AP1000 I&C RAI Status

420.001 -- Westinghouse has not submitted the updated Tier 1 description of Section 2.5.2 to cover the protection and monitoring system (PMS) Common Qualified Platform (Common Q) design. The staff considers this item still open.

Westinghouse position is that Tier 1 is not product-specific and does not need to be changed. This item to be discussed at March 5 meeting.

420.005 -- Westinghouse states that the qualification process for the non-safety soft control device will be based on standard Westinghouse processes for:

-Quality assurance
-Verification and validation on non-safety software
-Electrical & EMI [electromagnetic interference] testing

Are these documents available for staff audit?

This item to be discussed at March 5 meeting.

420.006 -- Revise response and DCD to include the EPRI topical report as a Tier 2* commitment.

Westinghouse agrees to add EPRI topical report and a Tier 2 commitment. RAI response 420.006 Revision 1 has been submitted.*

420.007 -- The description stated in the Westinghouse response to RAI 420.007 should be included in the Design Control Document (DCD).

Westinghouse agrees to add this material to the DCD. RAI response 420.007 Revision 1 has been submitted.

420.008 -- The description stated in the Westinghouse response to RAI 420.008 should be included in the DCD. In addition to the electrical isolation, Westinghouse should also address communication isolation.

Westinghouse agrees to add this material to the DCD. RAI response 420.008 Revision 1 has been submitted.

420.012 -- The component level manual actions and the backup supporting indication were not provided in the response. Please clarify that a common mode

Enclosure 3

failure at system level protection would not disable the component level actuation.

A common mode failure at system level protection can disable the component level actuation. The DAS manual controls are provided to address the concern about common mode failure. This is the same as AP600. This item to be discussed at March 5 meeting.

420.013 -- Please clarify was is meant by the phrase "do no significantly reduce" in the statement in the response that states that "[c]onnections and software that are used for plant monitoring and for surveillance of the reactor trip and ESF actuation system do not significantly reduce the reliability of or increase the complexity of these systems."

RAI response 420.013 Revision 1 has been submitted.

420.028 & 029 -- The supplemental safety evaluation report on Common Q has not been completed. The staff will make a determination whether they need additional information after the supplemental safety evaluation report is completed.

Westinghouse agrees to add a reference to the second Common Q supplemental SER when it is issued. This item to be discussed at March 5 meeting.

420.044 -- The staff will need a copy of the software requirement specification (SRS) so that we may take a detailed look at what the software for the safety system is and is not required to do. This cannot reasonably be performed in a visit to Westinghouse offices.

Please describe anticipated differences between this document and what is to be written for the AP1000.

A copy of the Ringhals Unit 2 TWICE Software Requirements Specification has been placed in the Westinghouse Rockville office for NRC review. This item to be discussed at March 5 meeting.

420.045 -- The staff does not consider RAI response a, b, e, f, and g to be methods of safety analysis and, while important steps in the engineering life cycle, are not considered methods of safety analysis. Items c and, to some degree, d meet the intent of the RAI with follow-up questions. A system level failure modes and effects analysis (FMEA) may be insufficient in detail to determine failure modes of such components as the gateway—and its components, the communication interfaces used between channels and isolation devices. What level of detail is considered sufficient for the proposed system level FMEA? Please provide a rationale for the level of detail

Westinghouse agreed to revise the RAI response and the DCD to include a Software Hazards Analysis as part of the COL action item to perform an FMEA. RAI response 420.045 Revision 1 has been submitted.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.001

Question:

420.1 (Design Control Document (DCD) Section 7.1)

DCD Section 7.1 states that the design certification of AP1000 focuses upon the process used to design and implement I&C systems for the AP1000. DCD Chapter 7 for the AP1000 has been written to permit the use of either the protection system hardware described in the AP600 DCD or the Common Q system. U.S. Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP), Chapter 7, Branch Technical Position (BTP) HICB-14, "Guidance on Software Review for Digital Computer-Based Instrumentation and Control Systems," identified certain information that needs to be reviewed with respect to digital I&C design process and implementation. It states that the information should include but not be limited to the following areas:

(1) Software Life Cycle Process Planning

- X Software management plan
- X Software development plan
- X Software quality assurance plan
- X Integration plan
- X Installation plan
- X Maintenance plan
- X Training plan
- X Operations plan
- X Software safety plan
- X Software verification and validation plan
- X Software configuration management plan

(2) Software Life Cycle Process Implementation

- X Safety analyses
- X Verification and validation analysis and test reports
- X Configuration management reports

(3) Software Life Cycle Process Design Outputs

- X Software requirements specifications
- X Hardware and Software architecture description
- X Software design specifications
- X Code listing
- X Build Documents
- X Installation configuration tables
- X Operations manuals
- X Maintenance manuals
- X Training manuals

In the AP600 design certification, Westinghouse has stated that the process described in WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design Verification and Validation Process Report," is the basis for the associated I&C system inspection, test, analysis and acceptance criteria (ITAAC) which allow the NRC to review the phased implementation of the I&C system design. WCAP-13383 has been designated as a Tier 2* item. AP1000 DCD Section 7.1.7 Reference 9, "CE-CES-195, Rev.01 - Software Program Manual for Common Q Systems," may serve the similar purpose as WCAP-13383 for AP600 design certification. However, review points should be established in the document to allow NRC to review and audit the design process. A formal commitment is required to include both WCAP-13383 and CE-CES-195 as Tier 2* documents. Any change to these documents will require NRC approval.

Because the DCD Chapter 7 for the AP1000 has been written to permit the use of either the protection system hardware described in the AP600 DCD or the Common Q system, the Tier 1 description 2.5.2, "Protection and Safety Monitoring System," should be modified to accommodate the design features in the Common Q system (items related to questions 420.28 and 420.29 also should be included in the ITAAC). Please provide an updated Tier 1 description of Section 2.5.2 for staff review.

Westinghouse Response:

The process described in WCAP-13383 (DCD 7.1.7, reference 3) is the basis for the I&C system ITAAC for the AP600 hardware. The process described in WCAP-15927 (see response to RAI 420.023) serves a similar purpose for the Common Q platform. WCAP-13383 is designated as Tier 2* in Revision 2 of the AP1000 DCD. Westinghouse agreed to designate WCAP-15927 and CE-CES-195 as Tier 2* in response to RAI 420.023.

Westinghouse has proposed DCD changes to accommodate the design features of the Common Q platform. See responses to RAIs 420.028 and 420.029 for details.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

An updated DCD Tier 1 (ITAAC) 2.5.2 to allow the use of either the protection system hardware described in the AP600 DCD or the Common Q system was provided in response to RAI 420.040.

Design Control Document (DCD) Revision:

See responses to RAIs 420.023, 420.028, 420.029, and 420.040.

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.005

Question:

420.5 (DCD 7.1.3.3)

DCD 7.1.3.3 states that each soft control device can control safety-related and nonsafety-related equipment. Describe how the soft control devices interface with the redundant safety-related components. What type of safeguard in the design can prevent unauthorized or erroneous data entry into the protection system? Discuss the qualification process for the soft control device.

Westinghouse Response:

The citation above refers to the nonsafety-related soft control devices provided by the Data Display and Processing System (DDS). The DDS soft controls can be used to operate components in either the nonsafety-related Plant Control Systems (PLS) or the safety-related Protection and Safety Monitoring Systems (PMS).

The real-time data network of the nonsafety-related DDS is interfaced with the four channels of the safety-related PMS through four independent, qualified channel gateways. These gateways electrically protect the PMS equipment from failures of the nonsafety DDS equipment.

Automatic PMS operation protects against improper DDS operation of PMS systems and components. Specifically, whenever protective setpoints are exceeded, PMS protection signals are prioritized to override manual inputs from the nonsafety-related soft controls so as to place the safety-related components in their safe states.

These control signals are validated by the safety system prior to action being taken. The validation either takes the form of logic that prevents inhibiting of an automatic safety function or confirmation of action with the operator where there is no automatic safety function. Further details are available in Appendix 4 of the Common Q Topical Report.

Unauthorized PMS command entries by soft control are limited by system login and security features. Unauthorized PMS data entries are prevented by system login and security features, as well as key locks, door alarms, and key lock switches on PMS equipment cabinets. Data updates and software changes will be made using either the PMS maintenance and test panel or a portable workstation using a specialized configuration tool. Safety system constants, variables, and/or setpoint data are not subject to change through the soft control devices. Therefore, erroneous data entry into the PMS from the nonsafety-related soft controls is not possible.

The qualification process for the non-safety soft control device will be based on standard Westinghouse processes for:

- Quality assurance
- Verification and validation of non-safety software
- Electrical & EMI testing

Design Control Document (DCD) Revision:

None

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.006 (Response Revision 1)

Question:

420.6 (DCD 7.1.2.14.2)

Please provide the Commercial Dedication process ITAAC for staff review.

Westinghouse Response:

The Commercial Dedication ITAAC is located in Table 2.5.2-8, Item #13. A copy is provided below.

Table 2.5.2-8 (cont.)
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
13. The use of commercial grade computer hardware and software items in the PMS is accomplished through a process that specifies requirements for: a) Review of supplier design control, configuration management, problem reporting, and change control. b) Review of product performance. c) Receipt acceptance of the commercial grade item. d) Acceptance based on equipment qualification and software validation in the integrated system.	Inspection will be performed of the process defined to use commercial grade components in the application.	A report exists and concludes that the process has requirements for: a) Review of supplier design control, configuration management, problem reporting, and change control. b) Review of product performance. c) Receipt acceptance of the commercial grade item. d) Acceptance based on equipment qualification and software validation in the integrated system.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

Design Control Document (DCD) Revision:

None

PRA Revision:

None

NRC Additional Comments:

Revise response and DCD to include the EPRI topical report as a Tier 2* commitment.

Westinghouse Additional Response:

EPRI TR-106439 will be added to DCD Tier 2 section 7.1.2.14.2, 7.1.7 and the DCD Table 1-1 as shown below.

Design Control Document (DCD) Revision:

Table 1-1
Index of AP1000 Tier 2 Information Requiring NRC Approval for Change

Item	Expiration at First Full Power	Tier 2 Reference
WCAP-13383, "AP600 Instrumentation and Control Hardware & Software Design, Verification & Validation Process Report," Rev 1.	Yes	Chapter 7 Table 1.6-1
WCAP-14605, "Westinghouse Setpoint Methodology for Protection Systems, AP600," Rev 0	Yes	Chapter 7 Table 1.6-1
CE-CES-195, "Software Program Manual for Common Q Systems," Rev 01	Yes	Chapter 7 Table 1.6-1
WCAP-15927, "Design Process for AP1000 Common Q ?Safety Systems," Rev 0	Yes	Chapter 7 Table 1.6-1
Verification and Validation	Yes	7.1.2.14
~~Conformance with Industry Standards~~Design Process	Yes	~~7.1.4.1.8~~7.1.2.14.1
Commercial Dedication	Yes	7.1.2.14.2

Item	Expiration at First Full Power	Tier 2 Reference
TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications"	Yes	7.1.2.14.2 7.1.7

7.1.2.14.2 Commercial Dedication

[*WCAP-13383 (Reference 3) and CENPD-396-P (Reference 8) provide for the use of commercial off-the-shelf hardware and software through a commercial dedication process. The commercial dedication process will follow the guidelines outlined in EPRI TR-106439 (Reference 15)*]* Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant as described in subsection 13.5.1.

7.1.7 References

[*15 TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, October 1996.*]*

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.007 (Response Revision 1)

Question:

420.7 (DCD 7.1.2.5)

Describe the Qualified Data Processing Subsystems (QDPS) in more detail. DCD takes credit on the QDPS in the Defense-in-Depth and Diversity analysis. Describe the relationship between the QDPS and the RTS/ESFAS. Are the QDPS sharing sensors with the RTS or the ESFAS? (Figure 7.1-1 showing some sensors feed into plant protection subsystem directly while some sensors feed into QDPS subsystem). If the QDPS has separate sensors, do they have same qualification requirement as RTS/ESFAS ?

Westinghouse Response:

The Qualified Data Processing Subsystem (QDPS), a subsystem of the Protection and Safety Monitoring System (PMS), provides safety-related display of selected parameters in the control room. Power is provided to the QDPS from the Class 1E dc and UPS system for 72 hours after a loss of all ac power (station blackout). After 72 hours, the ancillary diesel generators provide power for the QDPS. QDPS is a two-train subsystem (Divisions B and C). The PMS, including the QDPS, is diverse from the Diverse Actuation System (DAS). Sensors are not shared between PMS and DAS.

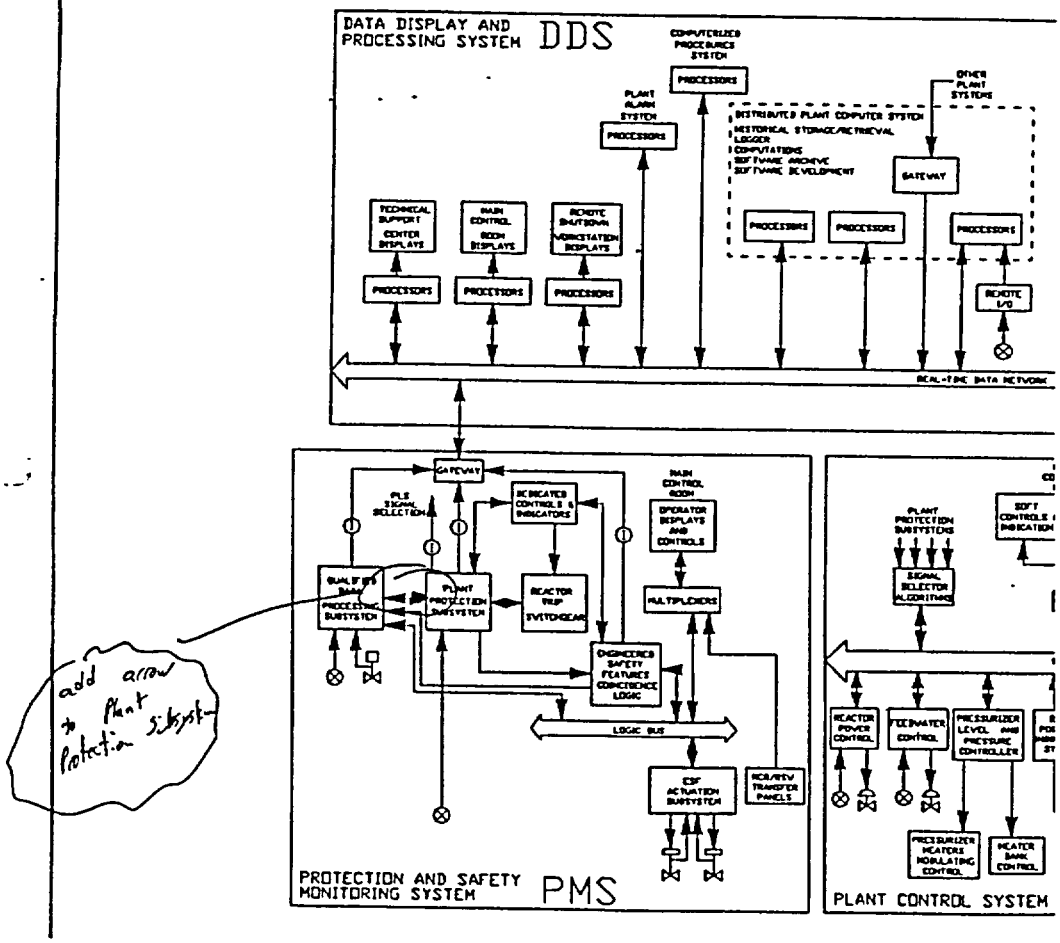
The RTS/ESFAS signals are processed by the Plant Protection Subsystem of PMS. Within PMS, some sensors are shared between the Plant Protection Subsystem and QDPS. Shared sensors are processed first by the QDPS because the QDPS will need this sensor for more than 24 hours following a station blackout. 24-hour batteries power the Plant Protection Subsystem; therefore, the Plant Protection Subsystem can not be used for QDPS functions.

The typical input parameter for RTS/ESFAS is four-way redundant with one sensor for each of the four divisions. If that parameter is also needed by QDPS, the B and C division sensors are processed first by QDPS then sent to the Plant Protection Subsystem. The A and D division sensors are not shared with QDPS and thus are processed directly by the Plant Protection Subsystem. If an RTS/ESFAS parameter is not needed by QDPS, it is processed directly by the Plant Protection Subsystem in all four divisions.

Design Control Document (DCD) Revision:

DCD Figures 7.1-1 and 7.1-2 will be revised to show two-way communication between the QDPS and the Plant Protection Subsystem. See attached mark-ups.

REVISION to DCD Figure 7.1-1



REVISION to DCD Figure 7.1-2

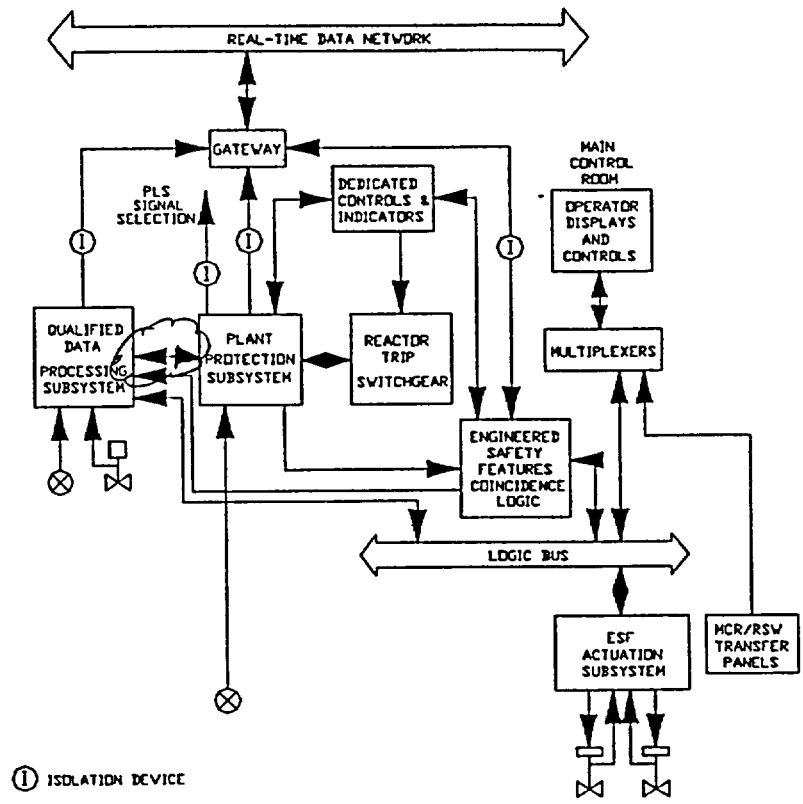


Figure 7.1-2

Protection and Safety Monitoring System

PRA Revision:

None

NRC Additional Comments:

The description stated in the Westinghouse response to RAI 420.007 should be included in the Design Control Document (DCD).

Westinghouse Additional Response:

DCD section 7.1.2.5 will be revised as shown below:

Design Control Document (DCD) Revision:

7.1.2.5 Qualified Data Processing Subsystems

The Qualified Data Processing Subsystem (QDPS), a subsystem of the PMS, provides safety-related display of selected parameters in the control room.

The ~~qualified data processing (~~QDPS~~)~~ subsystems are a redundant configuration consisting of sensors, QDPS hardware, and qualified displays.

The qualified data processing subsystems perform the following functions:

- Provide safety-related data processing and display
- Provide the operator with sufficient operational data to safely shut the plant down in the event of a failure of the other display systems
- Provide qualified and nonqualified data to the real-time data network for use by other systems in the plant
- Process data for main control room display, and to meet Regulatory Guide 1.97 requirements
- Provide data to the main control room, the remote shutdown workstation, the plant computer, other nonsafety-related devices, and nonqualified emergency response facilities in conformance with NUREG-0696

The QDPS hardware consists of safety-related modular data gathering units. The QDPS receives inputs from process sensors and safety-related digital systems. The QDPS consolidates the input data, performs conversions to process units, and formats the data for data link transmission.

Figure 7.1-8A illustrates the qualified data processing subsystem for the Eagle I&C architecture. Figure 7.1-8B illustrates the qualified data processing subsystem for the Common Q architecture.

Power is provided to the QDPS from the Class 1E dc and UPS system for 72 hours after a loss of all ac power (station blackout). After 72 hours, the ancillary diesel generators provide power for the QDPS. QDPS is a two-train subsystem (Divisions B and C). The PMS, including the QDPS, is diverse from the Diverse Actuation System (DAS). Sensors are not shared between PMS and DAS.

The RTS/ESFAS signals are processed by the Plant Protection Subsystem of PMS. Within PMS, some sensors are shared between the Plant Protection Subsystem and QDPS. Shared sensors are processed first by the QDPS because the QDPS will need this sensor for more than 24 hours following a station blackout. 24-hour batteries power the Plant Protection Subsystem; therefore, the Plant Protection Subsystem can not be used for QDPS functions.

The typical input parameter for RTS/ESFAS is four-way redundant with one sensor for each of the four divisions. If that parameter is also needed by QDPS, the B and C division sensors are processed first by QDPS then sent to the Plant Protection Subsystem. The A and D division sensors are not shared with QDPS and thus are processed directly by the Plant Protection Subsystem. If an RTS/ESFAS parameter is not needed by QDPS or if it is not needed after 24-hours, it is processed directly by the Plant Protection Subsystem in all four divisions.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.008 (Response Revision 1)

Question:

420.8 (DCD Figure 7.1-2)

Describe the "GATEWAY" design and its interface with the Protection and Safety Monitoring System.

Westinghouse Response:

The purpose of the Protection and Safety Monitoring Gateway is to interface the safety PMS to the non-safety real-time data network that supports the remainder of the instrumentation and control system. The Gateway has two subsystems. One is the safety subsystem that interfaces to the Plant Protection Subsystem, the Engineered Safety Features Coincidence Logic and the Qualified Data Processing Subsystem. The other is the non-safety subsystem that interfaces to the real-time data network. The two subsystems are connected by a fiber optic link that provides electrical isolation.

The primary flow of information between the two Gateway subsystems is from the safety subsystem to the non-safety subsystem. This information is a combination of plant process parameter values and equipment status information. The information that flows from the non-safety subsystem to the safety subsystem is limited to the following:

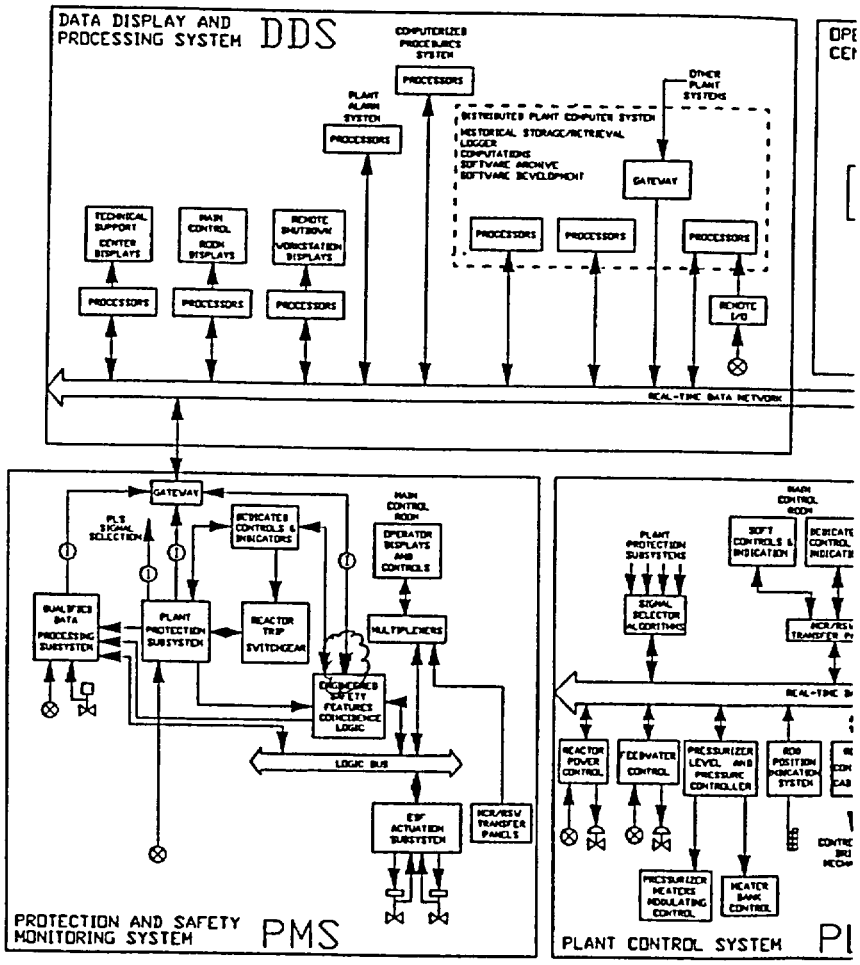
- The safety and non-safety subsystems exchange periodic interface signals that the communication controllers at each end of the link use to ensure that the link is functioning properly. These signals are used only by the communication controllers and are not propagated to the rest of the safety system. There is no application function in the safety system that uses this information.

- The main control room and the remote shutdown workstation operator consoles are non-safety. The soft control inputs to the PMS from these locations are provided from the non-safety subsystem to the safety subsystem of the Gateway.

Note that there is an error in DCD Figure 7.1-1. The gateway needs to communicate <u>to</u> the Engineered Safety Features Coincidence Logic (as well as from the ESF Coincidence Logic) to accomplish the second function listed above. DCD Figure 7.1-2 (Revision 1) shows this link correctly.

Design Control Document (DCD) Revision:

Revise DCD Figure 7.1-1 as shown.



PRA Revision:

None

NRC Additional Comments:

The description stated in the Westinghouse response to RAI 420.008 should be included in the DCD. In addition to the electrical isolation, Westinghouse should also address communication isolation.

Westinghouse Additional Response:

DCD section 7.1.2.8 will be revised as shown below:

Design Control Document (DCD) Revision:

7.1.2.8 Communication Functions

The communication functions provide information from the plant protection subsystem, the ESF coincidence logic, the ESF actuation subsystems, and the QDPS subsystems to external systems. This includes outputs to the plant control system and the data display and processing system. Isolation devices provide electrical isolation between the protection and safety monitoring system and the external systems.

The communication functions are accomplished via channelized gateways as shown in Figure 7.1-1.

The PMS Gateway interfaces the safety PMS to the non-safety real-time data network that supports the remainder of the instrumentation and control system. The Gateway has two subsystems. One is the safety subsystem that interfaces to the Plant Protection Subsystem, the Engineered Safety Features Coincidence Logic and the Qualified Data Processing Subsystem The other is the non-safety subsystem that interfaces to the real-time data network. The two subsystems are connected by a fiber optic link that provides electrical isolation.

The primary flow of information between the two Gateway subsystems is from the safety subsystem to the non-safety subsystem. This information is a combination of plant process parameter values and equipment status information. The information that flows from the non-safety subsystem to the safety subsystem is limited to the following:

- The safety and non-safety subsystems exchange periodic interface signals that the communication controllers at each end of the link use to ensure that the link is functioning properly. These signals are used only by the communication controllers and are not propagated to the rest of the safety system. There is no application function in the safety system that uses this information.

- The main control room and the remote shutdown workstation operator consoles are non-safety. The soft control inputs to the PMS from these locations are provided from the non-safety subsystem to the safety subsystem of the Gateway.

The gateway provides both electrical and communication isolation between the non-safety systems and the PMS. Other than the isolation function, the gateway is not required for any PMS safety function. There is no potential signal from the non-safety system than will prevent the PMS from performing its safety functions.

Analog inputs required for both control and protection functions are processed independently with separate input circuitry. The input signal is classified as safety-related and is, therefore, isolated in the protection and safety monitoring system cabinet before being sent to the control system.

The plant protection and safety monitoring system also provides data to the plant control system pertaining to signals calculated in the subsystems, and to the data display and processing system.

Non-process signals are also provided to external systems. The non-process outputs inform the external systems of cabinet entry status, cabinet temperature, dc power supply voltages, and subsystem diagnostic status. Cabinet temperature sensing does not affect the safety-related function. The information is gathered for the sole purpose of analysis by external systems.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.012

Question:

420.12 (DCD 7.1.7, item 7)

DCD 7.1.7, item 7, WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Section 4.10.2, states that the protection and monitoring system (PMS) provides both system-level and component-level manual means of actuating ESF functions, and the diverse actuation system (DAS) provides manual means of actuating selected ESF functions. To support manual ESF actuation, both the PMS and the DAS provide plant information to the operator. Identify all the PMS and the DAS system-level and component-level manual actuation devices for every ESF function and the related supporting indications to the operator.

Westinghouse Response:

The manually actuated functions of the Protection and Safety Monitoring System (PMS) are described in DCD Tier 1 Section 2.5.2 and DCD Tier 2 Sections 7.1.2 and 7.3. The operator can perform the manual operations as specified in DCD Tables 7.2-4 and 7.3-3 using non-safety soft controls available at the operator workstations. In addition, the PMS provides a minimum inventory of safety-related dedicated manual actuation controls for the system-level actuations as specified in Table 18.12.2-1. The PMS manual controls are located on the Dedicated Safety Panel in the Main Control Room.

DCD Table 7.5-1 provides a list of the post-accident monitoring variables that are provided to the operator. All the variables listed in Table 7.5-1 are available on the non-safety operator workstations. Selected variables, as indicated in Table 7.5-1, are also available on the safety-related Qualified Data Processing Subsystem (QDPS) subsystem of PMS. The QDPS is described in DCD Tier 2 Section 7.1.2.5. Status of the PMS-actuated equipment is also displayed by the QDPS. The minimum inventory of displays and alerts is listed in DCD Tier 1 Table 2.5.2-5 and DCD Tier 2 Table 18.12.2-1.

The manually actuated functions and supporting indications of the Diverse Actuation System (DAS) are described in DCD Tier 1 Section 2.5.1 and DCD Tier 2 Section 7.7.1.11. Dedicated manual actuation controls are provided for the functions specified in DCD Tier 1 Table 2.5.1-2. DAS sensors and displays are listed in DCD Tier 1 Table 2.5.1-3 and described in DCD Tier 2 Section 7.7.1.11. The use of these indications to support diverse manual actuation is described in Section 7.7.1.11 under "Indication" on page 7.7-17. Status of the DAS-actuated equipment is not displayed by DAS, but rather by the post-accident monitoring system variables on QDPS; see Table 7.5-1.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

Design Control Document (DCD) Revision:

None

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.013 (Response Revision 1)

Question:

420.13 (DCD 7.1.7, item 7)

DCD 7.1.7, item 7, WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Section 4.11 states that the signal conditioning and data acquisition functions associated with these signals are performed by an independent subsystem in the PMS, not associated with the reactor trip or ESF actuation functions. Describe the system configuration with respect to this statement for both the AP600 system hardware and the Common Q system hardware.

Westinghouse Response:

The sentence cited from WCAP-15775 may be misleading and does not directly address NUREG/CR 6303 Guideline 13; therefore, WCAP-15775 will be modified as shown below.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

WCAP Revision:

WCAP-15775 will be revised as shown:

4.11 Plant Monitoring – Guideline 13

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, diverse operator indications. No sensors are shared between the RTS/ESFAS and the DAS. Diverse and independent signal conditioning and data acquisition functions will be performed in the RTS/ESFAS and DAS such that a postulated software common mode failure in either platform will not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the PMS to the PLS and the DDS. The connections between the PMS and the PLS and DDS contain isolation devices to prevent failures in the PLS or DDS from affecting operation of the PMS. ~~The signal conditioning and data acquisition functions associated with these signals are performed by an independent subsystem in the PMS, not associated with the reactor trip or ESF actuation functions.~~ Once signals leave the PMS through the isolation devices, they are no longer classed as safety, and are not used to provide any safety functions.

The signals from PMS to PLS and DDS meet the independence requirements of GDC-24, IEEE-603, IEEE-379, and IEEE-384.

No credible failure of the PLS or DDS will prevent the safety system from performing its safety function. Connections and software that are used for plant monitoring and for surveillance of the reactor trip and ESF actuation system do not significantly reduce the reliability of or increase the complexity of these systems.

The automatic functions of the PMS are designed to protect the AP1000 from potential operator-induced transients which may result from failures in the DDS or PLS.

NRC Additional Comments:

Please clarify was is meant by the phrase "do no significantly reduce" in the statement in the response that states that "[c]onnections and software that are used for plant monitoring and for surveillance of the reactor trip and ESF actuation system do not significantly reduce the reliability of or increase the complexity of these systems."

Westinghouse Additional Response:

WCAP-15775 will be revised as shown below:

WCAP Revision:

WCAP-15775 will be revised as shown:

4.11 Plant Monitoring – Guideline 13

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, diverse operator indications. No sensors are shared between the RTS/ESFAS and the DAS. Diverse and independent signal conditioning and data acquisition functions will be performed in the RTS/ESFAS and DAS such that a postulated software common mode failure in either platform will not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the PMS to the PLS and the DDS. The connections between the PMS and the PLS and DDS contain isolation devices to prevent failures in the PLS or DDS from affecting operation of the PMS. Once

signals leave the PMS through the isolation devices, they are no longer classed as safety, and are not used to provide any safety functions.

The signals from PMS to PLS and DDS meet the independence requirements of GDC-24, IEEE-603, IEEE-379, and IEEE-384.

No credible failure of the PLS or DDS will prevent the safety system from performing its safety function. The Gateway provides the ~~C~~connections ~~and software~~ that are used for plant monitoring and for surveillance of the reactor trip and ESF actuation subsystems~~ do not significantly reduce the reliability of or increase the complexity of these systems~~. The DDS provides the software and hardware that are used for displaying plant parameters and monitoring system performance.

The automatic functions of the PMS are designed to protect the AP1000 from potential operator-induced transients which may result from failures in the DDS or PLS.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.028

Question:

420.28 (DCD 7.1.7 item 11)

In the NRC's safety evaluation report (SER) on Common Q design (Reference 11 on DCD 7.1.7), the staff identified the following plant-specific action items for licensee to follow when the Common Q design is implemented in a specific plant. Please address each of these items applicable to the AP1000 Design Certification. If the action item can not be implemented during the design certification stage, then the action should be included in the Tier 1 Material (ITAAC).

1. Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements. (See Common Q SER Section 4.1.1.1.2)

2. A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the Flat-Panel Display System (FPDS). The review of the implementation of such a hardware user interface would be a plant-specific item. (See SER Section 4.1.2)

3. If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and is not to be used such that is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant-specific FMEAs. (See SER Section 4.2.1.2)

4. Each licensee implementing a Common Q application must verify that its plant environment data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. (See SER sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3)

CENP configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots. (See SER Section 4.2.2.1.2)

5. On the basis of its review of the CENP's software development process for application software, the staff concludes that the Software Program Manual (SPM) specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activity that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design output for specific application on a plant-specific basis. (See SER 4,3,2)

6. When implementing a Common Q safety system (i.e.,PAMS, CPCS, or DPPS), the licensee must review CENP's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. (See SER Sections 4.1.1.4, 4.4.1.3, 4.4.2.3, and 4.4.3.3)

7. The Operator's Module (OM) and the Maintenance Test Panel (MTP) provide the human machine interface for the Common Q platform. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis. (See SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 4.4.4.3.6)

8. If the licensee installs a Common Q PAMS, CPCS, or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is replaced, and meets the functionality requirement applicable to those systems. (See SER Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3)

9. Modifications to plant procedures and/or technical specifications due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification. (See SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 5.0)

10. A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) must prepare its plant-specific model for the design to be implemented and perform the PMEA for that application. (See SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 5.0)

11. If a licensee installs a Common Q PAMS, CPCS, DPPS or integrated solution, the licensee shall demonstrated that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control systems and meet the requirements of HICB BTP-19 in the NRC Standard Review Plan Chapter 7. (See SER Sections 4.1.6, 4.4.2.3, 4.4.3.3, 4.4.4.3.3, and 5,0)

12. A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing. (See SER Section 4.4.3.3)

13. The analysis of the capacity of the shared resources to accommodate the load increase due to sharing. (See SER Section 4.4.4.3.1)

14. The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items (See SER Section 5.0)

Westinghouse Response:

On August 11, 2000; the NRC issued a safety evaluation report regarding Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform, Appendices 1,2,3,4, Rev. 01 and CE-CES-195, Rev. 01, Software Program Manual for Common Q Systems. Section 6 of the safety evaluation report identified 14 plant specific action items (PSAIs). The applicability of each PSAI to the AP1000 Design Certification is discussed below.

PSAI 6.1
Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements.

Discussion: The suitability of all new components is assessed to meet applicable requirements in accordance with the Quality Assurance Program. Performance requirements for these components are assured, for example, by specifying them in purchase contracts, observing vendor testing and analysis, reviewing vendor documentation, performing design reviews by the engineering department, and by performing validation tests after installation. The Quality Assurance Program is described in DCD Chapter 17.

The Input/Output subsystem has been designed to fully meet the functional requirements for Common Q safety systems. The Input/Output subsystem will be deemed capable of performing its design function by successful completion of testing, culminating in a Factory Acceptance Test (FAT) to be performed by the vendor. Acceptance criteria will be based on the system requirements specification.

PSAI 6.2
A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The review of the implementation of such a hardware user interface would be a plant-specific action item.

Discussion: AP1000 safety systems will utilize the Flat Panel Display System (FPDS) as developed by Westinghouse for Common Q safety systems. An alternative hardware interface will not be used. Therefore, this action item is not applicable.

PSAI 6.3
If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and it is not to be used such that it is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant specific FMEAs.

Discussion: The FPDS' to be implemented in AP1000 I&C safety system are not required to be operational when the safety system is called upon to initiate automatic safety functions. The plant-specific FMEA will address the loss of the FPDS (see item 6.10 below). Additionally, the NRC has stated that this action item has been resolved and is considered closed. Therefore, no further evaluation is required.

PSAI 6.4
Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests.

Westinghouse configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots.

Discussion: Common Q safety equipment will be located in the Auxiliary Building in a mild (non-harsh) environment. Therefore, age related degradation is expected to be insignificant for temperature and humidity.

The AP1000 temperature and humidity conditions for qualification of protection and safety monitoring system equipment are presented in DCD Appendix 3D. Temperature and humidity qualification of the protection and safety monitoring system equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, item 4.

The protection and safety monitoring system seismic Category I equipment will be tested or analyzed to confirm that it can withstand seismic design basis loads without loss of safety function. The seismic qualification of the protection and safety monitoring system seismic Category I equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, item 2.

The protection and safety monitoring system equipment will be tested or analyzed to confirm that it has electrical surge withstand capability (SWC), and can withstand the electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before during and following a design basis accident without loss of safety function for the time required to perform the safety function (DCD Tier 1 (ITAAC) 2.5.2, item 3).

PSAI 6.5
On the basis of its review of the Westinghouse software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant specific basis.

Discussion: In accordance with the Quality Assurance Program, administrative control procedures are used to establish software quality assurance and configuration management for process computer software, firmware and associated software development, computer systems, and associated documentation. They ensure that the integrity of a process software product is known and preserved throughout its life cycle (from development to retirement). These controls also apply to the development tools and systems used to develop and test process software. The Quality Assurance Program is described in DCD Chapter 17. The software life cycle process is covered by DCD Tier 1 (ITAAC) 2.5.2, item 11.

PSAI 6.6
When implementing a Common Q safety system (i.e. PAMS, CPCS, or DPPS), the licensee must review Westinghouse's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report.

Discussion: The accuracy and response time of the AP1000 safety systems will be commensurate with the Chapter 15 Safety Analysis. The Combined License applicant is responsible for the setpoint analysis (DCD Section 7.1.6). The setpoint analysis (including accuracy and time response) is covered by DCD Tier 1 (ITAAC) 2.5.2, item 10.

PSAI 6.7
The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis.

Discussion: This is a human factors issue. The human factors engineering program is described in DCD Chapter 18. The human factors program is the responsibility of the Combined License applicant and is covered by DCD Tier 1 (ITAAC) 3.2.

PSAI 6.8
If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems.

Discussion: The AP1000 is a new plant safety system installation; therefore, this action item is not applicable.

PSAI 6.9
Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification.

Discussion: The AP1000 is a new plant safety system installation; therefore, this action item is not applicable. The Combined License applicant is responsible for plant procedures (see DCD Section 13.5).

PSAI 6.10
A licensee implementing any Common Q applications (i.e., PAMS, CPCS, or DPPS) must prepare its plant specific model for the design to be implemented and perform the FMEA for that application.

Discussion: An FMEA will be performed for each AP1000 safety system. The FMEAs will confirm that no single failure of a safety system component will defeat more than one of the four protective channels, assuring proper protective action at the system level. DCD Table 1.8-2 and Section 7.2.3 will be modified as shown below to add this item.

PSAI 6.11
If a licensee installs Common Q PAMS, CPCS, DPPS or Integrated Solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control system and meets the requirements of HICB BTP-19.

Discussion: The response to RAI Number 420.014 provides a discussion on AP1000's compliance with BTP HICB-19.

PSAI 6.12
A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing.

Discussion: A formal methodology will be defined for response time testing of AP1000 safety systems. This methodology is covered by DCD Tier 1 (ITAAC) 2.5.2, item 10.

PSAI 6.13
The analysis of the capacity of the shared resources to accommodate the load increase due to sharing.

Discussion: The shared resource issue relates to multiple Common Q based systems using the same resources such as the AF100 bus or an Operator Module. An analysis will be performed to ensure that the capacity of shared resources for AP1000 safety systems is commensurate with anticipated loads. This issue will be addressed as part of the design process that is covered by DCD Tier 1 (ITAAC) 2.5.2, item 11.

PSAI 6.14
The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items.

Discussion:
Section 7.1.4.1 of the DCD describes conformance of the AP1000 safety system Instrumentation to applicable safety criteria. The safety-related system instrumentation described in subsection 7.1.1 is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. Applicable General Design Criteria are listed in Section 3.1, NRC Regulatory Guides in subsection 1.9.1, and Branch Technical Positions in subsection 1.9.2. Industry Standards are cited as references.

Design Control Document (DCD) Revision:

Table 1.8-2 (Sheet 3 of 6)

SUMMARY OF AP1000 STANDARD PLANT
COMBINED LICENSE INFORMATION ITEMS

Item No.	Subject	Subsection
7.1-1	Setpoint Calculations for Protective Functions	7.1.6
7.2-1	FMEA for protection system	7.2.3

7.2.3 Combined License Information

Combined License applicants referencing the A1000 certified design will provide an FMEA for the protection and safety monitoring system ~~This section has no requirement for information to be provided in support of the Combined License application.~~

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.029

Question:

420.29 (DCD 7.1.7, item 11)

In the NRC's safety evaluation report on Common Q design (Reference 11 in DCD 7.1.7), the staff identified 10 Generic Open Items. Provide a discussion on the resolution on each of those open items. If a specific item can not be resolved during the design certification stage, then the action should be included in the Tier 1 Material (ITAAC).

Westinghouse Response:

On August 11, 2000; the NRC issued a safety evaluation report regarding Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform, Appendices 1,2,3,4, Rev. 01 and CE-CES-195, Rev. 01, Software Program Manual for Common Q Systems. Section 7 of the safety evaluation report identified 10 generic open items (GOIs). Each GOI and its resolution are discussed below.

GOI 7.1
Westinghouse (formerly CENP) "has committed to develop a new I/O module or re-design some of those already considered for use in the Common Q platform in order to meet the performance requirements of EPRI TR-107330."

Resolution: A new I/O module, the AI685, has been developed and qualified. The previous resistance-temperature detector (RTD) and thermocouple (T/C) modules did not have adequate sampling time for inputs required for protection. The AI685 can be configured for use as a voltage, RTD, or T/C analog input and has been qualified for environmental, seismic and EMC conditions. The design and qualification is documented in, "Summary Qualification Report of Hardware Testing for Common Q Applications", 00000-ICE-37764, Revision 00. This report was submitted to the NRC in August 2002. An NRC Meeting was held October 2, 2002 to review the Common Q August submittal. The NRC is currently evaluating the information submitted and is working to provide Westinghouse with a supplemental safety evaluation report that is expected to close GOI 7.1.

GOI 7.2
Westinghouse (formerly CENP) "has not yet finalized the selection of the Common Q power supplies."

Resolution: The Common Q Power Supply System has been developed and qualified. This is documented in, "Summary Qualification Report of Hardware Testing for Common Q Applications, 00000-ICE-37764, Revision 00. This report was submitted to the NRC in August 2002. An NRC Meeting was held October 2, 2002 to review the Common Q August submittal. The NRC is currently evaluating the information submitted and is working to provide Westinghouse with a supplemental safety evaluation report that is expected to close GOI 7.2.

GOI 7.3
Westinghouse (formerly CENP) "has not submitted information on the design or dedication of the hardware watchdog timer and it has not yet been subjected to testing for environmental qualification."

Resolution: The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q Systems. Environmental qualification testing of the PM646A has been completed. This is documented in, "Summary Qualification Report of Hardware Testing for Common Q Applications, 00000-ICE-37764, Revision 00. This report was submitted to the NRC in August 2002. A revision to the Common Q Topical Report was also submitted that describes the use of the internal PM646A watchdog timer. An NRC Meeting was held October 2, 2002 to review the Common Q August submittal. The NRC is currently evaluating the information submitted and is working to provide Westinghouse with a supplemental safety evaluation report that is expected to close GOI 7.3.

GOI 7.4
Westinghouse (formerly CENP) "has committed to arrange a value-added reseller agreement with QSSL that is similar to BA AUT-99-ADVANT-00, the value-added reseller agreement it has with ABB products. A value-added reseller agreement is needed to satisfy the configuration control and incoming inspection requirements of EPRI TR-106439."

Resolution: On June 22, 2001 the NRC issued, "Safety Evaluation by the Office of Nuclear Reactor Regulation related to the Closeout of Several of the Common Qualified Platform Category 1 Open Items." This report states that the staff has reviewed the value-added reseller agreement with QNX Software Systems Limited (QSSL), the vendor for the flat panel display system (FPDS) operating system and display system, and concludes that it satisfies the configuration control and incoming inspection guidance of EPRI TR-106439. The reseller agreement is, therefore, acceptable. This closes GOI 7.4.

GOI 7.5
Westinghouse (formerly CENP) "will perform additional EMC tests and measurements on the PM646."

Resolution: The PM646 processor module has been modified to the PM646A. This modification involved the removal of an internal terminating resistor for the High-Speed Data links (HSLs). The link termination resistor is now external to the module, permitting several high-speed data links to be connected in parallel. Additional EMC tests and measurements were performed using the PM646A. These tests are documented in, "Summary Qualification Report

of Hardware Testing for Common Q Applications", 00000-ICE-37764, Revision 00. This report was submitted to the NRC in August 2002. A revision to the Common Q Topical Report was also submitted that describes the modification of the PM646 to the PM646A. An NRC Meeting was held October 2, 2002 to review the Common Q August submittal. The NRC is currently evaluating the information submitted and is working to provide Westinghouse with a supplemental safety evaluation report that is expected to close GOI 7.5.

GOI 7.6
Westinghouse (formerly CENP) "has not yet conducted seismic and environmental qualification testing on the non-AC160 hardware components. Items not yet tested include the FPDS, watchdog timer, and power supply modules."

Resolution: Seismic and environmental qualification testing on the non-AC160 hardware components has been completed. These components include the FPDS and the power supply modules. The external watchdog timer is no longer required. The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q Systems. The seismic and environmental testing is documented in, "Summary Qualification Report of Hardware Testing for Common Q Applications", 00000-ICE-37764, Revision 00. This report was submitted to the NRC in August 2002. A revision to the Common Q Topical Report was also submitted that describes the use of the internal PM646A watchdog timer. An NRC Meeting was held October 2, 2002 to review the Common Q August submittal. The NRC is currently evaluating the information submitted and is working to provide Westinghouse with a supplemental safety evaluation report that is expected to close GOI 7.6.

GOI 7.7
"The staff has reviewed the information in the SVVP about software module testing and finds that the information provided is not sufficient for the staff to arrive at a conclusion about the adequacy of the scope of the tests for validating a software module."

Resolution: On June 22, 2001 the NRC issued, "Safety Evaluation by the Office of Nuclear Reactor Regulation related to the Closeout of Several of the Common Qualified Platform Category 1 Open Items." This report states that Westinghouse submitted additional information indicating in which sections of CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems", and topical report CENPD-396-P, Rev. 1, "Common Qualified Platform," the staff would find the Westinghouse Nuclear Automation (WNA) procedures for performing software module testing. The staff has reviewed the indicated sections and concludes that the procedures specified therein satisfy the software verification and validation program (SVVP) requirements of IEEE Std 7-4.3.2-1993 with regard to testing of software modules and are, therefore, acceptable. This closes GOI 7.7.

GOI 7.8
Westinghouse (formerly CENP) "needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components."

Resolution: This GOI relates to the "level 3 loop controllers" referenced in the Integrated Solution Appendix. The level 3 controllers provide component control based on signals from the ESFAS. This component will require a future submittal for NRC staff review; therefore GOI 7.8 will remain an open item. The Combined License applicant will be responsible for resolution of this GOI. DCD Table 1.8-2 and Section 7.1.6 will be revised accordingly. DCD Tier 1 Section 2.5.2 (ITAAC) does not need to be revised because it adequately covers the functional and design process requirements for the protection system.

GOI 7.9

"The staff has reviewed the approach for the integrated solution of using the ITPs and the AF100 buses to provide separation of safety and nonsafety signals and finds that there is not sufficient detail to permit an evaluation against the independence requirements set forth in IEEE Std 7-4.3.2. This must be the subject of a future {Westinghouse (formerly CENP)} submittal."

Resolution: On June 22, 2001 the NRC issued, "Safety Evaluation by the Office of Nuclear Reactor Regulation related to the Closeout of Several of the Common Qualified Platform Category 1 Open Items." This report states that Westinghouse has revised Appendix 4, "Common Qualified Platform Integrated Solution," to provide additional information on the use of the interface and test processors (ITPs) and the AF100 buses to provide separation of safety and non-safety signals. The staff has reviewed the revised information in Appendix 4, Rev. 2 on the use of the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that the conceptual approach as presented therein is consistent with the independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concludes that this conceptual approach may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital instrumentation and control (I&C) upgrades. This closes GOI 7.9 as far as the conceptual approach is concerned, but the evaluation of each forthcoming design remains a plant-specific action item because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants. The Combined License applicant will be responsible for resolution of this plant-specific action item.

In the AP1000 I&C configuration the interface between the safety system and the non-safety system will be implemented via the maintenance and test panel (MTP). The function of this interface is to provide communications between the AF100 bus of the Common Q safety system and the data highway of the non-safety system. The physical means of transferring data between the safety system and non-safety system is a Fast Ethernet data link using fiber optic media. One node of the Ethernet data link is the MTP flat panel display system. The other node of the Ethernet data link is a non-safety workstation, which is a drop on the non-safety system data highway.

GOI 7.10

"The evaluation of the design for the multichannel operator station control for the integrated solution requires detail beyond the scope of the present submittals."

Resolution: On June 22, 2001 the NRC issued, "Safety Evaluation by the Office of Nuclear Reactor Regulation related to the Closeout of Several of the Common Qualified Platform Category 1 Open Items." This report states that Westinghouse has revised Appendix 4 to provide additional information on the multi-channel operator station control. Westinghouse does not intend for Appendix 4, Rev. 2 to contain sufficient detail to permit the staff to evaluate any plant-specific multiple upgrade. However, Westinghouse requested the staff to evaluate the concept of the multi-channel operator station with regard to potential adverse multi-channel interaction.

The staff reviewed the design concepts presented in Appendix 4, Rev. 2, and found that the multi-channel operator stations can control most Class 1E components directly and use the ITPs and the AF100 buses discussed in GOI 7.9 above, to provide separation of safety and non-safety signals. In the AP1000 design the Class 1E signals will override any erroneous signal that may originate from non-safety equipment; therefore, manual release switches are not needed.

The AP1000 control room uses the compact workstation (CW) variation of the non-safety, multi-channel operator station. In the CW design, the multi-channel operator stations are part of the safety system. They utilize the Common Q FPDS, which the staff has approved as a Class 1E HMI device, subject to its successful performance during qualification testing. Westinghouse has determined that each CW console meets all qualification and single failure requirements for display and control of Class 1 E functions. As a result, the Common Q channelized operator modules and channelized post accident monitoring instrumentation and safe shutdown displays, which serve as credited backup HMI devices for the non-safety multi-channel operator station design, would not be required in the AP1000 CW version of the implementation of the multi-channel operator station. Therefore, the AP1000 MCR soft control display units are not classified as Class 1E and are not required to be environmentally qualified. These components will be removed from DCD Table 3.11-1.

The staff reviewed the revised information in Appendix 4, Rev. 2 with regards to the use of the multi-channel operator station including the Integrated Solution CW variation and found the conceptual approach to be free of potential for adverse multi-channel interaction and is consistent with the Class 1E independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concluded that the conceptual approach employing multi-channel operator stations may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital I&C upgrades. This closes GOI 7.10 as far as the conceptual approach is concerned. The evaluation of each forthcoming design remains a plant-specific action item because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants. The Combined License applicant will be responsible for resolution of this plant-specific action item. DCD Table 1.8-2 and Section 7.1.6 will be revised accordingly. DCD Tier 1 Section 2.5.2 (ITAAC) does not need to be revised because it adequately covers the functional and design process requirements for the protection system.

Design Control Document (DCD) Revision:

Table 1.8-2 (Sheet 3 of 6)

SUMMARY OF AP1000 STANDARD PLANT
COMBINED LICENSE INFORMATION ITEMS

Item No.	Subject	Subsection
7.1-1	Setpoint Calculations for Protective Functions	7.1.6
7.1-2	Resolution of generic open items and plant-specific action items.	7.1.6

Table 3.11-1 (Sheet 17 of 45)

ENVIRONMENTALLY QUALIFIED ELECTRICAL AND MECHANICAL EQUIPMENT

Description	AP1000 Tag No.	Envir. Zone (Note 2)	Function (Note 1)	Operating Time Required (Note 5)	Qualification Program (Note 6)
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSA01~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSA02~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSB01~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSB02~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSC01~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSC02~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSD01~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~
~~MCR Soft Control Display Unit~~	~~PMS-JY-SCSD02~~	~~3~~	~~ESF~~	~~24 hr~~	~~E~~

7.1.6 Combined License Information

Combined License applicants referencing the AP1000 certified design will provide a calculation of setpoints for protective functions consistent with the methodology presented in Reference 5. Reference 5 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans.

Combined License applicants referencing the A1000 certified design will provide resolution for generic open items and plant-specific action items resulting from NRC review of the I&C platform.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.044

Question:

420.44 (DCD Tier 1, Section 2.5.2)

Provide a copy of the Software Requirements Specification for the PMS software including the safety requirements that the software is to perform.

Westinghouse Response:

A copy of the Ringhals Unit 2 TWICE Project Safety System Software Requirements Specification, NABU-DS-00117-SSP, Revision C/PRE, February 2002, can be made available for NRC review at Westinghouse offices. This is as an example of a Software Requirements Specification. An AP1000 Software Requirements Specification for the protection and safety monitoring system (PMS) software will be prepared during the detailed design of the PMS and will be similar to the Ringhals document.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.045 (Response Revision 1)

Question:

420.45 (DCD Tier 1, Section 2.5.2)

Describe the method of safety analysis that will be performed on the PMS and its components to ensure the PMS will perform as specified and that failure have been identified.

Westinghouse Response:

Several activities will be performed to validate that the protection and safety monitoring system (PMS) will meet the stated functional requirements. These include the following:

a. Subjecting the PMS to environmental and seismic testing or referencing the results of applicable tests that have already been conducted, on the product line (ITAAC 2.5.2, items 2 and 4),
b. Subjecting the PMS to Electromagnetic Interference (EMI) testing or referencing the results of applicable tests that have already been conducted on the product line (ITAAC 2.5.2, item 3),
c. Performing a system level Failure Mode and Effects Analysis (FMEA) to demonstrate the PMS architecture is not susceptible to postulated single random failures (COL item, see response to RAI 420.028),
d. Use of a structured software life cycle process, per IEEE Std. 7-4.3.2, to minimize the possibility of software common mode failure errors (ITAAC 2.5.2, item 11), and
e. Subjecting the PMS to a Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) to validate the system meets the stated functional requirements (ITAAC 2.5.2, items 5, 6, 8, and 9),
f. Performing preoperational tests as described in DCD subsection 14.2.9.1.12,
g. Performing startup tests as described in DCD subsections 14.2.10.1.8 and 14.2.10.1.10.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

NRC Additional Comments:

The staff does not consider RAI response a,b,e,f, and g to be methods of safety analysis and, while important steps in the engineering life-cycle, are not considered methods of safety analysis. Items c and, to some degree, d meet the intent of the RAI with follow-up questions. A system level failure modes and effects analysis (FMEA) may be insufficient in detail to determine failure modes of such components as the gateway—and its components, the communication interfaces used between channels and isolation devices. What level of detail is considered sufficient for the proposed system level FMEA? Please provide a rationale for the level of detail

Westinghouse agreed to revise the RAI response and the DCD to include a Software Hazards Analysis as part of the COL action item to perform an FMEA.

Westinghouse Additional Response:

The FMEA will include a Software Hazards Analysis. DCD section 7.2.3 will be revised as shown below:

Design Control Document (DCD) Revision:

7.2.3 Combined License Information

Combined License applicants referencing the A1000 certified design will provide an FMEA for the protection and safety monitoring system. The FMEA will include a Software Hazards Analysis.

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

RAI Number: 420.046

Question:

420.46 (DCD Tier 1, Sections 2.5.1, 2.5.3, 2.5.4, 2.5.5, 2.5.6, and 2.5.7)

Describe the architecture of the real-time data network and how the information is used to control and monitor the plant. This includes the network in the PLS and the one that interfaces with the DDS, DCS PLS, IIS, SMS and the DAS.

Westinghouse Response:

Chapter 7 of the DCD currently depicts the real-time data networks in two segments. The first segment is located entirely within the Plant Control System (PLS). The second segment resides primarily in the Data Display and Processing System (DDS), but also interfaces to the Protection and Safety Monitoring System (PMS), the Incore Instrumentation System (IIS), and the Special Monitoring System (SMS). That segmentation is not driven by a functional requirement and will be removed from DCD Figure 7.1-1.

There is one real-time data network that provides the communication backbone for all of the non-Class 1E instrumentation and control systems. The network will also interface to the Class-1E systems through electrical isolation devices and communication buffering devices that are part of the safety system and prevent degradation of the safety function. While the exact implementation and topology of the real-time data network will depend on the communication technology available at the time of deployment, the following characteristics are required:

1. Availability commensurate with the requirements of functions using the network
2. Maximum Data Latency commensurate with the requirements of functions using the network

The real-time data network is primarily used to provide the following control and monitoring functions:

1. Distributed Non-Safety Plant Control System (PLS) - The PLS is used to control the reactor, the turbine, and balance of plant functions. The network is used for manual soft control, supervisory control, alarming, data logging, maintenance, and diagnostics.

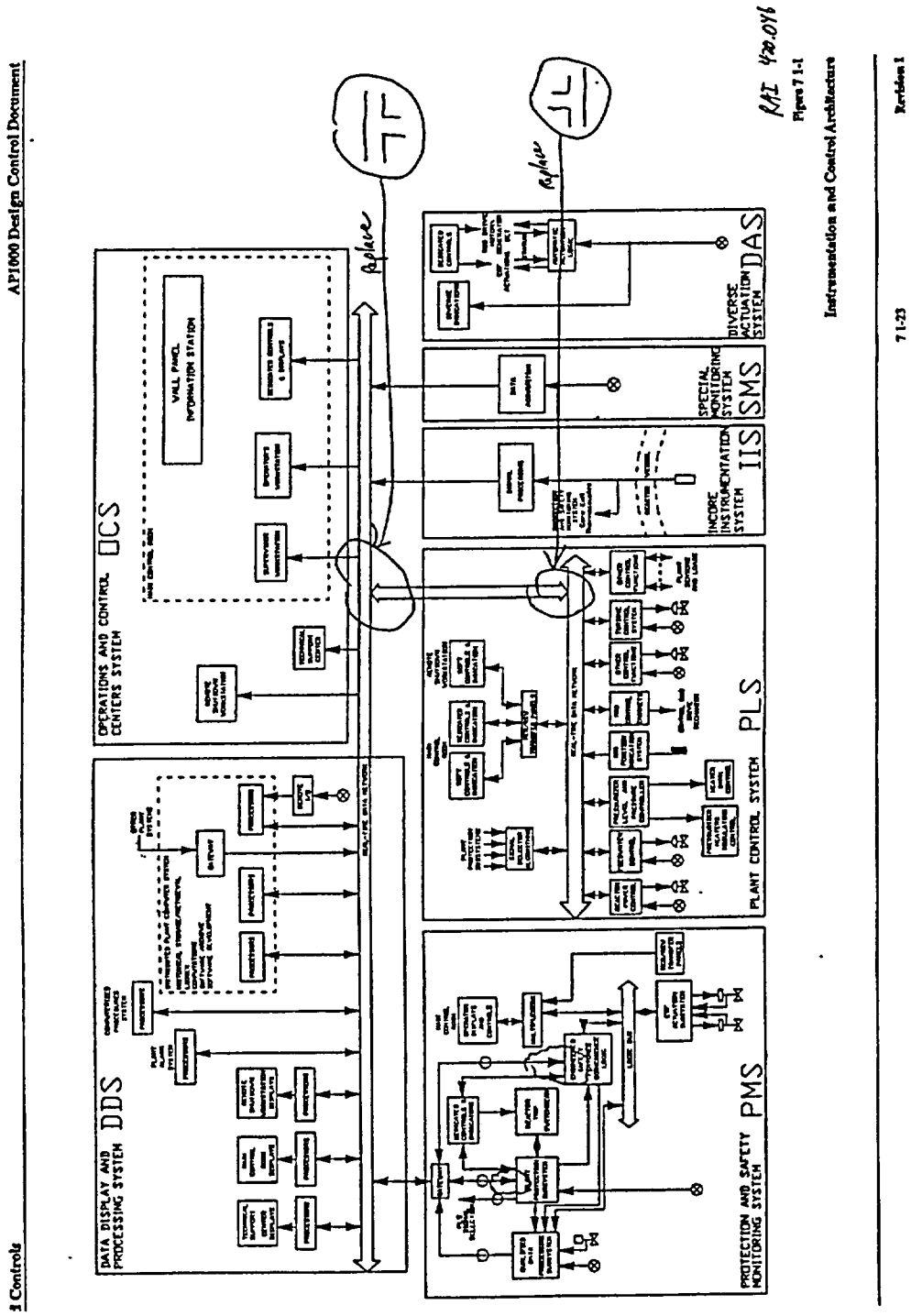
2. Data Display and Processing System (DDS) – The DDS provides the traditional plant computer functions including historical data storage and retrieval, data display, data logging, nuclear application programs (plant models and associated calculations). These functions are implemented using a number of computational and display resources that are distributed on the real-time data network. These resources include workstations, storage devices, and computational processors.

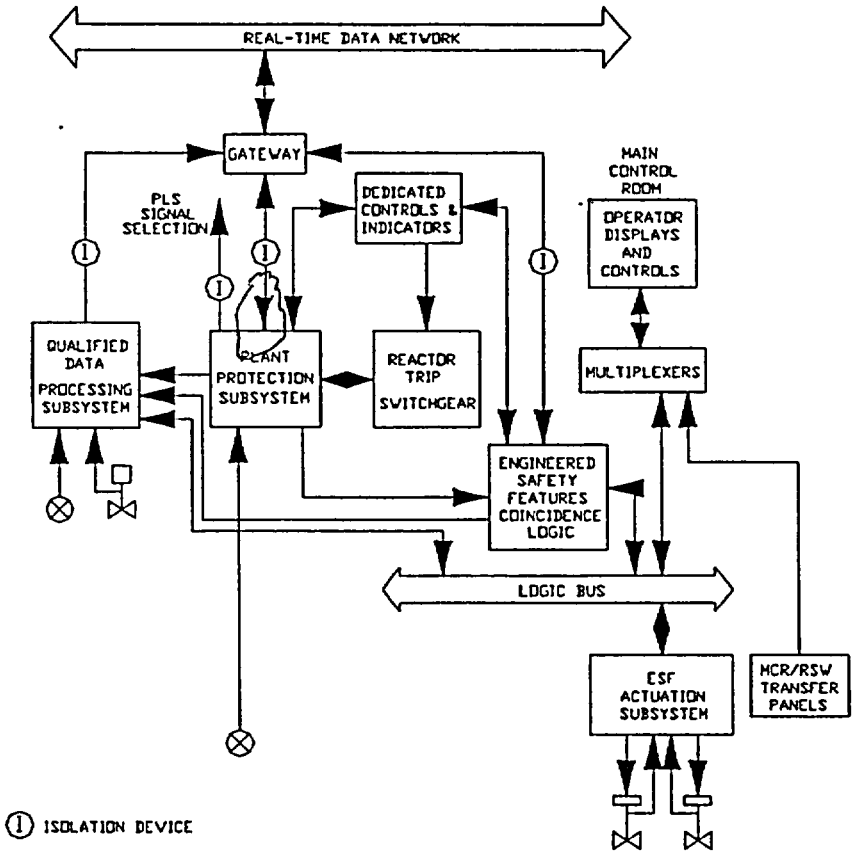
3. Supervision and Limited Control of the Safety Systems - The real-time data network is connected to a Gateway in each of the safety divisions. The Gateway provides electrical and functional isolation between the safety system and the non-safety system. The primary data flow between the systems is the transfer of plant status, safety system status, and diagnostic information from the safety system to the non-safety systems. The primary use of this data is for plant computer functions and historical data logging. Data flow from the non-safety system into the safety system is used primarily for manual control of the ESF system. These control signals are validated by the safety system prior to action being taken. The validation either takes the form of logic that prevents inhibiting of an automatic safety function or confirmation of action with the operator where there is no automatic safety function. Further details are available in Appendix 4 of the Common Q Topical Report. DCD Figure 7-1.1 will be revised within the PMS to make the arrows between the gateway and both the plant protection subsystem and the engineered safety features coincidence logic bi-directional. Figure 7.1-2 will be revised to make the arrow between the gateway and the plant protection subsystem bi-directional.

4. Interfaces to Other Systems – Gateways and firewalls provide for the controlled transfer of data between the real-time data network and external system.

It should be noted that the Diverse Actuation System is a completely standalone system and does not interface to the real-time data network.

Design Control Document (DCD) Revision:


AP1000 Design Control Document
3 Controls
OPERATIONS AND CONTROL CENTERS SYSTEM
OCS
VALL PANEL INFORMATION STATION
DATA DISPLAY AND PROCESSING SYSTEM
DDS
REAL-TIME DATA NETWORK
PLANT CONTROL SYSTEM
PLS
PROTECTION AND SAFETY MONITORING SYSTEM
PMS
INCORE INSTRUMENTATION SYSTEM
IIS
SPECIAL MONITORING SYSTEM
SMS
DIVERSE ACTUATION SYSTEM
DAS
Replace
Replace
RAI 420.046
Figure 7.1-1
Instrumentation and Control Architecture
7.1-23
Revision 1



RAI 420.046

Figure 7.1-2

Protection and Safety Monitoring System

AP1000 DESIGN CERTIFICATION REVIEW

Response to Request For Additional Information

PRA Revision:

None