limit.

The development of the safety functions is complete when it establishes all the functional design requirements essential to avoid the unacceptable results for all the event categories. To assist in developing all the required safety functions, a matrix is used to relate the safety functions to the unacceptable results. This enables the plant analyst to gain a functional overview of the safety functions and their effects. Table III lists the safety functions identified for the Pilgrim 2 unit. Table IV is the matrix showing the correspondence between the safety functions and the unacceptable results for the Pilgrim 2 SFPSA.

TABLE II

UNACCEPTABLE RESULTS FOR PILGRIM 2 SFPSA

EXPECTED OPERATIONAL OCCURRENCES

A. Radioactive Material Release

1. Radioactive material release to the environment exceeding the limits of 10CFR50, proposed Appendix I.

B. Fuel Limits

1. DNBR < 1.3 (W-3 correlation)
2. Fuel centerline temperature ≥ UO_2 melting temperature

C. Reactivity Limits

1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.
2. Inability to achieve and maintain a shutdown margin following the event.

D. Primary System Stress

1. Primary system stress in excess of that for which the primary system is designed, as determined by the following:
   a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST.
   b. Primary system pressure > allowable when reactor coolant system temperature < LST.
   c. Primary system thermal transients in excess of those considered in the primary system design.

E. Secondary System Stress

1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following:
   a. Secondary system pressure > 1320 psia.
   b. Secondary system thermal transients in excess of those considered in the secondary system design.

F. Plant Environmental Conditions

1. Uninhabitability of the control room and other plant locations where manual actions are essential.

INFREQUENT OPERATIONAL OCCURRENCES

A. Radioactive Material Release

1. Radioactive material release to the environment exceeding the limits of 10CFR20.

B. Fuel Limits

1. DNBR < 1.3 (W-3 correlation)

2. Fuel centerline temperature ≥ UO_2 melting temperature

C. Reactivity Limits

1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.

2. Inability to achieve and maintain a shutdown margin following the event.

D. Primary System Stress

1. Primary system stress in excess of that for which the primary system is designed, as determined by the following:

   a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST.

   b. Primary system pressure > allowable when reactor coolant system temperature < LST.

   c. Primary system thermal transients in excess of those considered in the primary system design.

E. Secondary System Stress

1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following:

   a. Secondary system pressure > 1320 psia.

   b. Secondary system thermal transients in excess of those considered in the secondary system design.

F. Plant Environmental Conditions

1. Uninhabitability of the control room and other plant locations where manual actions are essential.

ACCIDENTS

A. Radioactive Material Release

1. Radioactive material release to the environment that would result in exceeding the guideline values of 10CFR100.

B. Fuel Limits

1. Fuel centerline temperature ≥ UO_2 melting temperature.
2. Peak fuel cladding temperature in excess of 2200° F.
3. Oxidation of fuel cladding at any location in excess of 17%.
4. Metal-water reaction generating more H_2 than 1% of the H_2 that would be generated if all cladding reacted.

C. Reactivity Limits

1. Inability to achieve a shutdown margin at no load reactor coolant temperature immediately following automatic reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.
2. Inability to achieve and maintain a shutdown margin following the event.

D. Primary System Stress

1. Primary system stress in excess of that for which the primary system is designed, as determined by the following:
   a. Primary system pressure > 2750 psia when reactor coolant system temperature is ≥ LST.
   b. Primary system pressure > allowable when reactor coolant system temperature < LST.
   c. Primary system thermal transients in excess of those considered in the primary system design.

E. Secondary System Stress

1. Secondary system stress in excess of that for which the secondary system is designed, as determined by the following:
   a. Secondary system pressure > 1320 psia.
   b. Secondary system thermal transients in excess of those considered in the secondary system design.

F. Containment Stress

1. When containment is required, containment stress in excess of that for which the containment is designed, as determined by the following:
   a. Containment pressure > 60 psig.
   b. Thermal transients affecting either containment concrete or liner plate in excess of those considered in the containment design.
   c. Existence of a flammable or explosive mixture of hydrogen and oxygen (i.e. > 4% H_2 with ≥ 5% O_2 or > 5% O_2 with ≥ 4% H_2) in areas of the plant where safety systems are located wh[illegible] are required in response to the origin[illegible] accident.

G. Plant Environmental Conditions

1. Exposure of station personnel in the control room in excess of 5 Rem whole body, 15 Rem skin, and 30 Rem thyroid over the duration of the accident.
2. Uninhabitability of the control room and other plant locations where manual actions are essential.

TABLE III

SAFETY FUNCTIONS FOR PILGRIM SFPSA

Safety Function *	Functional Description
Trip Reactivity Control	Rapid insertion of negative reactivity into the core to produce subcritically immediately following an evaluated event.
Transient Reactivity Control	Insertion of negative reactivity into the core sufficient to compensate for cooldown of the reactor coolant system.
Long Term Reactivity Control	Establishment of a sufficient boron concentration in the core such that the reactor is maintained subcritical following the event.
Emergency Core Cooling - Injection Phase	Provision of coolant to the reactor core immediately following an accident and prior to the time that manual action can be taken.
Emergency Core Cooling-Recirculation Phase	Provision of coolant to the reactor core some time after the accident has occurred and at a time when manual action can be taken and in such a way that the core coolant is recirculated back into the primary system after it leaks out.
Reactor Heat Removal	Cooling of the core by other than injection of coolant directly to the core.
Pressure Control - Primary System	Maintenance of primary system pressure within allowable pressure limits and ensuring that the primary steam bubble remains in the pressurizer.
Pressure Control - Secondary System	Maintenance of secondary system pressure within allowable pressure limits.
Pressure Control - Containment	Maintenance of containment pressure within allowable pressure limits when containment is required.
Temperature Control - Containment	Maintenance of containment temperature within allowable temperature limits when containment is required.

* Where appropriate, safety function descriptions are modified with such phrases as "initial", "long term", "above LST", etc.

Safety Function *	Functional Description
Combustible Gas Control	Conditioning of post-accident atmosphere or treatment of accident-generated flammables to prevent formation of flammable or explosive mixtures.
Radioactive Material Treatment	Mechanical or chemical treatment of radioactive materials to reduce the quantity that escape or are discharged to the environs.
Establish Containment	Trapping of radioactivity inside the containment to prevent escape to the environs.
Primary System Isolation	Isolation of all or part of the primary system to prevent coolant loss or radioactivity discharge.
Secondary System Isolation (blowdown)	Isolation of all or part of the secondary system to prevent or reduce the discharge of secondary system coolant into the containment, so that containment temperature and pressure are maintained within allowable limits.
Secondary System Isolation (heat sink)	Isolation of all or part of the secondary system to prevent or reduce the discharge of secondary coolant, so that at least one steam generator can function as a heat sink for primary system energy.
Secondary System Isolation (radioactivity)	Isolation of all or part of the secondary system to prevent the discharge of radioactive materials to the environs.
Steam Generator Inventory Control	Maintenance of a proper level in at least one steam generator for use as a primary system heat sink and prevention from injecting cold feedwater into a dry and hot steam generator.
Control Station Habitability	Conditioning of the post-event control station (Control room and other locations where manual actions are essential) atmosphere to ensure habitability and control of personnel radiation exposure.

TABLE IV

SAFETY FUNCTIONS AND UNACCEPTABLE RESULTS MATRIX FOR PILGRIM 2 SFPSA

Safety Functions	Fuel Limits	Reactivity Limits	Primary System Stress	Secondary System Stress	Containment Stress
Trip Reactivity Control	Acc: B. 1 EOO: B. 1-2 IOO: B. 1-2	Acc: C. 1 EOO: C. 1 IOO: C. 1	Acc: D. 1. a EOO: D. 1. a IOO: D. 1. a		
Transient Reactivity Control		Acc: C. 2 EOO: C. 2 IOO: C. 2			
Long Term Reactivity Control		Acc: C. 2 EOO: C. 2 IOO: C. 2			
Emergency Core Cooling - Injection Phase	Acc: B. 1-4				
Emergency Core Cooling - Recirculation Phase	Acc: B. 1-4				
Reactor Heat Removal	Acc: B. 1, 2 EOO: B. 2 IOO: B. 2				
Pressure Control - Primary System			Acc: D. 1. a, b EOO: D. 1. a, b IOO: D. 1. a, b		
Pressure Control - Secondary System				Acc: E. 1. a EOO: E. 1. a IOO: E. 1. a	
Pressure Control - Containment					Acc: F. 1. a

Alphanumeric references refer to unacceptable results as listed on Table II

SAFETY FUNCTION	Radiological Release	Fuel Limits	Primary System Stress	Secondary System Stress	Containment Stress	Environmental Conditions
Temperature Control - Containment					Acc: F. 1. b	
Combustible Gas Control					Acc: F. 1. c	
Radioactive Material Treatment	Acc: A. 1 EOO: A. 1 IOO: A. 1					
Establish Containment	Acc: A. 1					
Primary System Isolation	Acc: A. 1					
Secondary System Isolation (blowdown)					Acc: F. 1. a, b	
Secondary System Isolation (heat sink)		Acc: B. 1-4 EOO: B. 1-2 IOO: B. 1-2				
Secondary System Isolation (Radioactivity)	Acc: A. 1					
Control Station Habitability						Acc: G. 1-2 EOO: F. 1 IOO: F. 1
Steam Generator Inventory Control		Acc: B. 1-4 EOO: B. 1-2 IOO: B. 1-2	Acc: D. 1. a, b, c EOO: D. 1. a, b, c IOO: D. 1. a, b, c	Acc: E. 1. a, b EOO: E. 1. a, b IOO: E. 1. a, b		

Legend: Acc = Accident
EOO = Expected Operational Occurrences
IOO = Infrequent Operational Occurrences

Operating States

Because each postulated event must be evaluated over the full range of normal plant conditions in which the event is possible, it is convenient to identify and define various plant operating states. The analyst can then more easily evaluate each event over the range of plant conditions within each operating state. The operating states to be used for the analysis of a specific plant are dependent upon the plant design. Table V defines the operating states used for the Pilgrim 2 unit, a two-loop pressurized water reactor.

TABLE V

PLANT OPERATING STATES FOR PILGRIM 2

Operating State	Reactivity Control Status	Primary System Status	Reactor Power
A - Refueling	All CEA's may be withdrawn *	O psig T < 210° F	Nil
B - Cold Shutdown	< 1 shutdown group withdrawn; all others inserted ****	O psig T < 210° F	Nil
C - Shutdown Cooling	< 1 shutdown group withdrawn; all others inserted ****	210° F < T < 350° F pressure per allowable ***	Nil
D - Heatup/Cooldown	< 1 shutdown group withdrawn; all others inserted ****	350° F < T < 556° F pressure per allowable ***	Nil
E - Hot Shutdown	< 1 shutdown group withdrawn; all others inserted **	2250 psia 556° F	Nil
F - Hot Standby	Any allowable CEA positions **	Temp/pressure per allowable	< 15%
G - Power	Any allowable CEA positions **	Temp/pressure per allowable	15 - 100%

* Reactor boron concentration such that reactor would have at least a 5% shutdown margin with all CEA's fully withdrawn.

** Reactor boron concentration such that reactor would have at least a 2% shutdown margin at no load reactor coolant temperature following reactor trip with the most reactive CEA fully withdrawn and all other CEA's fully inserted.

*** Pressure-temperature limits applicable during heatup and cooldown of reactor coolant system.

**** Reactor boron concentration such that reactor would have at least a 2% shutdown margin with all CEA's fully inserted.

Event Analysis

With the placement of each postulated event in its category, and with the unacceptable results and safety functions identified for event category, the analysis of each specific event can be performed.

The analysis of an event begins with the complete definition of the event. This includes the identification of the event (e.g., steamline break inside containment), the range of plant process variables which apply to the event (e.g., 350°F to 580°F for average reactor coolant temperature), and the listing of the applicable plant operating states (e.g., power operation, hot shutdown). After the event is completely defined, the analyst selects a specific set of initial plant process parameters (e.g., 100% power, rated temperature) to begin the event analysis. With this set of initial parameters, each unacceptable result associated with the event's category is examined to determine which unacceptable results could or could not occur as a result of the event. For example, the analyst determines that the unacceptable result concerning the existence of a flammable or explosive mixture of hydrogen and oxygen could not occur for a steamline break accident occurring outside containment.

Having determined which unacceptable results could occur for the event, a matrix such as that shown in Table IV is used to determine the safety functions associated with the specific set of initial parameters. To achieve these safety functions the specific plant safety systems and their required responses, or safety actions, are identified. A safety system is a system, active or passive, which must furnish the safety action as a result of a postulated plant event.

After identification of the required safety systems and their safety actions, the sensed variables are identified that cause or require the special system responses. In cases where the system does not automatically respond, the operator action required to initiate the safety system (e.g., starting the pump locally from the control room) is identified. As the safety systems and their actions are identified, they are arranged in functional order forming success paths, or protection sequences, leading to the required safety function. The arrangement of success paths becomes the Safety Sequence Diagram for the event. The Safety Sequence Diagram (SSD) becomes the analyst's major output in the SFPSA. Figure 1 is the format of the SSD's developed for the Boston Edison Pilgrim 2 analysis.

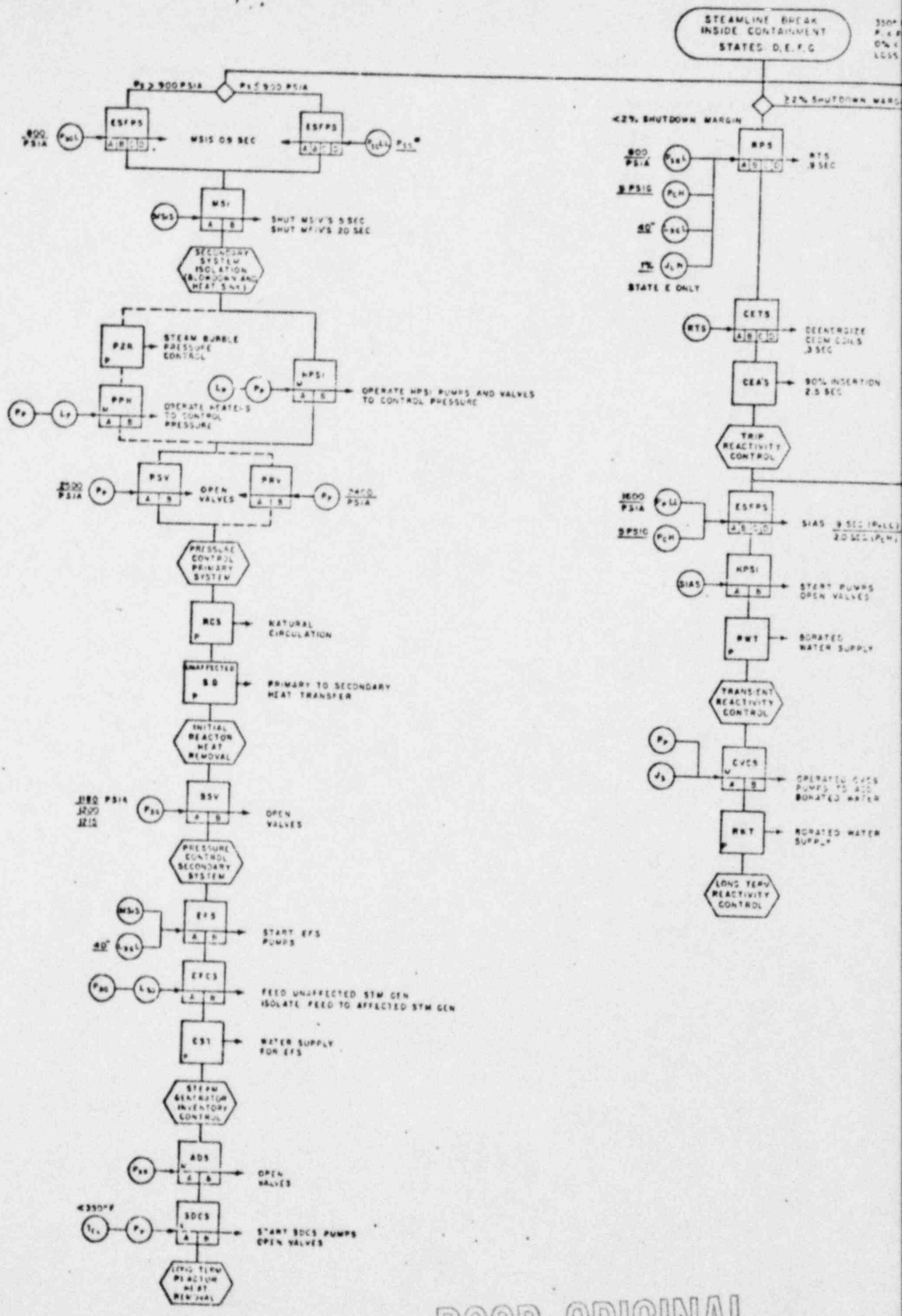
To depict the level of redundancy in the plant design on the SSD, a sufficient number of independent parallel paths is developed for each safety function such that no single component failure can prevent the achievement of the required safety function. Because many of the Pilgrim 2 systems (e.g., engineered safety features) have been designed with functional redundancy, certain safety functions require only one success path, i.e., no single active component failure can prevent the safety systems in the success path from achieving their special responses. If the analysis reveals a safety function for which functional redundancy does not exist, either with a parallel independent success path or safety system redundancy, then the plant design, configuration or functional response must be changed to achieve this redundancy.

The analysis of the postulated event is continued for its entire duration including post-event activities until some planned operation is resumed or the plant achieves a stable condition. A planned operation is considered resumed when the actions taken are identical to those described by normal operating procedures.

After the success paths and safety functions required for the initial set of plant conditions have been identified and illustrated on the Safety Sequence Diagram, the analyst will vary each plant process parameter from its initial condition value throughout its entire range for the event. During this parameter variation process, the analyst ensures that all required safety functions have been identified. If any additional required safety functions are identified, their required success paths must be determined in the same manner as done for the initial set of plant conditions. Additionally, as the parameters are varied, the analyst also determines which of the "initial condition" safety functions are still required. Each of these required safety functions is reviewed to ensure that the safety systems in the success path will provide their required safety actions under the different plant conditions. During this process, if any new success paths are discovered, they are diagrammed on the Safety Sequence Diagram with appropriate notation as to the specific conditions under which they are required. Also, where the event mechanism itself is variable (e.g., size and location of a pipe break), the variable characteristic is considered over its full range to assure that all success paths are identified.

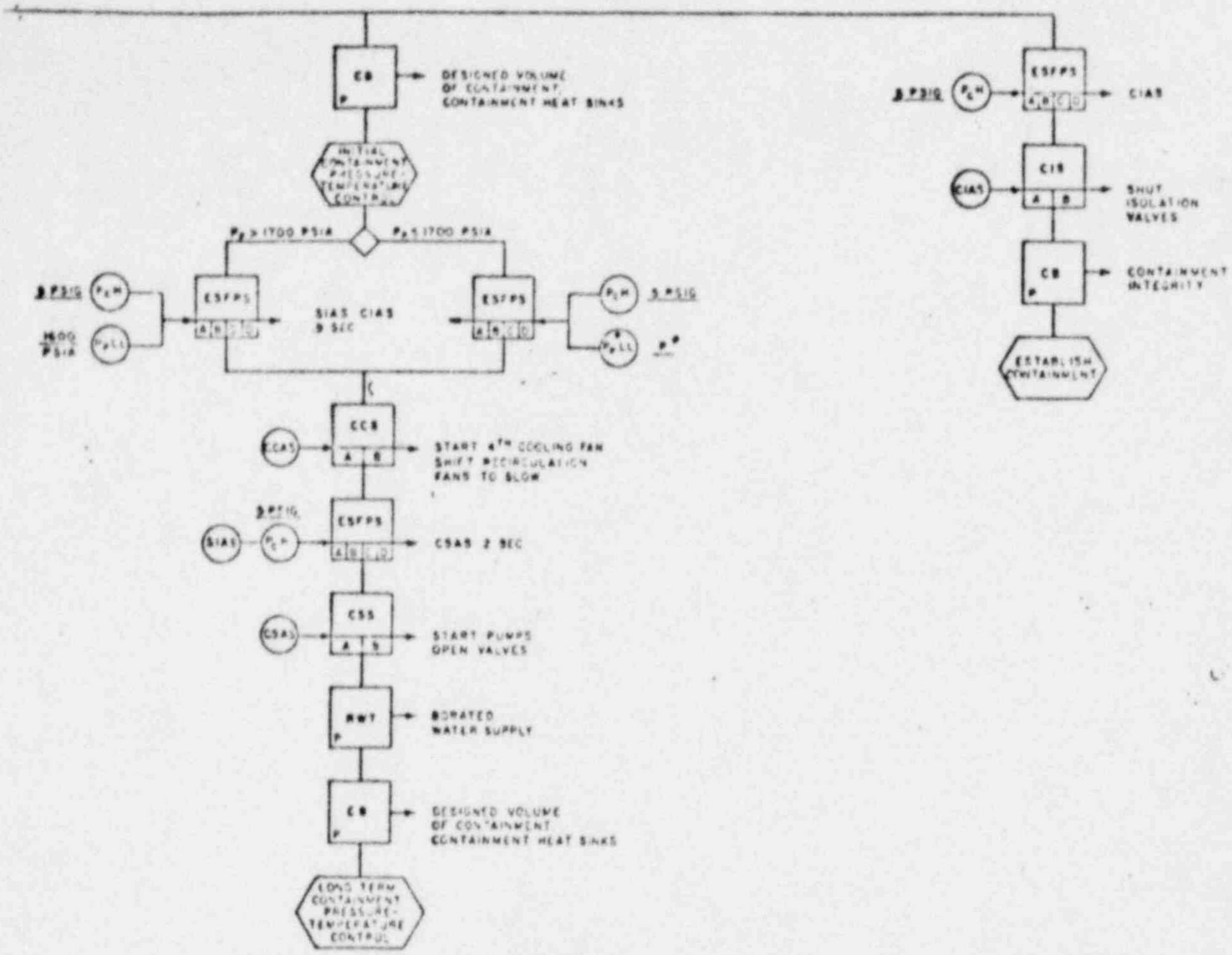
This parameter variation analysis for each safety sequence enables the analyst to identify the limiting set of parameters for each success path and each safety system. This type of systematic analysis is used to demonstrate the plant's ability to safely respond to any postulated event. The historical concept of the "worst case" is an unusable concept for a systems analysis of a nuclear power plant. Considering the number of systems and components which must function during an accident, no single set of initial conditions can possibly describe the most limiting set for all systems. Rather than any one "worst case" condition, there exists a spectrum of "worst cases" which must be analyzed on a systems basis to properly design a nuclear power station.

◄Figure 1 overleaf



STEAMLINE BREAK INSIDE CONTAINMENT
STATES D, E, F, G
ESFPS
MSIS 0.9 SEC
800 PSIA
MSI
SHUT MSIV'S 5.5 SEC
SHUT MFIV'S 20 SEC
SECONDARY SYSTEM ISOLATION (BLOWDOWN AND HEAT SINK)
PZR
STEAM BUBBLE PRESSURE CONTROL
PPH
OPERATE HEATERS TO CONTROL PRESSURE
HPSI
OPERATE HPSI PUMPS AND VALVES TO CONTROL PRESSURE
PSV
PRV
OPEN VALVES
2500 PSIA
PSIA
PRESSURE CONTROL PRIMARY SYSTEM
RCS
NATURAL CIRCULATION
UNAFFECTED SG
PRIMARY TO SECONDARY HEAT TRANSFER
INITIAL REACTOR HEAT REMOVAL
SSV
1180 PSIA
OPEN VALVES
PRESSURE CONTROL SECONDARY SYSTEM
EFS
START EFS PUMPS
40"
EFCS
FEED UNAFFECTED STM GEN
ISOLATE FEED TO AFFECTED STM GEN
CST
WATER SUPPLY FOR EFS
STEAM GENERATOR INVENTORY CONTROL
ADS
OPEN VALVES
SDCS
START SDCS PUMPS
OPEN VALVES
LONG TERM REACTOR HEAT REMOVAL
<2% SHUTDOWN MARGIN
RPS
RTS .9 SEC
STATE E ONLY
CETS
DEENERGIZE CEDM COILS .3 SEC
CEA'S
90% INSERTION 2.5 SEC
TRIP REACTIVITY CONTROL
1600 PSIA
ESFPS
SIAS
HPSI
START PUMPS OPEN VALVES
RWT
BORATED WATER SUPPLY
TRANSIENT REACTIVITY CONTROL
CVCS
OPERATE CVCS PUMPS TO ADD BORATED WATER
RWT
BORATED WATER SUPPLY
LONG TERM REACTIVITY CONTROL

EVENT CLASSIFICATION
ACCIDENT



NOTE:
REFER TO TABLE III FOR DEFINITION OF ABBREVIATIONS

STEAM LINE BREAK INSIDE CONTAINMENT
SAFETY SEQUENCE DIAGRAM

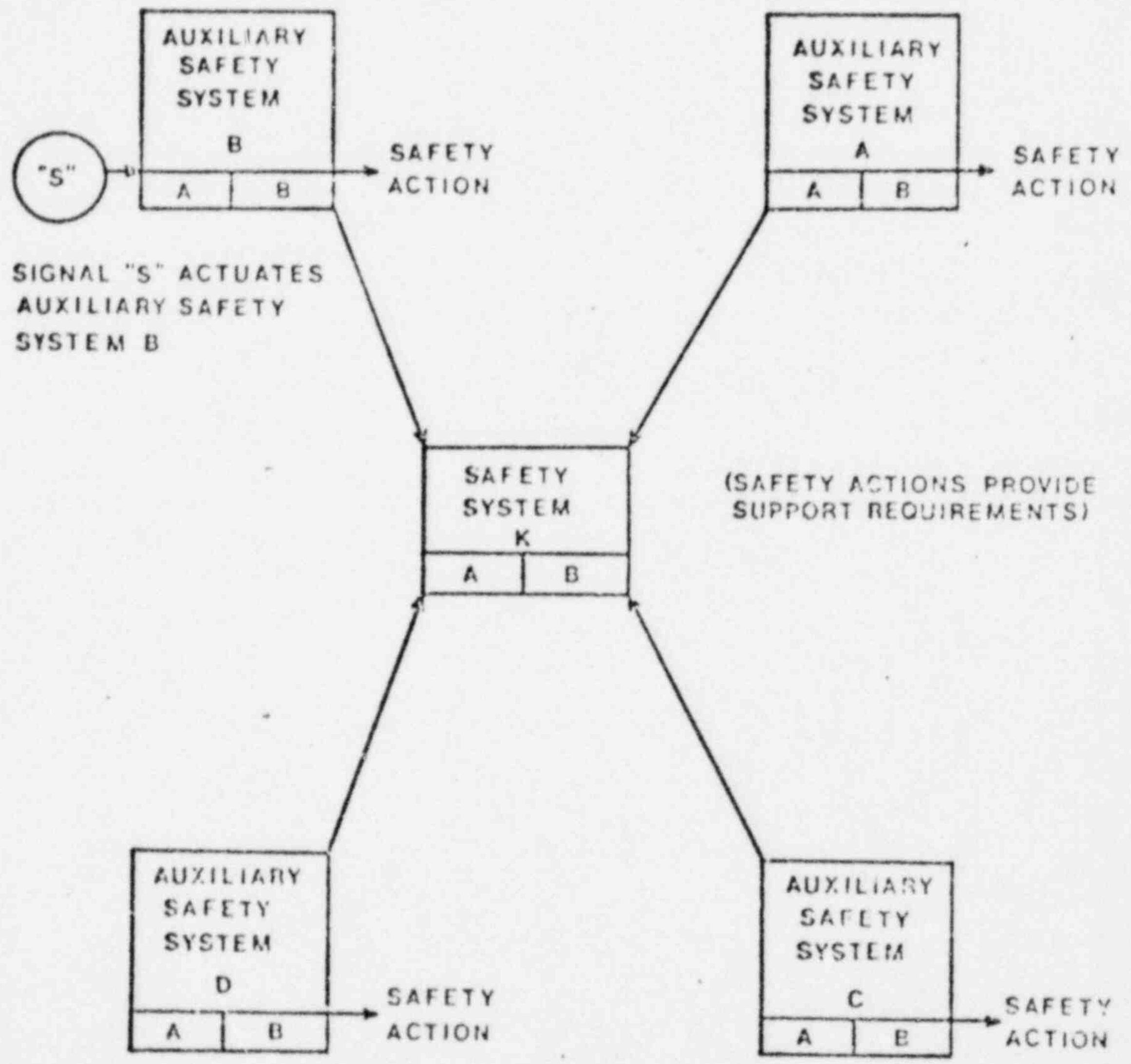
Figure 2

Safety Sequence Diagram

When all the plant process parameter variations have been considered, the Safety Sequence Diagram (SSD) for the particular event is completed. The SSD displays those prime, or major, plant safety systems whose responses are essential to providing the safety actions required for the postulated event. The SSD shows these safety systems in their functional (not necessarily chronological) sequences following the postulated event. In addition, the SSD shows which plant process variables are monitored or sensed by these safety systems as initiating signals. Figure 2 is an example of the Safety Diagram for the accident "Steamline Break Inside Containment", as developed for the Pilgrim 2 unit.

Safety System Auxiliary Diagram

After completion of the SSD for a postulated event, each safety system displayed on the SSD is analyzed to determine the specific support requirements necessary to produce its safety action. Examples of these support requirements are electric power, component cooling, or instrument air supply. The analyst refers to the SSD to determine every sequence in which a safety system is required, thereby ensuring all support requirements are identified. After identification of the support requirements, the plant systems that provide these support requirements are identified. These systems are the Auxiliary Safety Systems. A Safety System Auxiliary Diagram is then prepared on which the prime safety system and its auxiliary safety systems are displayed. Figure 3 is the format for a Safety System Auxiliary Diagram as used in the Boston Edison Pilgrim 2 analysis.

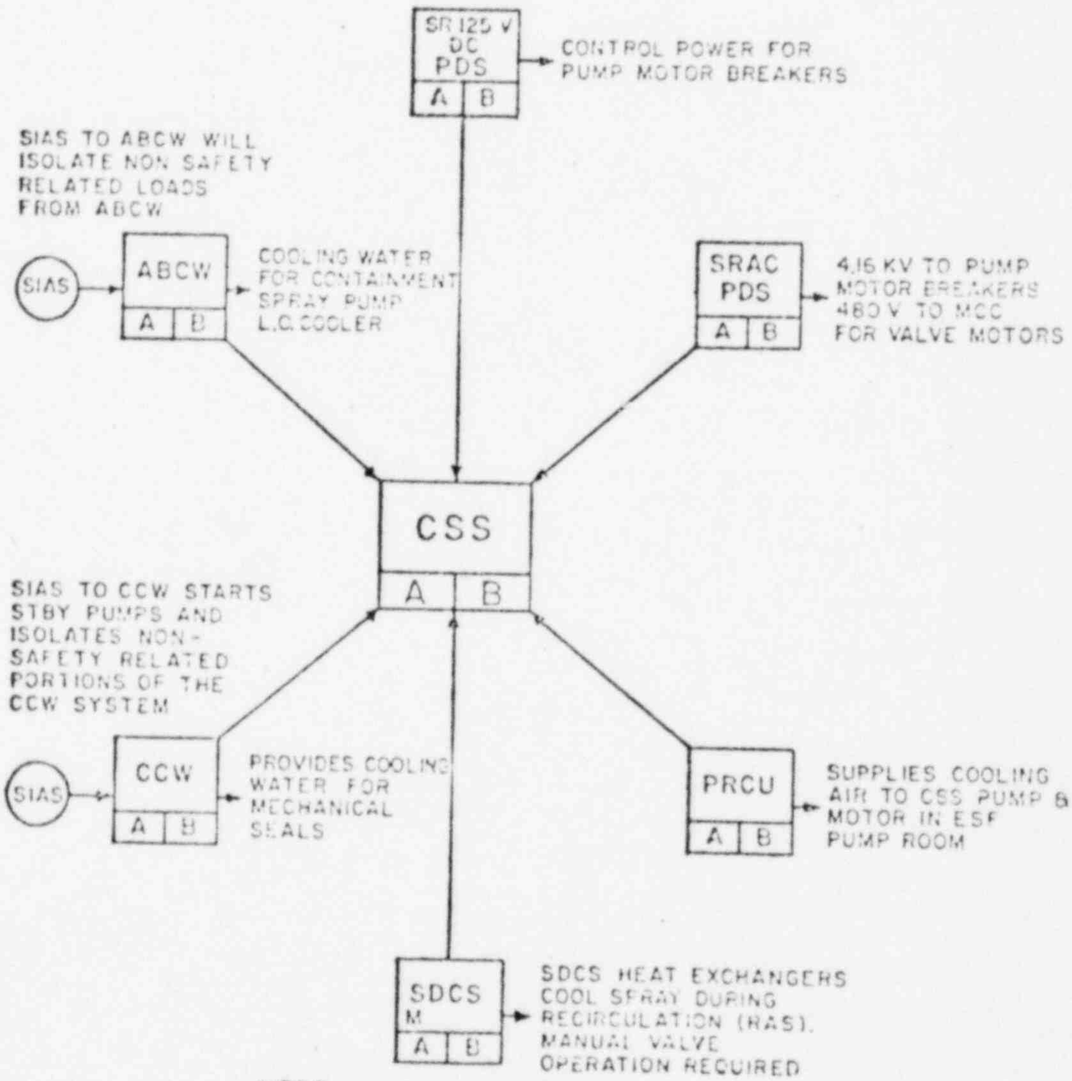


SAFETY SYSTEM AUXILIARY DIAGRAM FORMAT

FIGURE 3

In developing the Safety System Auxiliary Diagram the analyst ensures that each support requirement is functionally redundant by developing design information about the plant sufficient to positively identify the auxiliaries essential to the required response of the safety system, and by identifying plant design changes so that the auxiliary systems can support their safety system with the needed level of redundancy.

To complete any Safety System Auxiliary Diagram the analyst must review the Safety Sequence Diagrams for all the postulated events to identify all safety sequences in which the subject safety system appears. Figure 4 is the Safety System Auxiliary Diagram for the Containment Spray System of the Boston Edison Pilgrim 2 nuclear unit.



NOTE:

REFER TO TABLE VI FOR DEFINITION OF ABBREVIATIONS

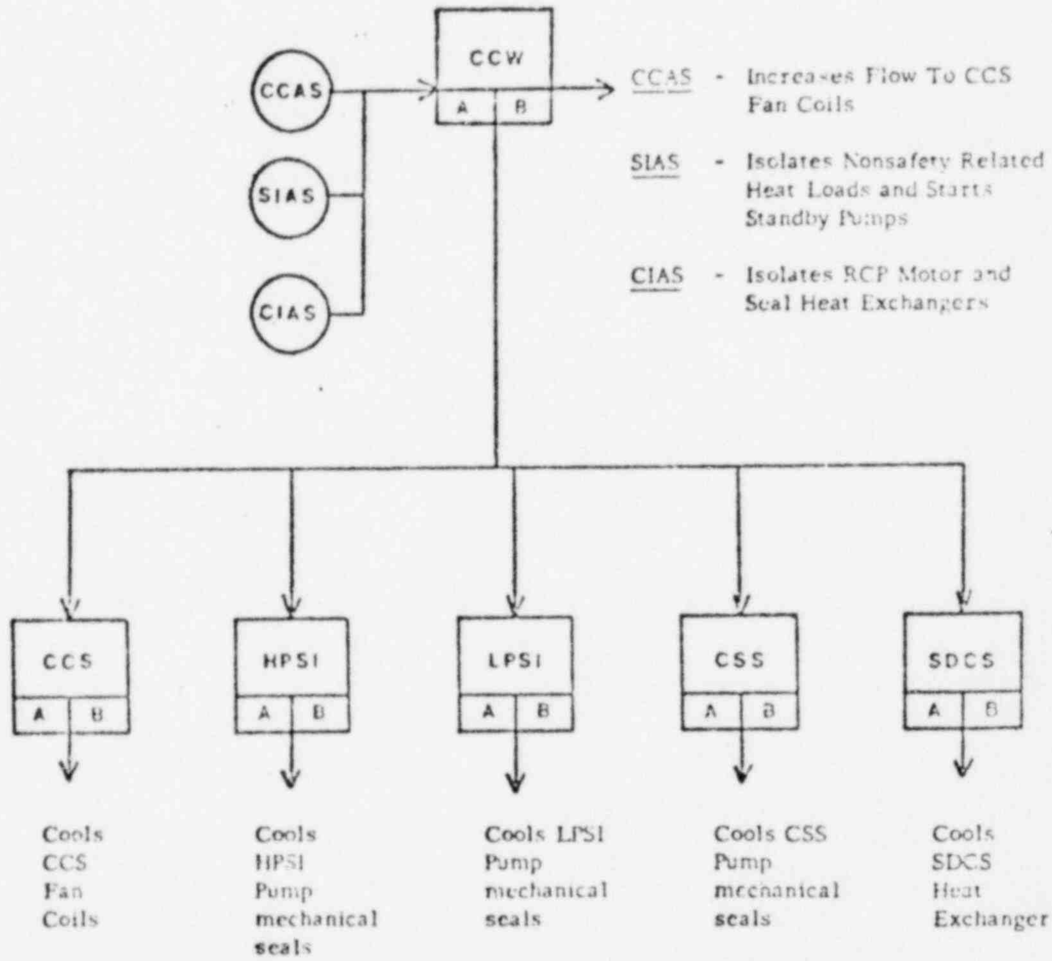
CONTAINMENT SPRAY SYSTEM

SAFETY SYSTEM AUXILIARY DIAGRAM

FIGURE 4

Auxiliary Safety System Commonality Diagram

After completion of the Safety Sequence Diagrams for each postulated event and the Safety System Auxiliary Diagrams, the Auxiliary Safety System Commonality Diagram (ASSCD) for each Auxiliary Safety System is developed. This diagram indicates all the safety systems that a given Auxiliary Safety System supports. ASSCD is developed mainly as an information diagram, rather than a primary design review diagram. ASSCD allows evaluation of the overall plant response to the operations of each Auxiliary Safety System, considering such effects as that of a single active failure to the component cooling water system. Figure 5 is the ASSCD for the Component Cooling Water System of the Pilgrim 2 station.



NOTE:

REFER TO TABLE VI FOR DEFINITION OF ABBREVIATIONS

COMPONENT COOLING WATER SYSTEM
AUXILIARY SAFETY SYSTEM COMMONALITY DIAGRAM
FIGURE 5

POOR ORIGINAL

TABLE VI

ABBREVIATIONS USED ON SFPSA DIAGRAMS

ABCW	Auxiliary Building Cooling Water
ADS	Atmospheric Steam Dump System
CB	Containment Structure
CCAS	Containment Cooling Actuation Signal
CSS	Containment Cooling System
CCW	Component Cooling Water
CEA	Control Element Assemblies
CETS	Control Element Trip System
CIAS	Containment Isolation Actuation Signal
CIS	Containment Isolation System
CSAS	Containment Spray Actuation Signal
CSS	Containment Spray System
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
EFCS	Emergency Feed Control System
EFS	Emergency Feed System
ESFPS	Engineered Safety Features Protection System
HPSI	High Pressure Safety Injection
LPSI	Low Pressure Safety Injection
MFIV	Main Feed Isolation Valves
MSI	Main Steam Isolation System
MSIS	Main Steam Isolation Signal
MSIV	Main System Isolation Valves
PPH	Pressurizer Proportional Heaters
PRCU	Pump Room Cooling Unit
PRV	Power Relief Valves
PSV	Primary Safety Valves
PZR	Pressurizer
RCS	Reactor Coolant System
RPS	Reactor Protection System
RTS	Reactor Trip System
RWT	Refueling Water Tank
SDCS	Shutdown Cooling System
SG	Steam Generator
SIAS	Safety Injection Actuation Signal
SRPDS	Safety Related Power Distribution System
SSV	Secondary Safety Valves
$J_L H$	High Logrithmic Power
J_S	Startup Neutron Flux Level
L_P	Pressurizer Level
L_{SG}	Steam Generator Level
$L_{SG}L$	Low Steam Generator Level
$P_C H$	High Containment Pressure
P_P	Pressurizer Pressure
$P_P L$	Low Pressurizer Pressure
$P_P LL$	Low-Low Pressurizer Pressure
P_S	Steam Pressure
$P_{SG}L$	Low Steam Generator Pressure
$P_{SG}LL$	Low-Low Steam Generator Pressure
T_{CL}	Cold Leg Temperature

The Role of SFPSA in the Design Process

Under the requirements of 10CFR50, systems, structures and components important to nuclear plant safety must be identified and designed to ensure that they will perform reliably in service. This requirement is satisfied by subjecting all such safety related items to a quality assurance program conforming to the requirements of 10CFR50, Appendix B. The systematic process employed by the SFPSA, as shown on the resulting SSD's and SSAD's, makes it possible to easily identify and classify the various systems, structures, and components of the plant in relation to safety. In particular, the SSD's and SSAD's become a key tool or mechanism to satisfy the design verification requirements of a nuclear quality assurance program under Criterion III (Design Control) of 10CFR50, Appendix B. The following paragraphs describe how the SFPSA results are used in the design process.

The Quality Assured Items List

Each system, component, and structure required to mitigate the consequences of a nuclear plant accident must be subjected to the Nuclear Quality Assurance Program and must be listed on the Quality Assured Items List. Upon completion of the required Safety Sequence Diagrams (SSD's) and Safety System Auxiliary Diagrams (SSAD's), the process of identifying these quality assured items and placing them on the Quality Assured Items List is simple and systematic. Each accident SSD and the associated SSAD's is reviewed. Because the prime safety systems and their supporting auxiliary systems required to achieve the safety functions are diagramed on the SSD's and SSAD's, the task of quality assured system identification is complete. To identify the specific components and structures within the plant systems and larger structures that must be quality assured, each safety system and auxiliary safety system is examined to determine the specific components of these systems that must function to produce the required system responses. The structures in which the systems and components are located, including passive structures shown on the SSD (e.g., the containment, or the refueling water tank), are identified as structures to be quality assured.

The significant amount of analytical effort expended to perform the SFPSA has made the development of the sometimes controversial Quality Assured Items List easy and systematic.

Seismic Design Review

The SFPSA facilitates the identification of the systems, components and structures that must be classified Seismic Category I under the requirements of AEC Regulatory Guide 1.29. In a manner similar to the identification of quality assured items, the accident SSD's are reviewed, and sufficient systems, components and structures are classified Seismic Category I to provide at least one success path for each required safety function. The SSAD for each safety system in the success path is reviewed to identify those auxiliary systems required to support the Category I safety systems. Such auxiliary safety systems are also classified Seismic Category I.

To identify the specific components and structures to be Seismic Category I, each prime safety system and auxiliary safety system is studied in detail, as done in the Quality Assured Items List study. The specific components and structures which must function to produce the safety actions of these systems are classified as Seismic Category I.

Redundancy and Separation

During the development of the SSD's and SSAD's, success paths are determined for each safety function. Each success path represents a sequence that is capable of achieving its safety function given any single active component failure. This capability is shown with either physical redundancy (e.g., two independent trains of the Safety Injection System) or functional redundancy (e.g., either the High Pressure Safety Injection System or the Chemical & Volume Control System supplying borated water). Thus, with the SSD's and SSAD's finished, the complete systems level redundancy of the plant is shown diagramatically.

During the review of the safety system design of the plant, the information on the SSD's and SSAD's is used to ensure that the designs do reflect the required redundancy shown on the diagrams. The design reviewer refers to the SSD's and SSAD's as he tests the designs for susceptibility to single failures. During review of physical arrangement drawings, the SSD's and SSAD's are used to check the adequacy of physical separation, thus ensuring that the plant is properly designed against the effects of pipe whip, jet impingement, flooding, fire, etc.

Effects of Pipe Breaks

Because an SSD has been developed for every pipe break that must be postulated in plant design considering the various plant systems and the various sizes of breaks, the specific systems and structures that must respond to each specific pipe break can be easily identified. During the analysis of a particular pipe break the information on the SSD's and SSAD's is used to identify the specific systems, components and structures that must be protected for that particular break. Pipe whip restraints and jet deflectors are located to protect those specific systems, components and structures, whereas damage to other plant equipment is acceptable. For example, if a particular two inch pipe break in the reactor coolant system does not require the use of the Chemical & Volume Control System (CVCS), there is no reason to protect the CVCS piping following that two inch reactor coolant system pipe break, and no pipe whip restraints or jet deflectors would be specified for this purpose. However, if the High Pressure Safety Injection System is required for this rupture, it will be protected from damage due to pipe whip and jet impingment. Thus, all the items which must be protected are systematically identified and protected, but the number of pipe restraints and deflectors is minimized.

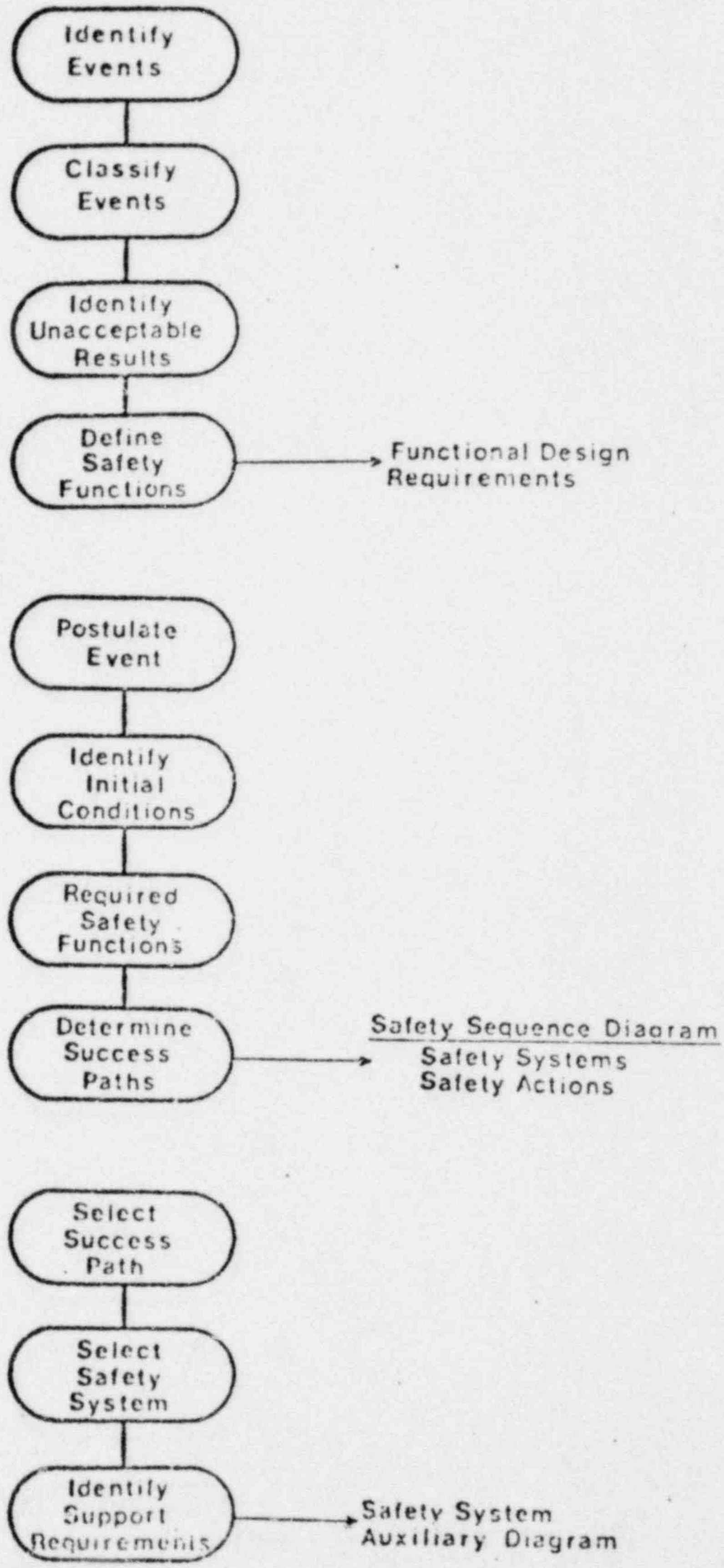
Summary

The systematic approach of the SFPSA provides assurance that each system, component or structure required for safety is identified and designed in accordance with all applicable requirements.

When the SFPSA is complete, each required safety function that must be achieved is clearly identified; the time sequence in which the necessary safety actions must occur is delineated; the degree of redundancy provided in plant design is established; and the need for station design to provide intelligence for operator manual control is defined. The SFPSA distinguishes between those plant systems that are required for the public health and safety and those that are required only for equipment protection. The SFPSA is the mechanism whereby each safety system receives a complete and consistent design review. The SFPSA helps to ensure that no one safety system has been "over designed" at the expense of another.

When performed early in the design process of a nuclear project, the SFPSA operates to greatly reduce, or even eliminate, design changes later in the project, when such changes would be much more costly. Because the SFPSA is a continuing analysis throughout the design phase of the project, it becomes the most useful and meaningful comprehensive representation of the plant safety system design, illustrating on easily understood diagrams the practical results of large volumes of engineering drawings, specifications, and design information.

SAFETY FUNCTION AND PROTECTION SEQUENCE ANALYSIS



Question F.20

Your reply notes that an in-depth reliability assessment is being performed on the Midland AFW systems:

a. Studies performed by several operating nuclear plants have concluded that a significant improvement in reliability and plant availability results from addition of a second motor-operated auxiliary feedwater pump. We require that the benefits from such an addition be included as part of the results of your reliability assessment of the Midland AFW system.

b. Other than the auxiliary feedwater system, what Midland systems and changes will be the subjects of your reliability assessments? State your planned completion date for these analyses.

Response

a. The Midland auxiliary feedwater (AFW) system reliability analysis, currently being performed by Pickard, Lowe and Garrick, Inc., will include a comparison of the reliability of the Midland two 100% pump system to the typical one 100% plus two 50% pump system found at other plants. Preliminary results from Pickard, Lowe and Garrick indicate that the predicted availability of Midland's two 100% pump system is higher than that of the typical three-pump system because both motor-driven 50% pumps must operate following a failure of the 100% turbine-driven pump in order to provide sufficient water to the steam generators to assure system success (decay heat removal).

   The results of this analysis combined with the capability to power the turbine driven main feedwater pumps from the auxiliary boiler, if necessary, will demonstrate that a third AFW pump is not required for Midland Units 1 and 2.

b. Formal, in-depth reliability assessments are planned for no other Midland systems at this time.

Question F.21

On what basis did you determine that pressurizer heater banks 5 and 6 alone will provide sufficient heating capacity if only these banks are uprated to safety grade? Identify the limiting transient or accident which established the required heating capacity. What provisions for equipment failure are provided in this selection?

Response

The limiting transient which establishes the heater capacity is natural circulation of the reactor coolant system (RCS) with a loss of offsite power. The number of pressurizer heaters per bank was calculated by taking into account the following information:

a. The loss through the pressurizer insulation results in an approximate heat loss of 28 kW.

b. The loss through the uninsulated pressurizer areas around the horizontal heater bundles results in an approximate heat loss of 15 kW.

c. B&W experience shows that the heat losses in Items a and b above may account for approximately 40% of the total losses. Additional losses may occur through 1) conduction paths such as supports for the pressurizer, instrument lines, and loss-of-coolant accident and seismic restraints, 2) uninsulated surfaces such as relief valves and spray lines, and 3) chimney losses caused by airflow between insulation and heated surfaces. This may result in an additional heat loss of up to 64 kW.

Thus, the total estimated heat loss from the system is 107 kW. Due to the electrical arrangement of heater groups, the value of 126 kW was selected.

Redundant Class 1E heater banks of 126 kW allow for a failure of one bank of heaters without loss of system capability. The impact of a control or power failure has been mitigated through design as discussed in the FSAR in response to NRC Question 031.27. This response discussed the incorporation of redundant Class 1E pressurizer heater controls and power supplies as shown in FSAR Question/Response Figures 7.4-1 through 7.4-10.

Question F.22

You note that the existing pressurizer heater low level interlock design is being reviewed to determine its adequacy in the event of loss of liquid inventory in the pressurizer. Describe how energized pressurizer heaters fail when uncovered and provide justification that such failure would not threaten or cause failure of the reactor coolant pressure boundary.

Response

The pressurizer heaters use a concentric coil design: an inner coil and an outer coil insulated from each other and the sheath by compacted magnesium oxide (MgO). During normal operation, heat generated by the two energized resistors (inner and outer coils) is removed by reactor coolant (RC) surrounding the sheath of the heater. In the event that an energized heater should become uncovered, the heat removal medium would be saturated steam rather than RC and less heat transfer would occur. This, in turn, would cause the temperature of the inner coil to rise above its normal operating temperature to the point that the thermal capability of the inner resistance coil and the immediately surrounding MgO would be exceeded. This condition would be expected to occur within a few minutes (less than 10 minutes). This mode of failure, which is the expected mode of failure for the postulated condition, would result in an open circuit path along the length of the inner coil, thus rendering the heater inoperative.

RC pressure boundary areas which could be postulated to be adversely affected by the over-temperature operation of uncovered heaters followed by an insurge of RC are: heater sheath, sheath-to-diaphragm weld, diaphragm, and pressurizer shell/heater bundle forging. Analyses of the heater sheath, sheath-to-diaphragm weld, and diaphragm predict areas of high thermally-induced stresses. These one-time stresses do not predict failure in these areas but do result in increases in the calculated fatigue usage factors.

Due to the physical separation between the pressurizer shell and the actively heated length of the pressurizer heaters and due to the short predicted over-temperature on-time of the pressurizer heaters, no significant adverse effects to the pressurizer shell/heater bundle forging areas are expected.

Therefore, for the postulated operation of pressurizer heaters in a saturated steam environment, the failure mode would be an open circuit along the actively heated length of the inner coil. This abnormal, short duration heater operation and resulting failure of the internal resistance heating element would not compromise the integrity of the RC pressure boundary.

Question F.23

You state that a subcooling meter will be provided with redundant safety grade hot leg temperature and reactor coolant system pressure input. Clarify whether it is your intent to provide a subcooling meter which is itself safety grade. If not, justify your position. Specify the detection and indicating range and sensitivity for this meter and its inputs.

Response

As previously stated, Consumers Power Company is committed to providing a subcooling meter with redundant safety-grade hot leg temperature and reactor coolant system pressure input. However, the detailed design specifics of this instrumentation have not been finalized. Consistent with the NRC clarification letter of October 30, 1979, Short-Term Lessons Learned (NUREG 0578), and the recently issued proposed revision to Regulatory Guide 1.97, the subcooling meter will consist of either safety-grade calculational devices and display or a highly reliable single channel instrument which is environmentally qualified to the conditions of its intended operation and testable, with a backup procedure for use of steam tables. The intended range for this device is 200F subcooled to 35F superheated.

Question F.24

You state that the technical feasibility of providing a low flow indication as a means of confirming core cooling during natural circulation modes of cooldown is being assessed. What criteria are being used for this assessment? What power requirements for this instrumentation are intended?

Response

Consumers Power Company is reviewing the technical feasibility of providing a low flow indication as a means of confirming core cooling during natural circulation modes of cooldown. The criteria being used to assess methods of providing this indication include the following.

a. The instrumentation should be seismically and environmentally qualified Class 1E.

b. The instrument range should provide indication coverage from -12% to +12% design flow.

c. The low flow indication should be readily available following transfer from forced circulation to natural circulation operation (i.e., instrument calibration should remain unaffected by forced circulation operations or by the transfer to or from forced circulation to natural circulation).

If an instrument capable of meeting the above criteria is identified, it is intended that it be powered from a Class 1E power supply.

Question F.25

In view of the experience from the TMI-2 accident, justify your proposed use of non safety grade equipment (core exit thermocouples with the plant computer) as a means of determining adequate core cooling. What physical or practical limitations, if any, preclude use of a safety-grade system for this purpose? Your justification should be coupled with the fact that a positive, direct means for detection and removal of a gas bubble from the reactor vessel head is not yet included in your proposals. Include in your discussion what backup is provided for operation when the plant computer is down. Also, specify the range and sensitivity of the detection and indication measurements.

Response

In view of the experience from the TMI-2 accident, nonsafety-grade core exit thermocouples appear to be adequate as a diverse indication of core cooling. As of March 27, 1980, 48 of 52 core exit thermocouples are still providing valid readings. Based on the "TMI-2 environmental type test" and on the fact that other methods are available for determining adequate core cooling, the use of nonsafety-grade core exit thermocouples is considered adequate.

Consumers Power Company's position is that the installation of reactor coolant system (RCS) loop high point vents precludes the necessity for venting the reactor vessel head. Ongoing analysis of this issue will be reviewed for impact on RCS vent design.

The use of a safety-grade core exit thermocouple system is impractical, if not impossible, in terms of seismic qualification and compliance with separation criteria to meet single failure requirements. Likewise, individual safety display of each thermocouple measurement would be excessive. Additionally, the modifications necessary to seismically qualify these instruments are impractical.

Core exit thermocouples do not represent the sole method of determining adequate core cooling. Hot leg temperature, cold leg temperature, loop flow indication (as discussed in the response to Question F.24), reactor coolant (RC) pressure, pressurizer level, and power-operated relief valve (PORV) and pressurizer safety relief valve position are all provided as safety-grade indications for determining adequate core cooling. In combination, these parameters characterize the plant status with respect to the core cooling function. Detailed design of the instrument upgrades required to provide all these parameters as safety grade has not been finalized. Instrument sensitivities are therefore unavailable. However, it is our intention to provide safety-grade indication of hot leg and cold leg temperature from 150 to 750F, loop flow as indicated in the response to Question F.24, RC pressure from 0 to 2,500 psi, pressurizer level from 0 to 400 IWC, and PORV and pressurizer safety-relief valve position.

Because this safety-grade instrumentation provides sufficient indication for determining adequate core cooling, the use of nonsafety-grade core exit thermocouples is adequate as yet another diverse indication of core cooling.

Question F.26

To prevent automatic tripping of the reactor coolant pumps due to ESFAS initiated by overcooling events, you state that the Midland pump trip logic will include coincidence circuitry sensing pump motor current. This input is intended to actuate on degraded pump current indicative of significant RCS void formation characteristic of a LOCA; but for overcooling events, the extent of void formation should not reach a point where degraded pump current will trip the pumps and undesirable pump trip will thus be avoided. Describe the significant elements of the development program for this circuitry, including that phase directed to the distinction of a valid motor current signal. What criteria will distinguish a valid signal? How will the system be verified in an actual nuclear power plant or under realistic conditions? Provide your current schedule for this program.

Response

Consumers Power Company (CPCo) is pursing the development of an automatic reactor coolant (RC) pump trip design generically through participation in the Babcock & Wilcox (B&W) Owners Group. The goal of this effort is a design which will trip the RC pumps for all events identified by B&W analyses as being required to assure compliance with 10 CFR 50, Appendix K criteria, while limiting to the extent practicable pump trip for nonloss-of-coolant accident (non-LOCA) events. In CPCo's December 4, 1979 reply to your 10 CFR 50.54(f) request, it was stated that the Midland automatic pump trip circuitry would incorporate a coincidence circuitry sensing RC pump motor current to minimize unnecessary pump trips.

Subsequent to this response, difficulties have been encountered in implementing this design concept, especially in the analysis of the correlation between the total RC system void, the localized void at the RC pump suction, and the corresponding RC pump motor current. As a result, B&W is reviewing the feasibility of an RC pump motor current providing an acceptable coincidence signal while also investigating alternative concepts for providing this feature. The response to your detailed questions concerning program development and design criteria must await better definition of the design concept to be pursued.

Question F.27

After the PORV closed during the transient at Crystal River Unit 3 on February 26, 1980, the reactor coolant system pressure increased from approximately 1300 psi to 2400 psi in less than 3 minutes. The last 600 psi (from 1800 to 2400 psi) of this increase occurred in less than 1 minute. This caused lifting of the code safety valves. Operating guidelines for B&W supplied plants typically recommend termination of high pressure injection when hot and cold leg temperatures are at least 59°F below the saturation temperature of the existing reactor coolant system pressure and the action is necessary to prevent the indicated pressurizer level from going off scale.

In view of this characteristic of rapid repressurization, what operator action, and basis thereof, is proposed to reduce the potential for lifting of the Midland code safety valves?

Response

Initial reactor coolant system (RCS) depressurization during the transient at Crystal River Unit 3 resulted in the initiation of high-pressure injection (HPI) and the subsequent lifting of the pressurizer code safety valves. Operator control of the HPI system during this scenario was predicated upon assuring adequate core cooling as indicated by an acceptable subcooling margin. The satisfaction of this condition must take priority over concerns for filling the pressurizer solid. A modification of operating procedures to limit pressurizer safety valve lifting at the expense of core cooling is obviously unacceptable and the current Babcock & Wilcox operating guidelines must remain in force.

In order to reduce the potential for lifting the pressurizer code safety valves, reliable indications must be made available to the operator to ensure that during similar transients, conditions satisfying small break guideline criteria for terminating HPI flow can be promptly recognized. At Midland, indications necessary to assure this capability will be provided. In the event of total loss of both nonnuclear instrumentation (NNI) and integrated control system (ICS) power, indications in the control room of pressurizer level, hot leg temperature, RCS pressure, and saturation margin will be available to the operator. This will limit the potential for HPI challenging the pressurizer code safety valves and will eliminate the necessity of discharging excessive RC coolant through these valves while determining whether HPI flow may be terminated.