REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR:8311210360 DOC.DATE: 83/11/10 NOTARIZED: NO DOCKET #
FACIL:50-397 WPPSS Nuclear Project, Unit 2, Washington Public Powe 05000397
AUTH.NAME AUTHOR AFFILIATION
SORENSEN,G.C. Washington Public Power Supply System
RECIP.NAME RECIPIENT AFFILIATION
SCHWENCER,A. Licensing Branch 2

SUBJECT: Forwards response to FSAR Questions 031.143-031.159 re control sys failures.Single bus failure will not severely restrict plant operator ability to monitor plant status through control room indicators.

DISTRIBUTION CODE: B001S COPIES RECEIVED:LTR 1 ENCL 1 SIZE: 21
TITLE: Licensing Submittal: PSAR/FSAR Amdts & Related Correspondence

NOTES:

	RECIPIENT ID CODE/NAME		COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME		COPIES LTTR	COPIES ENCL
	NRR/DL/ADL		1	0	NRR LB2 BC		1	0
	NRR/LB2 LA		1	0	AULUCK,R.	01	1	1
INTERNAL:	ELD/HDS2		1	0	IE FILE		1	1
	IE/DEPER/EPB	36	3	3	IE/DEPER/IRB	35	1	1
	IE/DEQA/QAB	21	1	1	NRR/DE/AEAB		1	0
	NRR/DE/CEB	11	1	1	NRR/DE/EHEB		1	1
	NRR/DE/EQB	13	2	2	NRR/DE/GB	28	2	2
	NRR/DE/MEB	18	1	1	NRR/DE/MTEB	17	1	1
	NRR/DE/SAB	24	1	1	NRR/DE/SGEB	25	1	1
	NRR/DHFS/HFEB	40	1	1	NRR/DHFS/LQB	32	1	1
	NRR/DHFS/PSRB		1	1	NRR/DL/SSPB		1	0
	NRR/DSI/AEB	26	1	1	NRR/DSI/ASB		1	1
	NRR/DSI/CPB	10	1	1	NRR/DSI/CSB	09	1	1
	NRR/DSI/ICSB	16	1	1	NRR/DSI/METB	12	1	1
	NRR/DSI/PSB	19	1	1	NRR/DSI/RAB	22	1	1
	NRR/DSI/RSB	23	1	1	REG FILE	04	1	1
	RGN5		3	3	RM/DDAMI/MIB		1	0
EXTERNAL:	ACRS	41	6	6	BNL(AMDTS ONLY)		1	1
	DMB/DSS (AMDTS)		1	1	FEMA-REP DIV	39	1	1
	LPDR	03	1	1	NRC PDR	02	1	1
	NSIC	05	1	1	NTIS		1	1

TOTAL NUMBER OF COPIES REQUIRED: LTTR 53 ENCL 46

[illegible]

TITLE: [illegible]

SUBSYSTEM: [illegible] Generation for the Power Supply System

[illegible]

RESULTS: A module responsible for the exceptions [illegible] control system [illegible] feature will not severely restrict plant operation capability to [illegible] from [illegible]

DISTRIBUTION: [illegible]

TITLE: The [illegible] Related Correspondence

NOTES:

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

[illegible]

Washington Public Power Supply System
P.O. Box 968 3000 George Washington Way Richland, Washington 99352 (509) 372-5000

Docket No. 50-397

November 10, 1983
G02-83-1040

Director of Nuclear Reactor Regulation
Attention: Mr. A. Schwencer, Chief
Licensing Branch No. 2
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: NUCLEAR PROJECT NO. 2
SUPPLY SYSTEM RESPONSE TO FSAR
QUESTIONS 031.143 - 031.159

Reference: Letter, A. Schwencer (NRC) to D.W. Mazur (Supply System), subject, "Request for Additional Information - Control System Failures," dated October 5, 1983

The Washington Public Power Supply System hereby provides replies to the subject FSAR questions which were submitted as an attachment to the reference. Our reply consists of this letter and one attachment.

If you have any questions or desire further information, please contact P.L. Powell, Manager, WNP-2 Licensing.

Alan Hosler for

G. C. Sorensen, Manager
Regulatory Programs (340)

GCS:ROV:pp

Attachment: Responses

cc: R. Auluck, NRC
W.S. Chin, BPA
A.D. Toth, NRC Resident Inspector

B001
1/1

ATTACHMENT

031.143 It appears that control room indicators were not included in the devices listed in Appendix B. Verify that as part of your review, it was determined that sufficient control room indication exists to allow the operator(s) to determine the status of the plant while going to cold shutdown following the loss of each Class 1E and non-Class 1E bus.

Response: The WNP-2 Cold Shutdown Power Bus Failure Analysis Report states the analysis performed identified no situation where a single bus power failure would prevent plant personnel from achieving reactor cold shutdown. This conclusion is based primarily on the analysis presented in Appendix A of the report, which concludes no single bus supplies power to the normal shutdown path and the two alternate shutdown paths. In most cases, single busses provide power to systems active in only one shutdown path.

The conclusion reached is also based on the fact that sufficient control room indicators exist to allow plant personnel to determine the plant status in the event of any single bus power failure. In the event of the failure of any one Class 1E or non-Class 1E power bus, the plant operators can still easily bring the plant to cold shutdown as the failure of one bus does not affect control equipment or control room indicators in all three shutdown paths. Even in the unlikely event of a loss of one complete division of Class 1E power, indicators critical to verifying plant status such as reactor pressure, power level, water level, drywell pressure and suppression pool temperature are still available from a separate division of power. Any single bus power failure will not severely restrict the plant operators' ability to monitor plant status through control room indicators.

031.144 It is indicated in Section 2.9 and 2.10 that if an alternate shutdown path is required, then existing procedures should be modified or new procedures developed to provide the operator with the appropriate actions to be taken following a bus loss. Verify that the modified and/or new procedures will be in place prior to fuel load.

Response: WNP-2 Emergency Operating Procedures (EOPs) have been prepared and modified in accordance with the BWR Owners' Group Emergency Procedures Guidelines (EPGs), Revision 2. These procedures are structured to provide for cooldown through a continually degrading scenario until, for example, the one remaining cooldown path is open safety relief valves and an operating low pressure ECC pump. The emphasis of the procedures is to provide alternate shutdown capabilities or paths based on the available equipment, not based on the loss of a particular power bus or loss of specific pieces of equipment, i.e., symptom based procedures. Operator training follows this philosophy to implement alternate shutdown paths. Therefore, whether or not the inability to use the normal shutdown path is from loss of a power bus or equipment failure, the operator will select an alternate shutdown cooling path. The Emergency Operating Procedures provide the flexibility for selecting any or multiple shutdown cooling paths depending on the degree of degradation of the normal path.

The WNP-2 Abnormal Operating Procedures are currently being revised to emphasize the loss of normal RHR shutdown cooling paths resulting from power losses identified in the IEB 79-27 analysis. These procedures will be in place by fuel load.

031.145 It is necessary when a bus loss affecting the normal shutdown path occurs, that the control room operator(s) be alerted to this fact. Appendix A identified some bus losses requiring shutdown via an alternate path for which the only indication of bus failure is the loss of position indication lamps for certain devices (power buses PP-1B-A and PP-7A-C are two examples). The staff does not consider the loss of position indication lamps to be a positive indication of a power bus failure affecting the capability to achieve a normal reactor shutdown. All buses relied on to achieve a normal shutdown should be alarmed in the control room. Provide a commitment to implement loss of power alarms for all buses whose failure adversely affects the capability to shutdown via normal procedures that are not presently alarmed.

Response: The notation in the report of "Loss of Position Indication Lamps", "O/L Trip Ann.", do not adequately reflect the extensive alarm and annunciation available to the operator to recognize loss of power to any given bus. Conformance to Reg. Guide 1.47, Reg. Guide 1.97, and the Safety Parameter Display System have contributed to the multiple indications of loss of bus power. It must be emphasized (see response to Q031.144) that the operating procedures and EOPs are based on system availability and symptoms, not based on noting a particular failure mode. In complying with Reg. Guide 1.47, the Supply System has installed a comprehensive Bypass and Inoperability Status Board System. This system is comprised of, first, system level annunciators for each of the safety systems. This provides the operator with immediate recognition of available alternate shutdown system should they be necessary. Next, component level indicators are provided near the system level annunciator to indicate the cause of the system bypass or inoperability. Included in the component annunciation are indications for:

a) Loss of pump motor control power
b) Loss of MOV control/motive power
c) Logic power failure

If a given set of the annunciators alarm simultaneously, the specific power bus failure can be identified. Therefore, the Bypass and Inoperabiity Status Board System provides system level information for the operator to carry out shutdown utilizing available systems and the EOPs, as well as providing information on the root cause for a system or component failure.

In compliance with Reg. Guide 1.97, voltage indication for the 4.16kV, all vital 480 volt buses, batteries, battery chargers, and inverter voltage and amperage are displayed in the control room. The 4.16kV, batteries, battery chargers, and inverter voltages are also annunciated. These voltage indications, as well as PP-7A-A and PP-8A-A, are available on the TDAS/SPDS system.

031.145 (Cont'd)

In summary, the annunciator and alarm system at WNP-2 is tiered to provide the operator system level information to assist in selecting the shutdown path without requiring evaluation of extraneous or possibly confusing alarms. The component alarms of the Bypass and Inoperability Status Board provide positive indication of loss of power so that corrective action can be effected as required. In addition, status information for all standby power such as the 4.16kV, all vital 480V buses, all battery, battery chargers, and inverter voltages and amperages are read out in the control room on panel P-800. A panel dedicated to bus power annunciation would be superfluous to these already existing indications.

031.146 Verify that IE Circular No. 79-02, "Failure of 120 Volt Vital AC Power Supplies," dated January 11, 1979 was re-reviewed to include both Class 1E and non-Class 1E power supply inverters as required for operating reactors via IE Bulletin 79-27, "Loss of Non-Class IE Instrumentation and Control Power System Bus During Operation," dated November 30, 1979.

Response: IE Circular 79-02 was reviewed to include both Class 1E and Non-Class 1E inverters. This re-review confirmed the adequacy of the initial review.

031.147 Part a. Why is it necessary to use HPCS (i.e., the division II & III alternate cooldown path) upon loss of power bus MC-8B? It appears that the normal shutdown path (i.e., main steam, condenser, feedwater, etc.) is still available.

Response: Appendix A and Figure 1 of the WNP-2 Cold Shutdown Power Bus Failure Analysis Report identify the shutdown components and systems unavailable to the plant operators due to the loss of each specific power bus. Note that upon the postulated failure of power bus MC-8B, loss of certain shutdown functions occur in three separate shutdown paths: Normal (N), Division I (A1) and Division II (A2). Upon the failure of bus MC-8B, the normal cooldown path (N) is available to the point where high pressure cooldown is completed. However, it is prudent to identify the safety-related cooldown path which is available to the plant operators to attain cold shutdown since some components in both the Division I and Division II shutdown paths are unavailable. The safety-related path which remains available is HPCS (Division III) with a transfer to the Division I (A1) path. Therefore, although some components in both the Division I and Division II paths are unavailable, the ability to reach cold shutdown using safety-related equipment is not compromised.

This report addresses the safety implications of a single power bus failure. Alternate paths utilizing safety grade equipment are presented even though other alternatives, such as shutdown paths employing non-safety grade equipment or actions to restore power to the affected bus, may be the preferred actions.

031.147 Part b. Breaker trip annunciation and/or O/L (overload) trip annunciation is relied on to alert the operator(s) to a loss of power condition for a number of buses,. It is not clear that this annunciation would always be provided (i.e., loss of bus power for other reasons would not result in annunciation). Justify the adequacy of these alarms.

Response: The response to Q031.145 was written to also include response to this question. Please refer to Q031.145 response.

031.147, Part c. Loss of power bus MC-7B requires use of an alternate low pressure cooldown path following high pressure cooldown using the normal shutdown path. Note 4 states that since both paths are not required simultaneously, further analysis is not necessary. Verify that for this and similar cases (i.e., all references to note 4) adequate alarms and procedures exist to instruct the operator(s) of the need to use the alternate shutdown path.

Response: Following high pressure cooldown, the failure of a power bus which affects high pressure and low pressure cooldown, e.g., bus MC-7B, may require the use of an alternate low pressure cooldown path. Since both high pressure and low pressure cooldown paths are not required simultaneously, further analysis of the effects of the bus loss is not required. This is stated in Note 4 of the WNP-2 Cold Shutdown Power Bus Failure Report.

031.147
Part c.
(Cont'd)

Failure of a major power bus (i.e., 6.9kV through 480V) is annunciated in the control room. This provides plant operators with information the bus is lost. The review and analysis presented in Figure 2 and Appendix A of the report show conclusively plant operators will have knowledge of individual bus or circuit failures. The sixth column in the tables of Appendix A (the column labelled ANN. TRIP OR LOSS OF CNTRL SIGNAL) identifies the control signals lost as well as the breaker trip annunciations, under voltage annunciations, out of service indications, etc., provided to the plant operators upon the loss of each specific power bus. In addition, the loss of position indication lamps for motor operated valves will indicate a loss of bus power. (See response to Question 031.145 for additional information.)

The Emergency Operating Procedures provide adequate instructions for plant operators to use in bringing the reactor to cold shutdown in the event of a single bus loss which affects the low pressure cooldown path after high pressure cooldown has been accomplished. This applies to any references to Note 4 of the WNP-2 Cold Shutdown Power Bus Failure Analysis Report.

031.148 Postulated damage to non-safety related (control) systems from high energy line breaks (HELBs) was limited to jet impingement and/or pipe whip. This is not acceptable. The effects of HELBS on control systems should also include environmental effects such as humidity, pressure, temperature, etc. Provide the results of the analyses of HELBs in the vicinity of non-safety related systems which include environmental effects on these systems. Describe the methodology used to determine which non-safety related (control) systems are postulated to be affected by the environmental effects of a given HELB.

Response: The results presented in paragraph 3.2.1 of our response to IE Bulletin 79-22 (GO2-83-509) identified the worst case combination of control system failures due to pipe whip and jet impingement effects of HELBs, as being:

1) Loss of Feedwater Heating
2) Feedwater Controller Failure, Maximum Demand
3) Loss of Feedwater Flow (Pipe Break)
3) Pressure Regulator Failure, Closed
5) MSIV Closure
6) Turbine Trip, Bypass On

This combination also bounds all HELB effects when including consideration of potential control system failures due to environmental conditions. This is because there are only two additional control system failure effects possible that, when combined with the above, could represent a worse case and neither failure is considered possible due to environmental effects of the HELB. Therefore, by considering the synergistic effect of the combined control system failures, environmental effects are also represented by the analysis presented in Section 3.2.1. However, failure of the remaining two control systems is discussed in more detail below.

The additional potential Control Systems Failures are:

7) Turbine Trip, Bypass Off
8) Loss of RPS from turbine stop valve position and control valve emergency trip fluid pressure.

The failure of the bypass valves is only possible due to a hydraulic line failure approximately 140 feet from the source break. This is not considered possible as a result of environmental, jet impingement, or pipe whip effects. Loss of RPS signals would require an immediate environmentally induced failure of a minimum of two cables contained in four separate Class IE routed conduits or in the enclosed panels at the HP turbine. We do not consider this to be credible in the time frame required for a reactor scram.

However, to ensure completeness of the control system failure studies, the above failures were included in a new bounding combination of events and analyzed by General Electric. The worst combination of control system failures then become:

031.148 (Cont'd)

1) Loss of Feedwater Heating
2) Feedwater Controller Failure - Maximum Demand
3) Turbine Trip, Bypass Off
4) Loss of Direct Scram from Turbine RPS Signals and EOC RPT Signals

For the event, the reactor Δ CPR was .3743. The peak vessel pressure was less than 1227 PSIG and the peak cladding temperature was less than 1190^{0}F, which is considerably less than the allowable peak vessel pressure (1375 PSIG) and the allowable peak cladding temperature (2200^{0}F). Therefore, the localized low CPR will not cause any temperature or pressure damage to the reactor coolant pressure boundary.

In summary, the combined effects analyses presented in Section 3.2.1 and in the above response, represent the bounding cases of control system failure from HELBs, including failures initiated by jet impingement, pipe whip, or environmental effects.

031.149 Verify that for each HELB event and its consequential control systems failures, that redundant safety related systems are available (i.e., unaffected by the event) to mitigate the effects of the event. The intent here is to assure that the consequences of the event can be mitigated given a single failure within the systems used to mitigate the event.

Response: The only safety related systems affected by this HELB study are the turbine induced RPS signals and the EOC RPT signals; all other safety related systems are available to mitigate the effects of the event. The loss of either of these safety related systems due to the HELB is not considered credible but was analyzed in the event described in the response to Question 031.148. No single failure in a safety system can prevent the mitigation of the analyzed HELB events.

031.150 There is no technical basis for excluding events that are not capable of occurring at 100% power from the analysis. All operating modes should be considered. The analysis should be revised accordingly.

Response: The events identified in Section 2.1.2 as not applicable because they could not occur at 100% power operation have been reanalyzed. These events should be revised to read as follows:

5) RHR Shutdown Cooling Malfunction Decreasing Temperature (Chapter 15.1.6)
Applicable Event

17) Failure of RHR Shutdown Cooling (Chapter 15.2.9)
Applicable Event

24) Rod Withdrawal Error - Refueling (Chapter 15.4.1.1). This event is not applicable as it is not the result of a HELB.

25) Rod Withdrawal Error - Startup (Chapter 15.4.1.2). This event is not applicable as it is not the result of a HELB.

28) Abnormal Startup of Idle Recirculation Loop (Chapter 15.4.4)
Applicable Event

29) Fast Opening of One Main Recirculation Valve (Chapter 15.4.5).
Applicable Event

30) Fast Opening of Both Main Recirculation Valves (Chapter 15.4.5).
Applicable Event

31) Misplaced Bundle Accident (Chapter 15.4.7). This event is not applicable as it is not the result of a HELB.

Analysis of these additional events was performed with the following results:

Events #5 and #17 involving RHR Shutdown Cooling are only possible as a single event and are bounded by FSAR Chapter 15 analysis.

Events #28, #29 and #30 involve increased recirculation flow. Initiation of any of these events due to a HELB would require that the initiating HELB be located in the Reactor Building. Since our initial analysis determined that no applicable events occur in the Reactor Building, this event could not occur as a combined event but only as a single event as previously analyzed in FSAR Chapter 15.

The remaining operational modes, cold shutdown and refueling, are not included due to the absence of high energy lines. Therefore, all applicable operating modes have been considered.

031.151 Under Item 3 of Section 2.1.3, verify that for ruptured process tubing, the worst case failures of associated instrumentation are assumed (e.g., for level 8 trip signals, assuming these instrument channels are not environmentally qualified, the level 8 signal is assumed to occur or to not occur whichever is worse for the senario being considered).

Response: Item 3 of Section 2.1.3 was not meant to imply determination was made as to whether or not process tubing crimped or ruptured. For each process tube failure, the worst case consequence of the associated instrumentation failure was assumed.

031.152 Could a HELB resulting in loss of feedwater heating (see Section 3.1.1) also affect feedwater and turbine-generator controls (i.e., are controls for these systems located in any of the "environmental zones" where this HELB could occur?)

Response: Section 3.1 of the report defines single event analysis and associated mechanisms for failure. Multiple event analysis, including loss of feedwater heating, feedwater flow and turbine generator controls are discussed in Section 3.2 of the report and question 031.148.

031.153 Verify that no credit was taken in the analysis for non-safety related equipment (e.g., feedwater pump trip on level 8) to mitigate the effects of HELBS and consequential control systems failures.

Response: No credit was taken for non-safety related equipment to mitigate the effects of HELBS and consequential control system failures.

031.154 It is assumed in the analysis that the turbine bypass system functions following a turbine trip. Why was a turbine trip without bypass not considered in Section 3.2?

Response: In the analysis, the direct effects of pipe whip and/or jet impingement were considered. The control signal which operates the bypass valves for pressure control was considered to have failed. However, the bypass valves open independently of the pressure control signal on a turbine trip. The loss of control valve emergency trip fluid experienced on a turbine trip automatically opens the bypass valves for 3 to 5 seconds. As these bypass valve controls were not directly damaged, the integrity of the valves remained and the valves were assumed to work properly. However, bypass valve failure was assumed for the new bounding case described in the response to question 031.148.

031.155 For HELB events it is not necessary to remain above the minimum critical power ratio (MCPR) safety limit. However, verification should be provided that the worst case event combinations considered are bounded by a small fraction (<10%) of 10 CFR Part 100 guidelines. The worst case events may change as a result of the environmental considerations discussed in Item 6 above.

Response: The worst case event described in response to question 031.148 does exceed the reactor MCPR limits for a very short duration. However, the peak vessel pressure and temperature remained considerably less than the allowables. Therefore, the localized low CPR will not cause any temperature or pressure damage to the reactor coolant pressure boundary and the event is bounded by a small fraction (< 10%) of 10 CFR Part 100 guidlines.

031.156 Provide a list of non-safety related (control) systems considered in your review (i.e., those systems described in Section 1.2.1 as potentially affecting reactor pressure, water level, critical power ratio, feedwater temperature, and/or the performance of safety-grade equipment).

Response: The non-safety and safety related (control) systems considered in our analysis were:

System No.	Title
3.0	Reactor Recirculation System
7.0	High Pressure Core Spray System
9.0	Residual Heat Removal System
19.0	Leak Detection System
46.0	AC Electrical Distribution System
48.0	Main Turbine Systems
51.0	Main Generator Systems
63.0	Main Steam System
64.0	Extraction Steam System
65.0	Sealing Steam System
66.0	Condenser Air Removal Sustem
69.0	Condensate System
72.0	Feedwater Systems
74.0	Heater Vents and Drains Systems
78.0	Control and Service Air System

031.157 It appears that this analysis only considers the effects of multiple control systems failures due to the failure of instrument lines (either broken or plugged) and the associated effects on all sensors connected to the line. Are there any individual sensors (not sharing an instrument line with other sensors) that provide inputs to two or more control systems? If so, the failure of these sensors should be analyzed to determine if the effects are bounded by the analysis in Chapter 15 and if they result in an event that requires action or response beyond the capability of the operators or safety systems.

Response: The WNP-2 Common Sensors Failures Evaluation Report was prepared to address NRC concerns regarding the failure of components of control grade systems whose malfunction could seriously impact plant safety. Common sensors, sensors which provide input to two or more control systems, were identified and the consequences of a broken or plugged common sensor line were evaluated.

During this evaluation it was determined that there are no individual instruments (instruments not sharing a sensing line with other instruments) which provide inputs to two or more control systems whose failure or malfunction could impact plant safety. The report examines the consequences of failure or malfunction of sensing lines common to instruments whose output provides signals to two or more control systems. No transients were identified which are not bounded by the current WNP-2 FSAR Chapter 15 Analysis.

031.158 Verify that for all sensor failures (incuding multiple failure due to instrument line failures) resulting in control systems malufunctions requiring protective actions, redundant safety related systems are available (i.e., unaffected by the failures) to mitigate the effects of the event. The intent here is to assure that the effects of the event can be mitigated given a single failure within the systems used to mitigate the event.

Response: The Common Sensor Failure Table included in the subject report, under the heading of Secondary Effect, reports the consequences of individual instrument failures. This analysis includes the impact on all systems which receive the erroneous signal and the subsequent effects on systems initiations, inhibit signals or terminations. This analysis also identifies the backup or redundant systems available to mitigate the consequences of the postulated failure, if any are required. The report considers all instruments that affect control systems whose failure could impact plant safety. The report goes beyond single instrument failures and considers the combined effect of failures or malfunctions of two or more instruments on all systems affected. Section 4.0 of the report demonstrates the combined effects are bounded by the current WNP-2 FSAR Chapter 15 Analysis.

It should be noted the analysis addresses plant upset, i.e., transient, conditions as requested by the NRC and, as such, follows the guidelines established in Reg. Guide 1.70 and the Standard Review Plan. Single additional failures in mitigating systems are not considered in the WNP-2 Common Sensors Failures Evaluation Report.

031.159 Clarify the sentence "There were no single effects that mitigate the total failure consequences." in Section 3.4 (Analyze Combined Effects) of the analysis.

Response: The sentence "There were no single effects that mitigated the total failure consequences." in Section 3.4 should read "There were no single effects that exceeded the total failure consequences". The sentence is intended to state there is no consequence of a single instrument failure which is not bounded by the combined effect consequences of all instrument failures on any given instrument line. The worst case failure was postulated for each instrument line.