ENCLOSURE 4

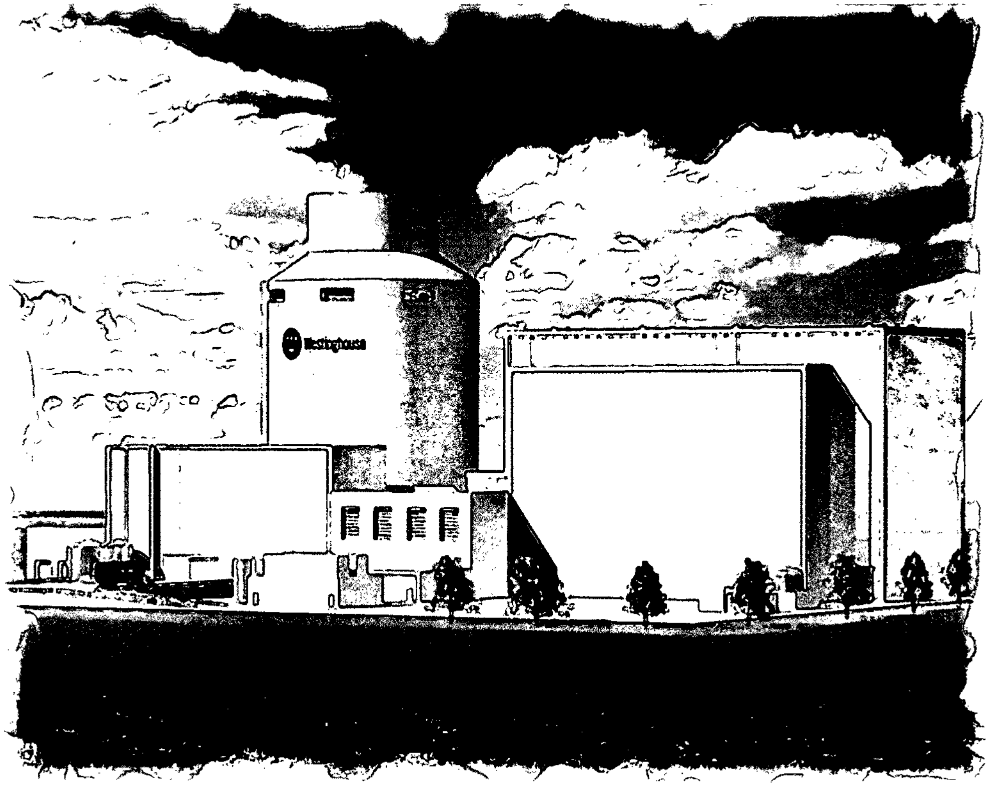
Westinghouse Non-Proprietary

Transmittal of Proprietary
Presentation Material for Regarding Instrumentation and Controls (I & C) for the
AP1000 Meeting with NRC

February 21 and 22, 2007

AP1000 I&C NRC Meeting

February 21 and 22, 2007



WESTINGHOUSE NON-PROPRIETARY CLASS 3

Agenda

Wednesday February 21, 2007		
1	Introduction	*Andrea Sterdis*
Closed Proprietary Meeting		
2	Overview of the Common Q Platform and Licensing	*Martin Ryan*
3	Design and Implementation Process Overview	*Warren Odess-Gillett*
4	High Level Architecture Overview	*Warren Oddess-Gillett*
Thursday February 22, 2007		
5	PMS Design	*Carl Vitalbo*
6	DCD Chapter 7 Amendment	*Tom Hayes*
7	Discussion of Technical Reports Submitted to NRC	*Tom Hayes*
8	NRC Questions and Feedback	*All*
9	Plan Going Forward	*Andrea Sterdis*
Open Public Meeting		
10	Meeting Summary	*Andrea Sterdis/All*

AP1000 I&C Meeting

Andrea L. Sterdis, Manager
AP1000 Licensing and Customer Interface

WESTINGHOUSE NON-PROPRIETARY CLASS 3

Meeting Objectives

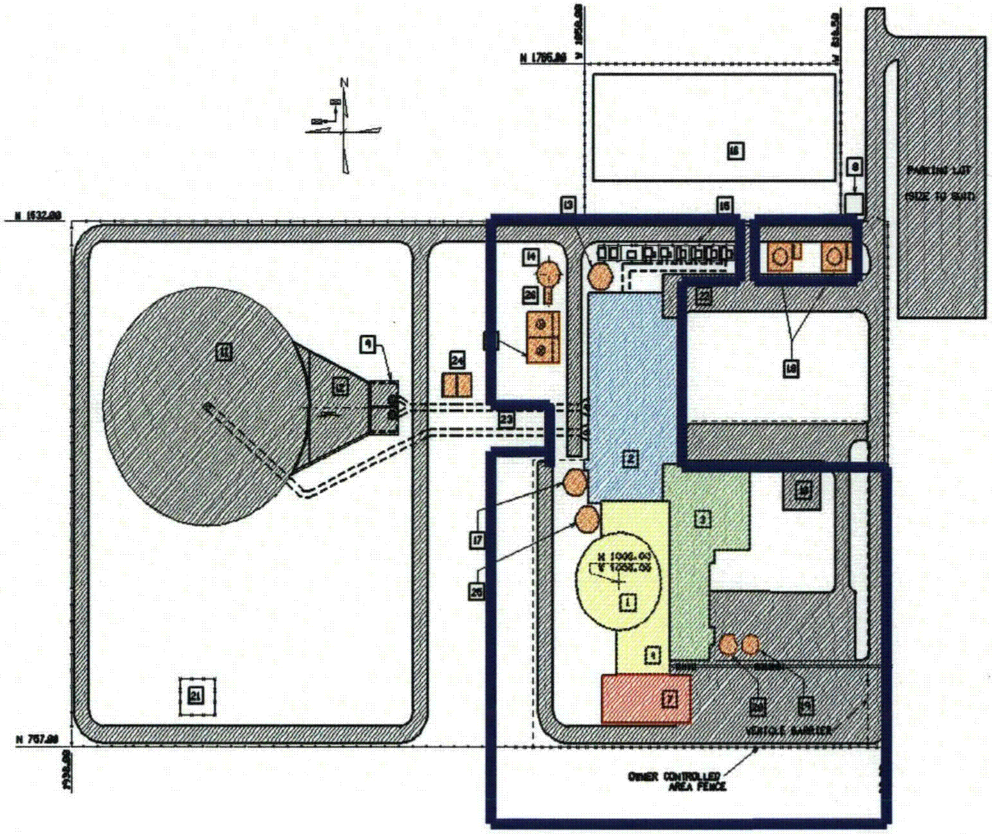
- Provide an Overview of the Common Q Platform and Licensing
- Provide an Overview of the Design and Implementation Process
- Provide an Overview of the Architecture
- Review I&C Status
  - Technical Reports including Pending Chapter 7 Revision TR
- Review PMS Process and DAC issues to discuss DAC closure
- Develop plan going forward

AP1000 Pre-Application Licensing Approach

- Pre-Application activities build on AP1000 Design Certification
- Design Certification was approved December 30, 2005
- Pre-Application activities are active now
- COL Applications are expected in Fall of 2007

What's In the Certified Scope? (DCD Fig. 1.2-2)

- The AP1000 Design Certification includes more scope than the traditional NSSS
- Only areas not included in the standard design scope and certification scope are the site specific aspects (e.g. circulating water and switchyard design)



Licensing Approach and Activities

- Pre-Application Review
- COL Information Item Closures
- DAC Completion
- As-Built Verification and Inspections

AP1000

Pre-Application Review

- Westinghouse is preparing reports to address COL information items and other design completion activities in support of expected COL applications.
- Pre-application activities are in support of standardization of AP1000 COL applications.
- Pre-application activities support the NRC Design Centered Review Approach.

Pre-Application Review

- The technical reports document COL information item closure activities
- A limited number of design changes are documented in technical reports
- NuStart review and oversight of technical report preparation and other pre-application activities promote standardization of AP1000 COL applications.

Pre-Application Review

- Submittal of technical reports by Westinghouse to provide standard AP1000 Design information
- NRC Staff Review (Interaction as necessary)
- NRC SER Preparation
- Application to all COL Applications via reference to technical reports and corresponding SERs

Potential Part 52 Revision

- Revision of AP1000 Design Certification Rule
  - Part 52 does not currently provide for revision
  - Substantial industry comments on NOPR for revising Part 52 to permit revision
  - Indication is that revised rule will include mechanism for revision
    - Draft rule language issued
    - Awaiting SRM and Revised Rule
- If revised Part 52 allows, Westinghouse plans to submit a revised DCD in May 2006.

COL Information Items Closures

- NRC Review and approval of technical reports documenting COL information items closure activities will:
  - Provide one standard approach by COL applicants
  - Require one review by NRC
  - Remove the review of these items from the critical path in application review.
- Reports for approximately half of scheduled COL information items have been submitted for NRC review.

AP1000

Overview of the Common Q Platform and Licensing

Marty Ryan

WESTINGHOUSE NON-PROPRIETARY CLASS 3

Topics for Discussion

- Common Q Platform Overview
- Common Q Equipment Qualification
- Common Q Configuration Management
- Common Q Licensing Status

Common Q Platform Overview

Common Q Platform Overview
Safety Systems Licensing Strategy

- Westinghouse has qualified and licensed a group of components for Safety Critical applications
- This is referred to as the **"Common Q (qualified) Platform"**
- The Common Q platform was defined in Topical Reports to NRC
  [ ]a,c
- Common Q was licensed via a SER issued by the NRC on the Topical Report

Common Q Platform Overview System Applications

- Common Q Platform is a group of building blocks that can be configured to build Safety-Related Systems
- A full spectrum of Class 1E systems can be implemented with Westinghouse's Common Q platform including:
  - Reactor Protection System (RPS)
  - Engineered Safety Features Actuation System (ESFAS)
  - Post Accident Monitoring Systems (PAMS)
  - Diesel Load Sequencer
  - Core Protection Calculators (CPC)

Common Q Platform Overview
Strategy

AP1000

- Started as a Owners Group initiative
- Now a strategic initiative for Westinghouse Electric Company worldwide with systems installed, designed, and planned in:
  - Oskarshamn 1 Modernization in Sweden
  - UCN 5 & 6 and KEDO Digital Plant Protection System in Korea
  - Ringhals Unit 2 Modernization in Sweden
  - Safety system upgrades in US including:
    - Core Protection Calculator
    - Diesel Load Sequencer
    - PAMS
    - AP1000

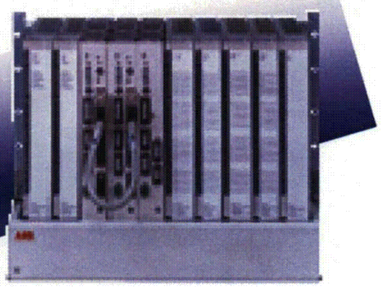
Common Q Platform Overview Hardware

- Common Q Platform consists of the following hardware:
  - Advant Controller 160
    - PM646 Processor Module
    - S600 I/O
    - Communication Interface
  - Flat Panel Display System (FPDS)
    - PC Node Box
    - Flat Panel Display
    - Communication Interface
  - Power Supply System
  - Component Interface Module (CIM)
  - Termination Unit (TU)

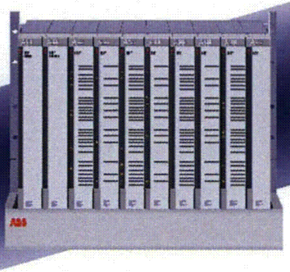
Common Q Platform Overview
Advant Controller 100 Series

A versatile family of Process Controllers

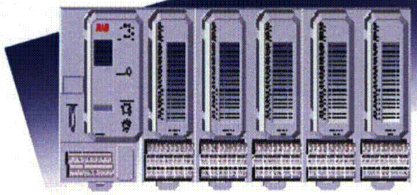
Advant Controller 160



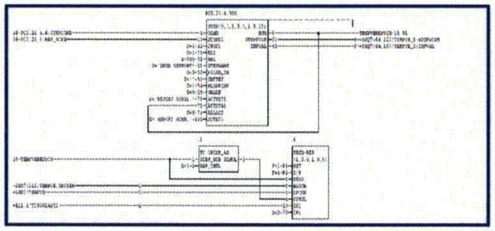
Advant Controller 110



Advant Controller 70



AMPL Control
Configuration

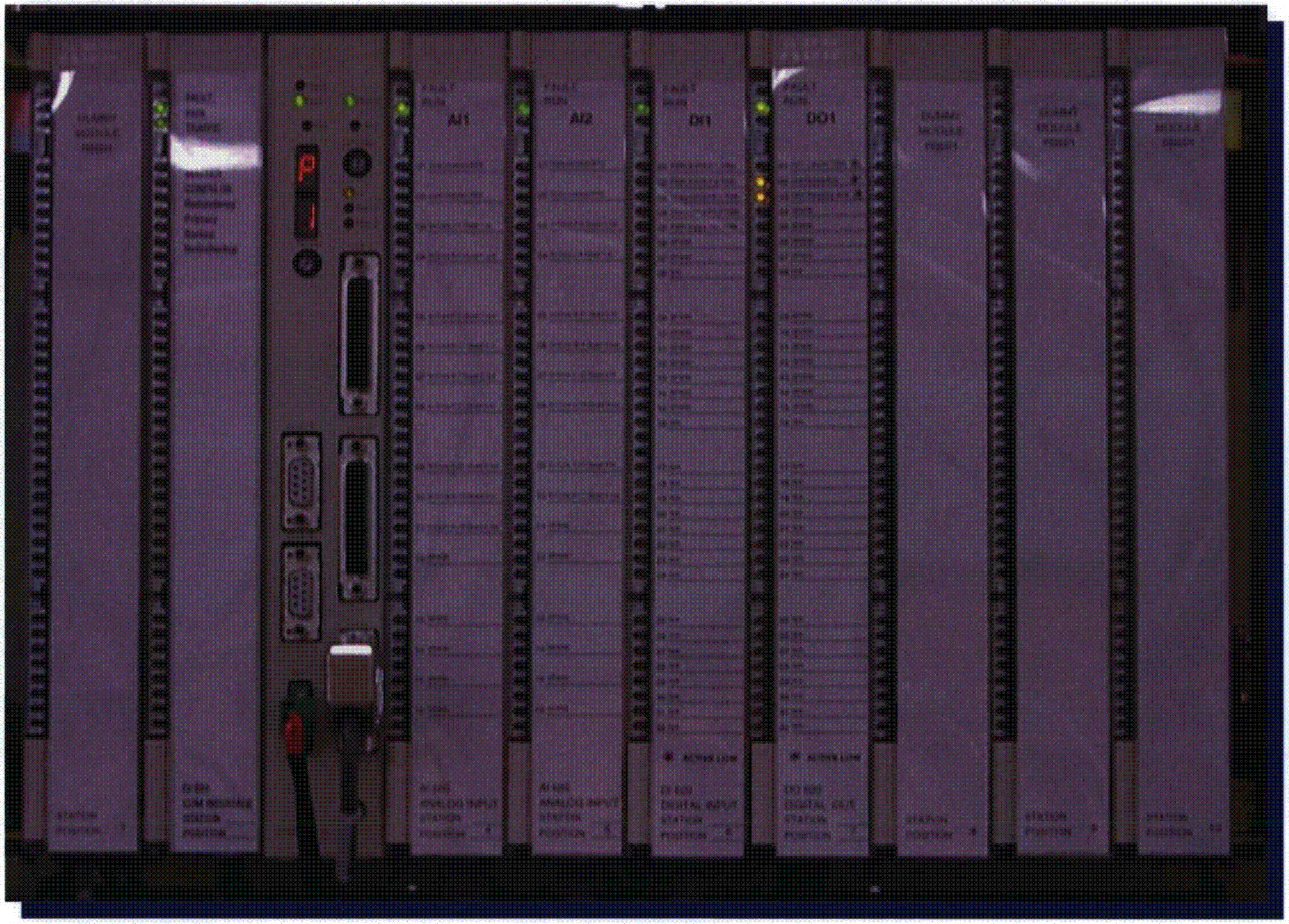


Advant AC160 Controller
Worldwide Applications

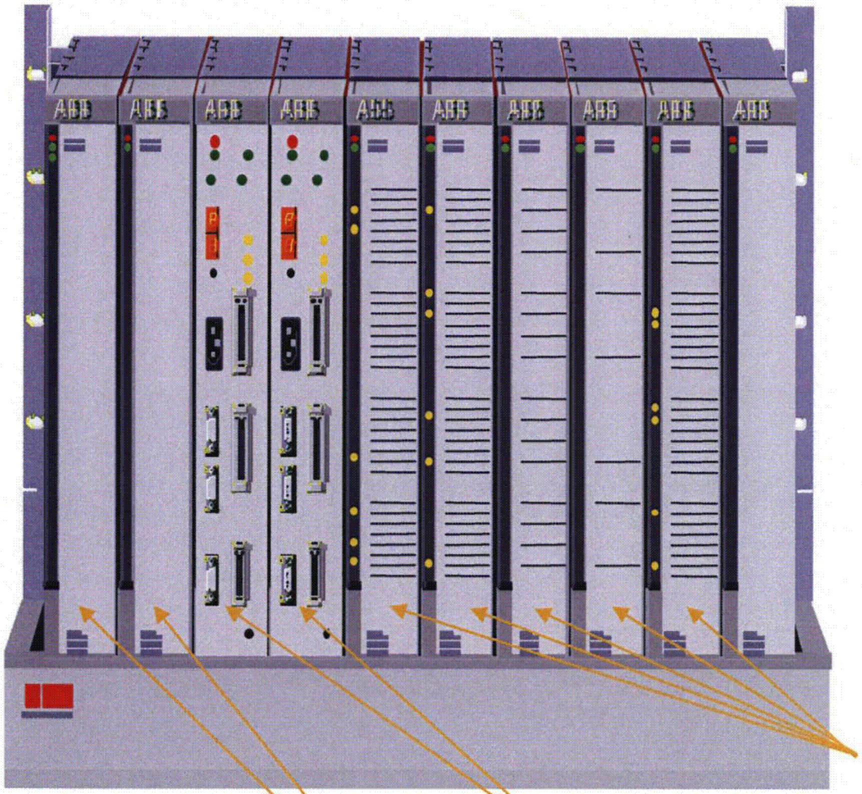
a,c

Common Q Platform Overview
Actual AC160 Controller

AP1000



Common Q Platform Overview
Advant AC160 Controller



- Executes the protection algorithms
- Includes:
  - Processor Modules
  - Communication Interfaces
  - I/O Modules

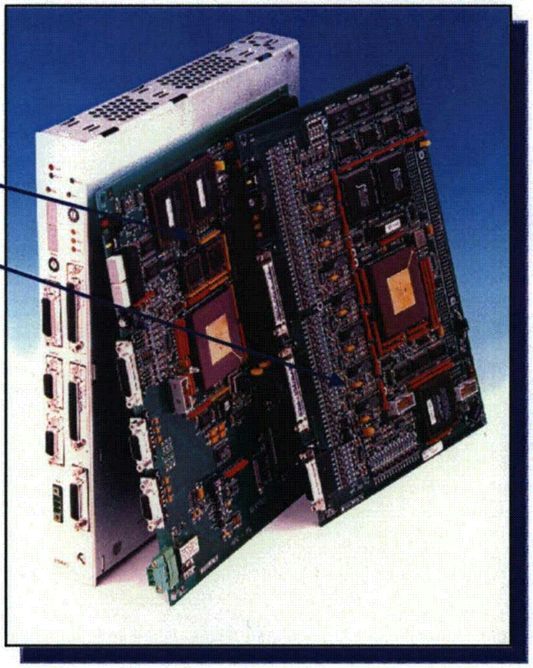
I/O

Processor Modules w/ HSL

Communication I/F Modules

Common Q Platform Overview
PM646 Processor Module

- [ ]^{a,c}
  - Processor Section (PS)
  - Communications Section (CS)
- Multi-tasking CPU with 31 independent tasks
- [ ]^{a,c}
- Self diagnostics: watchdog and memory checking
- Non-volatile FlashPROM for application program
- Two serial ports - connections for Engineering Station and programming tool



Common Q Platform Overview PM646 Processor Module

a,c

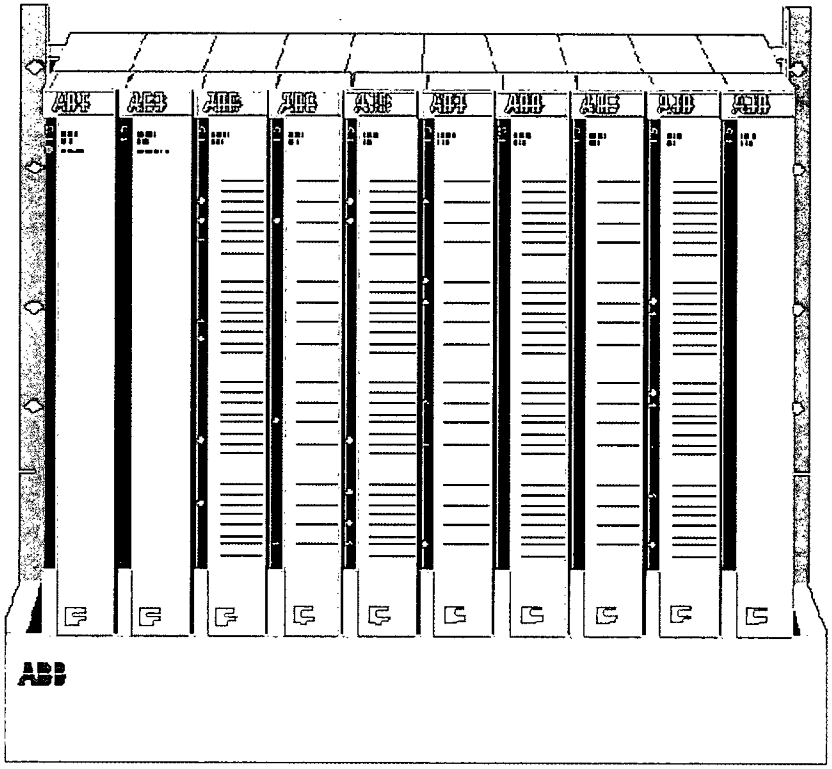
Common Q Platform Overview
PM646 Processor Module

a,c

Common Q Platform Overview
S600 I/O

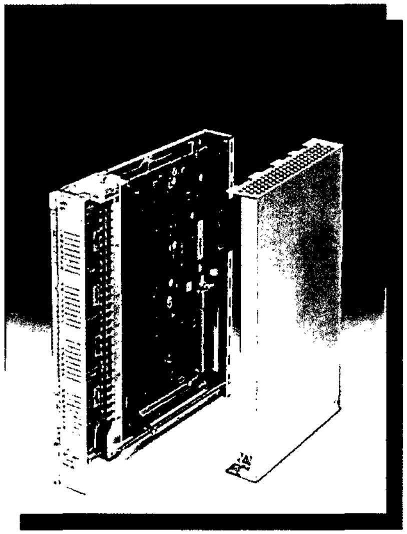
AP1000

- Local I/O system
- Backplane Input Output Bus (BIOB) communications bus
  - I/O extension bus
- Diagnostics
  - Module type
  - Module position
  - Module operation
  - Connector integrity
- Run/Fault LEDs



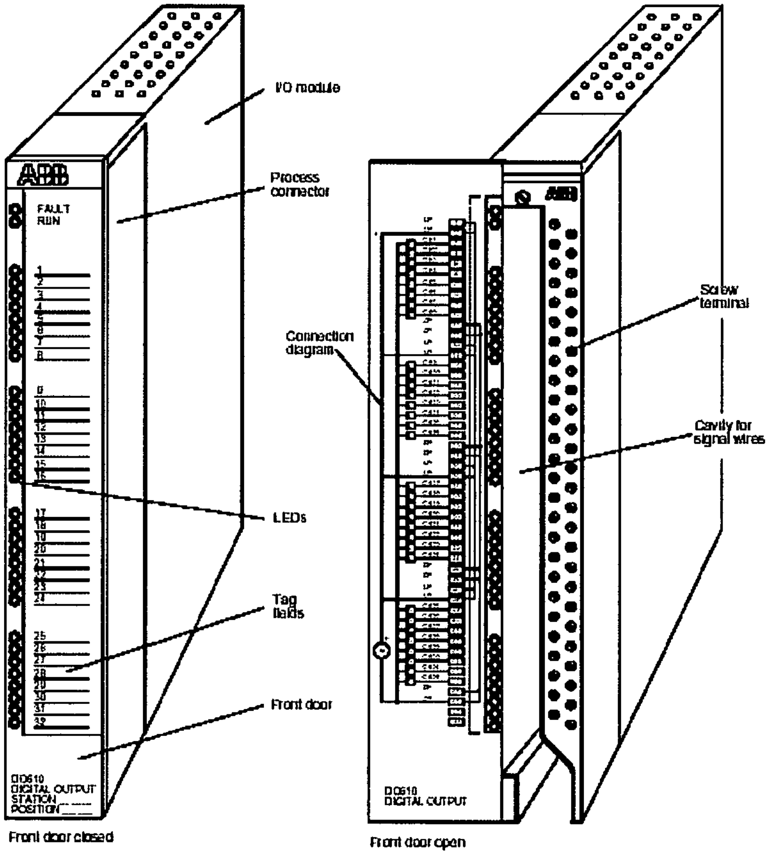
Common Q Platform Overview
S600 Local I/O

- Digital Input
  - [ ]a,c
- Digital Output
  - [ ]a,c
- Analog Input
  - [
  -
  -]a,c
- Analog Output
  - [ ]a,c
- Pulse Counter
- Hot-Swap Capability



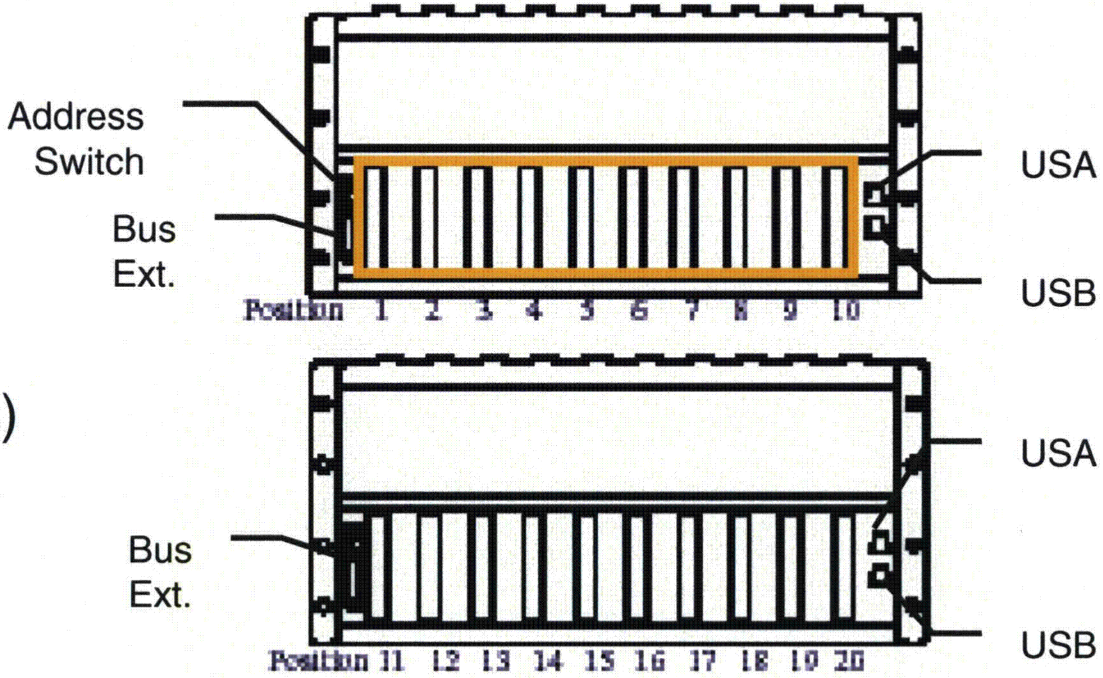
Common Q Platform Overview
S600 I/O

- Front process connections
- Hot replacement of modules
  - User support for maintenance



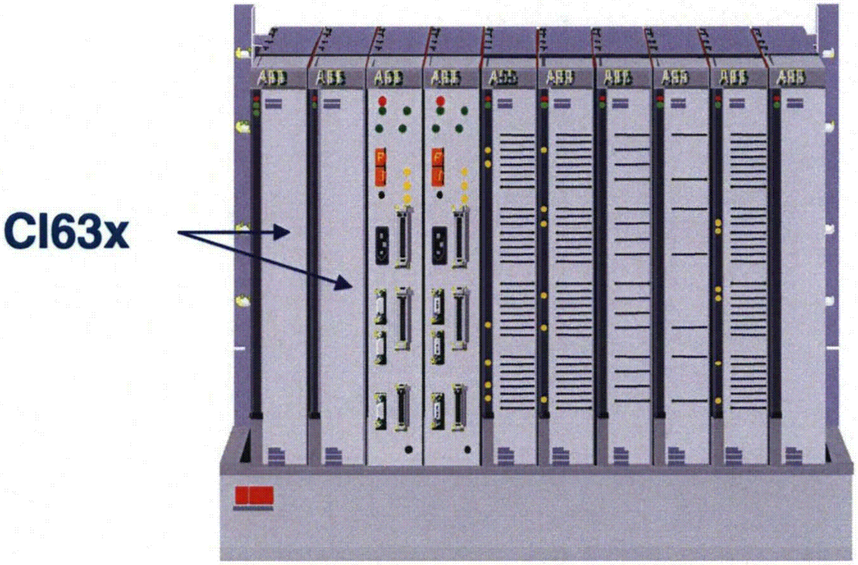
Common Q Platform Overview
Advant Controller 160 Subrack

- 19” steel subrack
  - Seismic support
  - Fan assembly (24 VDC fans)
- 10 modules per subrack
- BIOB (48-pin connectors)
- External PS voltage terminals
- Subrack
  - Address switch
  - Bus connector
  - Extension Subrack has bus connector only


Address Switch
Bus Ext.
USA
USB
Position 1 2 3 4 5 6 7 8 9 10
Bus Ext.
USA
USB
Position 11 12 13 14 15 16 17 18 19 20

Common Q Platform Overview
CI63x Interface Module

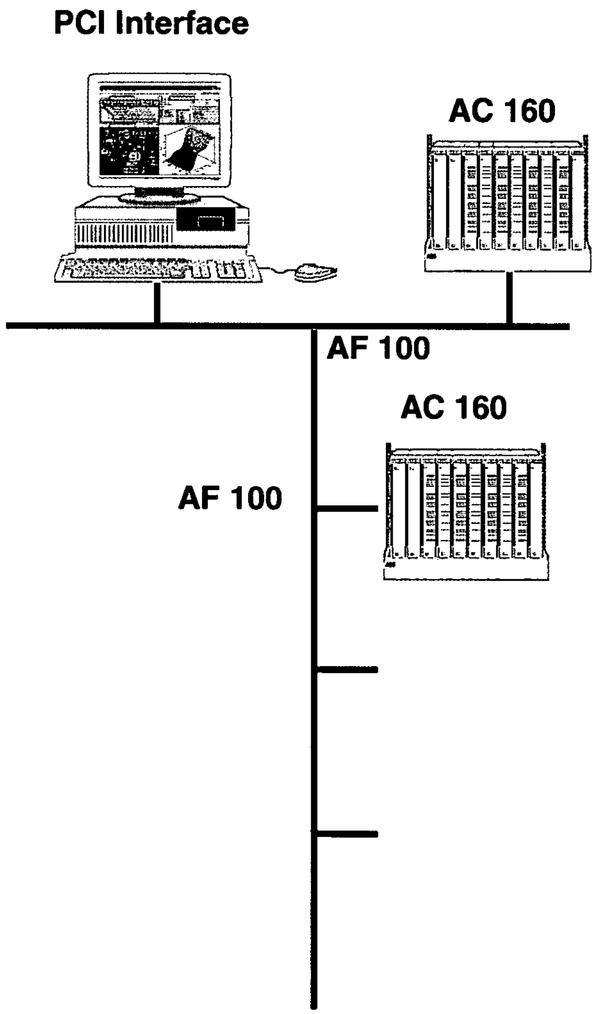
a,c



Common Q Platform Overview
Advant Fieldbus AF100 Network

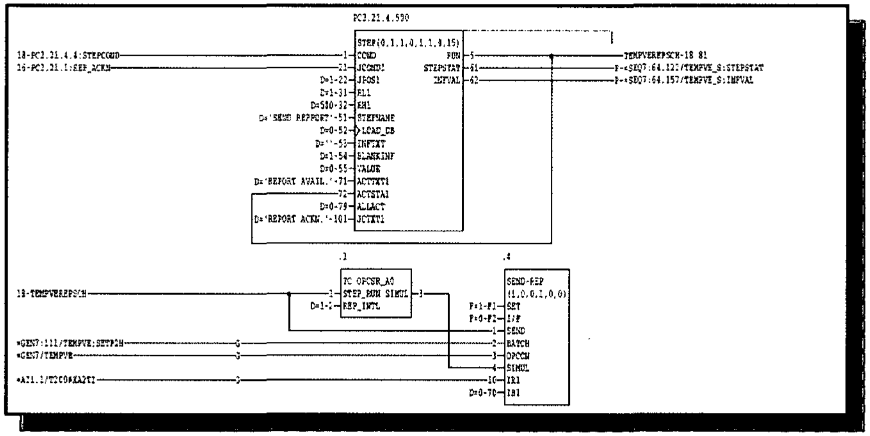
- Networking

a,c



Common Q Platform Overview
AMPL Control Configuration - Features

- ABB Advant® Master Programming Language (AMPL) is used to configure the AC160 Controller
- Comprehensive library
- Complete configuration
- Adaptable
- High degree of reusability
- Easy to configure
- Usage of Type Circuits
- On-line and off-line capability



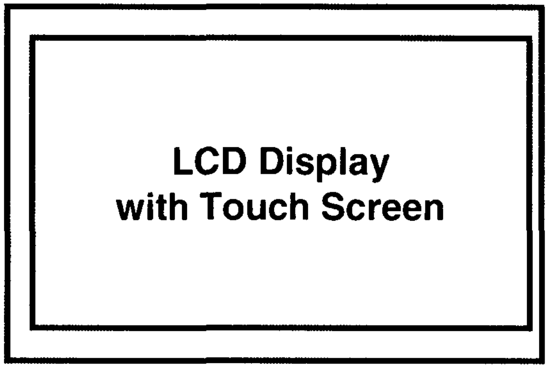
Common Q Platform Overview
AMPL Control Configuration - Features

- Electrical Control
  - Motors and drives
  - Interlocks
- Sequence Control
  - Startups and shutdowns
  - Object display for monitoring and alarm
- Regulatory Control
  - Temperatures
  - Flows, levels, pressure
  - Advanced control
- Mathematical Control
  - Advanced calculations
- Applications Control
  - Examples: Digesters, Paper Machine Control, Blast Furnace Control

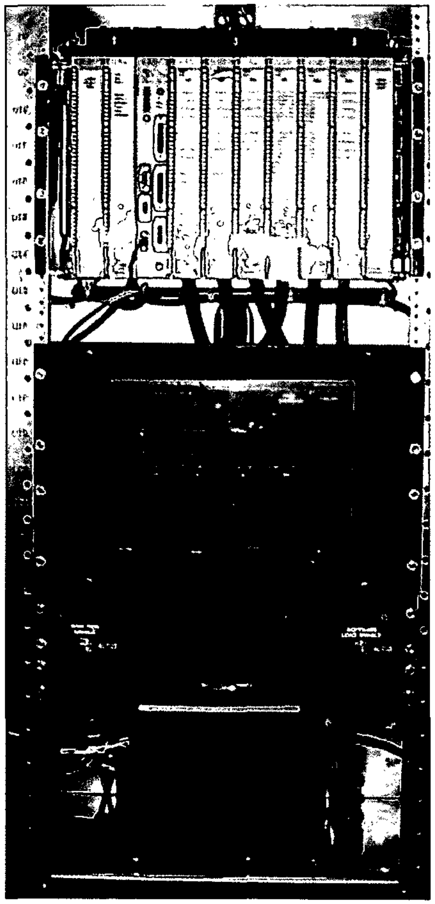
Common Q Platform Overview
AMPL Control Configuration - Features

- Common high-level language for all controllers
- One common high-level language for Programmable Logic Controller (PLC), instrumentation and advanced functions
- Specially developed for process control applications
- Function block oriented
- High configuration productivity by use of “Typical Solutions”
- Automatic, on-line (“as built”), graphic documentation

Common Q Platform Overview
Flat Panel Display System


LCD Display
with Touch Screen

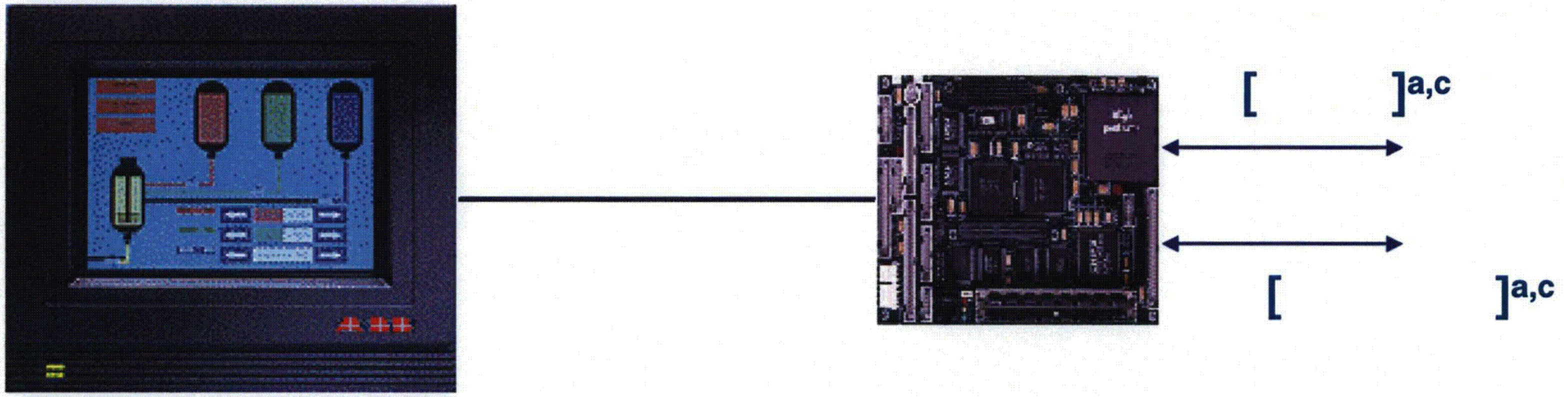
a,c



Common Q Platform Overview
Flat Panel Display System (FPDS)

- Operator Interface in Control Room
- Maintenance and Test Panel in system cabinet
- [ ]a,c
- Licensed for Class 1E Applications
- [ ]a,c
- Qualification & Configuration Control
- 12 inch, 15 inch, 18 inch Displays and PC Node Box

Common Q Platform Overview
Flat Panel Video Display



- Color Thin Film Transistor Technology
- Touch Screen Graphical User Interface

- x86 Processor with EPROM
- CD ROM
- Hard Disk
- [ ]^{a,c}
- AF100 Interface
- [ ]^{a,c}

Common Q Platform Overview
Flat Panel Display System (FPDS)

a,c

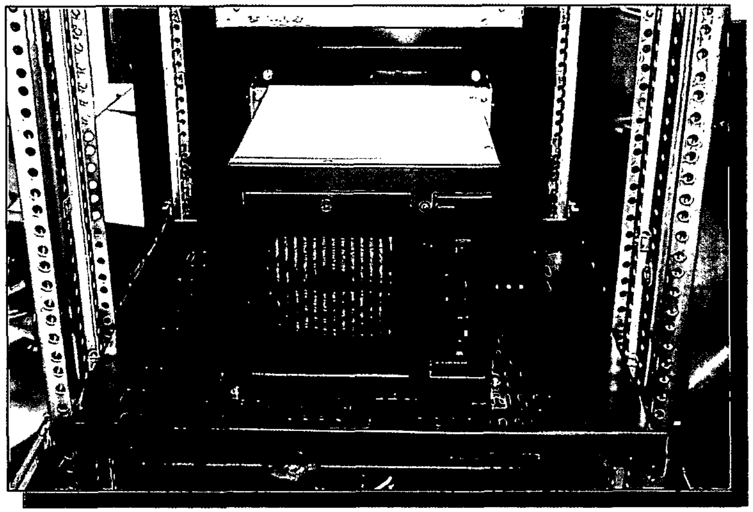
15 Inch Display

Maintenance and Test Display and Keyboard

Common Q Platform Overview
Flat Panel Display System

- PC Node Box
  - Single board computer

a,c



Common Q Platform Overview
Power Supply

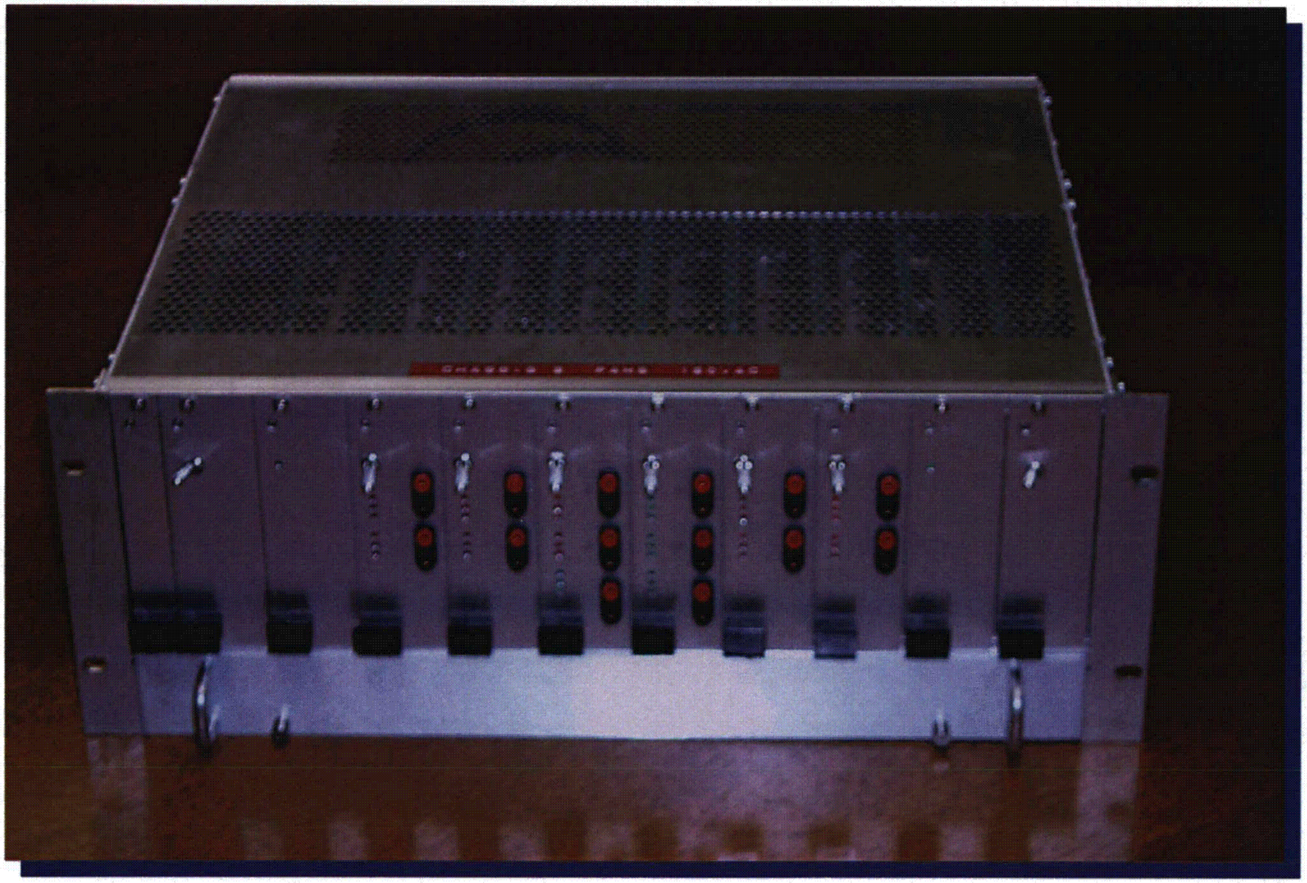
- Provides all cabinet powering functions in a singular modular assembly
- Available Output Voltages:
  - 24 V up to 500 Watts
  - 15 V up to 250 Watts
  - 5 V up to 250 Watts
  - 48 V up to 500 Watts
  - 5.0 V to 30.5 V variable by control voltage (0.1 to 1.3 V)
  - Other voltages available by sub-vendor for other applications

Common Q Platform Overview
Power Supply

a,c

Common Q Platform Overview
Power Supply

19 inch Rack Assembly



Common Q Platform Overview
Component Interface Module (CIM)

- Object oriented I/O and control card for binary plant components
  - Simplifies design
  - Segments failure and maintenance effects
- Used for safety and non-safety components

a,c

- Additional information will be provided later

Common Q Platform Overview Termination Unit (TU)

- Primary functions:
  - Terminals to land field signals
  - Overload protected sensor current loop power
  - Overload protected contact wetting power
  - Limited signal conditioning (dropping resistors for current to voltage conversion)
  - Support for sensor sharing
  - Test injection/field disconnects

Common Q Platform Overview
Termination Unit (TU)

a,c

Interface process I/O signals with S600 I/O modules.

Common Q Platform Overview
Termination Unit (TU)

- AI685 TU

a,c

[ ]

- AO650 TU

a,c

[ ]

- DI621 TU

a,c

[ ]

Common Q Platform Overview
Termination Unit (TU)

- DO620 TU

  [ ] a,c

- Relay Disconnect TU

  [ ] a,c

- Y Feed-through TU

  [ ] a,c

Common Q Platform Overview
Termination Unit (TU)

- HSL TU

[ ] a,c

- Reactor Trip Matrix TU

[ ] a,c

- 2oo3 Vote & Pulse TU

a,c [ ]

Common Q Platform Overview
Cabinet Assembly

a,c

Common Q Platform Overview
Summary

- One common solution provides
  - Reduced technical support costs
  - Reduced unique spare parts
  - Long term parts availability
- Modern technology provides
  - Improved reliability
  - Self-diagnostics
  - Automated testing
  - Hot-swap capability
  - Extended manual surveillance intervals

Common Q Equipment Qualification

Common Q Equipment Qualification

- Equipment utilized for Safety System applications requires a test process to ensure the equipment operates before, during, and after a design basis event (DBE)
- AC160 equipment has been successfully subjected to this test process
- The testing includes:

[ ] a,c

- Testing also addressed criteria to support other markets (e.g., Korea, Europe)

Common Q Equipment Qualification

- Two Qualification Programs were performed for Common Q
- Program 1 [

  ]a,c
- Program 2 [

  ]a,c

Common Q Equipment Qualification Program 1 Equipment Qualification

- Two test specimens were subjected to the planned qualification:

a,c

Common Q Equipment Qualification

Program 1 Environmental/Seismic Test Specimen (View 1)

a,c

Common Q Equipment Qualification

Program 1 Environmental/Seismic Test Specimen (View 2)

a,c

Common Q Equipment Qualification Program 1 Seismic Test

- AC160 equipment was tested to ensure that it could withstand without loss of safety function or physical integrity:

a,c

- Demonstrates that during a seismic event, all equipment remains physically intact, not causing damage or loss of safety equipment functionality.

Common Q Equipment Qualification Program 1 Environmental Test

a,c

Common Q Equipment Qualification Program 1 EMI Test

- AC160 equipment was operated inside a test chamber to determine:
  - Emissions radiated into the environment
  - Susceptibilities when subjected to a harsh (EMI/RFI) environment

a,c

[ ]

Common Q Equipment Qualification Program 1 EMI Test Chamber

a,c

Common Q Equipment Qualification Program 2

- Closeout Common Q SER Issues
- Leverage test for existing contracts
  - Ulchin 5 & 6 DPPS/DEFAS
  - APS CPC
  - BGE PAMS
  - TWICE
- Perform test such that results can be utilized for many other contracts as well
  - Revised Environmental Test for all equipment

Common Q Equipment Qualification
NRC Open SER Hardware Issues

- Common Q Qualification required the following:

[ ] a,c

Common Q Equipment Qualification Program 2 Approach

- Perform testing in a manner similar to Program 1 to facilitate closure on Common Q issues
- Reuse as much previous Program 1 test procedures, processes, and results as possible
- Create separate test cells for the different products / requirements
- Reported results to NRC as a revision to previous Topical submittal utilizing defined methodology

Common Q Equipment Qualification Program 2 Test

- Testing at [ ]^{a,c} was conducted from 8/4/2001 through 9/22/2001
- NRC and customer witnesses at testing
  - [ ]^{a,c} representative witnessed Group 1 Seismic
  - NRC representative witnessed portions of EMC and Group 2 Seismic

Common Q Equipment Qualification Program 2 Mechanical Pre-Aging Test

AP1000

- Electromechanical components that are potentially susceptible to wear and are required to operate were aged to end of life condition prior to commencement of tests

a,c

[ ]

Common Q Equipment Qualification Program 2 Environmental Test

- Subjected Test Cell 1A and 1B to new environmental profile that envelopes the requirements defined in the Common A Topical Report

  [

  –

  –

  ]a,c

Common Q Equipment Qualification

AP1000

Program 2 Environmental Test Specimen (Front/Rear View)

a,c

Common Q Equipment Qualification Program 2 Seismic Test

a,c

[ ]

Common Q Equipment Qualification
Seismic Test Comparison of 1999 vs. 2001

a,c

Common Q Equipment Qualification Program 2 Seismic Test Specimen

a,c

Common Q Equipment Qualification

Program 2 PC Node Box Seismic Specimen

a,c

Common Q Equipment Qualification Program 2 Seismic Test Specimen

a,c

Common Q Equipment Qualification Program 2 AC160 Test Specimen (Front View)

a,c

Common Q Equipment Qualification Program 2 EMC Test

a,c

Common Q Equipment Qualification Program 2 EMC Radiated Emissions 102 Test

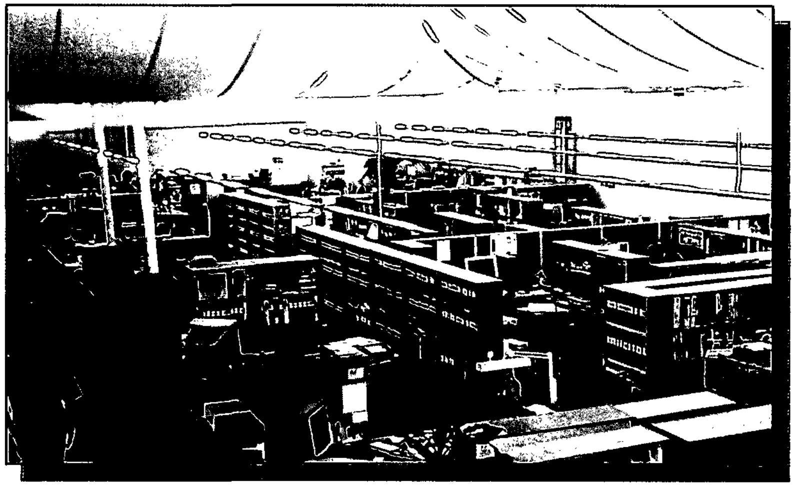
a,c

Common Q Equipment Qualification Summary

- As a result of these qualification programs and supplemental retests the Common Q equipment is suitable for use in safety-related systems

Common Q Configuration Management

Common Q Configuration Management
ABB Vasteras Facility



- ABB's design organizations to support the AC160 include operations in:
  - Vasteras, Sweden
  - Mannheim, Germany
  - Minden, Germany

a,c

Common Q Configuration Management ENICS Vasteras Manufacturing Facility

a,c

Common Q Configuration Management Documentation

a,c

Common Q Configuration Management Hardware

a,c

Common Q Configuration Management

a,c

Common Q Configuration Management Firmware

a,c

Common Q Configuration Management AC160 Software

a,c

Common Q Configuration Management Repairs

a,(

Common Q Configuration Management
Configuration Control

a,c

Common Q Configuration Management PM646A PS Section Digital Image

a,c

Common Q Configuration Management
Configuration Control

a,c

Common Q Configuration Management Obsolescence and Last Time Buy (LTB)

a,c

Common Q Configuration Management AC160 Product Long-Term Support

a,c

Common Q Configuration Management
AC160 Configuration Management Summary

a,c

Common Q Licensing Status

Common Q Licensing Status Strategy

a,c

Common Q Licensing Status
Scope of Generic SER

- Acceptance of software quality assurance program
- Acceptance of module-based equipment qualification
- Acceptance of Common Q building blocks for the following applications:
  - Digital PPS and ESFAS
  - Core Protection Calculator
  - Post Accident Monitoring Systems
  - Integrated Solution

Common Q Licensing Status
Common Q Topical Report

- Main Body
  - Description of basic building blocks
  - Address all key Standard Review Plan (NUREG-0800) topics for advanced digital systems
    - Hardware and software qualification
    - Configuration management
    - Application development
    - Compliance with regulatory criteria
- Appendices
  - Appendix 1 - Post Accident Monitoring System
  - Appendix 2 - Core Protection Calculator System
  - Appendix 3 - RPS/ESFAS
  - Appendix 4 - Integrated Solution
- Software Program Manual for Common Q Systems

Common Q Licensing Status
NRC Safety Evaluation Status

- August 11, 2000 - NRC Safety Evaluation (SE) provided acceptance of the Common Q Topical Report and Appendices 1, 2, 3, and 4.
  - 10 Generic Open Items (GOIs)
  - 14 Plant-Specific Action Items (PSAIs)
- June 22, 2001 - NRC Safety Evaluation, Revision 1
  - Closed 4 GOIs (4, 7, 9, 10) and 3 PSAIs (3, 11, 14)
- February 24, 2003
  - Closed 5 GOIs (1, 2, 3, 5, 6)

Common Q Licensing Status
NRC Safety Evaluation Status (cont'd)

a,c

Common Q Licensing Status
DCD References vs. Current Documentation

	DCD	Current Documentation
Software Program Manual for Common Q Systems (SPM)	CE-CES-195, Rev. 1	WCAP-16096-NP-A, Rev. 1A (approved via ML042730580)
Common Q Platform Topical Report	[ ]^{a,c}	[ ]^{a,c} (approved via ML030550776)
Common Q Platform Integrated Solution	[ ]^{a,c}	[ ]^{a,c} (approved via ML011690170)
Design Process for Common Q Safety Systems	[ ]^{a,c}	[ ]^{a,c}

AP1000

Design and Implementation Process Overview

Warren Odess-Gillett
Principal Engineer

WESTINGHOUSE NON-PROPRIETARY CLASS 3

Mapping of BTP-14, DCD and SPM Phases

a,c

Different terminology represent the same activities.

List of Documents by DCD Phase

Design Requirements Phase Documents

- Includes the following documents
  - Project plans

a,c

  - Design methodology

a,c

This phase is complete. Design acceptance criteria met for design requirements phase and all documents are available for inspection.

Design Requirements Phase Documents (Cont'd)

1. RRAS AP1000 NuStart I&C Program Project Plan
   [ ]^{a,c}
2. RRAS AP1000 NuStart I&C Program Project Quality Plan
   [ ]^{a,c}
3. AP1000 NuStart Protection and Safety Monitoring System Project Plan [ ]^{a,c}
4. AP1000 NuStart Protection and Safety Monitoring System Software Project Plan [ ]^{a,c}

Design Requirements Phase Documents (Cont'd)

5. Software Program Manual for Common Q Systems (WCAP-16096-NP-A)

6. Design Process for Common Q Safety System
   [ ]a,c

7. Verification & Validation Process for the Common Q Safety Systems
   [ ]a,c

8. Testing Process for Common Q Safety Systems
   [ ]a,c

9. Common Q Software Configuration Management Guidelines
   [ ]a,c

Design Requirements Phase Documents (Cont’d)

10. Coding Standards & Guidelines for Common Q Systems [ ]^{a,c}

11. AP1000 NuStart Protection and Safety Monitoring System Project Concept Phase V&V Summary Report [ ]^{a,c}

Establishment of plans and methodologies complete and provide a complete package for Design Requirements Phase.

Future Lifecycle Phases

a,c

System Definition Phase Documents

1. PMS Functional Requirements Documents [
   ]a,c
2. AP1000 Detailed Functional Diagrams [
   ]a,c
3. PMS Component Functional Logic Documents [
   ]a,c
4. Post-Accident Monitoring System Functional Specification
   [ ]a,c
5. PMS Architecture Drawings [ ]a,c
6. Protection and Safety Monitoring System Design Requirements
7. Protection and Safety Monitoring System Design Specification

System Definition Phase Documents

8. Protection and Safety Monitoring System Software Requirements Specification
9. FMEA of AP1000 Protection and Safety Monitoring System [ ]a,c
10. Software Hazard Analysis of AP1000 Protection and Safety Monitoring System [ ] a,c
11. V&V System Definition Phase Summary Report
12. Requirements Traceability Report

Specification of functional requirements (includes System Design documentation and Software Requirements definition).

Hardware and Software Development Phase Documents (Design Portion)

a,c

1.

2.

3. Hardware Design Drawings
4. FMEA of AP1000 Protection and Safety Monitoring System (Update if necessary)
5. Software Hazard Analysis of AP1000 Protection and Safety Monitoring System (Update if necessary)
6. V&V Design Phase Summary Report
7. Requirements Traceability Report

Documentation and review of hardware and software (design documentation).

Hardware and Software Development Phase Documents (Implementation)

1. PMS Code Listings
2. [ ]^{a,c}
3. [ ]^{a,c} Test [ ]^{a,c} Procedures [ ]^{a,c} Circuits)
4. [ ]^{a,c} Test [ ]^{a,c} Procedures [ ]^{a,c}
5. [ ]^{a,c} Test [ ]^{a,c} Procedure
6. [ ]^{a,c} Test [ ]^{a,c} Procedure
7. [ ]^{a,c} Test Reports
8. [ ]^{a,c} Test Reports

Hardware and Software Development Phase Documents (Implementation)

9. [ ]^{a,c} Test Report
10. [ ]^{a,c} Test Report
11. [ ]^{a,c} Report
12. V&V Code Review reports
13. V&V Implementation Phase Summary Report
14. Requirements Traceability Report

Documentation and review of hardware and software (software coding, test procedures/reports).

System Integration and Test Phase Documents

1. [ ]a,c Test [ ]a,c Procedures (individual channels)
2. [ ]a,c
3. [ ]a,c Test Reports
4. [ ]a,c
5. Final V&V Report
6. Requirements Traceability Report

Performance of system tests and the documentation of system test results.

Installation Phase Documents

1. [ ]^{a,c} Test [ ]^{a,c} Procedure
2. [ ]^{a,c} Test Report
3. Operation and Maintenance Manual
   - [ ]^{a,c}

Performance of installation tests and inspections.

BTP-14: Software Management Plan

- AP1000 Program Operating Procedures
  - [ ]^{a,c}
- Project Plan-RRAS AP1000 NuStart I&C Program
  - [ ]^{a,c}
- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 2
- AP1000 NuStart PMS Project Plan
  - [ ]^{a,c}
- AP1000 NuStart PMS Software Project Plan
  - [ ]^{a,c}

BTP-14: Software Management Plan

BTP-14 requirements for a Software Management Plan are fulfilled by the aforementioned documents

BTP-14: Software Development Plan

- RRAS AP1000 NuStart I&C Program Project Quality Plan
  - [ ]a,c
- Computer Software Development Process
  - [ ]a,c
- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 1
- Design Process for Common Q Safety Systems
  - [ ]a,c

BTP-14: Software Development Plan (cont.)

- Coding Standards & Guidelines for Common Q Systems
  - [ ]a,c
- AP1000 NuStart PMS Software Project Plan
  - [ ]a,c

These documents satisfy the BTP-14 requirements for a Software Development Plan

BTP-14: Software Quality Assurance Plan

- Computer Software Development Process
  - [ ][a,c]
- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 4

These documents satisfy the BTP-14 requirements for a Software Quality Assurance Plan

BTP-14: Software Integration Plan

- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 7.5.2.2
- Design Process for Common Q Safety Systems
  - [ ]a,c
- Testing Process for Common Q Safety Systems
  - [ ]a,c

These documents satisfy the BTP-14 requirements for a Software Integration Plan

BTP-14: Software Installation Plan

- Common Q Software Program Manual
  - WCAP-16096-NP-A, Sections 3.5.2.1, 4.3.2.6, 5.5.7, 6.2.2.5
- Design Process for Common Q Safety Systems
  - [ ]a,c

[ ]a,c

Other BTP-14 Plans

- Software Maintenance Plan
  - Common Q Software Program Manual
    - WCAP-16096-NP-A, Section 7
- Software Training Plan
  - Common Q Software Program Manual
    - WCAP-16096-NP-A, Sections 1.4.2, 3.3.3, 3.5.1, 4.14
- Software Operations Plan
  - Common Q Software Program Manual
    - WCAP-16096-NP-A, Sections 3.5.2.3, 4.3.2.7, 5.5.8, 6.2.6.6, 7
- Software Safety Plan
  - Common Q Software Program Manual
    - WCAP-16096-NP-A, Section 3

Other BTP-14 Plans

a,c

BTP-14: Software V&V Plan

- Computer Software Development Process
  - [ ]a,c
- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 5
- V&V Process for Common Q Safety Systems
  - [ ]a,c
- Testing Process for Common Q Safety Systems
  - [ ]a,c
- AP1000 NuStart PMS Software Project Plan
  - [ ]a,c

BTP-14: Software V&V Plan

The aforementioned documents satisfy the BTP-14 requirements for a Software V&V Plan.

BTP-14: SW Configuration Management

- Computer Software Development Process
  - [ ]a,c
- Project Document Index
  - [ ]a,c
- Common Q Software Program Manual
  - WCAP-16096-NP-A, Section 6
- Common Q SW Configuration Management Guidelines
  - [ ]a,c

These documents satisfy the BTP-14 requirements for a Software Configuration Management Plan.

BTP-14 Documentation Requirements

The requirements for BTP-14, “Software Life Cycle Process Planning”, have been satisfied for the AP1000 Design Requirements Phase.

AP1000
High-Level I&C Architecture

Al Crew
Consulting Engineer

WESTINGHOUSE NON-PROPRIETARY CLASS 3

AP1000 I&C Architecture Outline

- Design Status
- High-Level Architectural Overview
- Architectural Points of Interest
    - Diverse Actuation System (DAS) Diversity
    - Class 1E – Non-Class 1E Communications
    - Component Interface Module (CIM)
    - Manual Control of Safety Components
- Conclusion

Design Status

AP1000 I&C Systems Design Status

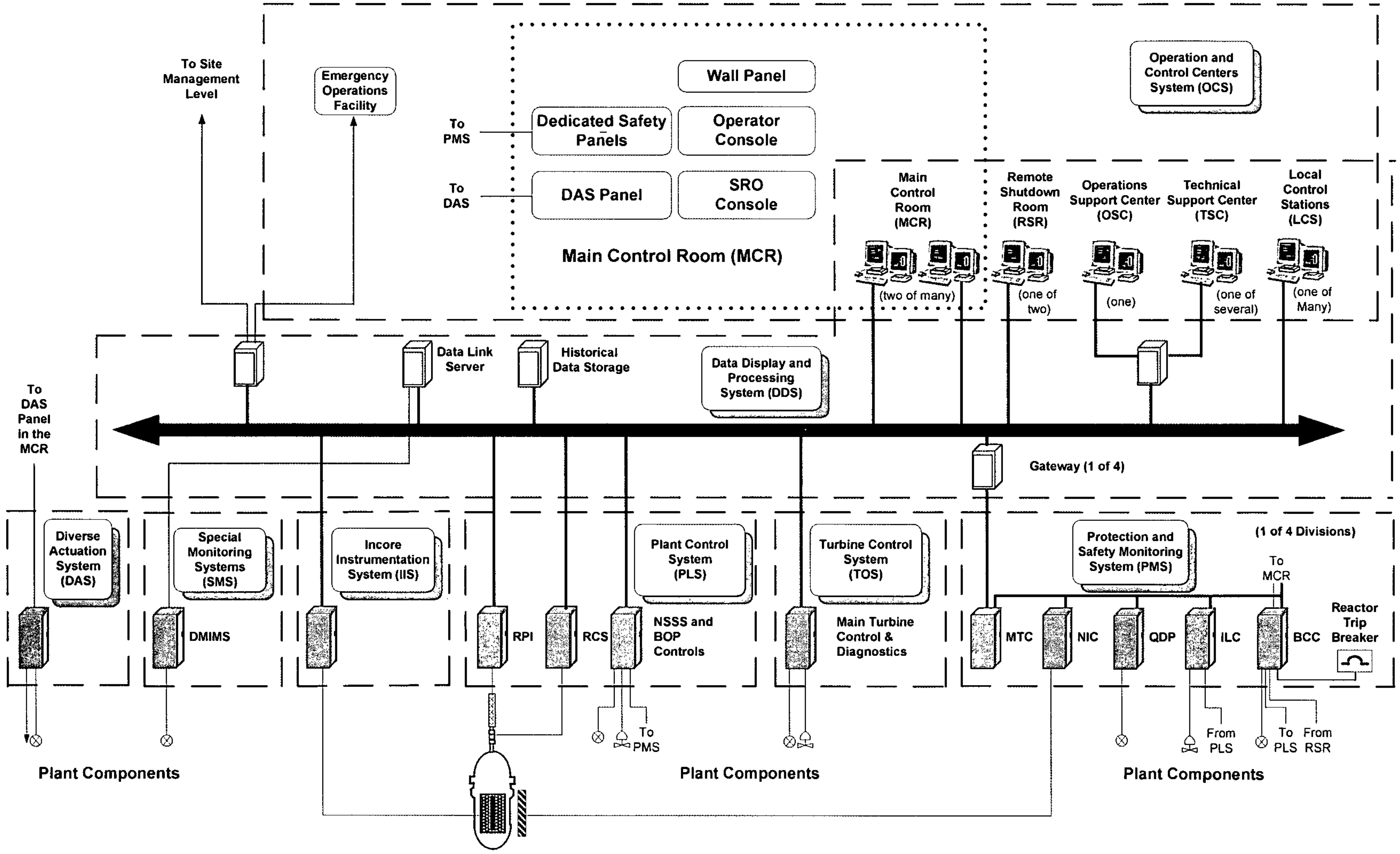
AP1000

- I&C systems are included in the Certified Design
  - Functional requirements consistent with safety analyses and PRA
  - The design process
  - Test and acceptance criteria
  - A conceptual design

A detailed I&C design is being developed based on the functional requirements, using the certified design process, and meeting the certified acceptance requirements.

High Level Architectural Overview

AP1000 I&C Systems Overall Diagram



To Site Management Level
Emergency Operations Facility
To PMS
To DAS
Wall Panel
Dedicated Safety Panels
Operator Console
DAS Panel
SRO Console
Main Control Room (MCR)
Operation and Control Centers System (OCS)
Main Control Room (MCR)
Remote Shutdown Room (RSR)
Operations Support Center (OSC)
Technical Support Center (TSC)
Local Control Stations (LCS)
(two of many)
(one of two)
(one)
(one of several)
(one of Many)
To DAS Panel in the MCR
Data Link Server
Historical Data Storage
Data Display and Processing System (DDS)
Gateway (1 of 4)
Diverse Actuation System (DAS)
Special Monitoring Systems (SMS)
DMIMS
Incore Instrumentation System (IIS)
RPI
RCS
Plant Control System (PLS)
NSSS and BOP Controls
To PMS
Turbine Control System (TOS)
Main Turbine Control & Diagnostics
Protection and Safety Monitoring System (PMS)
(1 of 4 Divisions)
To MCR
MTC
NIC
QDP
ILC
BCC
Reactor Trip Breaker
From PLS
To PLS
From RSR
Plant Components
Plant Components
Plant Components

AP1000 I&C Systems
Major I&C Systems

- Protection and Safety Monitoring System (PMS)
  - RT, ESF, NI, QDPS, and component control (Westinghouse Common Q)
- Diverse Actuation System (DAS)
  - Backs up PMS (Platform/Vendor Selection in Progress)
  - Different architecture, hardware & software from PMS
- Plant Control System (PLS)
  - BOP, NSSS, rod control, rod position indication (Emerson Ovation)
- Data Display and Processing System (DDS)
  - Non-Class 1E displays, alarms, analysis, logging, archiving (Emerson Ovation)
  - Non-Class 1E communication network

AP1000 I&C Systems
Major I&C Systems (Cont'd)

- Operation and Control Centers System (OCS)
  - Integration of human interfaces from PMS, PLS, TOS, DDS, and DAS
  - Includes main control room, remote shutdown room, etc.
- Main Turbine Control & Diagnostic System (TOS)
  - Turbine control and protection (platform/vendor selection in progress)
- In-core Instrumentation System (IIS)
  - In-core flux detectors to DDS, thermocouples to PMS or DAS
- Special Monitoring Systems (SMS)
  - Digital metal impact monitor (Westinghouse DMIMS)

Architectural Points of Interest

AP1000 I&C Systems
Architectural Points of Interest

- DAS Diversity
- Class 1E – Non-Class 1E Communications
- Component Interface Module (CIM)
- Manual Control of Safety Components

The last three topics are interrelated. Each topic will not be fully covered until all three are complete.

Architectural Points of Interest

DAS Diversity

AP1000 I&C Systems
DAS Diversity

- Non-Class 1E System
- Functionality is Defined in the Certified Design
  - Limited scope system, based on the PRA
  - Backs up PMS where postulated common mode failure is risk-important
- Automatic Functions Are Microprocessor-based
  - Different architecture, hardware & software than PMS (DAS platform not yet selected)
- Manual Controls and Indications Use No Software
  - Direct wiring to actuation devices

AP1000 I&C Systems
DAS Diversity (Cont'd)

- System Sensors are Separate from PMS and PLS
- PMS and DAS Actuate Some Common Equipment (e.g., valves)
  - DAS signals are independent from PMS
  - Independent actuation devices
    - Separate solenoid valves on AOVs
    - Separate igniters on squib valves
    - Separate inputs to the MCCs for MOVs

DAS is separate, independent, and diverse from PMS.

Architectural Points of Interest

Class 1E – Non-Class 1E Communications

AP1000 I&C Systems
Class 1E – Non Class 1E Communications

- The Certified Design identifies the need for:
  - Data Flow from PMS to PLS for control purposes
  - Data Flow from PMS to DDS for information system purposes
  - Data Flow from DDS to PMS for system actuation purposes
  - Data Flow from PLS to PMS for component control purposes

The Certified Design requires communication between the Safety System and the Non-safety Systems.

AP1000 I&C Systems
Class 1E – Non-Class 1E Communications

- The Certified Design includes the following ITAACs (in 2.5.2):
  - 7.a) The PMS provides process signals to the PLS through isolation devices.
  - 7.b) The PMS provides process signals to the DDS through isolation devices.
  - 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function.
  - 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls.

AP1000 I&C Systems
Class 1E – Non-Class 1E Communications

- The DCD implements all data flows via channelized bidirectional network gateways.
- Technical Report 42 (TR-42) (APP-GW-GLR-017) describes changes to the design to implement various types of data flow in different manners.
- The TR-42 changes:
  - Reduce the dependence on the gateways
  - Make the gateways uni-directional
  - More clearly establish the points of electrical, communication, and functional isolation

AP1000 I&C Systems
Class 1E – Non Class 1E Communications

a,c

Slide 18

Westinghouse

AP1000 I&C Systems
Transmitter Sharing for Control

a,c

AP1000 I&C Systems
Value Sharing for Control

a,c

AP1000 I&C Systems
Plant Data and PMS Status Sharing

a,c

AP1000 I&C Systems
Uni-directional Gateway Topology

a,c

Slide 22

AP1000 I&C Systems
Operator Initiated Actions

a,c

Slide 23

AP1000 I&C Systems
Manual Component Control

a,c

AP1000 I&C Systems
Ovation Remote I/O Topology

a,c

Architectural Points of Interest

Component Interface Module (CIM)

AP1000 I&C Systems
CIM Motivation

a,c

AP1000 I&C Systems
CIM within the I&C Architecture

a,c

AP1000 I&C Systems
CIM Physical Layout is Modular

a,c

AP1000 I&C Systems
CIM Module Layout

a,c

AP1000 I&C Systems
CIM Block Diagram

a,c

AP1000 I&C Systems
Key CIM Design Features

a,c

AP1000 I&C Systems
Key CIM Continuous On-Line Test Features

a,c

Architectural Points of Interest

Manual Control of Safety Components

AP1000 I&C Systems
Manual Control of Safety Components

- PMS Manual ESF System-Level Actuations (Actuation Only)
  - Dedicated switches in the main control room
  - Connected directly to the “Voting Logic” in each PMS division
- PMS Other Manual ESF System-Level Controls (Blocks and Resets)
  - Uses Common Q soft controls
  - Implemented on Common Q safety displays in the MCR
  - Commands sent to the “Voting Logic” over the Common Q Communication Network

AP1000 I&C Systems
Manual Control of Safety Components

- DDS Manual ESF System Level Actuations (Actuation)
  - Dedicated switches in the RSR
  - Signals pass through qualified isolators to “Voting Logic” in each PMS division
  - Isolators provide electrical and communication isolation
  - PMS logic provides functional isolation
  - PMS disables this function unless operation is Xfr’ed to RSR
- DAS Manual ESF System-Level Actuations (Actuation)
  - Dedicated hardwired switches in MCR on DAS panel
  - Diverse reactor trip and selected ESF functions can be actuated through this separate path.

AP1000 I&C Systems
Manual Control of Safety Components

- Component-level Control for Components with Non-Onerous Consequences
  - PLS Manual ESF Component-Level Control (Actuation and Restoration)
    - Uses Ovation soft controls from the MCR or RSR
    - Commands sent to a CIM in PMS over the Ovation remote I/O bus
    - Fiber provides electrical isolation
    - CIM communication function provides communication isolation
    - CIM priority logic function provides functional isolation

AP1000 I&C Systems
Manual Control of Safety Components

- Component-level Control for Components with Onerous Consequences
  - PMS Manual ESF Component-Level Control (Actuation and Restoration) from the MCR (Normal)
    - Uses Common Q soft controls
    - Implemented on Common Q safety displays
    - Commands sent to component logic over the Common Q Communication Network
  - PMS Manual ESF Component-Level Control (Actuation and Restoration) from the Equipment Room (Unusual)
    - Dedicated maintenance and test switches on the CIM
  - DAS Squib Valve Actuation from the South End of the Auxiliary Building (Very Unusual)
    - Manual means to actuate squib valves

Conclusion

AP1000 I&C Systems
Conclusion

The AP1000 I&C Systems' Safety – Non-safety communication and manual control of safety components meet the independence requirements of IEEE-603 and IEEE 7-4.3.2.

AP1000 Protection & Safety Monitoring System

Carl A. Vitalbo
Fellow Engineer

WESTINGHOUSE NON-PROPRIETARY CLASS 3

PMS Outline

- Channel Definition
- PMS Architecture
- Redundancy within a Division
- QDPS
- Interdivisional Communication
- Summary

PMS Channel Definition

	Function	Conventional Westinghouse Plant	AP1000
Channel **IEEE-603: An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.**	• Interface to field sensors • Comparison to setpoint	• 7100 • 7300 • Eagle-21 coil	Bistable Processor Logic optical
Voting Logic	• RT & ESF coincidence logic	contact • Relay Logic • SSPS	Local Coincidence Logic
Component Control	• Manual actuation of individual safety system components	• Auxiliary Relay Racks	Integrated Logic Processor

PMS Architecture Four Divisions

a,c

PMS Reactor Trip Function

a,c

PMS ESF Actuation

a,c

PMS QDPS Function

a,c

PMS Design Features

a,c

PMS Divisional Redundancy

a,c

PMS Design Features

- Facilitates periodic testing.
- Minimizes potential for Limiting Conditions of Operation (LCO) scenarios.
- Facilitates identification of failure.
- Reactor trip requires 2oo4 coincidence (same as conventional Westinghouse plant), but decreases potential for spurious trip because one division can only open one set of breakers.

PMS Interdivisional Communication

a,c

PMS Summary

- PMS architecture complies with IEEE-603 for interdivisional communications.
- Interdivisional communications are consistent with previous Westinghouse architectures.
- Reactor trip & ESF coincidence logic is performed by separate hardware (same as conventional Westinghouse plants).

AP1000 DCD
Chapter 7 Amendment
TR-80

Tom Hayes
AP1000 I&C Technical Lead

WESTINGHOUSE NON-PROPRIETARY CLASS 3

DCD Chapter 7 Amendment (TR-80)

- Why do we need TR-80?
  - Numerous changes to match current best design practices have been identified via design efforts.
- Intent of TR-80
  - Provide one consolidated compilation of proposed changes to DCD Chapter 7.
- Format of TR-80
  - Similar format to previous TRs
  - Previous TRs that changed Chapter 7 will be referenced
  - New changes will be described with DCD mark-ups included
  - Some of the changes will affect DCD chapters other than Chapter 7
  - Complete Chapter 7 will be provided as an Appendix
- Schedule
  - Planned submittal April 2007

DCD Chapter 7 Amendment

- Previously transmitted Chapter 7 changes:
  - TR-28 – Setpoint Calculations
    - Satisfies COL Item 7.1-1
    - Discussed with NRC October 4, 2006
  - TR-39 – Instrumentation & Control (I&C) Design Changes
    - Refined functional details
    - Discussed with NRC October 4, 2006
  - TR-42 – Resolution of Generic Open Items and Plant-Specific Action Items
    - Satisfies COL Item 7.1-2
    - Discussed with NRC October 4, 2006
  - TR-43 – Failure Modes and Effect Analysis/Software Hazards Analysis (FMEA/SHA)
    - Satisfies COL Item 7.2-1
    - Discussed with NRC October 4, 2006

DCD Chapter 7 Amendment

- Additional Chapter 7 changes include:
  - Remove references to Eagle platform
    - Common Q is the platform chosen for implementation.
    - Revise/delete figures to match Common Q implementation.
    - Remove design detail from Chapter 7 and replace with references to TR-89.
  - Elimination of Protection and Safety Monitoring System (PMS) control room multiplexer
    - Multiplexer is part of Eagle design.
    - Adds complexity for Common Q.
    - System-level actuations to a "lower level" in PMS
  - Diverse Actuation System (DAS) changes (TR-97)
    - Moves DAS squib valve controller to "dirty side" of Auxiliary Building to aid in response to a large fire.
    - Adds remote indication in "dirty" Auxiliary Building.
    - Removes references to "microprocessor" for automatic DAS (Tier 1 change).

DCD Chapter 7 Amendment

- Additional Chapter 7 changes include:
  - Plant Control System (PLS) logic changes
    - Revise PLS to match PMS changes
    - Match current Mechanical Shim (MSHIM) (gray rod control) design
    - Improve control system performance
    - Correct errors in terminology (e.g., signal selector not used for binary signals)
  - Cyber-security
    - Reference to cyber-security report (TR-104) will be added to Chapter 7

DCD Chapter 7 Amendment

- Additional Chapter 7 changes include:
  - Reference Common Q Software Program Manual and Westinghouse procedures for process description.
    - Update Common Q references to current version
    - Delete reference to WCAP-15927
  - Additional PMS logic changes
  - Revise words implying that Remote Shutdown Workstation (RSW) meets single-failure criterion.
  - Correct DCD Tables 7.5-7 and 7.5-9
    - MCR “dampers” were changed to “valves”

AP1000

I&C Technical Reports Submitted to NRC

Tom Hayes
AP1000 I&C Technical Lead

WESTINGHOUSE NON-PROPRIETARY CLASS 3

I&C Technical Reports Submitted

- TR-28 – Setpoint Calculations
  - Submitted May 31, 2006
  - Discussed with NRC October 4, 2006
  - No Requests for Additional Information (RAIs) received to date
- TR-39 – I&C Design Changes
  - Submitted May 22, 2006
  - Discussed with NRC October 4, 2006
  - RAI responses submitted February 8, 2007
  - Revision 1 planned following resolution of RAIs
- TR-42 – Resolution of Generic Open Items and Plant-Specific Action Items
  - Submitted May 27, 2006
  - Discussed with NRC October 4, 2006
  - RAIs combined with TR-88

I&C Technical Reports Submitted

- TR-43 – FMEA/SHA
  - Submitted June 30, 2006
  - Discussed with NRC October 4, 2006
  - No RAIs received to date
- TR-88 – Data Communications
  - This subject was discussed with the NRC on October 4, 2006 and earlier in this meeting
  - Submitted December 13, 2006
  - RAIs received February 2, 2007
- TR-89 – Protection System Architecture
  - This subject was discussed with the NRC on October 4, 2006 and earlier in this meeting
  - Submitted February 16, 2007
  - No RAIs received to date

TR-42 Overview

- **TR-42, APP-GW-GLR-017, "Resolution of Common Q NRC Items"**
  - Dispositions 14 Plant Specific Action Items (PSAIs)
  - Dispositions 10 Generic Open Items (GOIs)
    - This includes:
      - Sufficient Information to Close (for AP1000) GOI 7.8, "Loop Controllers" (Control of Safety System Components)
      - Sufficient Information to Close (for AP1000) GOI 7.9, "Separation of Signals" (Safety/Non-safety Communication)

TR-88 Overview

- **TR-88, APP-GW-GLR-065, "AP1000 I&C Data Communication and Manual Control Safety Systems and Components"**
  - Provides Clarification and Amplification to Support NRC Review of
    - Control of Safety System Components
    - Safety/Non-safety Communication
  - Provides Information on the Component Interface Module (CIM)
    - Presented in TR-88 in lieu of the "Common Q revision" promised by TR-42

Conclusions

TR-88 provides clarification and amplification of TR-42, relating to control of safety system components and to safety/non-safety communication.

Provides the CIM information, which TR-42 promised in a "Common Q revision."

There are no design changes between TR-42 and TR-88.

I&C Future Technical Reports

- TR-80 – DCD Chapter 7 Amendment
  - Planned submittal April 2007
- TR-97 – DAS Platform Technology and Remote Indication
  - APP-GW-GLN-022
  - Planned submittal March 2007
- TR-104 – Cyber-Security
  - Planned submittal May 2007

AP1000

Plan Going Forward
Design Acceptance Criteria
Closure Process

Andrea L. Sterdis, Manager
AP1000 Licensing and Customer Interface

WESTINGHOUSE NON-PROPRIETARY CLASS 23

Design Acceptance Criteria

- For design certification, the requirements of 10 CFR Part 52 apply in addition to those of 10 CFR Part 50.
- Part 52 requires a level of design detail beyond a simple commitment to conformance with the existing requirements.
- 10 CFR 52.47(b)(1) also states that “this rule must provide an essentially complete nuclear power plant design except for site-specific elements..”

Design Acceptance Criteria

- 10 CFR 52.47(a)(2) specifies the following:
  - The application must contain a level of design information sufficient to enable the Commission to judge the applicant's proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. The Commission will require, prior to design certification, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if such information is necessary for the Commission to make its safety determination.

Design Acceptance Criteria

- For AP1000, Design Certification did not include completed design in three areas
  - Piping
  - I&C
  - Human Factors
- SECY-02-0059 defines acceptability of DAC during Design Certification review for all 3 areas
- DAC approach defined as a possible substitute for required design details (but should be limited)
- DAC enables the staff to make a final safety determination, subject only to satisfactory design implementation and verification by the COL applicant, through appropriate use of ITAAC.
- The staff defined DAC as a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas, in making a final safety determination to support a design certification.
- The acceptance criteria for DAC become the acceptance criteria for ITAAC, which are part of the design certification and referred to as Tier 1, Material (or Tier 1, Information).

Design Acceptance Criteria

- For AP1000, all 3 DAC areas are being addressed through the implementation of detailed design

Design ITAAC

- Protection and Safety Monitoring I&C DAC
  - Design Certification included trips, ESF actuations and minimum inventory for dedicated indication and control
  - Design Certification included the certification of the five phase design and implementation process
    - Conceptual (project definition) phase
    - System definition phase
    - Hardware and software design and implementation
    - System integration and test phase
    - Installation phase (including final V&V)

Design ITAAC

- Protection and Safety Monitoring I&C DAC
  - A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following:
    - a) Establishment of plans and methodologies.
    - b) Specification of functional requirements.
    - c) Documentation and review of hardware and software.
    - d) Performance of system tests and the documentation of system test results.
    - e) Performance of installation tests and inspections.

Design ITAAC

- Protection and Safety Monitoring I&C (cont'd)
  - Conceptual (project definition) phase
    - Planning and programmatic documents provided to NRC for their inspection October 2006
  - System definition phase underway; Revisions to Functional Diagrams in process
    - Functional Design completion sufficient to close (11b)
  - Hardware and Software design planned and scheduled
    - Sufficient progress should allow this DAC to be closed in the same time frame as the COL reviews
  - Remaining 2 acceptance criteria (11d) and (11e) require equipment to be procured and installed; Replace with As-Built ITAAC, Not DAC

Design ITAAC Closure Process

- The same for all DAC
  - Vendor completes sufficient design
  - Interaction with staff to confirm "sufficient"
  - Technical Reports submitted for NRC review; detailed design documentation available for staff inspection/audit
  - Acceptable staff reasonable assurance conclusion reached
  - DAC items are closed
    - Design Certification Amendment
      - Revision of Tier 1 information to delete the ITAAC

      or
    - Individual SERs
      - Each COLA references the TR(s) and the associated SER

Plans Going Forward

- Westinghouse Actions
- NRC Actions