

CENPD-396-NP
APPENDIX 4
REVISION 01

COMMON QUALIFIED PLATFORM
INTEGRATED SOLUTION

MAY 2000

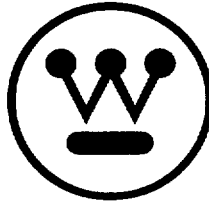
CE NUCLEAR POWER LLC



Legal Notice

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK PERFORMED BY CE NUCLEAR POWER LLC. NEITHER CE NUCLEAR POWER LLC NOR ANY PERSON ACTING ON ITS BEHALF:

- MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED INCLUDING THE WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, WITH RESPECT TO THE ACCURACY, COMPLETENESS, OR USEFULNESS OF THE INFORMATION CONTAINED IN THIS REPORT, OR THAT THE USE OF ANY INFORMATION, APPARATUS, METHOD OR PROCESS DISCLOSED IN THIS REPORT MAY NOT INFRINGE PRIVATELY OWNED RIGHTS; OR
- ASSUMES ANY LIABILITIES WITH RESPECT TO THE USE OF, OR FOR DAMAGES RESULTING FROM THE USE OF, ANY INFORMATION, APPARATUS, METHOD OR PROCESS DISCLOSED IN THIS REPORT.



Westinghouse Electric Company
CE Nuclear Power LLC

**Common Qualified Platform
Integrated Solution**

CENPD-396-NP

Appendix 4

Revision 01

May 2000

This document is the property of CE Nuclear Power LLC and is to be used only for the purpose of the agreement under which it is furnished.



TABLE OF CONTENTS

A4.1	Introduction	3
A4.2	Functional Requirements.....	3
A4.3	System Description	3
A4.3.1	Safety System Description.....	3
A4.3.1.1	CPCS and PPS Level 1	5
A4.3.1.2	PPS Level 2 (RPS/ESFAS).....	5
A4.3.1.3	Level 3 Controllers.....	5
A4.3.1.4	HMI Devices	6
A4.3.1.4.1	PAMI Displays and Operators Module.....	6
A4.3.1.4.2	The Integration Of HMI Devices	6
A4.3.1.5	Diverse Control and Monitoring Features.....	7
A4.3.1.5.1	Diverse Manual Actuation of ESFAS	7
A4.3.1.5.2	Diverse Display Of Key Safety Function Indicators.....	7
A4.3.2	Non-Safety Control System	8
A4.3.2.1	General Description of the Non-Safety Control System.....	10
A4.3.2.1.1	Data Processing System	10
A4.3.2.1.2	Main Control Room Operator Stations.....	10
A4.3.2.1.3	Remote Shutdown Panel.....	11
A4.3.2.1.4	Fixed Position Indicators	11
A4.3.2.2	Safety System Interfaces of the Non-Safety Control System.....	11
A4.3.2.2.1	Manual Control of a Safety System Component	12
A4.3.2.2.2	Data Acquisition of Safety System Signals	13
A4.3.2.3	Description Of Diverse System Characteristics	13
A4.3.2.3.1	OS500 Workstation	13
A4.3.2.3.2	AC450 Controller.....	14
A4.3.2.3.3	Masterbus 300 Network.....	16
A4.3.2.3.4	Level 3 Controllers	17
A4.3.3	Defense-In-Depth and Diversity.....	17
A4.3.3.1.1	AC160 Common Mode Failure	17
A4.3.3.1.2	AF100 Common Mode Failure.....	18
A4.3.3.1.3	Operators Module or MTP Common Mode Failure	18
A4.3.3.1.4	Level 3 Controllers	18
A4.4	Approach for Demonstrating Adequate CMF Coping Capability for the Integrated Solution.....	19
A4.4.1	Methodology for CMF Assessment for a Full Implementation of the Integrated Solution.....	19
A4.4.2	Methodology for Phased Implementation of I&C Upgrades.....	19
A4.5	NRC Scope Of Review	20
A4.5.1	Integration of Shared Services.....	20
A4.5.2	ESFAS Level 3 Loop Controllers	21
A4.5.3	Defense-in-Depth and Diversity	28
A4.5.3.1	Hardware Qualification Plan for Non-Safety Control Systems	29
A4.5.4	Interface Between Safety and Non-Safety Channels	30
A4.5.5	Multi-channel Operator Station Control.....	30
A4.5.6	Independence of Main Control Room and Remote Shutdown Panel.....	31



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)

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 links 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 Displays and Operators Module

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

The Post Accident Monitoring Instrumentation/Indication (PAMI) displays are connected to this network. []

and calculated data is then transmitted over the in-channel [] I/O bus for display on the PAMI []

]

Both the PAMI and Operators Module displays employ the Common Q [] technology described in the topical report.

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

Figure 1 shows use of manual actuation switches in the control room to comply with the NRC's Defense-in-Depth and Diversity Position 4. 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.

Manual actuation using these switches bypasses the complex portion of the safety system operating in Levels 1 and 2 on the AF100 bus, to communicate directly with the simple loop controllers at Level 3. The software in the loop controllers does not allow a failure in the higher levels of the protection system to interfere with manual actuation from the Position 4 switches. This configuration is consistent with Branch Technical Position 19 in NUREG-0800, Chapter 7, Revision 04, and with Nuplex 80+ CESSAR-DC. The communication from the switches to the Level 3 loop controllers must be diverse from the communication used in the protection system. The use of hardwired communication as shown in Figure 1 is an acceptable method.

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. Figure 1 shows that signals for these displays are provided directly from the Level 3 loop controllers via a dedicated serial interface, which is diverse from the AF100 link.

The displays use the same Common Q Flat Panel Display technology as discussed in the topical report. Data acquisition is performed by the



simple, reliable controllers implemented in Level 3. The software in the Level 3 controllers does not allow a failure in Level 1, Level 2 or in an AF100 bus to interfere with communication to the Position 4 Displays. This method of displaying these parameters using means which are diverse from the safety software which is considered to be subject to the postulated CMF, is consistent with the Nuplex 80+ CESSAR-DC.

A4.3.2 Non-Safety Control System

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

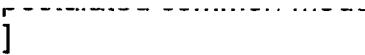
] 



Figure 3[

Integrated Solution Standard Architecture - Non-Safety



]

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

The Operator Stations have two data communication paths. There is the [] Information Network []. The other connection is to the Plant Data Network [



]

A4.3.2.1.3 Remote Shutdown Panel

The Remote Shutdown Panel would have the same similar functionality for non-safety control as described for the safety systems. The MCR Transfer Switch [] would then allow [] commands from the Remote Shutdown Panel []. The functionality of the MCR transfer switch is described in the Nuplex 80+ CESSAR-DC, Section 7.4.1.1.10.

A4.3.2.1.4 Fixed Position Indicators

The Integrated Solution also addresses replacement of spatially dedicated indicators that require 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.

To minimize the display devices, the Integrated Solution is using the DIAS concept of providing single displays with Process Representation Values, rather than channelized displays. These displays and their interfaces will be Class 1E.

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

[



]

A4.3.2.2.1 Manual Control of a Safety System Component

[

1



]

A4.3.2.2.2 Data Acquisition of Safety System Signals

The [] linkage between the safety systems and non-safety control system is the process instrument signals. These process instrument signals are [] fed to the non-safety control systems []

].

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

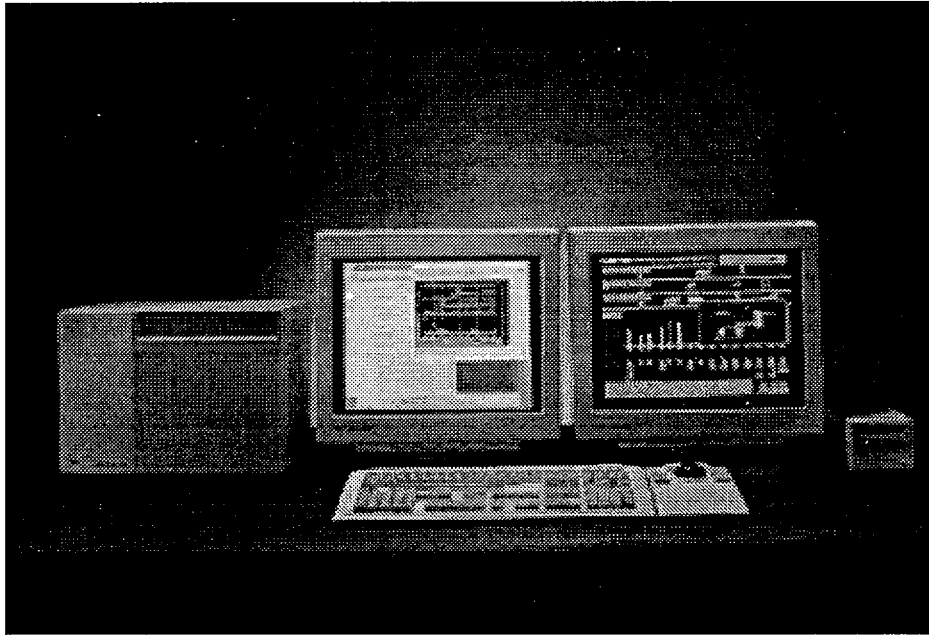
The [] 500 Operator Station used for the Non-Safety Control System can [] be [] interface board [] configured with one or two high-resolution monitors, an alphanumeric or function keyboard, a mouse or trackball. The workstations run appropriate combinations of ABB AdvaCommand and Advainform software for on-line HMI display capability.

This hardware and software is sufficiently diverse from the Common Q Flat Panel Display System used for the protection systems, [' ' ' ']



...] The OS500 Workstations would provide an alternate HMI for safety system status indication and control if a CMF were to affect the capability of the FPDS.

Figure 4
OS 500 Workstation

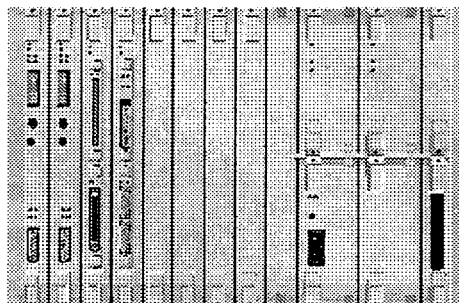


A4.3.2.3.2 AC450 Controller

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



[



]

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

[

]

¹ Includes processor and I/O modules. AF100 common mode failure discussed separately.



A4.3.3.1.2 AF100 Common Mode Failure

[

]

A4.3.3.1.3 Operators Module or MTP Common Mode Failure

[

]

In addition, the Position 4 manual initiation switches provide another level of diverse actuation of safety systems should the FPDS become disabled.

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

The steps that would be performed to demonstrate adequate capability to cope with a CMF of the software used in a digital upgrade of the protection system of an operating plant are outlined below. These steps follow the same methodology as used for certification of System 80+.

- 1) Identify the I&C systems relied upon for the plants Chapter 6 and Chapter 15 analyses.
- 2) Identify other I&C systems not subject to the same CMF based on implementation of the Common Q Integrated Solution.
- 3) Perform qualitative evaluations using System 80+ methodology. Determine specific Chapter 6 and Chapter 15 events which require further evaluation or analyses.
- 4) Perform EOP evaluations to determine operator response times to be credited, based on the methodology used for System 80+.
- 5) Perform quantitative best estimate analyses of the remaining subset of events. Credit automatic responses and operator actions via I&C systems not subject to the same CMF.
- 6) Apply acceptance criteria based on plant specific design limits to demonstrate the acceptability of the response for these events.

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

- 1) Perform bounding analysis for integrated solution. Document diverse I&C equipment credited.
- 2) For each phase of the upgrade, perform an evaluation to verify that the diverse I&C equipment which was credited to cope with a CMF for the upgraded equipment will be available.



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*

[

]

[Bus

This bus is still dedicated to one safety channel for in-channel communications. [

]

Interface and Test Processor (ITP)



The ITP's function, described in the PPS appendix, interfaces with the PPS [] and ESFAS []

Maintenance and Test Panel (MTP)

The MTP [] and its functions are described in the PAMS, CPC and PPS appendices. In those appendices, each safety system had a dedicated MTP for system diagnostics and maintenance for each channel. Each channel will still have a dedicated MTP []

]

Operators Module (OM)

The same is true for the OM. [] Each safety channel will still have dedicated OMs[]

]

A4.5.2 ESFAS Level 3 Loop Controllers

[]















A4.5.3 Defense-in-Depth and Diversity

] This concept [
] is supported in Nuplex 80+ CESSAR-DC:

A control signal from each switch is directed to Loop Controllers which are PLC based devices at the lowest level in the digital control hierarchy. ... Under normal plant operating conditions, the Loop Controller provides output signals to the plant components in response to digitized input signals received through a communication network interface. The hardwired manual input signal from the control room switches will override input data received from the network communication interface to actuate the plant components. Diverse manual actuations status indication is provided in the main control room.

Reliability of implementing this override function at the Loop Controller PLC can be assured due to the simplicity of the device. The software in the Loop Controller PLC's resides in memory that is typically less than 6 Kbytes. The PLC responds to a limited number of digital input signals which direct the software to start or stop a pump, or open or close a valve with consideration of only a limited number of interlocking signals. Testing will be performed on loop controller PLC's for which the manual override function is implemented to assure that a common mode failure of the protective system software will not prevent the hardwired manual signals from actuating their associated ESF functions. This feature of the System 80+ design provides an additional level of protection against a postulated common mode failure of protective system software.²

² Nuplex 80+ CESSAR-DC, Section 7.3.1.1.6



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

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

]

This approach [] has been shown generically in the Nuplex 80+ CESSAR-DC to provide acceptable plant safety analysis performance[].



A4.5.4 *Interface Between Safety and Non-Safety Channels*

The testing and cross channel functions of the ITP are described in the PPS appendix of this topical report. [

inter-channel test is described in the PPS appendix. [] The function of

A4.5.5 *Multi-channel Operator Station Control*



[

]

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

[Main Control Room (MCR) and the
Remote Shutdown Panel (RSP) [] are isolated []
] to ensure that a fire in the MCR or RSP does not propagate[

]