Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-97-4947
DCP/NRC0709
Docket No.: STN-52-003

February 26, 1997

Document Control Desk
U. S. Nuclear Regulatory Commission
Washington, DC 20555

ATTENTION: T. R. QUAY

SUBJECT: REFERENCES AND CHANGES FOR SSAR CHAPTER 7

Dear Mr. Quay:

Hulbert Li (NRC) has contacted Westinghouse regarding some documents which do not appear in the AP600 SSAR Chapter 7, but which he plans to reference in his input to the AP600 Final Safety Evaluation Report. Each of these 5 references is addressed by this letter.

1. WCAP-14080 is the AP600 Instrumentation and Control Software Architecture and Operation Description. Because it is a valid reference for the AP600, Westinghouse is revising Section 7.1 and Table 1.6-1 of the SSAR to include a reference to WCAP-14080, as marked on the attached. This markup will be incorporated into Revision 11 of the AP600 SSAR.

2. WCAP-11341, from November 1986, is a Noise, Fault, Surge, and Frequency Interference test report for the Westinghouse Eagle-21 systems. This report is not applicable to the AP600 I&C design and thus is not an appropriate reference for the AP600 design certification.

3. WCAP-13633 is the AP600 Instrumentation and Control Defense in Depth Diversity Report. While this report is applicable to AP600, the SSAR references only those documents which are used as input to the various SSAR sections. Since WCAP-13633 was not used as a source document for SSAR Chapter 7, it should not be referenced therein. For your information, WCAP-13633 was transmitted to the NRC by letter ET-NRC-93-0264 and is the WCAP referred to as an ongoing defense in depth analysis of the protection and safety monitoring system in the responses to RAIs 420.5 and 420.7.

4. WCAP-13559 is the Operational Assessment which, while a valid reference for SSAR Section 20.7, was not used as input to SSAR Chapter 7 and should not be referenced therein. WCAP-13559 Revision was transmitted to the NRC by letter NSD-NRC-96-4818 in September, 1996.

5. WCAP-14605 is the Westinghouse Setpoint Methodology for Protection Systems - AP600 from May 1996. By error of omission, SSAR Revision 10 did not include the SSAR markup which was agreed upon in early December 1996. That SSAR markup, also attached, will be included in Revision 11 of the SSAR.

1/1 E004

040095

Chapter 7 Changes for SSAR Revision 11

Given the oversight described above, SSAR Chapter 7 has been reviewed to confirm the changes which were supposed to be incorporated into Revision 10 were incorporated. The changes being made to SSAR Chapter 7 in Revision 11, which were previously approved by the NRC for SSAR Revision 10, are:

- Section 7.7.1.11 regarding qualification of DAS equipment, including actuated devices.
- Changes reflecting COL applicant responsibility for a setpoint study per WCAP-14605.
- Revised figures 7.2-1 and 7.2-12 (changes were made only to the text in Revision 10).

In addition to those changes previously approved by the NRC, Westinghouse will be making the following changes to SSAR Chapter 7 in Revision 11:

- Changes to reflect resolution of NRC PAM/ERG comments (Tables 7.5-5, 7.5-7, 7.5-9).
- Changes to 7.3.1.2 reflect isolation of auxiliary spray and CVS letdown.
- Changes to 7.4.3 resulting from resolution of NRC comments on minimum inventory (SSAR Chapter 18) to reflect the remote shutdown workstation.
- Changes to reflect the Westinghouse design changes resulting from NRC's new post-72 hour position.

Most of the attached changes were faxed to Tom Kenyon/Hulbert Li on 02/18/97 with some minor changes made since then. The attached markups are considered Enclosure 1 of this letter. Other than changes which may result from the AP600 Shutdown Evaluation, which would be communicated as a package separate from this letter, no more changes to SSAR Chapter 7 are anticipated.

Status of DSER Open Items

Enclosure 2 is a DSER open item tracking system (OITS) report for all of the DSER Chapter 7 items which are not statused as "resolved" by the NRC. With the changes to be incorporated into SSAR Revision 11, and excluding the ITAAC items, Westinghouse has no outstanding actions for DSER Chapter 7.

Items 1052 and 1053 are considered to be NRC action to document concurrence or disagreement with the Westinghouse position regarding interlocks for the accumulator isolation valve and IRWST discharge valve. When these valves and their interlocks were changed from safety-related to nonsafety-related, these interlocks were removed from SSAR Chapter 7. While Westinghouse considers this an acceptable approach based on the following, it has not been accepted by the NRC.

Westinghouse Position for DSER Open Items 1052 and 1053

The accumulator isolation valve and IRWST discharge valve interlocks were changed from safety-related to nonsafety-related based on their never having been required to change position to mitigate an accident. However, since the SSAR Chapter 15 safety analyses assume that both accumulators and both IRWST injection lines are always available, valve mispositioning (prior to an

accident) or spurious closure (during an accident) are not allowed and are therefore prevented by the following, as described in SSAR Section 6.3:

1. Power is locked out at the motor control center when RCS pressure is greater than 1000 psig.

2. With power locked out, redundant (nonsafety-related) valve position indication is provided on the main control board. Alarms (nonsafety-related) are activated in case the valves are closed with RCS pressure greater than 1000 psig. These position indications and alarms are powered by different nonsafety-related power supplies.

3. The following surveillances are required by the AP600 Technical Specifications
   a. Verify MOVs open every 24 hr
   b. Verify power is removed every 31 days

In addition, the valves have a confirmatory open signal during an accident (SI or ADS stage 4 signal) and an automatic open signal when the close permissive clears during plant startup.

Summary

Enclosure 1 will be included in SSAR Revision 11. NRC is requested to review Enclosure 2 and provide Westinghouse with an NRC status for each item, including 1052 and 1053 for the interlocks.

Please contact Robin K. Nydes at (412) 374-4125 if you have any questions regarding this letter or AP600 SSAR Chapter 7.

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

jml

Attachment

cc: Tom Kenyon, NRC - (1L, 1E1, 1E2)
Hulbert Li, NRC - (1L, 1E1, 1E2)

Changes Previously Approved by NRC to be Incorporated in SSAR Revision 11

Operability, Availability, and Testing

The diverse actuation system is designed to provide protection under all plant operating conditions in which the reactor vessel head is in place. The automatic actuation processors, in each of the two redundant automatic subsystems of the diverse actuation system, are provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during online calibration, testing activities or maintenance, the normal activation function is bypassed. Testing of the diverse actuation system is performed on a periodic basis.

Equipment Qualification and Quality Standards

The diverse actuation system is capable of functioning during and after normal and abnormal events and conditions that include:

- Excessive temperature
- Ambient vibration
- Radio frequency and electromagnetic interference

The diverse actuation system equipment is designed and qualified in accordance with the industry standards listed in subsection 7.1.4.1.8. The adequacy of the hardware and software is demonstrated through the verification and validation program discussed in subsection 7.1.2.15. This program provides for commercial dedication of commercial off-the-shelf hardware and software. As the diverse actuation system performs many of the protection functions associated within the ATWS systems used in existing plants, the diverse actuation system is designed to meet the quality guidelines established by Generic Letter 85-06, "Quality Assurance Guidelines for ATWS Equipment that is not Safety-Related."

7.7.1.12 Signal Selector

The plant control system for the AP600 derives some of its control inputs from signals that are also used in the protection and safety monitoring system. The advantages of this design are:

- The nonsafety-related plant systems are controlled from the same measurements which provide protection. This permits the control system to function in a manner which maintains margin between operating conditions and safety limits, and reduces the likelihood of spurious trips.

- Reducing the number of redundant measurements for any single process variable reduces the overall plant complexity at critical pressure boundary penetrations. This leads to a reduction in separation requirements within the containment, as well as to a decrease in plant cost and maintenance requirements.

To obtain these advantages, measures are taken to provide the independence of the protection and control systems. The criteria for these measures are contained in the Standard IEEE

Operation procedures prohibit testing two divisions at the same time. There are no built-in interlocks to prevent simultaneous testing of two integrated protection cabinets. However, the use of bypasses by the tester provides that the protection and safety monitoring system cannot be placed in an unsafe condition if the procedure prohibiting simultaneous testing is violated. For example, testing two divisions results in two bypasses, which causes the voting logic to revert to a one-out-of-two coincidence for the remaining two unbypassed divisions. Attempting to test three or four divisions at the same time causes a plant trip. The operational procedure restricting simultaneous testing of two or more divisions is for operability reasons to avoid unnecessary trips.

In addition to periodic tests, the system performs error detection and data link testing as part of its normal operation. Where practical, the on-line error detecting features are designed to automatically place the channel in which the error was detected into a trip or bypass state (either by direct bypass or reconfiguration). When a channel is automatically placed into a trip state, the operator has the option to subsequently place that channel in a bypass state. If the automatic configuration of the channel is not practical, the on-line error detecting feature causes alarm annunciation to the operator.

7.1.2.13 Safety-Related Display Instrumentation

Safety-related display instrumentation provides the operator with information to determine the effect of automatic and manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in Chapter 15. This instrumentation also provides for operator display of the information necessary to meet Regulatory Guide 1.97. A description of the equipment used to provide this function is provided in subsection 7.1.2.6. A description of the data provided to the operator by this instrumentation is provided in Section 7.5.

7.1.2.14 Auxiliary Supporting Systems

The safety-related system equipment is supported by the supply of uninterruptable electrical energy. This electrical power is supplied by the Class 1E dc and UPS system discussed in Chapter 8.

change on next page

7.1.2.15 Verification and Validation

Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program are provided in WCAP-13383 (Reference 4). The software development process which is documented in this document is consistent with the following standards:

- ANSI/IEEE ANS-7-4.3.2 (1993); "Application Criteria for Programmable Digital Computer Systems in Safety Systems for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations"

- IEC 880-1986; "Software for Computers in the Safety Systems for Nuclear Power Generating Stations"
- IEEE 828-1983; "IEEE Standard for Software Configuration Management Plans"
- IEEE 829-1983; "IEEE Standard for Software Test Documentation"
- IEEE 830-1984; "IEEE Standard for Software Requirements Specifications"
- IEEE 1012-1986; "IEEE Standard for Software Verification and Validation Plans;"
- IEEE 1042-1987; "IEEE Guide to Software Configuration Management (ANSI)"

WCAP-13383 also provides for the use of commercial off-the-shelf hardware and software through a commercial grade dedication process.

7.1.3 Plant Control System

The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The plant control system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The plant control system also provides control of the nonsafety-related decay heat removal systems during shutdown. The plant control system accomplishes these functions through use of the following:

- Rod control
- Pressurizer pressure and level control
- Steam generator water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The plant control system provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The plant control system acts to maximize margins to plant safety limits and maximize the plant transient performance. The plant control system also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance.

The plant control system includes the equipment from the process sensor input circuitry through to the modulating and nonmodulating control outputs as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Nonmodulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The control cabinets contain the process sensor inputs and the modulating and nonmodulating outputs. The plant control system also includes equipment to monitor and control the control rods.

7.1.4.2.22 Conformance to the Requirements for Identification of Redundant Safety System Equipment (Paragraph 4.22 of IEEE 279-1971)

Distinctive markings are applied to redundant divisions of the protection and safety monitoring system.

The color coded nameplates described below provide identification of equipment, associated with protective functions and their divisions associations.

Division	Color Coding
Division A	BROWN with WHITE lettering
Division B	GREEN with BLACK lettering
Division C	BLUE with WHITE lettering
Division D	YELLOW with BLACK lettering

Non-cabinet mounted protective equipment and components have an identification tag or nameplate. Small electrical components such as relays, have nameplates on the enclosure that houses them.

7.1.5 AP600 Protective Functions

Protective functions are those necessary to achieve the system responses assumed in the safety analyses, and those needed to shut down the plant safely. The protective functions are grouped into two classes, reactor trip and engineered safety features actuation.

Reactor trip is discussed in Section 7.2. Engineered safety features actuation is discussed in Section 7.3.

7.1.6 Combined License Information

For ~~This section has no~~ the only requirement ~~for information to be provided in support of the Combined License application,~~ is for calculation of setpoints for protective functions ~~setpoints~~ consistent with the methodology presented in Reference 8.

Combined License applicants referencing the AP600 certified design will provide a

5

AP600

7.1.7 References

1. IEEE 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generator Stations."

2. IEEE 796-1983, "IEEE Microcomputer System Bus."

3. WCAP-13382 (P), WCAP-13391 (NP), "AP600 Instrumentation and Control Hardware Description."

4. WCAP-13383 (P), WCAP-13392 (NP), "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report."

5. IEEE 279-1971, "IEEE Criteria for Protection Systems for Nuclear Power Generating Stations."

6. IEEE 384-1981, "IEEE Criteria for Independence or Class 1E Equipment and Circuits."

7. WCAP-8897 (P), WCAP-8898 (NP), "Bypass Logic for the Westinghouse Integrated Protection System."

8. WCAP-14605(P), WCAP-14606(NP), "Westinghouse Setpoint Methodology for Protection Systems, AP600."

9. WCAP-14080(P), WCAP-14081(NP), "AP600 Instrumentation and Control Software Architecture and Operation Description", Revision 0.

Table 1.8-2 (Sheet 3 of 4)

SUMMARY OF AP600 STANDARD PLANT COMBINED LICENSE INFORMATION ITEMS

Item No.	Subject	Subsection
6.4-2	Local Toxic Gas Services and Monitoring	6.4.7
6.4-3	Procedures for Training for Control Room Habitability	6.4.7
6.6-1	Inspection Programs	6.6.9.1
6.6-2	Construction Activities	6.6.9.2
7.1-1	Setpoint Calculations for Protective Functions	7.1.6
8.2-1	Offsite Electrical Power	8.2.4
8.3-1	Onsite Electrical Power	8.3.3
9.1-1	Fuel Storage and Handling	9.1.6
9.5-1	Offsite Communications Interfaces	9.5.2.5.1
9.5-2	Emergency Response Facility Communications	9.5.2.5.2
9.5-3	Security Communications	9.5.2.5.3
9.5-4	Cathodic and Environmental Protection for Fuel Oil Tanks	9.5.4.7
10.1-1	Erosion-Corrosion Monitoring	10.1.3
10.2-1	Turbine Maintenance and Inspection	10.2.6
10.4-1	Circulating Water Supply	10.4.12.1
10.4-2	Condensate, Feedwater and Auxiliary Steam System Chemistry Control	10.4.12.2
10.4-3	Potable Water	10.4.12.3
11.2-1	Liquid Radwaste Processing by Mobile Equipment	11.2.4.1
11.2-2	Cost Benefit Analysis of Population Doses from Liquid Effluents	11.2.4.2
11.2-3	Identification of Ion Exchange and Adsorbent Media for Liquid Radwaste	11.2.4.3
11.2-4	Dilution and Control of Boric Acid Discharge	11.2.4.4
11.3-1	Cost Benefit Analysis of Population Doses from Gaseous Effluents	11.3.4.1
11.3-2	Identification of Adsorbent Media for Gaseous Radwaste	11.3.4.2
11.4-1	Solid Waste Management System Process Control Program	11.4.6
11.5-1	Plant Offsite Dose Calculation Manual (ODCM)	11.5.7
12.1-1	ALARA and Operational Policies	12.1.3
12.2-1	Additional Contained Radiation Sources	12.2.3
12.3-1	Administrative Controls, Criteria and Methods for Radiological Protection	12.3.5

core cooling monitor. The incore instrument assemblies house both fixed incore detectors and core exit thermocouples. The incore instrumentation system is described in subsection 4.4.6.1.

7.1.2 General Protection Subsystem Configuration

The protection and safety monitoring system is illustrated in Figure 7.1-2. The functions of the protection and safety monitoring system have been decomposed into physically and electrically separate microprocessor based subsystems. Each subsystem is located on an independent computer bus to prevent propagation of failures and to enhance availability. In most cases, each subsystem is implemented in a separate card chassis. Subsystem independence is maintained through the use of the following:

- Separate dc power sources with output protection to prevent interaction between subsystems upon failure of a subsystem.
- Separate input or output circuitry to maintain independence at the subsystem interfaces.
- Deadman signals: A device, circuit, or function that forces a predefined operating condition upon the cessation of a normally dynamic input parameter to improve the reliability of hard-wired data that crosses the subsystem interface.
- Optical coupling or resistor buffering between two subsystems or between a subsystem and an input/output (I/O) module.

WCAP-13382 (Reference 3) provides a description of the hardware elements which comprise the protection and safety monitoring system configuration. WCAP-14080 (Reference 9) provides a description of the software architecture and operation.

7.1.2.1 Functional Components

The type and number of boards used to implement the functions of a microprocessor based subsystem are purposely limited to aid serviceability and to restrict the number of spares. In addition, the basic function of a particular board remains fixed among subsystems to facilitate the development and maintenance of the subsystem software. IEEE 796 (Reference 2) bus cards are typically used to provide functions as listed below.

Functional Processor

The functional processor performs the major computations required to achieve the specific function of the microprocessor based subsystem. Tasks performed by the functional processor include movement of data between subsystem memories or I/O registers for the purpose of input or output, on-line compensation of the analog inputs, conversion of input data to engineering units, and diagnostic testing. A functional processor is included in each subsystem.

Table 1.6-1 (Sheet 11 of 15)

MATERIAL REFERENCED

SSAR Section Number	Westinghouse Topical Report Number	Title
6.2	WCAP-14382	WGOTHIC Code Description and Validation
	WCAP-8077 (P) WCAP-8078	Ice Condenser Containment Pressure Transient Analysis Methods
	WCAP-8264-P-A (P) WCAP-8312-A	Westinghouse Mass and Energy Release Data for Containment Design
	WCAP-10325 (P)	Westinghouse LOCA Mass and Energy Release Model for Containment Design - March 1979 Version
	WCAP-8822 (P) WCAP-8860	Mass and Energy Releases Following A Steam Line Rupture
	WCAP-7907-P-A (P) WCAP-7907-A	LOFTRAN Code Description
	WCAP-12945-P (P)	Code Qualification Document for Best Estimate Analysis
	WCAP-14407 (P) WCAP-14408	WGOTHIC Application to AP600
6.3	WCAP-8966	Evaluation of Mispositioned ECCS Valves
7.1	WCAP-13382 (P) WCAP-13391	AP600 Instrumentation and Control Hardware Description
	WCAP-13383 (P) WCAP-13392	AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report
	WCAP-8897 (P) WCAP-8898	Bypass Logic for the Westinghouse Integrated Protection System
7.2	WCAP-13594 (P) WCAP-13662	FMEA of Advanced Passive Plant Protection System
	WCAP-14605 (P) WCAP-14606 (NP)	Westinghouse Setpoint Methodology for Protection Systems - AP600
8.3	WCAP-13856	AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process
10.2	WCAP-11525	Probabilistic Evaluation of Reduction in Turbine Valve Test Frequency

(P) Denotes Document is Proprietary

Table 1.6-1 (Sheet 11 of 15)

MATERIAL REFERENCED

SSAR Section Number	Westinghouse Topical Report Number	Title
6.2	WCAP-14382	WGOTHIC Code Description and Validation
	WCAP-8077 (P) WCAP-8078	Ice Condenser Containment Pressure Transient Analysis Methods
	WCAP-8264-P-A (P) WCAP-8312-A	Westinghouse Mass and Energy Release Data for Containment Design
	WCAP-10325 (P)	Westinghouse LOCA Mass and Energy Release Model for Containment Design - March 1979 Version
	WCAP-8822 (P) WCAP-8860	Mass and Energy Releases Following A Steam Line Rupture
	WCAP-7907-P-A (P) WCAP-7907-A	LOFTRAN Code Description
	WCAP-12945-P (P)	Code Qualification Document for Best Estimate Analysis
	WCAP-14407 (P) WCAP-14408	WGOTHIC Application to AP600
6.3	WCAP-8966	Evaluation of Mispositioned ECCS Valves
7.1	WCAP-13382 (P) WCAP-13391	AP600 Instrumentation and Control Hardware Description
	WCAP-13383 (P) WCAP-13392	AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report
	WCAP-8897 (P) WCAP-8898	Bypass Logic for the Westinghouse Integrated Protection System
7.2	WCAP-13594 (P) WCAP-13662	FMEA of Advanced Passive Plant Protection System
8.3	WCAP-13856	AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process
10.2	WCAP-11525	Probabilistic Evaluation of Reduction in Turbine Valve Test Frequency
	WCAP-14080(P) WCAP-14081	AP600 Instrumentation and Control Software Architecture and Operation Description

(P) Denotes Document is Proprietary

Changes Reflecting Resolution of NRC PAM/ERG Comments

Table 7.5-5

Summary of Type B Variables

Function Monitored	Variable	Type/Category
Reactivity Control	Neutron flux	B1
	Control rod position	B3
	Boric acid concentration	B3
Reactor Coolant System Integrity	RCS pressure	B1
	RCS wide range T_{hot}	B1
	RCS wide range T_{cold}	B1
	Containment water level	B1
	Containment pressure	B1
Reactor Coolant Inventory Control	Pressurizer level	B1
	Pressurizer reference leg temperature	B1
	Pressurizer pressure	B1
	Reactor vessel - hot leg water level	B3
Reactor Core Cooling	Core exit temperature	B1
	RCS subcooling	B1
	RCS wide range T_{hot}	B2
	RCS wide range T_{cold}	B2
	RCS pressure	B2
	Reactor vessel - hot leg water level	B2
Heat Sink Maintenance	IRWST water level	B1
	PRHR flow	B1
	PRHR outlet temperature	B1
	PCS storage tank water level	B1
	Passive containment cooling water flow	B1
	IRWST to RNS suction valve status	B1
Containment Environment	Containment pressure	B1
	Remotely operated containment isolation valve ~~position~~ status	B1

Table 7.5-7 (Sheet 1 of 4)

Summary of Type D Variables

System	Variable	Type/Category
Reactivity Control System	Reactor trip breaker status	D2
	Control rod position	D3
Pressurizer Level and Pressure Control	Pressurizer safety valve status	D2
	Pressurizer level	D2
	RCS pressure	D2
	Pressurizer pressure	D2
	Reference leg temperature	D2
RCS Loops	RCS wide range T_{hot}	D2
	RCS wide range T_{cold}	D2
	RCP breaker status	D2
	RCP bearing water temperature	D2
Secondary Pressure and Level Control	Steam generator PORV status	D2
	Steam generator PORV block valve status	D2
	Steam generator safety valve status	D2
	Main feedwater isolation valve status	D2
	Steam generator level (wide range)	D2
	Steam generator level (narrow range)	D2
	Steam generator blowdown isolation valve status	D2

Table 7.5-7 (Sheet 2 of 4)

Summary of Type D Variables

System	Variable	Type/Category
Secondary Pressure and Level Control (continued)	Steam line pressure	D2
	Main feedwater pump status	D2
	Main feedwater control valve status	D2
	Main steam line isolation valve status	D2
	Main steam line isolation bypass valve status	D2
Startup Feedwater	Startup feedwater flow	D2
	Startup feedwater control valve status	D2
	Startup feedwater isolation valve status	D2
	Main to startup feedwater crossover valve status	D2
Safeguards	Containment pressure	D2
	Accumulator level	D2
	Core makeup tank level	D2
	IRWST line isolation ~~to reactor vessel~~ valve status (MOV)	D3
	IRWST injection isolation ~~to reactor vessel~~ valve status (~~non-MOV~~ squib)	D2
	ADS first stage, second stage and third stage valve status	D2
	ADS fourth stage valve status (MOV)	D2
	ADS fourth stage valve status (non-MOV)	D2
	PRHR heat exchanger inlet isolation valve status	D3
	PRHR heat exchanger control ~~discharge isolation~~ valve status	D2
	Reactor vessel head vent valve status	D2
	CMT discharge isolation ~~to reactor vessel~~ valve status	D2
	CMT inlet isolation valve status	D2
	Accumulator isolation ~~to reactor vessel~~ valve status	D3

Table 7.5-7 (Sheet 4 of 4)

Summary of Type D Variables

System	Variable	Type/Category
Containment Cooling	Containment temperature	D2
	PCS water storage tank series isolation ~~to containment~~ valve status (MOV)	D2
	PCS water storage tank isolation ~~to containment~~ valve status (non-MOV)	D2
	Passive containment cooling water flow	D2
	PCS storage tank water level	D2
HVAC System Status	MCR return air isolation damper status	D2
	MCR toilet exhaust isolation damper status	D2
	MCR supply air isolation damper status	D2
	MCR air delivery isolation valve status	D2
	MCR air storage bottle pressure	D2
	MCR supply air radiation level	D2
Main Steam	Turbine stop valve status	D2
	Turbine control valve position	D2
	Condenser steam dump valve status	D2

Table 7.5-9 (Sheet 2 of 4)

Summary of Type F Variables

Variable	Type/Category
Startup feedwater control valve status	F3
Main feedwater flow	F3
Steam generator level (WR)	F3
Steam flow	F3
Main steam line isolation valve status	F3
Main feedwater pump status	F3
Startup feedwater pump status	F3
Condenser steam dump valve status	F3
Condensate storage tank level	F3
Pressurizer spray - cold leg to pressurizer valve status	F3
Auxiliary spray line isolation valve status	F3
Makeup flow	F3
Makeup pump status	F3
Letdown flow	F3
Circulating water pump breaker status	F3
Condenser backpressure	F3
Accumulator vent valve status	F3

Table 7.5-9 (Sheet 3 of 4)

Summary of Type F Variables

Variable	Type/Category
Boric acid tank level	F3
Boric acid flow	F3
Makeup ~~pump suction header~~ blend valve status	F3
Makeup flow control valve status	F3
RNS flow	F3
IRWST to RNS suction valve status	F3
RNS discharge to IRWST valve status	F3
CCS surge tank level	F3
CCS flow	F3
CCS pump status	F3
CCS flow to RNS valve status	F3
CCS flow to RCPs valve status	F3
CCS heat exchanger inlet temperature	F3
CCS heat exchanger outlet temperature	F3
Diesel generator status	F3
Containment fan cooler status	F3
Chilled water pump status	F3
Chilled water valve status	F3
Containment temperature	F3
Main control room supply air isolation damper status	F3
Main control room return air isolation damper status	F3
Main control room supply air radiation	F3
Service water flow	F3
Diesel generator load	F3
Voltage for diesel-backed buses	F3
Power supply to diesel-backed buses	F3
RNS pump status	F3

Table 7.5-9 (Sheet 4 of 4)

Summary of Type F Variables

Variable	Type/Category
Service water pump status	F3
Service water pump discharge valve status	F3
Service water pump discharge temperature	F3
Instrument air header pressure	F3
Spent fuel pool pump flow	F3
Spent fuel pool temperature	F3
Spent fuel pool water level	F3
Main to startup feedwater crossover valve status	F3
~~Gutter to containment sump valve status~~ IRWST gutter bypass isolation valve status	F3

Additional information on these process variables ~~A description of the process sensors~~ is included as part of the description of each process system provided in other chapters. The process variables measured by the protection and safety monitoring system are listed in Sections 7.2, 7.3, and 7.5.

7.1.2.8.2 Nuclear Instrumentation Detectors

Three types of neutron detectors are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The power range channels are capable of measuring overpower excursions up to 200 percent of full power.

The lowest range (source range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This generally is greater than two counts per second. The next range (intermediate range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps the higher portion of the intermediate range. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. Detector types for these three ranges are:

- Source range - proportional counter
- Intermediate range - pulse fission chamber
- Power range - uncompensated ionization chamber

7.1.2.8.3 Equipment Status Inputs

Some inputs to the protection system are not measurements of process or nuclear variables, but are discrete indications of the status of certain equipment. Examples include manual switch positions, contact status inputs, and indications provided by valve limit switches.

7.1.2.9 Intercabinet Communications

Integrated Protection Cabinet to Integrated Protection Cabinet

Isolated fiber-optic data links are used for these communications links. The global trip subsystem in each integrated protection cabinet controls this communication link. These are standard one-way (simplex) communications used to transmit bistable trip status between integrated protection cabinets for use in two-out-of-four reactor trip logic.

Integrated Protection Cabinet to Engineered Safety Features Actuation Cabinet

Isolated fiber-optic data links in each integrated protection cabinet transmit bistable trip outputs to the engineered safety features actuation cabinet for use in engineered safety features actuation logic. These data links are one-way links that only transmit data to the engineered safety features actuation cabinets.

Changes for Auxiliary Spray and CVS Letdown

Condition 2 consists of the manual actuation of either of two momentary controls in the main control room. Either control actuates all divisions and closes the nonessential fluid system paths from the containment.

Manual reset is provided to block the automatic actuation signal for containment isolation. Separate momentary controls are provided for resetting each division.

No other interlocks or permissive signals apply directly to the containment isolation function. Automatic actuation originates from a safeguards actuation (S) signal that does contain interlock and permissive inputs.

The functional logic that actuates containment isolation is illustrated in Figure 7.2-1, sheets 11 and 13.

7.3.1.2.2 In-Containment Refueling Water Storage Tank Injection

Signals to align the in-containment refueling water storage tank for injection are generated from the following conditions:

1. Actuation of the fourth stage of the automatic depressurization system (subsection 7.3.1.2.4)

2. Coincidence loop 1 and loop 2 hot leg levels below low-2 setpoint for a duration exceeding an adjustable time delay

3. Manual initiation

Each of the above conditions opens the in-containment refueling water storage tank injection valves, thereby providing a flow path to the reactor coolant system.

Condition 3 consists of two sets of two momentary controls. Manual actuation of both controls of either of the two control sets generates signals that open the in-containment refueling water storage tank injection valves. A two-control simultaneous actuation prevents inadvertent actuation.

No interlocks or permissive signals apply directly to the injection valves of the in-containment refueling water storage tank.

The functional logic relating to in-containment refueling water storage tank injection is illustrated in Figure 7.2-1, sheet 16.

Condition 1 results from a coincidence of two of the four divisions of reactor loop average temperature (T_{avg}) below the Low-2 setpoint coincident with the P-4 permissive (reactor trip). This blocks the opening of the steam dump valves. This signal also becomes an input to the steam dump interlock selector switch for unblocking the steam dump valves used for plant cooldown. This function may be manually blocked when the pressurizer pressure is below the P-11 setpoint. The block is automatically removed when the pressurizer pressure is above the P-11 setpoint.

Condition 2 consists of two controls. Either one of these controls can be used to manually initiate a steam dump block.

The functional logic relating to the steam dump block is illustrated in Figure 7.2-1, sheet 10.

7.3.1.2.17 Control Room Isolation and Air Supply Initiation

Signals to initiate isolation of the main control room and to initiate the air supply are generated from either of the following conditions:

1. High control room air supply radioactivity level
2. Loss of ac power sources

Condition 1 is the occurrence one of two control room air supply radioactivity monitors detecting a radioactivity level above the High-2 setpoint.

Condition 2 results from the loss of all ac power sources. A preset time delay is provided to permit the restoration of ac power from the offsite sources or from the onsite diesel generators before initiation. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by each of the two sensors connected to two of the four battery chargers. The two-out-of-four logic is based on an-undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

The functional logic relating to control room isolation and air supply initiation is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.18 Auxiliary Spray and Letdown Purification Line Isolation

A signal to isolate the auxiliary spray and letdown purification lines is generated upon the coincidence of pressurizer level below the Low-1 setpoint in any two of four divisions. This helps to maintain reactor coolant system inventory. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 12.

7.3.1.2.19 Containment Air Filtration System Isolation

A signal to isolate the containment air filtration system is generated upon the coincidence of containment radioactivity above the High-1 setpoint in any two of four divisions. This limits activity release to the environment. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.20 Normal Residual Heat Removal System Isolation

A signal for isolating the normal residual heat removal system lines is generated upon the coincidence of containment radioactivity above the High-2 setpoint in any two of four divisions. This signal also isolates the chemical and volume control system as discussed in subsection 7.3.1.2.15. This limits activity release to the environment. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.21 Spent Fuel Pool Isolation

A signal for isolating the spent fuel pool lines is generated upon the coincidence of spent fuel pool level below the Low setpoint in any one of two divisions. This helps to maintain the water inventory in the spent fuel pool due to line leakage. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

[ADD INSERT 7.3.1.2.22]

7.3.1.3 Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation

The interlocks used for engineered safety features actuation are designated as "P-xx" permissives and are listed in Table 7.3-2.

7.3.1.4 Bypasses of Engineered Safety Features Actuations

The channels used in engineered safety features actuation that can be manually bypassed are indicated in Table 7.3-1. A description of this bypass capability is provided in subsection 7.1.2.10. The actuation logic is not bypassed for test. During tests, the actuation logic is fully tested by blocking the actuation logic output before it results in component actuations.

7.3.1.5 Design Basis for Engineered Safety Features Actuation

The following subsections provide the design bases information for engineered safety features actuation, including the information required by Section 3 of IEEE 279-1971. Engineered safety features are initiated by the protection and safety monitoring system. Those design bases relating to the equipment that initiates and accomplishes engineered safety features are given in subsection 7.1.4.1. The design bases presented here concern the variables monitored for engineered safety features actuation and the minimum performance requirements in generating the actuation signals.

[INSERT 7.3.1.1.22]

7.3.1.2.22 Chemical and Volume Control System Letdown Isolation

A signal to isolate the letdown valves of the chemical and volume control system is generated upon the occurrence of a low-1 hot leg level in either of the two hot leg loops. This helps to maintain reactor system inventory. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 16. These letdown valves are also closed by the containment isolation function as described in subsection 7.3.1.2.1.

Table 7.3-1 (Sheet 7 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
16. Main Control Room Isolation and Air Supply Initiation (Figure 7.2-1, Sheet 13)			
a. High-2 control room supply air radiation	2	1/2	None
b. Undervoltage to Class 1E battery chargers	2/charger	2/2 per charger and 2/4 chargers[5]	None
17. Auxiliary Spray and Purification Line Isolation (Figure 7.2-1, Sheet 12)			
a. Low-1 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12. Automatically unblocked above P-12.
18. Containment Air Filtration System Isolation (Figure 7.2-1, Sheet 13)			
a. High-1 containment radioactivity	4	2/4-BYP[1]	None
19. Normal Residual Heat Removal System Isolation (Figure 7.2-1, Sheet 13)			
a. High-2 containment radioactivity	4	2/4-BYP[1]	None
20. Spent Fuel Pool Isolation (Figure 7.2-1, Sheet 13)			
a. Low spent fuel pool level	2	1/2	None
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves (Figure 7.2-1, Sheet 16)			
a. Automatic reactor coolant system depressurization (fourth stage)	(See items 3d and 3e)		
b. Coincident loop 1 and loop 2 ~~low~~ hot leg level low-2 (after delay)	1 per loop	2/2	None
c. Manual initiation	4 switches	2/4 switches[3]	None
22. Open IRWST Containment Recirculation Valves In Series with Check Valves (Figure 7.2-1, Sheet 15)			
a. Extended undervoltage to Class 1E battery chargers	2/charger	1/2 per charger and 2/4 chargers	None

Table 7.3-1 (Sheet 8 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
23. Open All IRWST Containment Recirculation Valves (Figure 7.2-1, Sheet 16)			
b. Safeguards actuation signal (automatic or manual) coincident with		(See items 1a through 1e)	
Low IRWST level (Low-3 setpoint)	4	2/4 BYP[1]	None
c. Manual initiation	4 switches	2/4 switches	None
24. Chemical and Volume Control System Letdown Isolation (Figure 7.2-1, Sheet 16)			
a. Low-1 hot leg level	1 per loop	1/2	None

Notes:

1. 2/4-BYP indicates automatic bypass logic. The logic is 2 out of 4 with no bypasses; 2 out of 3 with one bypass; 1 out of 2 with two bypasses; and, automatically actuated with three or four bypasses.

2. Any two channels from either tank not in same division.

3. Two switches must be actuated simultaneously.

4. Also, closes power-operated relief block valve of respective steam generator.

5. The two-out-of-four logic is based on undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

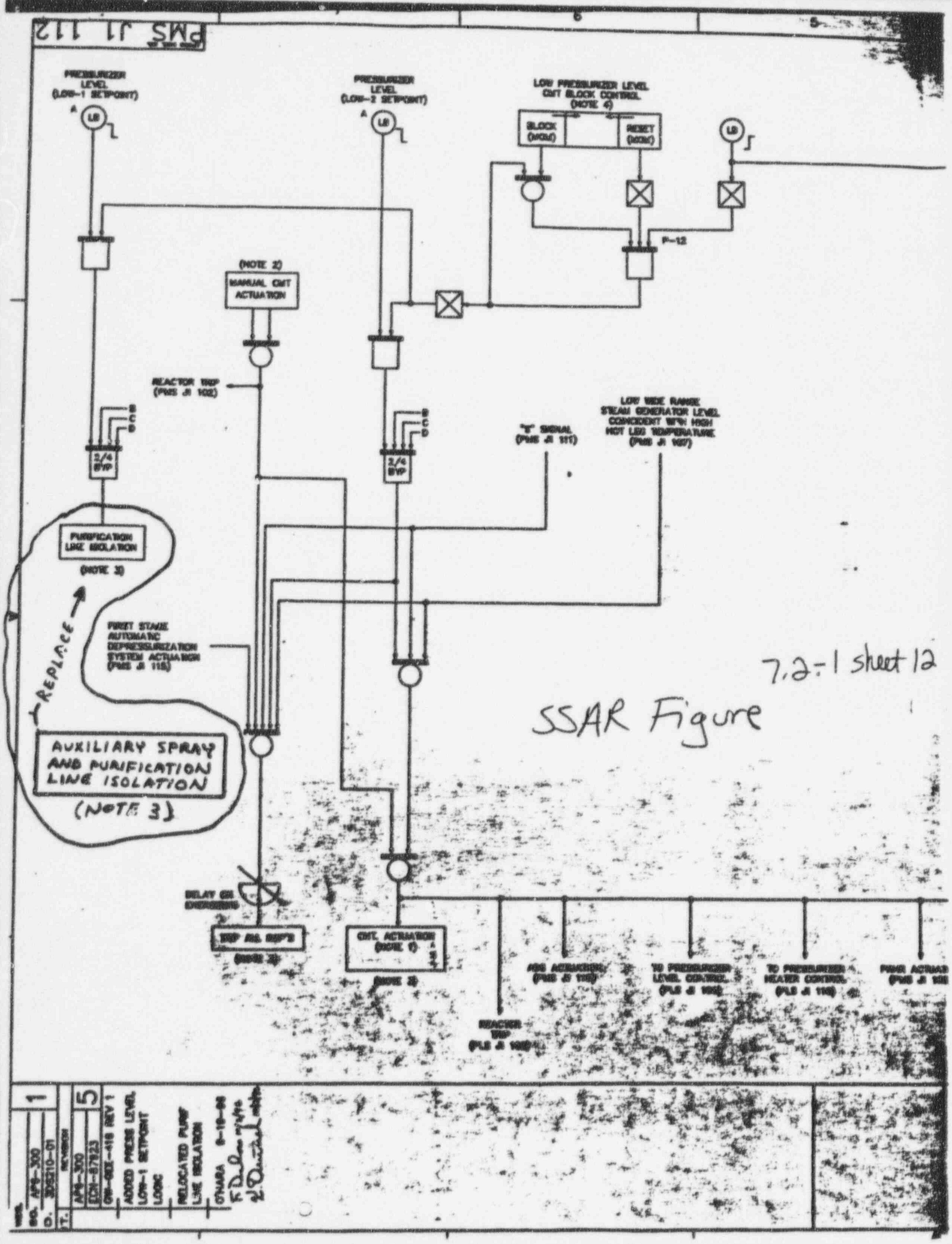
6. Any two channels from either loop not in same division.

7. Any two channels from either line not in same division.

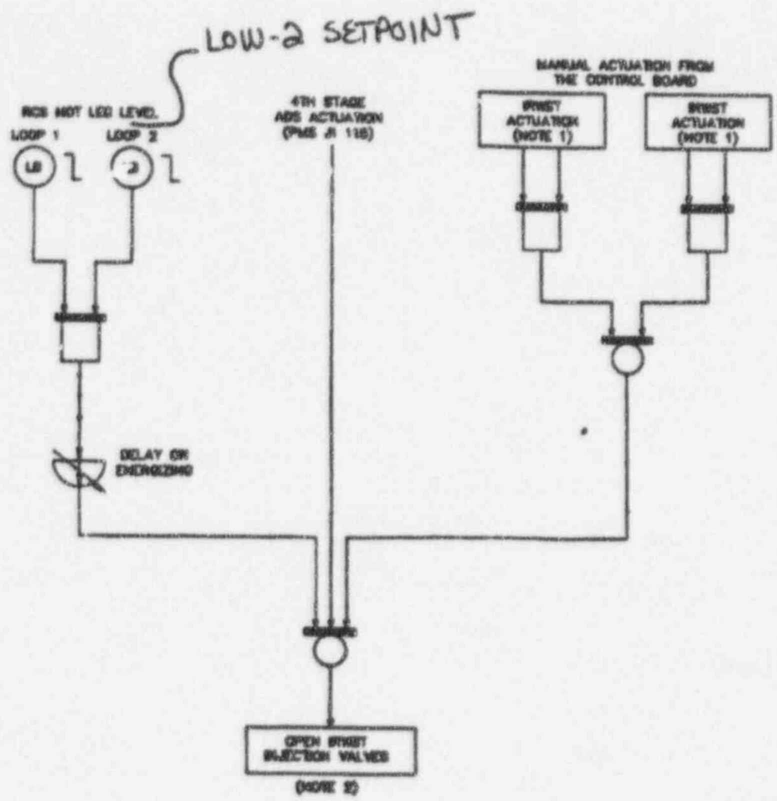
Table 7.3-2 (Sheet 3 of 3)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

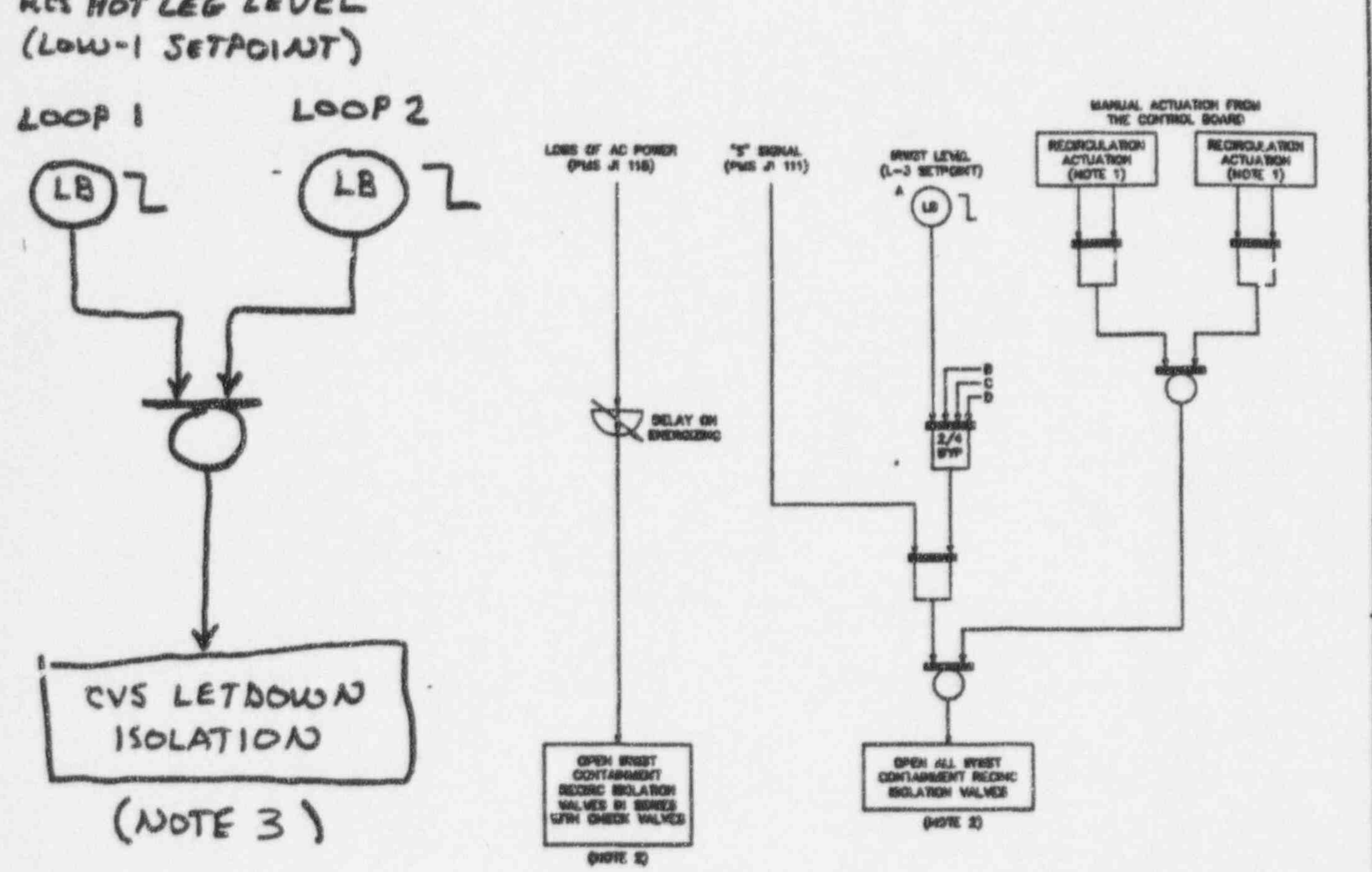
Designation	Derivation	Function
P-12	Pressurizer level below setpoint	(a) Permits manual block of core makeup tank actuation on low pressurizer level to allow mid-loop operation (b) Permits manual block of reactor coolant pump trip on low pressurizer level to allow mid-loop operation (c) Permits manual block of auxiliary spray and purification line isolation on low pressurizer level to allow mid-loop operation
$\overline{\text{P-12}}$	Pressurizer level above setpoint	(a) Prevents manual block of core makeup tank actuation on low pressurizer level (b) Prevents manual block of reactor coolant pump trip on low pressurizer level (c) Prevents manual block of auxiliary spray and purification line isolation on low pressurizer level (d) Provides confirmatory open signal to the core makeup tank cold leg balance lines



PMS J1 112
PRESSURIZER LEVEL (LOW-1 SETPOINT)
PRESSURIZER LEVEL (LOW-2 SETPOINT)
LOW PRESSURIZER LEVEL CMT BLOCK CONTROL (NOTE 4)
BLOCK
RESET
P-12
(NOTE 2)
MANUAL CMT ACTUATION
REACTOR TRIP (PMS J1 102)
2/4 BYP
"S" SIGNAL (PMS J1 111)
LOW WIDE RANGE STEAM GENERATOR LEVEL COINCIDENT WITH HIGH HOT LEG TEMPERATURE (PMS J1 107)
PURIFICATION LINE ISOLATION
(NOTE 3)
REPLACE
FIRST STAGE AUTOMATIC DEPRESSURIZATION SYSTEM ACTUATION (PMS J1 115)
AUXILIARY SPRAY AND PURIFICATION LINE ISOLATION
(NOTE 3)
7.2-1 sheet 12
SSAR Figure
CMT ACTUATION (NOTE 1)
ADS ACTUATION (PMS J1 115)
TO PRESSURIZER LEVEL CONTROL
TO PRESSURIZER HEATER CONTROL
REACTOR TRIP



SSAR Figure 7.2-1
Sheet 16



SSAR
Figure 7.2-1 sheet 16

NOTES:

1. THE MANUAL ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL DIVISIONS.

2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.

~~3. THE MANUAL RESET CONSISTS OF SEPARATE MOMENTARY CONTROLS. OPERATING EACH CONTROL WILL RESET A SEPARATE DIVISION.~~

3. CVS LETDOWN ISOLATION ALSO OCCURS DURING CONTAINMENT ISOLATION. SEE PMS J1 113.

Westinghouse Electric Corporation

AP600
ADVANCED PASSIVE LIGHT WATER REACTOR

ADVANCED CAD TECHNOLOGY
0177C018

R. O'HARA

Westinghouse Electric Corporation
ADVANCED TECHNOLOGY BUSINESS AREA

5D63525

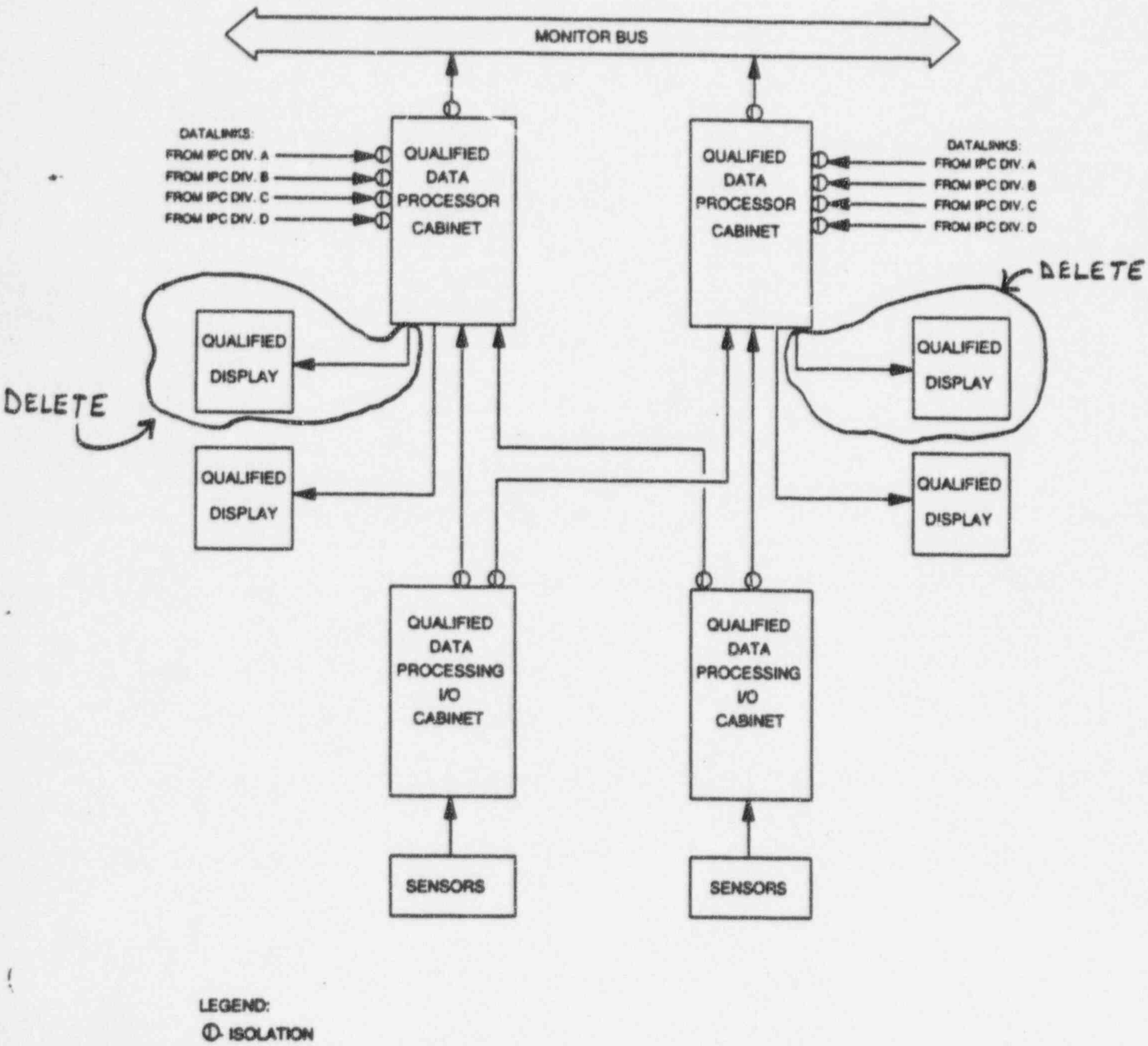
AP600 FUNCTIONAL DIAGRAMS
IRWST ACTUATIONS

D PMS J1 116 [illegible] 3

288064

33

Changes Reflecting Resolution of NRC Minimum Inventory (Remote Shutdown Workstation) Comments



CHANGE 3 SSAR MARKUP,
PAGE 3 OF 6

Figure 7.1-8

Qualified Data Processor

Condition 3 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator.

The functional logic relating to the tripping of the turbine is illustrated in Figure 7.2-1, sheet 14.

7.3.1.2.9 In-Containment Refueling Water Storage Tank Containment Recirculation

Signals to align the in-containment refueling water storage tank containment recirculation isolation valves are generated from the following conditions:

1. Automatic or manual safeguards actuation (subsection 7.3.1.1) in coincidence with low in-containment refueling water storage tank water level

2. Manual initiation

3. Extended loss of ac power sources

There are four parallel containment recirculation paths provided to permit the recirculation of the water provided by the in-containment refueling water storage tank. Two of these paths are provided with two isolation valves in series while the remaining two paths are provided with a single isolation valve in series with a check valve.

Conditions 1 and 2 result in the opening of all isolation valves in all four parallel paths. Condition 3 results in the opening of the two isolation valves that are in series with the check valves.

Condition 1 results from the coincidence of two of the four divisions of in-containment refueling water storage tank water level below the Low-3 setpoint, coincident with an automatic or manual safeguards actuation.

Condition 2 consists of two sets of two momentary controls. Manual actuation of both controls of either of the two control sets initiates recirculation in all four parallel paths. A two-control simultaneous actuation prevents inadvertent actuation.

Condition 3 results from the loss of all ac power for a period of time that approaches the 24-hour Class 1E dc battery capability to activate the in-containment refueling water storage tank containment recirculation isolation valves. The timed output holds on restoration of ac power and is manually reset after the batteries are recharged. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by either of the two sensors connected to two of the four battery chargers.

[INSERT 7.3.1.2.9]

No interlocks or permissive signals apply directly to the activation of the in-containment refueling water storage tank containment recirculation isolation valves. However, automatic

[INSERT 7.3.1.2.9]

The safeguards actuation signal, which is part of condition 1, is latched-in upon its occurrence. A deliberate operator action is required to reset this latch. This feature is provided so that the actuation signal to the recirculation isolation valves is not cleared by the reset of the safeguards actuation signal as discussed in subsection 7.3.1.1.

Condition 1 results from a coincidence of two of the four divisions of reactor loop average temperature (T_{avg}) below the Low-2 setpoint coincident with the P-4 permissive (reactor trip). This blocks the opening of the steam dump valves. This signal also becomes an input to the steam dump interlock selector switch for unblocking the steam dump valves used for plant cooldown. This function may be manually blocked when the pressurizer pressure is below the P-11 setpoint. The block is automatically removed when the pressurizer pressure is above the P-11 setpoint.

Condition 2 consists of two controls. Either one of these controls can be used to manually initiate a steam dump block.

The functional logic relating to the steam dump block is illustrated in Figure 7.2-1, sheet 10.

7.3.1.2.17 Control Room Isolation and Air Supply Initiation

Signals to initiate isolation of the main control room and to initiate the air supply are generated from either of the following conditions:

1. High control room air supply radioactivity level
2. Loss of ac power sources
3. Manual initiation

Condition 1 is the occurrence one of two control room air supply radioactivity monitors detecting a radioactivity level above the High-2 setpoint.

Condition 2 results from the loss of all ac power sources. A preset time delay is provided to permit the restoration of ac power from the offsite sources or from the onsite diesel generators before initiation. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by each of the two sensors connected to two of the four battery chargers. The two-out-of-four logic is based on an undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

[INSERT 7.3.1.2.17]

The functional logic relating to control room isolation and air supply initiation is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.18 Letdown Purification Line Isolation

A signal to isolate the letdown purification line is generated upon the coincidence of pressurizer level below the Low-1 setpoint in any two of four divisions. This helps to maintain reactor coolant system inventory. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 12.

[INSERT 7.3.1.2.17]

Condition 3 consists of two momentary controls. Manual actuation of either of the two controls will result in control room isolation and air supply initiation.

Table 7.3-1 (Sheet 7 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
16. Main Control Room Isolation and Air Supply Initiation (Figure 7.2-1, Sheet 13)			
a. High-2 control room supply air radiation	2	1/2	None
b. Undervoltage to Class 1E battery chargers	2/charger	2/2 per charger and 2/4 chargers[5]	None
c. Manual initiation	2 switches	1/2 switches	None
17. Purification Line Isolation (Figure 7.2-1, Sheet 12)			
a. Low-1 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12. Automatically unblocked above P-12.
18. Containment Air Filtration System Isolation (Figure 7.2-1, Sheet 13)			
a. High-1 containment radioactivity	4	2/4-BYP[1]	None
19. Normal Residual Heat Removal System Isolation (Figure 7.2-1, Sheet 13)			
a. High-2 containment radioactivity	4	2/4-BYP[1]	None
20. Spent Fuel Pool Isolation (Figure 7.2-1, Sheet 13)			
a. Low spent fuel pool level	2	1/2	None
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves (Figure 7.2-1, Sheet 16)			
a. Automatic reactor coolant system depressurization (fourth stage)	(See items 3d and 3e)		
b. Coincident loop 1 and loop 2 low hot leg level (after delay)	1 per loop	2/2	None
c. Manual initiation	4 switches	2/4 switches[3]	None
22. Open IRWST Containment Recirculation Valves In Series with Check Valves (Figure 7.2-1, Sheet 15)			
a. Extended undervoltage to Class 1E battery chargers	2/charger	1/2 per charger and 2/4 chargers	None

Table 7.3-3

SYSTEM-LEVEL MANUAL INPUT TO THE
ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Manual Control	To Divisions	Figure 7.2-1 Sheet
Manual safeguards actuation #1	A B C D	2 & 11
Manual safeguards actuation #2	A B C D	2 & 11
Manual passive residual heat removal actuation #1	A B	8
Manual passive residual heat removal actuation #2	A B	8
Manual steam line isolation #1	B D	9
Manual steam line isolation #2	B D	9
Steam/feedwater isolation and safeguards block control #1	B	9
Steam/feedwater isolation and safeguards block control #2	D	9
Manual feedwater isolation #1	B D	10
Manual feedwater isolation #2	B D	10
Manual steam dump interlock selector #1	B	10
Manual steam dump interlock selector #2	D	10
Pressurizer pressure safeguards block control #1	A	11
Pressurizer pressure safeguards block control #2	B	11
Pressurizer pressure safeguards block control #3	C	11
Pressurizer pressure safeguards block control #4	D	11
Manual core makeup tank actuation #1	A B C D	12
Manual core makeup tank actuation #2	A B C D	12
Core makeup tank actuation block control #1	A	12
Core makeup tank actuation block control #2	B	12
Core makeup tank actuation block control #3	C	12
Core makeup tank actuation block control #4	D	12
Manual containment cooling actuation #1 & #2	A B	13
Manual containment cooling actuation #3 & #4	A B	13
Manual containment isolation actuation #1	A B C D	13
Manual containment isolation actuation #2	A B C D	13
Manual depressurization system stages 1, 2, and 3 actuation #1 & #2	A B C D	15
Manual depressurization system stages 1, 2, and 3 actuation #3 & #4	A B C D	15
Manual depressurization system stage 4 actuation #1 & #2	A B C D	15
Manual depressurization system stage 4 actuation #3 & #4	A B C D	15
Manual IRWST actuation #1 & #2	A B C D	16
Manual IRWST actuation #3 & #4	A B C D	16
Manual containment recirculation actuation #1 & #2	A B C D	16
Manual containment recirculation actuation #3 & #4	A B C D	16
Manual control room isolation and air supply initiation #1	ABCD	13
Manual control room isolation and air supply initiation #2	ABCD	13

The design basis for the remote shutdown workstation does not require the installation of safety related, dedicated, fixed-position displays, alarms, and controls. The remote shutdown workstation has the same capabilities as the reactor operator's workstation in the main control room.

One remote shutdown workstation is provided. The remote shutdown workstation contains controls displays, and alarms for the safety-related equipment required to establish and maintain safe shutdown. Additionally, control of nonsafety-related components is available, allowing operation and control when ac power is available. ~~The remote shutdown workstation also receives inputs from the qualified data processing system for indication, similar to the main control room.~~

The controls, displays and alarms listed in Table 18.12.2-1 are retrievable from the remote shutdown workstation. Subsection 18.12.3 provides more discussion on the remote shutdown workstation displays, alarms, and controls.

The remote shutdown workstation is provided for use only following an evacuation of the main control room. No actions are anticipated from the remote shutdown workstation during normal, routine shutdown, refueling, or maintenance operations.

The remote shutdown workstation has sufficient communication circuits to allow the operator to effectively establish safe shutdown conditions. As detailed in subsection 9.5.2, communication is available between the following stations:

- Main control room
- Remote shutdown workstation
- Onsite technical support center
- Diesel generator local control station

Operator control capability at the remote shutdown workstation is normally disabled, and operator control functions are normally performed from workstations located inside the main control room; however, operator control capability can be transferred from the main control room workstations to the remote workstation if the control room requires evacuation. This operator control transfer capability can not be disabled by any single active failure coincident with the loss of offsite power.

The control transfer function is implemented by multiple transfer switches. Each individual transfer switch is associated with only a single safety-related or single nonsafety-related division. These switches are located behind an unlocked access panel. Entry into this access panel will result in alarms at the main control room and remote shutdown workstation. The access panel is located within a fire zone which is separate from the main control room. Actuation of these transfer switches results in additional alarms at the main control room and remote shutdown workstation, the activation of operator control capability from the remote workstation, and the deactivation of operator control capability from the main control room workstations. The ~~safety-related and nonsafety-related~~ operator displays located in the main control room and on the remote shutdown workstation are not affected by this control transfer function.

7.4.3.1.2 Controls at Other Locations

In addition to the controls and indicators provided at the remote shutdown workstation, the following controls are provided outside the main control room:

- Reactor trip capability at the reactor trip switchgear
- Turbine trip capability at the turbine

- Start/stop controls for the diesel generators, located at each diesel generator local control panel

7.4.3.1.3 Design Bases Information

According to GDC 19, the capability of establishing a shutdown condition and maintaining the station in a safe status in that mode is an essential function. The controls and indications necessary for this function are identified in subsection 7.4.2. To provide the availability of the remote shutdown workstation after control room evacuation, the following design features are provided:

- The remote shutdown workstation conforms with the guidelines provided by ANSI 58.6 1983 (Reference 1).

- ~~The remote shutdown workstation, including the safety-related controls and indications, is designed to withstand the safe shutdown earthquake with no loss of essential functions.~~

- The remote shutdown workstation achieves and maintains safe shutdown conditions from full power conditions and maintains safe shutdown conditions thereafter.

- The remote shutdown workstation achieves safe shutdown when offsite power is available and when offsite power is not available.

- The remote shutdown workstation operates safety-related systems, independent from the main control room.

- The remote shutdown workstation is designed for a single failure. When a random event, such as a fire, or an allowable technical specification maintenance results in one safety-related division being unavailable, a single failure in a redundant division is not postulated. When a random event other than fire causes a main control room evacuation, a coincident single failure in the systems controlled from the remote shutdown panel is considered.

- Access to the remote shutdown workstation is under administrative control.

7.4.3.2 Analysis

The analysis of the systems required for safe shutdown is provided in subsection 7.4.1. The following discussion is limited to the remote shutdown workstation.

Conformance to NRC General Design Criteria

General Design Criterion 19 - The remote shutdown workstation provides adequate controls and indications located outside the main control room to establish and maintain the reactor

and the reactor coolant system in a safe shutdown condition in the event that the main control room must be evacuated.

Conformance to NRC Regulatory Guides

Regulatory Guide 1.22 - The remote shutdown workstation is tested periodically during station operation.

Regulatory Guide 1.29 - The remote shutdown workstation is designed to withstand the effects of a safe shutdown earthquake without loss of function or physical damage. The remote shutdown workstation is classified as seismic Category I. Selected instrumentation and control devices are not safety-related but are as seismic Category II to prevent compromising the function of safety-related devices during or after a safe shutdown earthquake.

Conformance to IEEE 279-1971

which perform the control transfer function

The remote shutdown workstation and the design features which provide for the transfer of control capability from the main control room to the remote shutdown workstation conforms to applicable portions of IEEE 279-1971. The control circuits at the remote shutdown workstation are designed so that a single failure does not prevent maintaining safe shutdown. This is accomplished by redundant controls for the systems required for safe shutdown, using independent safety-related power divisions.

components in

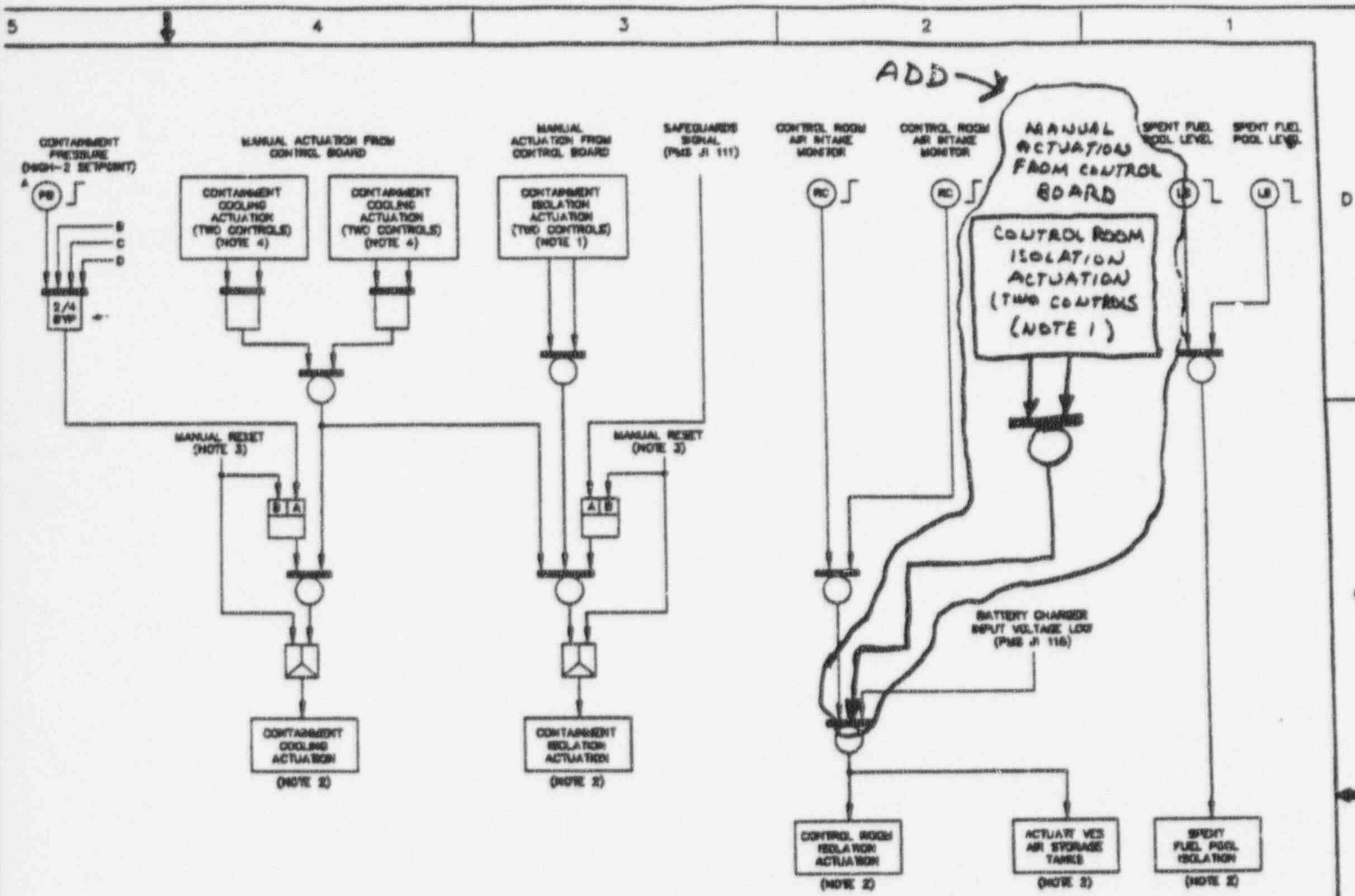
To prevent interaction between the redundant systems, the redundant control channels are wired independently and are separated from each other. Nonsafety-related circuits available for (but not required for) safe shutdown are electrically isolated from safety-related circuits.

7.4.4 Combined License Information

This section has no requirement for information to be provided in support of the Combined License application.

7.4.5 References

1. ANSI 58.6 1983, "Criteria for Remote Shutdown for Light Water Reactors."



NOTES:

1. TWO MOMENTARY CONTROLS ON THE CONTROL BOARD. OPERATING EITHER CONTROL WILL ACTUATE ALL DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. SEPARATE MOMENTARY CONTROLS ON THE CONTROL BOARD, ONE PER EACH DIVISION.
4. THE MANUAL CONTAINMENT COOLING ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL DIVISIONS.
5. TWO MOMENTARY CONTROLS ON THE CONTROL BOARD. OPERATING EITHER CONTROL WILL CAUSE THE REACTOR TRIP FUNCTION TO BE ACTUATED IN EACH OF THE FOUR DIVISIONS.

Westinghouse Electric Corporation

AP600
ADVANCED PASSIVE LIGHT WATER REACTOR

ADVANCED CAD TECHNOLOGY
0177ED13

PAC/BPO

Westinghouse Electric Corporation
ADVANCED TECHNOLOGY BUSINESS AREA

5D63525

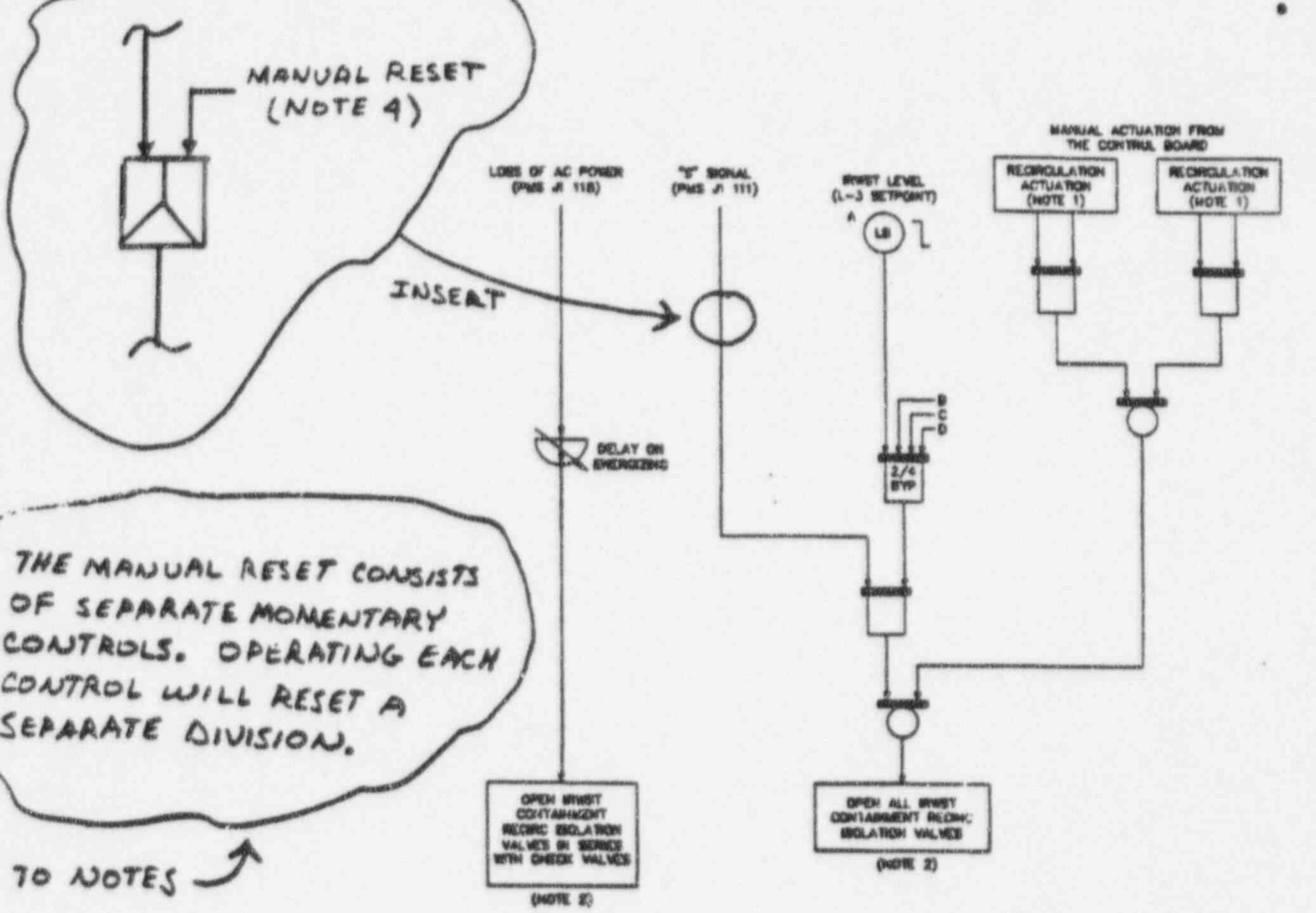
AP600 FUNCTIONAL DIAGRAMS
CONTAINMENT PROTECTION AND
OTHER PROTECTION

DPMS J1 113 5

332038 13

DG[illegible] 50883

SSAR Figure 7.2-1, Sheet 13



4. THE MANUAL RESET CONSISTS OF SEPARATE MOMENTARY CONTROLS. OPERATING EACH CONTROL WILL RESET A SEPARATE DIVISION.

ADD TO NOTES

NOTES:

1. THE MANUAL ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. ~~THE MANUAL RESET CONSISTS OF SEPARATE MOMENTARY CONTROLS. OPERATING EACH CONTROL WILL RESET A SEPARATE DIVISION.~~
3. CVS LETDOWN ISOLATION ALSO OCCURS DURING CONTAINMENT ISOLATION. SEE PMS J1 113.

ADVANCED CAD TECHNOLOGY
0177C016

Westinghouse Electric Corporation

AP600
ADVANCED PASSIVE LIGHT WATER REACTOR

Westinghouse Electric Corporation
ADVANCED TECHNOLOGY BUSINESS AREA

5D63525

AP600 FUNCTIONAL DIAGRAMS
IRWST ACTUATIONS

R. OCHARA

DPMS J1 116 3

288064

33

Changes Reflecting Resolution of NRC Post-72 Hour Position

The protection and safety monitoring system provides signal conditioning, communications, and display functions for Category 1 variables and for Category 2 variables that are energized from the Class 1E dc uninterruptible power supply system. The plant control system and the data display and processing system provides signal conditioning, communications and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E dc uninterruptible power system. The data display and processing system also provides an alternate display of the variables which are displayed by the protection and safety monitoring system. Electrical separation of the data display and processing system and the protection and safety monitoring system is maintained through the use of isolation devices in the data links connecting the two systems, as discussed in subsection 7.1.2.11. The portion of the protection and safety monitoring system which is dedicated to providing the safety-related display function is referred to as the qualified data processing cabinets. These cabinets are discussed in subsection 7.1.2.6 and are illustrated in Figure 7.1-8.

The qualified data processing cabinets are divided into two separate electrical divisions. Each of the two electrical divisions is connected to a Class 1E dc uninterruptible power system with sufficient battery capacity to provide necessary electrical power for at least 72 hours. If all ac power sources are lost for a period of time that exceeds 72 hours, the power supply system will be energized from ac power sources which are brought to the site from other locations. See Section 8.3.

the ancillary diesel generators or from

Instrumentation associated with primary variables that are energized from the Class 1E dc uninterruptible power supply system are powered from one of the two electrical divisions with 72 hour battery capacity. Instrumentation associated with other variables that are energized from the Class 1E dc uninterruptible power supply system are powered from one of four electrical divisions with 24 hour battery capacity. If a variable exists only to provide a backup to a primary variable, it may be powered by an electrical division with a 24 hour battery capacity. In such cases, provisions are provided to enable this variable to be powered by an alternate source if it is needed to resolve a discrepancy between two primary variables in the event that all ac power sources are lost for a period in excess of 24 hours.

Class 1E position indication signals for valves and electrical breakers may be powered by an electrical division with 24 hour battery capacity. This is necessary to make full use of all four Class 1E electrical divisions to enhance fire separation criteria. The power associated with the actuation signal for each of these valves or electrical breakers is provided by an electrical division with 24 hour battery capacity, so there is no need to provide position indication beyond this period. The operator will verify that the valves or electrical breakers have achieved the proper position for long-term stable plant operation before position indication is lost. Once the position indication is lost, there is no need for further monitoring since the operator does not have any remote capability for changing the position of these components.

Electrically operated valves, which have the electrical power removed to meet the single failure criterion, are provided with redundant valve position sensors. Each of the two position sensors is powered from a different non-Class 1E power source.

7.3.1.2.19 Containment Air Filtration System Isolation

A signal to isolate the containment air filtration system is generated upon the coincidence of containment radioactivity above the High-1 setpoint in any two of four divisions. This limits activity release to the environment. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.20 Normal Residual Heat Removal System Isolation

A signal for isolating the normal residual heat removal system lines is generated upon the coincidence of containment radioactivity above the High-2 setpoint in any two of four divisions. This signal also isolates the chemical and volume control system as discussed in subsection 7.3.1.2.15. This limits activity release to the environment. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.21 Spent Fuel Pool Isolation

A signal for isolating the spent fuel pool lines is generated upon the coincidence of spent fuel pool level below the Low setpoint in ~~any one~~ two of ~~two~~ three divisions. This helps to maintain the water inventory in the spent fuel pool due to line leakage. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.3 Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation

The interlocks used for engineered safety features actuation are designated as "P-xx" permissives and are listed in Table 7.3-2.

7.3.1.4 Bypasses of Engineered Safety Features Actuations

The channels used in engineered safety features actuation that can be manually bypassed are indicated in Table 7.3-1. A description of this bypass capability is provided in subsection 7.1.2.10. The actuation logic is not bypassed for test. During tests, the actuation logic is fully tested by blocking the actuation logic output before it results in component actuations.

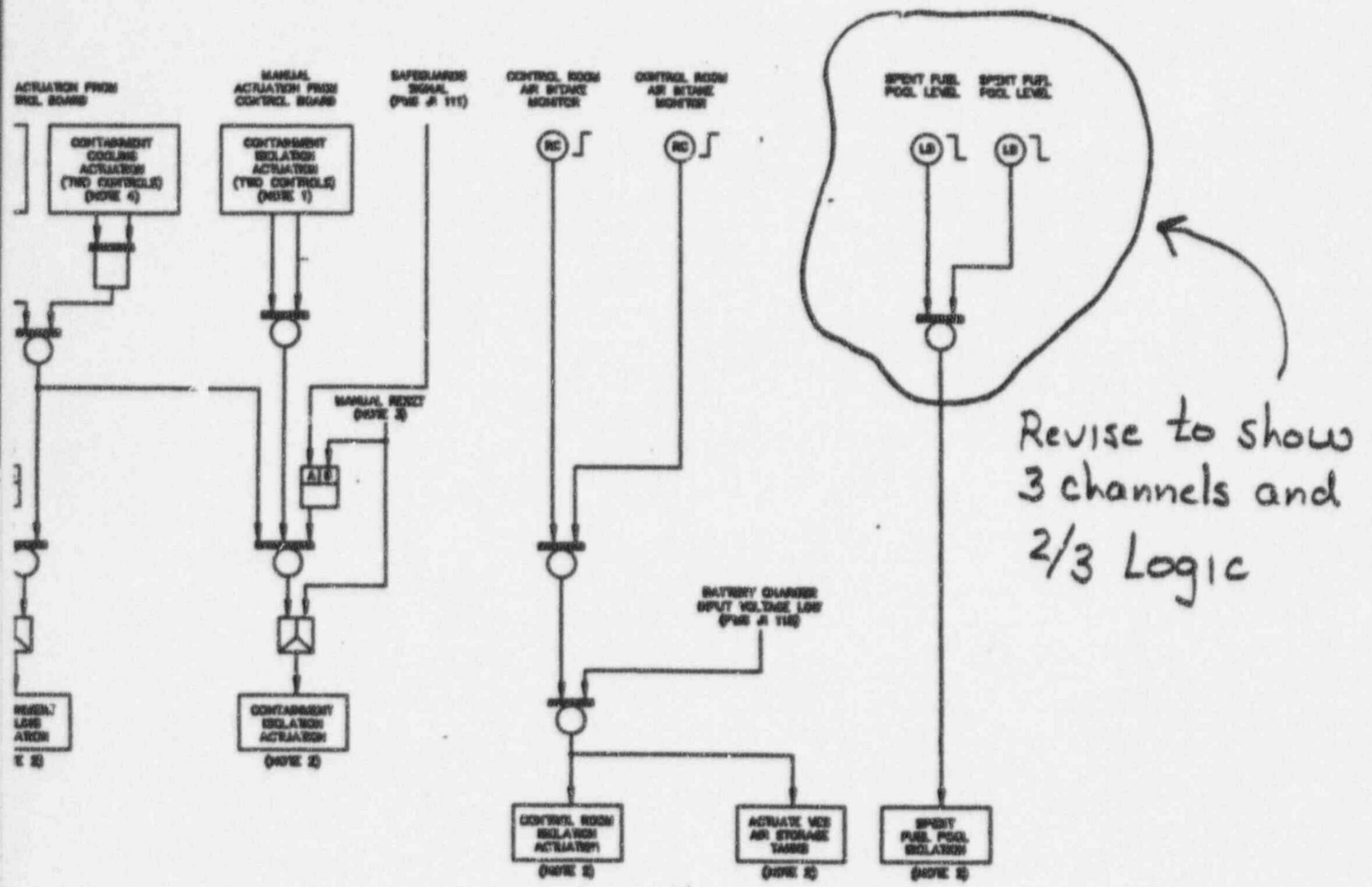
7.3.1.5 Design Basis for Engineered Safety Features Actuation

The following subsections provide the design bases information for engineered safety features actuation, including the information required by Section 3 of IEEE 279-1971. Engineered safety features are initiated by the protection and safety monitoring system. Those design bases relating to the equipment that initiates and accomplishes engineered safety features are given in subsection 7.1.4.1. The design bases presented here concern the variables monitored for engineered safety features actuation and the minimum performance requirements in generating the actuation signals.

Table 7.3-1 (Sheet 7 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
16. Main Control Room Isolation and Air Supply Initiation (Figure 7.2-1, Sheet 13)			
a. High-2 control room supply air radiation	2	1/2	None
b. Undervoltage to Class 1E battery chargers	2/charger	2/2 per charger and 2/4 chargers[3]	None
17. Purification Line Isolation (Figure 7.2-1, Sheet 12)			
a. Low-1 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12. Automatically unblocked above P-12.
18. Containment Air Filtration System Isolation (Figure 7.2-1, Sheet 13)			
a. High-1 containment radioactivity	4	2/4-BYP[1]	None
19. Normal Residual Heat Removal System Isolation (Figure 7.2-1, Sheet 13)			
a. High-2 containment radioactivity	4	2/4-BYP[1]	None
20. Spent Fuel Pool Isolation (Figure 7.2-1, Sheet 13)			
a. Low spent fuel pool level	~~2~~ 3	~~1/2~~ 2/3	None
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves (Figure 7.2-1, Sheet 16)			
a. Automatic reactor coolant system depressurization (fourth stage)	(See items 3d and 3e)		
b. Coincident loop 1 and loop 2 low hot leg level (after delay)	1 per loop	2/2	None
c. Manual initiation	4 switches	2/4 switches[3]	None
22. Open IRWST Containment Recirculation Valves In Series with Check Valves (Figure 7.2-1, Sheet 15)			
a. Extended undervoltage to Class 1E battery chargers	2/charger	1/2 per charger and 2/4 chargers	None



NOTES:

1. TWO MOMENTARY CONTROLS ON THE CONTROL BOARD. OPERATING EITHER CONTROL WILL ACTUATE ALL DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. SEPARATE MOMENTARY CONTROLS ON THE CONTROL BOARD, ONE FOR EACH DIVISION.
4. THE MANUAL CONTAINMENT COOLING ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL DIVISIONS.
5. TWO MOMENTARY CONTROLS ON THE CONTROL BOARD. OPERATING EITHER CONTROL WILL CAUSE THE REACTOR TRIP FUNCTION TO BE ACTUATED IN EACH OF THE FOUR DIVISIONS.

Figure 7.2-1 (Sheet 13 of 20)

Functional Diagrams
Containment & Other Protection

Table 7.5-1 (Sheet 7 of 12)

Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
Chilled water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Chilled water valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Spent fuel pool pump flow	0-1000 gpm	F3	None	None	1/pump	Non-1E	No	
Spent fuel pool temperature	50-250°F	D2, F3	Mild	None	1	Non-1E	No	
Spent fuel pool water level	0-100%	D2, F3	Mild	Yes	~~2~~ 3 (Note 4)	1E	Yes	
CMT to reactor vessel valve status	Open/ Closed	D2	Harsh	No	1/valve	Non-1E	No	
CMT inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT level	0-100%	D2, F2	Harsh	Yes	1/tank	1E	Yes	
IRWST to reactor vessel valve status (Non-MOV)	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
IRWST to reactor vessel valve status (MOV)	Open/ Closed	D3	None	None	1/valve	Non-1E	No	
ADS: first, second and third stage valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	

Table 7.5-1 (Sheet 12 of 12)

Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Post accident sampling station radiation	10^{-1}- 10^{7} mR/hr	E3	None	None	1	Non-1E	No	
Main steam line radiation level	10^{-1}- 10^{3} μCi/cc	C2, E2	Mild	None	1/line	Non-1E	No	
Technical support center radiation	10^{-1}- 10^{4} mR/hr	E3	None	None	1	Non-1E	No	
Meteorological parameters	N/A	E3	None	None	N/A	Non-1E	No	Site specific

Notes:

1. Total flow measurement is obtained from the sum of ~~three~~ four branch flow devices.
2. The same information is available in the technical support center via the monitor bus. Information available on the qualified data processing system is also available at the remote shutdown workstation.
3. Noble gas: 10^{-7} to 10^{5} μCi/cc
   Particulate: 10^{-13} to 10^{-7} μCi/cc
   Iodines: 10^{-12} to 10^{-6} μCi/cc
4. The number of instruments required after stable plant conditions is two. A third channel is available through temporary connections to resolve information ambiguity if necessary (See subsection 7.5.4).
5. Noble gas: 10^{-7} to 10^{-2} μCi/cc
   Particulate: 10^{-12} to 10^{-7} μCi/cc
   Iodines: 10^{-11} to 10^{-5} μCi/cc
6. Degree of subcooling is calculated from pressurizer pressure and RCS hot leg temperature.
7. This instrument is not required after 24 hours.

DSER Open Item Tracking System Report for Chapter 7
Items not Statused "Resolved" by NRC

AP600 Open Item Tracking System Database: Executive Summary

Date: 2/18/97

Selection: [nrc st code]<>'Resolved' And [DSER Section] like '7*' Sorted by Item #

Item No.	Branch	DSER Section/ Question	Type	Title/Description / Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
1038	NRR/HICB	7.1.4-1	DSER-OI		ITAAC/Deutsch, K.	Action N	Action N	NSD-NRC-96-4737	
				Westinghouse should describe in the SSAR, CDM, and ITAAC the digital system design process. Westinghouse should provide a detailed descritpiton of the digital system design process in the SSAR and CDM with a corresponding ITAAC.					
				Action W - WCAP-13383, which describes the digital system design process is being updated. The certified design material and ITAACs will be modified. The SSAR has been modified to reference the design process and to indicate the software design standards the design process conforms to. This information is provided in Revision 3 of the SSAR, Subsection 7.1.2.15. The WCAP and ITAAC revisions must be completed before this item can be closed out. NRC has requested a presentation when all elements are completed. WCAP-13383 rev due 5/30/96 rkn 5/7/96 WCAP-13383 in repro 6/14 for 6/17 release. rkn 6/14/96 Closed - Response provided by NSD-NRC-96-4737. Per an 11/21 W/NRC telecon, the NRC thinks the I&C ITAAC is deficient and requested that we "fix" the ITAAC or justify/explain deviations from the SRP 14.3.5 to NRC satisfaction. NRC to provide specific comments on the ITAAC. rkn 12/2					
1039	NRR/HICB	7.1.7-1	DSER-OI		ITAAC/Deutsch	Action N	Action N	NSD-NRC-96-4737	
				Westinghouse should describe a commercial grade item dedication program for digital systems. Westinghouse has not addressed the commercial grade item dedication program that is necessary to ensure sufficient quality in the design of safety-related and nonsafety-related I&C systems using commercial of-the-shelf equipment. The design, verification, and validation process for COTS software and hardware should be clearly documented for design certification.					
				Action W - WCAP-13383 is being updated to include a commercial grade item dedication process. The SSAR has been modified to reference this process. This information is provided in Revision 3 of the SSAR, Subsection 7.1.2.15. The WCAP revision must be completed before this item can be closed out. WCAP in repro 6/14 for 6/17 issuance. rkn 6/14 Closed - Response provided by NSD-NRC-96-4737. Same as item 1038. rkn 12/2					
1041	NRR/HICB	7.2.6-1	DSER-OI		ITAAC/Deutsch, K.	Action N	Action N		
				The staff has not yet completed its evaluation of the software architecture design. ...because WCAP 14080 was submitted in July 1994, the staff has not completed its review of the document and is continuing its evaluation of the software architecture based on both the proposed design and the associated design process. The results from this evaluation will be presented in the final SER for AP600.					
				Closed - Westinghouse has completed necessary submittals to support staff review. Per 11/21 W/NRC telecon, when the NRC agrees with the design process through their review of the ITAACs, this item will be closed. rkn 12/2					
1043	NRR/HICB	7.2.8-1	DSER-OI		ITAAC/Deutsch	Action N	Action N	NTD-NRC-95-4464	
				Westinghouse should provide a discussion concerning the qualification of digital equipment to the electromagnetic environment. Westinghouse has not addressed the issue of electromagnetic environmental qualification and has not committed to the appropriate standards.					
				Closed - List of standards reviewed by NRC during meeting on May 15-16. Standards incorporated into Revision 3 of the SSAR, Subsection 7.1.4.1.6. Per an 11/21 W/NRC telecon, the technical issues are resolved. When NRC agrees with design process thru ITAAC review, this item will be closed.					

Item No.	Branch	DSER Section/ Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
1044	NRR/HICB	7.2.8-2	DSER-OI		ITAAC/Deutsch, K.	Closed	Action W	NTD-NRC-95-4464	
				Westinghouse should provide information concerning environmental qualification of PMS components addressing local temperature rises above the room ambient experienced by the components during operation. It is desirable to have additional margin built into the design. The components should, therefore, be qualified by testing to higher temperatures than specified in the SSAR for a given room environment. Westinghouse should address this concern in the SSAR. Westinghouse should also provide mild environment equipment qualification in the CDM with the corresponding ITAAC.					
				Closed - Technical information agreeded to by NRC during meeting on May 15-16. Additional technical information regarding the equipment design margin to loss of HVAC has been incorporated into Revision 3 of the SSAR, Subsection 7.1.4.1.8. rkn 12/2 Westinghouse needs to decide approach to close this item. rkn 12/6 Action N - NRC still has the action to evaluate the Westinghouse proposal on procedural fix of instrument overheating after 24 hour period. (6/21 meeting with W/SPLB/HICB). Based on 11/21 W/NRC telecon, this approach is reasonable; see qualification program in SSAR Section 3.11. Action W - NRC requested W provide proposed COL item for qualification margin and instrument setpoint data or document in the CDM and corresponding ITAAC (W is considering options; did not commit to either approach). rkn 12/2 Westinghouse does not consider there to be an applicable COL action to identify. Technical information related to design margin against a loss of HVAC was provided in SSAR 7.1.4.1.6 and is considered technically resolved, as waws previously agreed to by NRC. This item is considered closed since there is no Westinghouse action required at this time to address this item (since the NRC relates this comment to the PMS ITAAC, the responsible engineer is changed to ITAAC). rkn 1/14/97. Action W - (from NRC on 1/28/97) Submit revised CMD & ITAAC to include COL action to include additional design margin to accomodate a loss of the normal HVAC. Provide an alarm if internal cabinet temperatures reach an excessive value. jww1/28 This was previously closed and is still considered closed, meaning there is no Westinghouse action identified or required o close this item; all necessary submittals have been made. For background, SSAR Section 7.1.4.1.6 was revised in Feb 1996 to address this. Specifically, there is a sentence which reads, "The cabinets containing the digital equipment are provided with temperature sensors which provide an alarm if internal cabinet temperatures reach an excessive value." This is closed. rkn 1/30/97. Per telecon with Hulbert Li today, the action is for Westinghouse to include this alarm in the ITAAC. rkn 2/18/97.					
1049	NRR/HICB	7.5.8-1	DSER-OI		ITAAC/Lindgren/Deuts	Action N	Action N		
				Westinghouse should describe the design features of the incore instrumentation system. In its response to Q492.5 dated July 25, 1994, Westinghouse states that information on the employment of fixed incore detectors in conjunction with an online power distribution monitoring system will be provided to the NRC to support the final SER.					
				Closed - The technical information was accepted by the I&C Branch of NRC during the meeting on May 15-16. This technical information has been incorporated into Revision 3 of the SSAR, Subsection 4.4.6.1. Open for ITAAC based on fax from NRC 1/21/97. rkn For Chapter 7 this item is resolved. (NRC/RSB to communicate any concerns with qualification of thermocouples and instrument coolant capability outside the scope of Chapter 7). rkn 12/2					

Item No.	Branch	DSER Section/ Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
1052	NRR/HICB	7.6.2-1	DSER-OI	Westinghouse should provide additional design details of the accumulator isolation valve interlocks important to safety to confirm that the design meets the relevant requirements of the SRP, including IEEE 279. Closed - Additional technical information has been incorporated into Revision 3 of the SSAR, Subsection 7.6.2.1. Figure 7.2-1 was also modified to include additional technical detail. Action NRC - Per 11/21 telecon, NRC to review technical information already provided since this operator is nonsafety, not important to safety, has separate power, positive 3 position indications, and power removed at-power (consistent with Tech Specs) and limit switch alarms. rkn 12/2 Technical information provided. NRC to advise to resolution status. rkn 1/14/97 Per fax, NRC considers this open for interlocks concern (FSER open item 7.6.2-1). rkn 1/21/97	Schulz, T.	Closed	Action N		
1053	NRR/HICB	7.6.3-1	DSER-OI	Westinghouse should provide additional design details of the IRWST discharge valve interlocks important to safety to confirm that the design meets the relevant requirements of the SRP, including IEEE 279. Closed - Additional technical information has been incorporated into Revision 3 of the SSAR, Subsection 7.6.2.2. Figure 7.2-1 was also modified to include additional technical detail. Action NRC - See 1052. rkn 12/2 Technical information has been provided. NRC to advise regarding resolution status. rkn 1/14/97. Per fax, NRC considers this open for interlocks concern (FSER open item 7.6.2-1). rkn 1/21/97	Schulz, T.	Closed	Action N		
1055	NRR/HICB	7.7.2-1	DSER-OI	Westinghouse should provide additional information concerning the design of the DAS. Closed - Technical information accepted by NRC during meeting on May 15-16. This additional technical detail has been incorporated into Revision 3 of the SSAR, Subsection 7.7.1.11. NRC action to review ITAAC. Per 11/21 telecon, this item is now subject to DAS ITAAC comment resolution/completion. rkn 12/2	ITAAC/Delose,Frank	Action N	Action N	NTD-NRC-95-4464	
2023	NRR/HICB	7.	DSER-OI50	27. No Commitment to Industry Standards for Digital Systems While the SSAR references IEEE standards 279, 384, 603 and 796 for the design of AP600 I&C systems, the staff is concerned that there is no reference to digital microprocessor-related standards. Specifically they are concerned about the lack of standards related to multiplexer architecture, communications protocols, and hardware/software design. The staff wants Westinghouse to make an explicit commitment to industry hardware and software related standards. No detailed documentation of the process and no phased ITAAC for verification of the design. Action W - Item 1037 closes all but final sentence of item. Remaining action to address "No detailed documentation of the process and no phased ITAAC for verification of the design". SSAR Ch 7.1 commits to a V&V program, meeting Standards, etc., such that NRC expectations are met. When the ITAAC for PMS is complete, this item will be closed. rkn 5/7/96 Closed - ITAAC submitted by NSD-NRC-96-4875 of 11/7/96. Per 11/21 telecon for DSER Ch 7, NRC wants to discuss ITAAC approach with Westinghouse.	ITAAC/Deutsch	Action N	Action N	NSD-NRC-4875	

AP600 Open Item Tracking System Database: Executive Summary

Date: 2/18/97

Selection: [nrc st code]<>'Resolved' And [DSER Section] like '7*' Sorted by Item #

Item No.	Branch	DSER Section/ Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
2025	NRR/HICB	7.	DSER-OI50	29. Environmental Qualification of DAS Equipment and Sensors The DSER indicates that the DAS equipment must be designed and qualified to the environment in which it needs to perform. The Westinghouse position is that the DAS equipment will be designed to function the environment in which it needs to perform. However, the DAS equipment will not be subjected to a full-blown 10 CFR 50.49 / IEEE 323 qualification program. Closed - SSAR Chapter 7 section 7.7.1.11 revised to address. Per an 11/21 telecon, NRC thinks the DAS sensors and actuated devices (e.g., PRHR solenoid valve) should be qualified to a higher (PMS) standard but Westinghouse does not agree. By 12/6 fax, W proposed SSAR change to clarify qualification; NRC to review approach. rkn 12/6 Completed in SSAR Rev 10. rkn 1/14/97 Whoops! I checked and it didn't get into SSAR Rev 10. It WILL get into Rev 11. See NSD-NRC-97-4947. rkn 1/30/97	SSARREV/Miller	Confrm-W	Action N		
2272	NRR/SRXB	7.6.2	MTG-OI	APRIL 19, 1995 (HSII) DISCUSSION ITEMS 15. Availability of Safeguards - Interlocks (SSAR Section 7.6.2): Section 7.6.2 of the SSAR discusses the interlock systems to verify the availability of safeguard functions, i.e., to ensure opening of the isolation valves of the accumulators, IRWST, and PRHRHXs. These valves are motor-operated, normally open valves, and are controlled from the main control room and remote shutdown work station. a. SSAR Section 7.6.2 states that, as a result of the confirmatory safeguard open signal (which will automatically open the isolation valves, overriding bypass features to allow the isolation valves to be closed), isolation of an accumulator with the RCS at pressure (or isolation of the IRWST gravity injection line when the tank is required to be operable, or isolation of the PRHRHX inlet line when the PRHRHX is required to be operable) is acceptable. What are the design reliability of these interlocks to ensure these isolation valves will be open upon the confirmatory safeguard open signals? Is this practice acceptable for current operating reactor to allow accumulator isolated at pressure? Closed - At he Reactor System Branch Meeting on 4/25/95, Westinghouse referred to the use of identical interlocks on the accumulators and IRWST as those currently used on the accumulators at current plants (power locked-out). CMTs and PRHR interlocks are not power locked out but instead redundant controllers are provided for each valve along with three-way redundant valve positions. Westinghouse also referred to the Revision 2 SSAR 6.3 for the design details. Revision 3 of the SSAR, Section 7.6 includes the interlock information. Based on 11/21 telecon, NRC doesn't think the SSAR Section 7.6 is sufficient and has been asked to provide specific comments. rkn 12/6 Closed since there is no Westinghouse action at this time. NRC to advise regarding status. rkn 1/14/97.	Deutsch	Closed	Action N		
2273	NRR/SRXB	7.6.2	MTG-OI	APRIL 19, 1995 (HSII) DISCUSSION ITEMS 15. Availability of Safeguards - Interlocks (SSAR Section 7.6.2): b. SSAR Section 7.6.2 also states that the maximum permissible time that an accumulator valve (or IRWST discharge valve, or PRHRHX inlet valve, respectively) is closed when the reactor is at pressure as specified in the TS. Where are they specified? Action W - Section 3.5.1 of the Tech Specs specifies the maximum permissble valve times. The revised Tech Specs will be submitted June 1996, at which time this item can be closed. Closed - With issuance of the Tech Specs in SSAR Rev. 9. Action NRC - Per 11/21 telecon, NRC to review Tech Specs to ensure this is resolved/closed. rkn 12/4 Westinghouse action is complete for this item. NRC to advise on status. rkn 1/14/97.	TECHSPEC/Schulz	Closed	Action N		

Item No.	Branch	DSER Section/ Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
4257	NRR/HICB	7	MTG-COM	Add WCAP-14080 as reference for SSAR Section 7.1 Westinghouse has confirmed this is an appropriate reference and transmitted the SSAR markups to NRC. This item is opened to ensure the marked changes are included in the next SSAR rev. rkn 1/15/97. Refer to NSD-NRC-97-4947 for changes to be included in SSAR Rev 11. rkn 1/31/97	SSARREV/Deutsch, Ke	Confirm-W	Confirm-W		