Westinghouse Non-Proprietary Class 3

WCAP-16097-NP-A
Appendix 4, Revision 0
(Previously released as CENPD-396-NP, Appendix 4)

May 2003

Common Qualified Platform Integrated Solution

Common Qualified Platform
Integrated Solution

WCAP-16097-NP-A
Appendix 4, Revision 0

CENPD-396-NP-A
Appendix 4, Revision 3

May 2003

REVISION ABSTRACT

Revision 00:
This is the original issue of this document. This document was previously released as CENPD-396-NP, Appendix 4. It is being prepared to create the accepted version in accordance with the USNRC Safety Evaluation dated February 24, 2003. The previously released document CENPD-396-NP, Appendix 4, Revision 2 has been modified as follows:

- Correction of typographical errors.
- Minor document format changes were made.
- References to CENP were replaced with Westinghouse.

TABLE OF CONTENTS

A4.1 Introduction

The purpose of this appendix is to describe the implementation of the Common Qualified Platform for an integrated configuration when digital upgrades are incorporated for multiple safety systems. As an example, this appendix describes the integration of the Core Protection Calculator System (CPCS), Plant Protection System (PPS) and the Post Accident Monitoring System (PAMS). The conceptual design discussed in this appendix is depicted with Advant non-safety system hardware. It is also possible to implement this conceptual design with other types of non-safety I&C systems.

A high level description is also included for a non-safety control system. This provides an example for discussion of the interfaces between the non-safety control system and the safety systems in the integrated solution. It also provides an example of the implementation of diversity between the non-safety control system and the safety systems in order to address the concern regarding a postulated common mode failure in the safety systems.

A4.2 Functional Requirements

The functional requirements for the integrated solution remain the same for each system incorporated. For detailed descriptions of the applicable functional requirements, refer to the Topical Appendices for the PAMS, CPCS, and PPS.

A4.3 System Description

A4.3.1 Safety System Description

Figure 1 is a functional diagram of the integration [
] using the Common Q Platform. This diagram depicts one functional channel of a 4-channel integrated safety system.

Figure 1[

]

A4.3.1.1 CPCS and PPS Level 1

[ ]

For a complete description of the [ ] interchannel communications [ ] refer to the main body of the Common Q Topical Report.

The PPS [ ] is shown with its interchannel [ ] communication [ ] and [ ] process interface modules. This PPS [ ] executes the bistable functions based on the process signals it receives [ ]. It transmits its bistable results[ ] to the [ ] RPS and ESFAS[ ], for two out of four coincidence logic processing and component/system actuation.

A4.3.1.2 PPS Level 2 (RPS/ESFAS)

The PPS [ ] consists of the Reactor Protection System (RPS) and the Engineered Safety Features Actuation System (ESFAS). [ ] These [ ] receive bistable status from all four channels [ ], and then perform the two-out-of-four local coincidence logic. In the case of the RPS, there is a direct interface to the Reactor Trip Switchgear [ ].

A4.3.1.3 Level 3 Controllers

[ ]

A4.3.1.4 HMI Devices

[ ]

A4.3.1.4.1 PAMI & Safe Shutdown Displays and Operators Module

There is an extension to the in-channel [ ] network [ ] that supports the integrated displays for the safety systems.

The channelized Post Accident Monitoring Instrumentation/Indication (PAMI) displays are connected to this network. [ ] I/O and calculated data is then transmitted over the in-channel [ ] bus for display on the PAMI displays.

The channelized Safe Shutdown Displays are also connected to the in-channel AF100 network. The process interface for the Safe Shutdown displays can originate from any AC160 residing on the in-channel network.

[ ]

The channelized PAMI and Safe Shutdown Displays, and the channelized Operators Modules employ the Common Q [ ] technology described in the topical report. All devices employ selectable navigation techniques to access the desired display information.

A4.3.1.4.2 The Integration Of HMI Devices

The advantage of the Common Q Platform becomes most apparent in the integrated solution. Each of the stand-alone safety systems (PPS, ESFAS, PAMS, CPCS) require both an Operators Module that would be located in the Control Room, and a Maintenance and Test Panel (MTP) that would be located in the safety cabinet. These HMI devices would all employ the same Common Q Flat Panel Display System hardware and software technology.

[ ]

A4.3.1.5 Diverse Control and Monitoring Features

A4.3.1.5.1 Diverse Manual Actuation of ESFAS

[ ]

For protective systems which fully implement digital technology for actuation and control of protective system functions, Position 4 requires that alternative means be provided for manual, system level actuation of the protective systems. The alternative means must be diverse from the digital protection systems such that the postulated CMF of the protective system software would not impact the ability of the alternate system to actuate protective functions.

[ ]

A4.3.1.5.2 Diverse Display Of Key Safety Function Indicators

NRC Position 4 also requires that displays for monitoring parameters that support the safety functions be provided by means which are diverse from the digital safety system.

[ ]

A4.3.2 Non-Safety Control System

Figure 3 is a functional diagram of the Integrated Solution architecture for non-safety control.

[ ]

Figure 3[

]

A4.3.2.1 General Description of the Non-Safety Control System

The top level functions are segmented as follows:

- Data Processing System
- Main Control Room
- Remote Shutdown Panel
- Office Workstations

A4.3.2.1.1 Data Processing System

This system performs high level, computational intensive functions

[ ]

The Data Processing System (DPS) uses the Plant Data Network to provide DPS calculation results to external users. This network usually uses a standard communication medium like Ethernet and a standard protocol like TCP/IP.

[ ]

The DPS is also connected to the [ ] Information Network. This communication path allows the DPS to communicate to the Operator Station

[ ]

A4.3.2.1.2 Main Control Room Operator Stations

This section provides clarification for the function of the Multi-Channel Operator Stations.

[ ]

A4.3.2.1.3 Remote Shutdown Panel Operator Stations

This section provides clarification for the function of the multi-channel operator stations.

[ ]

A4.3.2.1.4 Multi-Channel Fixed Position Indicators

This section provides an adequate basis for the Multi-channel Operator Station described in later sections. There are no NRC open issues relating to this section.

The Integrated Solution also addresses replacement of spatially dedicated (i.e. fixed position) indicators that require Class 1E qualification attributes such as seismic qualification.

The Nuplex 80+ CESSAR-DC describes a Discreet Indication and Alarm System (DIAS-N) that provides displays and alarms using the Nuplex 80+ Human Factors Engineering criteria established in Chapter 18 of that document. The DIAS concept, as described in CESSAR-DC, presents information to the operator via discreet indicators, alarm tiles and message windows located on the main control panels.

[ ]

A4.3.2.2 Safety System Interfaces of the Non-Safety Control System

This section is intended to specifically address the NRC Open Items 7.9 and 7.10 relating to the Inter-channel AF100 Network and the Multi-Channel Operator Station.

[ ]

A4.3.2.2.1 Safety System Control from Non-Safety Systems

[ ]

A4.3.2.2.2 Non-Safety Control Using Safety System Signals

[ ]

A4.3.2.3 Description Of Diverse System Characteristics

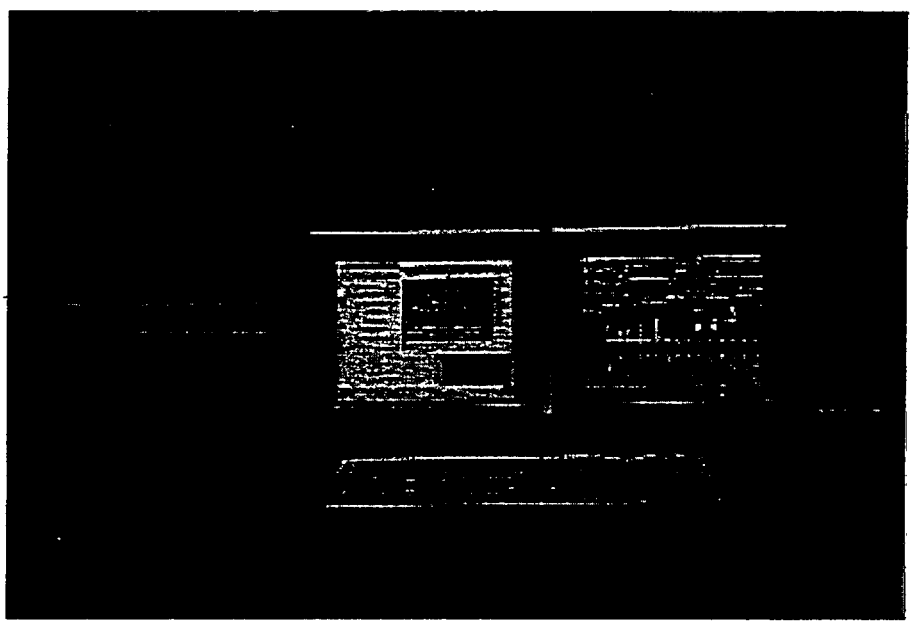
This section provides a description of the non-safety control system components to demonstrate the diversity between this system and the safety system.

[ ]

A4.3.2.3.1 OS500 Workstation

[ ]

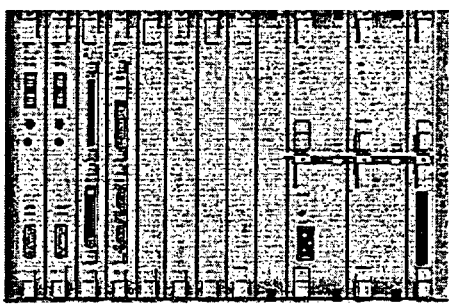
Figure 4
OS 500 Workstation



A4.3.2.3.2 AC450 Controller

The Advant Controller 450 used for the Non-Safety Control System is a controller that supports high-end functionality such as logic, sequencing, closed-loop control (including self-tuning adaptive control), positioning, and drive control. It can support up to 5400 I/O points, using local and remote interfaces.

Figure 5
AC450 Controller



[ ]

Figure 6
Differences Between AC450 and AC160

[ ]

A4.3.2.3.3 Masterbus 300 Network

The MasterBus 300 used for the Non-Safety Control System is an [ ] communication bus used in plant and control networks to handle high data transmission rates [ ]. MasterBus 300E (extended) supports radio or satellite transmission for geographically distributed processes.

[ ]

A4.3.2.3.4 Level 3 Controllers

[ ]

A4.3.3 Defense-In-Depth and Diversity

[ ]

A4.3.3.1.1 AC160 Common Mode Failure

[ ]

A4.3.3.1.2 AF100 Common Mode Failure

[ ]

A4.3.3.1.3 Operators Module or MTP Common Mode Failure

[ ]

A4.3.3.1.4 Level 3 Controllers

[ ]

A4.4 Approach For Demonstrating Adequate CMF Coping Capability For The Integrated Solution

A4.4.1 Methodology for CMF Assessment for a Full Implementation of the Integrated Solution

[ ]

A4.4.2 Methodology for Phased Implementation of I&C Upgrades

[ ]

A4.5 NRC Scope of Review

The purpose of this appendix is to obtain the NRC's approval

[ ]

A4.5.1 Integration of Shared Services

[ ]

A4.5.2 ESFAS Level 3 Loop Controllers

[ ]

A4.5.3 Defense-in-Depth and Diversity

This section is intended to obtain revision of Open Item 6.11 to specifically acknowledge acceptance of a bounding analysis approach for phased modernization.

[ ]

A4.5.3.1 Hardware Qualification Plan for Non-Safety Control Systems

This section is intended to address a concern regarding qualification of ATWS systems raised by the staff at the April 5, 2001 meeting. This is not an SER Open Issue.

The Common Q hardware qualification plan is targeted for components used in safety-related systems.

[ ]

A4.5.4 Interface Between Safety and Non-Safety Channels

This section is intended to specifically address the NRC Open Items 7.9 and 7.10 relating to the Inter-channel AF100 Network and the Multi-Channel Operator Station.

[ ]

A4.5.5 Multi-channel Operator Station Control

This section is intended to specifically address the NRC Open Items 7.9 and 7.10 relating to the Inter-channel AF100 Network and the Multi-Channel Operator Station.

[ ]

A4.5.6 Independence of Main Control Room and Remote Shutdown Panel

[ ]