



A BNFL Group company

AP1000 I&C Design (DCD Chapter 7 Overview)

March 5, 2003

Tom Hayes
Passive Plant Projects
412-374-4420 - hayestp@westinghouse.com



Slide 2



AP1000 I&C Systems

- DDS – Data Display and Processing System – same as AP600
- SMS – Special Monitoring System – same as AP600
- PMS – Protection System
- PLS – Plant Control System
- DAS – Diverse Actuation System
- IIS – Incore Instrumentation System – same as AP600 (except 42 vs. 38 detectors)



Slide 3

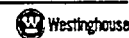


AP1000 Protection System

- Design process (not the design) was certified for AP600
 - The intent is to allow use of current technology
 - Product-specific design information has been deleted
- AP600 PMS design based on Eagle Technology (e.g., Sizewell)
- Common Q technology is now available



Slide 4



AP1000 Protection System

- Common Qualified Platform
 - Common Q design process not identical to AP600 licensed process
 - Common Q terminology (e.g., cabinet names) is different from Eagle
 - Attempted to use 'product-neutral' terminology in AP1000 DCD



Slide 5

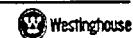


AP1000 Protection System

- Common Qualified Platform
 - Common Q features are not identical to Eagle
 - Common Q bypass logic only allows one bypass
 - If a second redundant channel needs to be removed from service, it must be placed in partial trip
 - Common Q testing features differ from Eagle



Slide 6



AP1000 Protection System

- AP1000 protection system functional design is the same as AP600 except:
 - Time delay added to turbine trip
 - Some changes to PAMS table:
 - Accumulator pressure replaces accumulator level
 - Added water-cooled chiller status
 - 22 editorial changes
 - 6 range changes
 - 8 category changes
 - 7 changes to QDPS requirements
 - 4 changes to qualification requirements
 - 3 changes to number of required instruments



Slide 7

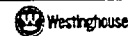


AP1000 Protection System

- Licensing basis for AP1000 is IEEE-603 (vs. IEEE-279 for AP600)
 - Both AP600 and AP1000 meet IEEE-603
 - Licensing basis change to IEEE-603 did not require any change to the design



Slide 8



AP1000 Plant Control System

- Changes from AP600 are those driven by plant differences, e.g.:
 - 3 single-speed feed pumps (vs. 2 variable-speed pumps for AP600)
 - Variable-speed RCPs for low reactor coolant temperature
 - 69 CRDMs with 267 steps (vs. 61 / 228 for AP600)
 - Rod control logic changes (4 gray rod banks vs. 2)



Slide 9



AP1000 Plant Control System

- Signal Selector Algorithm
 - Software function in distributed controllers
 - Not a hardware device
 - Selects 'best' value from redundant measurements
 - 3 signals are sufficient to meet control/protection system interaction requirements of IEEE 603



Slide 10



AP1000 Diverse Actuation System

- Limited scope system
 - PRA based displays & controls
 - Backs up PMS where common mode failure is risk important
- Microprocessor / software based (Automatic functions)
- Different architecture, hardware & software than PMS
- No multiplexing



Slide 11

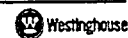


AP1000 Diverse Actuation System

- Manual controls and indications use no software
 - Direct wiring to actuation devices (e.g., pilot solenoids for AOVs)
 - Meets Branch Technical Position HICB-19, Position 4
- Separate sensors from PMS and PLS
- Same as AP600 except:
 - Containment hydrogen indicators deleted from DAS
 - Time delay added to turbine trip



Slide 12



AP1000 Advanced Control Room

- **Compact Control Room**
 - Designed for 1 Reactor Operator and 1 Supervisor
- **Displays**
 - Plant status / overview via wall panel (DDS, non 1E)
 - Detail display via workstation video displays (DDS, non 1E)
 - Small number of dedicated displays; safety (PMS, 1E) & diverse (DAS, non 1E)



Slide 13



AP1000 Advanced Control Room

- **Controls**
 - Soft controls (DDS, non 1E)
 - Small number of dedicated switches; safety (PMS, 1E) & diverse (DAS, non 1E)
- **Advanced Alarm Management**
- **Computer Based Procedures**



Slide 14

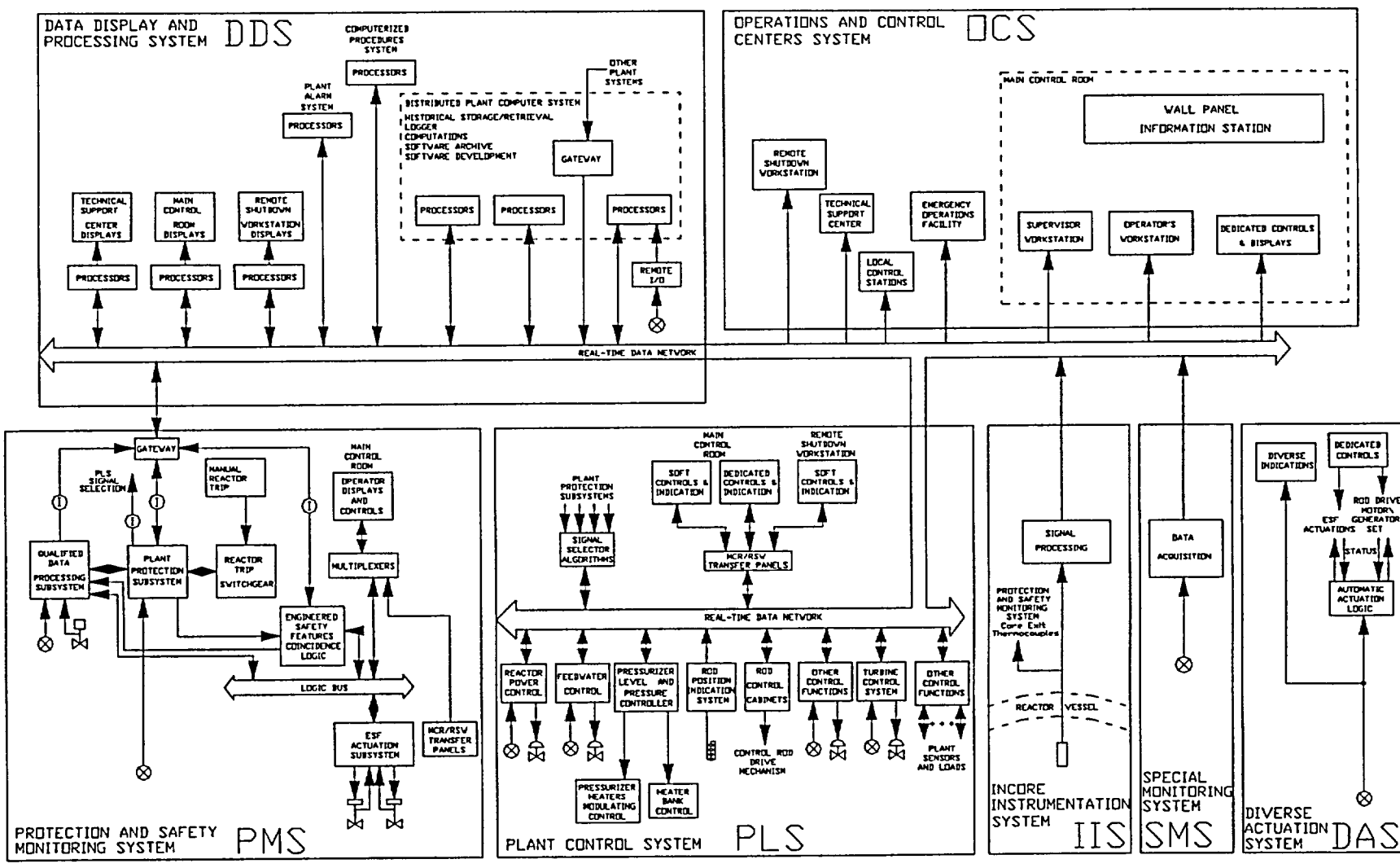


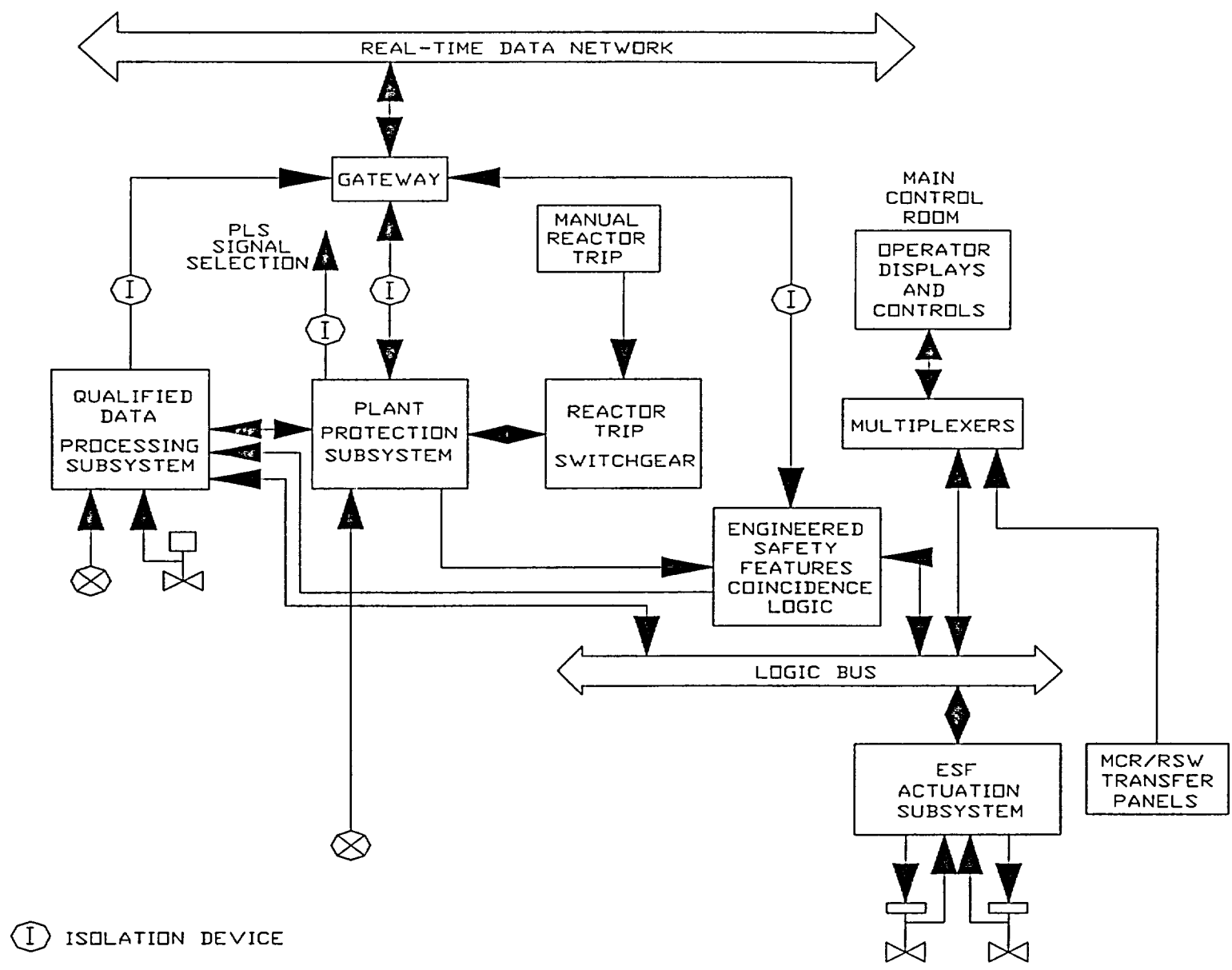
AP1000 Soft Controls

- Normal operations use non-1E soft controls on operator's desk (DDS)
 - No failure in the non-1E system will prevent automatic or manual 1E operation
- Remote Shutdown Workstation is same as one operator position
 - Non-1E

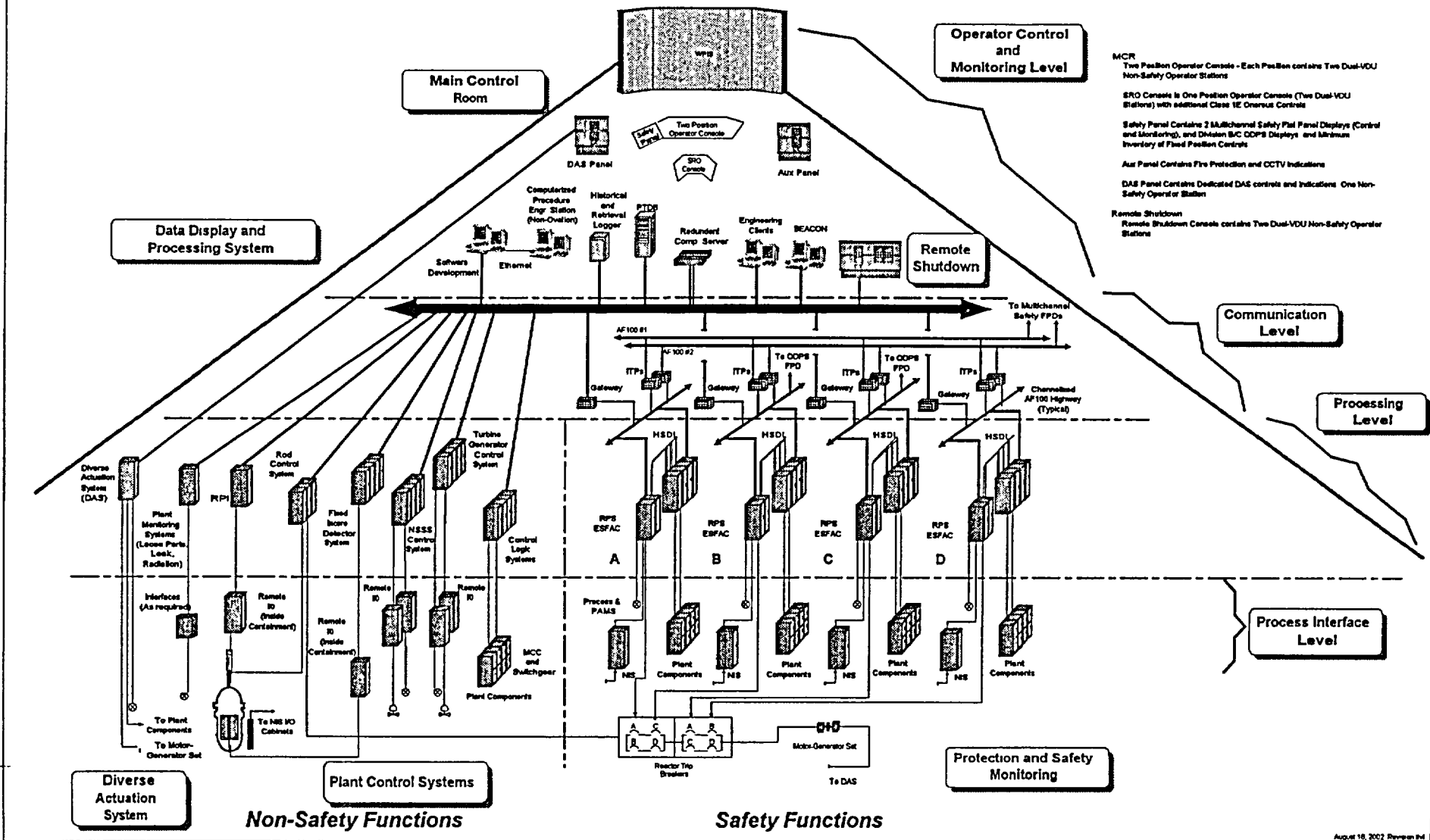
AP1000 Soft Controls

- Class 1E system-level backup provided by dedicated switches (PMS)
 - Component-level control also available at dedicated safety panel
- Small number of dedicated diverse switches (DAS)
 - Hardwired to actuation device

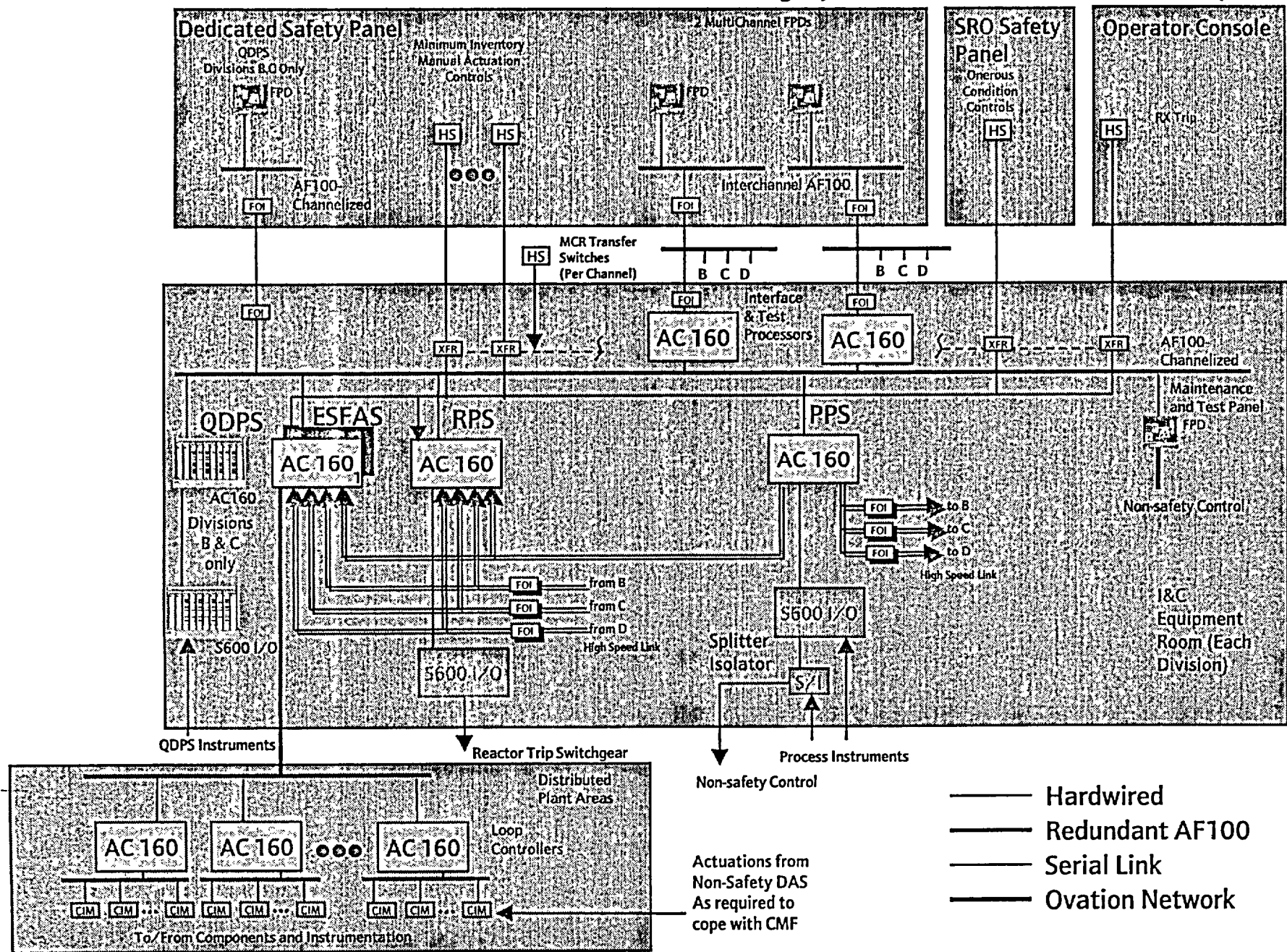




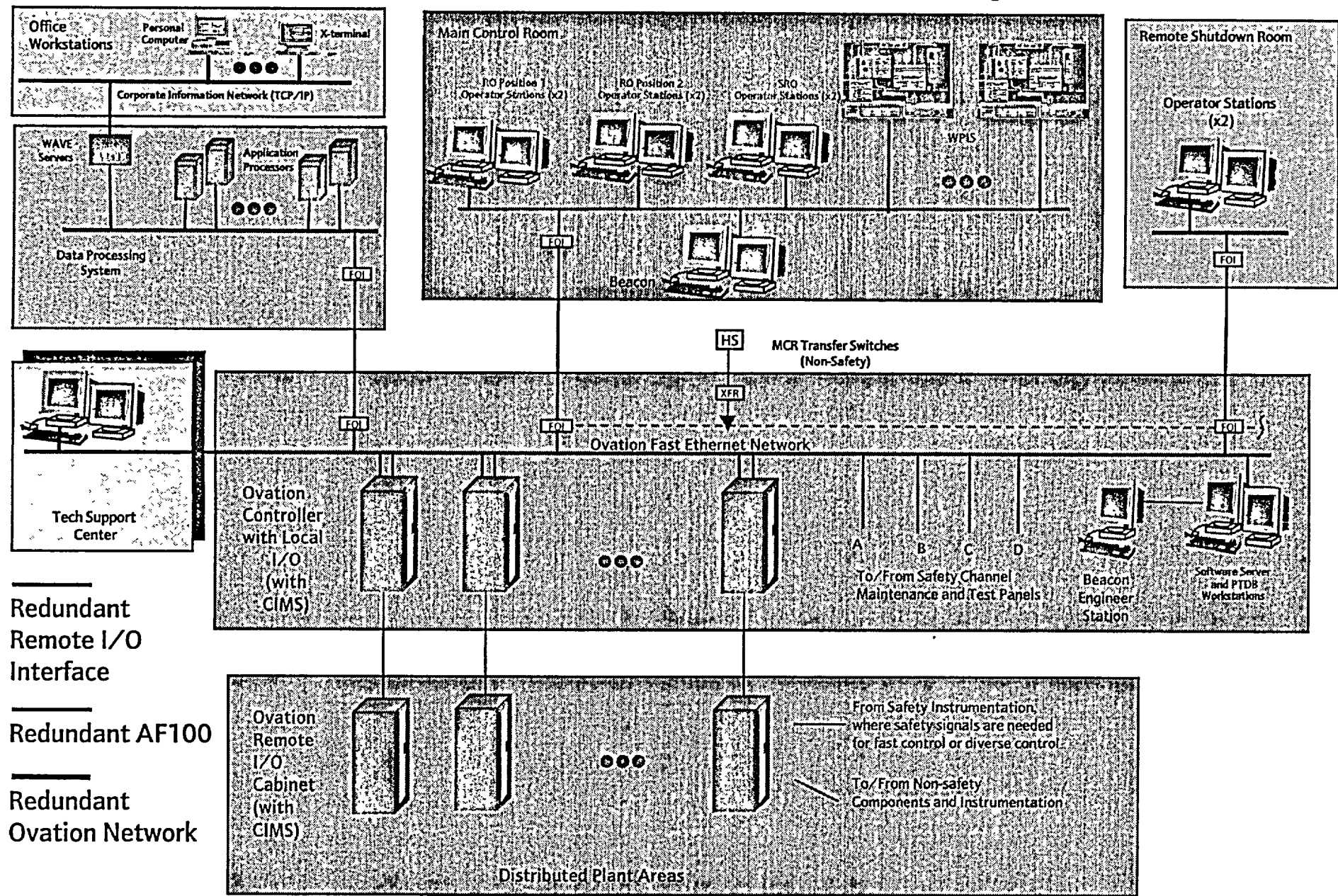
AP1000 I&C System Architecture



AP 1000 Architecture - Safety (one of four divisions)



AP 1000 Architecture - Non-Safety



Common Q Licensing Status

AP 1000 Meeting

Monroeville, Pennsylvania

March 5, 2003



00000A. 1

70787Alpha. 1



NRC Safety Evaluation Status

- August 11, 2000; the staff issued a Safety Evaluation (SE) regarding:
 - Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform
 - Appendices 1,2,3 & 4, Rev. 01
 - CE-CES-195, Rev. 01, Software Program Manual for Common Q Systems



00000A 2

70787Alpha.2



NRC Safety Evaluation Status (Continued)

- The Common Q SE identified 10 generic open items
 - Westinghouse intends to close all items by March 2003 except for item 7.8 (Identification of Loop Controllers in the Integrated Solution Appendix)
 - The closure of this item will be scheduled after the completion of the Common Q Phase 3 Project
- The Common Q SE identified 14 plant specific action items
 - Westinghouse intends to close out 3 of these items



NRC Safety Evaluation Status (Continued)

- December 21, 2000; Public meeting held at NRC office in Rockville, MD
 - Westinghouse formally requested that the NRC initiate a review for the purpose of closing out the Common Q open items identified in the Safety Evaluation



NRC Safety Evaluation Status (Continued)

- April 5, 2001; Public meeting held at NRC office in Rockville, MD
- Process for closing SE open items
- Category 1: Requires a revision to Appendix 4 and accompanying letter
 - Generic open items 7.4, 7.7, 7.9 and 7.10
 - Plant specific action items 6.3, 6.11 and 6.14



NRC Safety Evaluation Status (Continued)

- Category 2: Requires successful completion of supplemental qualification testing
 - Generic open items 7.1, 7.2, 7.3, 7.5 and 7.6
- Category 3: Requires a future submittal for staff review
 - Generic open item 7.8



NRC Safety Evaluation Status (Continued)

- May 11, 2001; Westinghouse submitted:
 - Westinghouse Nuclear Automation Strategy for the Closeout of the Common Qualified Platform Category 1 Open Items
 - CENPD-396, Appendix 4, Revision 2, April 2001; Common Qualified Platform Integrated Solution
 - Intended to closeout GOI 7.4, 7.7, 7.9 and 7.10
 - Provide clarification to PSAI 6.3, 6.11 and 6.14

70787Alpha.7



00000A.7



NRC Safety Evaluation Status (Continued)

- June 7, 2001; Westinghouse submitted:
 - Westinghouse Nuclear Automation Basis for Change to CENPD-396-P, Appendix 3, Common Qualified Platform, Digital Plant Protection System
 - Provided supplemental information for closing PSAI 6.3
 - Simultaneous loss of the OM and MTP does not prevent the DPPS channel from performing its safety related functions
 - DPPS trip setpoints and pertinent variables are monitored by the cross channel comparison feature of the ITP



NRC Safety Evaluation Status (Continued)

- June 22, 2001; NRC issued :
 - Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1
 - The staff has found that the closeout of the Category 1 open items are acceptable for referencing in licensing applications



NRC Safety Evaluation Status (Continued)

- August 4, 2001 through September 22, 2001;
Conducted equipment qualification testing at Wyle Labs
 - NRC representative witnessed portions of EMC and seismic testing



NRC Safety Evaluation Status (Continued)

- October 29, 2001 through November 15, 2001;
Performed supplemental EMC testing at Retlif Labs on power supplies
- January 20, 2002 through January 26, 2002;
Performed supplemental EMC testing at Retlif Labs on the new analog input card (AI685)



NRC Safety Evaluation Status (Continued)

- August 14, 2002; Westinghouse submitted:
 - Summary Qualification Report of Hardware Testing for Common Q Applications
 - Changes to the Common Qualified Platform Topical Report, CENPD-396-P, Rev. 01
 - Changes to the Common Qualified Platform Software Program Manual, CE-CES-195, Revision 1
 - Changes to the Common Qualified Platform Post Accident Monitoring Systems, CENPD-396-P, Appendix 1, Revision 1
 - Additional Information Regarding the Westinghouse Common Qualified Platform Core Protection Calculator System, CENPD-396-P, Appendix 2, Revision 1

70787Alpha.12



00000A. 12



NRC Safety Evaluation Status (Continued)

- October 2, 2002; Public meeting held at NRC office in Rockville, MD
- Discuss summary qualification report submitted in August
 - Provide closure of the generic open items on equipment qualification testing
- Discuss changes to Common Q topical report, PAMS and CPCS appendices, and SPM submitted in August



NRC Safety Evaluation Status (Continued)

- February 24, 2003; NRC issued:
 - Safety Evaluation for the Closeout of Generic Open Items and Approve Changes to Topical Report CENPD-396-P, Revision 1, “Common Qualified Platform”
 - The staff has completed its review and concluded that the five GOIs (GOIs 7.1, 7.2, 7.3, 7.5 and 7.6) are acceptably addressed and should be closed
 - Proposed changes revising the initial Common Q TR, the SPM, and Appendices 1 and 2 are acceptable
 - GOI 7.8 regarding the future integration of multiple Common Q safety systems will remain open

70787Alpha.14



00000A. 14



NRC Safety Evaluation Status (Continued)

- Remaining Actions:
 - Submit approved versions of Topical Report and Software Program Manual



Generic Open Items

- The Common Q SER identified 10 generic open items



7.1 New AI Card

- Requirements Specification for new AI card issued February 2001
- Successfully completed EQ testing
- This item closed per February 24, 2003 NRC safety evaluation



7.2 Common Q Power Supply

- P/S EQ testing completed - August/September 2001
- Issues discovered with Power Supplies during Wyle EMC testing were resolved and supplies re-tested successfully at Retlif
- This item closed per February 24, 2003 NRC safety evaluation



7.3 Watchdog Timer Module

- Internal PM646 WDT will meet requirements
- Watchdog Timer EQ testing completed - August/September 2001
- This item closed per February 24, 2003 NRC safety evaluation



7.4 QSSL VAR Agreement

- This item is closed per June 22 NRC safety evaluation

70787Alpha. 20



00000A. 20



7.5 Additional PM646 EMC Tests

- PM646A EMC testing completed - August/September 2001
- This item closed per February 24, 2003 NRC safety evaluation



7.6 FPD, WDT, P/S EQ Testing

- August 4, 2001 through September 22, 2001;
Conducted equipment qualification testing at Wyle Labs
- October 29, 2001 through November 15, 2001;
Performed supplemental EMC testing at Retlif Labs on power supplies
- This item closed per February 24, 2003 NRC safety evaluation



7.7 Module Testing

- This item is closed per June 22 NRC safety evaluation

70787Alpha.23



00000A. 23



7.8 Loop Controllers

- The closeout of this item will be scheduled after the completion of the Common Q Phase 3 project
- The loop controllers are being designed such that they are not vulnerable to postulated common cause failures. It will also be demonstrated that they are sufficiently diverse from the other Common Q modules.

7.9 Separation between Safety & Non-safety using AF100 & ITP

- The Integrated Solution appendix describes a connection between the safety systems and non-safety systems using the ITP as an IEEE-7.4.3.2 buffer circuit and the AF100 as the communications media
- This item is closed with respect to the conceptual approach, but the evaluation of each forthcoming design remains a PSAI 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



7.10 Multichannel Operator Module Control

- The IS appendix describes how an HMI device in the control room can address more than one safety-channel for component control
- This item is closed with respect to the conceptual approach, but the evaluation of each forthcoming design remains a PSAI 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



Plant Specific Action Items

- The Common Q SER identified 14 plant specific action items



6.3 FPD Limitations

- This item is closed per June 22 NRC safety evaluation



6.11 Common Q application must comply with CMF Requirements

- Westinghouse revised the Common Q Integrated Solution Appendix to provide a basis for a strategy of performing a one-time bounding CMF analysis for I&C upgrades .
- The NRC staff concluded that the Westinghouse plan for the implementation of a one-time, plant specific, bounding DID&D analysis for phased digital upgrades is acceptable



6.14 No Invalidation of previous TMI commitments

- Westinghouse asked the staff to explain why the TMI actions appear to receive more emphasis than other design basis items
- The NRC responded that the licensee must ascertain that the implementation of a Common Q digital replacement does not render invalid any of the plant's previously accomplished protection or safety functions, TMI-related or otherwise

70787Alpha.30



00000A. 30

