Westinghouse Non-Proprietary Class 3

WCAP-16097-NP-A
Appendix 2, Revision 0
(Previously released as CENPD-396-NP, Appendix 2)

May 2003

Common Qualified Platform Core Protection Calculator System

Common Qualified Platform
Core Protection Calculator System

WCAP-16097-NP-A
Appendix 2, Revision 0

CENPD-396-NP-A
Appendix 2, Revision 2

May 2003

REVISION ABSTRACT

Revision 00:
This is the original issue of this document. This document was previously released as CENPD-396-NP, Appendix 2. 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 2, Revision 1 has been modified as follows:

- A document titled, "Additional Information Regarding the Westinghouse Common Qualified Platform Core Protection Calculator System, CENPD-396-P, Appendix 2, Revision 1" was provided to the NRC via LTR-NRC-02-41, dated August 14, 2002. This document has been added as an Addendum to the Appendix. It describes changes to the CPCS configuration based on experience gained in working with the new Common Q Platform.
- The CPC Failure Modes and Effects Analysis has been superseded by a new analysis in the Addendum. Therefore, the original analysis has been deleted.
- The Reference to the Common Qualified Platform Topical Report has been updated.
- Correction of typographical errors.
- Minor document format changes were made.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ATTACHMENT: Standard Technical Specification Markup Pages (LCO 3.3.1, LCO 3.3.3)

ADDENDUM: Additional Information Regarding the Westinghouse Common Qualified Platform Core Protection Calculator System, CENPD-396-P, Appendix 2, Revision 1

A2.0 DIGITAL CORE PROTECTION CALCULATOR SYSTEM (CPCs)

The purpose of this Core Protection Calculator System (CPCS) appendix is to provide the functional requirements and conceptual design of the CPCS.

The scope of this CPCS appendix is to provide the functional requirements and conceptual design of the system based upon common-Q components. These requirements include CPC functional design, testing, major Man Machine Interface functions, system block diagrams, and the interface with the analog Plant Protection System (PPS) or Digital Plant Protection System (DPPS). Since the implementation of the CPCS is functionally identical in both the PPS and DPPS case, the abbreviation "PPS" shall be used throughout this appendix. Any differences in the CPC implementation necessitated by the substitution of a DPPS for a PPS will be addressed in the Integrated Solutions Appendix.

Brackets in this document indicate proprietary information. The bracket denoting the end of a proprietary segment of this report may appear one or more pages following the bracket denoting the start of the proprietary segment. As a result, care should be exercised in determining what information in this report is proprietary.

A2.1 FUNCTIONAL REQUIREMENTS

A2.1.1 Overview:

The CPCS shall generate trip and pretrip signals on Low Departure from Nucleate Boiling Ratio (Low DNBR) and High Local Power Density (High LPD), as well as CEA Withdrawal Prohibit (CWP) signals to the PPS, in the form of binary (contact) inputs. The PPS shall use these and other inputs to automatically actuate a Reactor Trip (RT) whenever the monitored processes violate predefined limits in at least two of the four redundant PPS channels.

The CPC system consists of four channels of equipment (Channels A, B, C, & D). The four channels of equipment are located inside the Auxiliary Protective Cabinet (APC), where the channels are physically separated and isolated from each other. The CPCS contains four CPC/Control Element Assembly Calculator (CEAC) systems, one per channel. Each CPC channel provides contact outputs to its respective PPS channel.

Each CPC/CEAC channel shall communicate with a CPC Operator's Module mounted in the Control Room. Each of the four Operator's Modules is fiber optically isolated from its associated CPC channel. The Operator's Module shall be used for CPC/CEAC channel monitoring, to provide the capability to manually

alter addressable constants, to initiate channel operating bypass at low power levels, and to initiate periodic surveillance testing.

The CPC/CEAC system shall include manually initiated automatic test capability for determining system operability. It shall also perform automatic hardware diagnostic testing. It shall be possible to initiate surveillance testing from the Operator's Module, or from a locally mounted maintenance and test panel (MTP). Except as noted below, the functions of the CPC/CEAC are identical to those in the present design.

A2.1.1.1 Operator's Module Functions

Each CPC channel shall have an Operator's Module (OM) mounted in the main control room. The Operator's Module shall be the primary means by which the operator communicates with the CPC and associated CEACs during normal operation. The OM shall have enhanced display capability as compared to the present OM implementation.

The Operator's Module shall have a flat panel display from which the following can be performed:

[ ]

A2.1.1.2 Maintenance and Test Panel (MTP) Functions:

A locally mounted MTP in each CPC channel shall interface with its associated CPC/CEAC.

[ ]

A2.1.1.3 CEA Position Display Functions:

A single non-Class 1E CEA Position Display (CEAPD) shall be mounted on the main control board. The CEAPD shall provide CEA position-related information on a large screen display, and shall be connected to the CPC/CEAC system MTPs in all four channels by fiber-optically isolated ethernet connections. The display shall also provide alarm on CEA Deviations, CEA Sensor failure, and data-link failure. Several display formats will be available. Operator display format and CPC/CEAC channel input selection shall be via an Operator's keypad located on the main control board.

The proposed CEAPD provides enhanced CEA position monitoring as compared to the present CEAC CEA position display on the Main Control Board.

[ ]

A2.1.1.4 CPC/CEAC Channel Inputs:

The CPC/CEAC system uses four redundant sets of inputs, one set per channel, for all input parameters except CEA position. CEA position is provided by two Reed Switch Position Transmitter (RSPT) inputs on each CEA.

[ ]

In addition to the RSPT inputs, the following analog inputs are monitored by each CPC channel:

- Cold Leg Temperature, analog voltage (two, from diagonally opposite cold legs)
- Hot Leg Temperature, analog voltage (two, one from each hot leg)
- Pressurizer Pressure, analog voltage (one, narrow range)
- Ex-core Flux, analog voltage (three, Upper, Middle, and Lower detectors)
- Reactor Coolant Pump Speed, pulse train proportional to RCP speed (one per RCP)

The above listed inputs are identical to those in the present design.

[ ].

A2.1.1.5 CPC/CEAC Channel Outputs:

The CPC channels process the channel inputs so as to provide DNBR and Local Power Density protection, and generate appropriate trip and pretrip binary (contact) output signals to their associated PPS channels.

The CPCS provides the following contact outputs to the PPS:

- Low DNBR-Trip
- High Local Power Density Trip
- Low DNBR Pretrip
- High Local Power Density Pretrip
- CEA Withdrawal Prohibit (CWP)

The PPS will process the CPC-generated inputs so as to produce a reactor trip on Low DNBR or High Local Power Density if at least two CPC channels indicate a trip condition in the same parameter.

[ ]

The Low DNBR and High LPD pretrip signals are processed in the PPS for indication and annunciation purposes. The CWP input is processed in the PPS so as to produce a CEA Withdrawal Prohibit to the Control Element Drive Mechanism Control System (CEDMCS) if any two or more of the four CPCs indicate a CWP condition.

[ ]

Each CPC channel also provides several output contacts, via interposing relays, for annunciator use, as defined in Section A2.1.2.2.2.

Each CPC channel provides the following analog outputs for use in indicators and recorders on the control board:

- DNBR Margin (difference between DNBR and trip setpoint)
- kW/ft Margin (difference between LPD and trip setpoint)
- Calibrated Ex-core Power (adjusted for CEA shadowing and cold leg temperature shadowing)
- RCS Flow (used during startup testing, but no dedicated indicator on MCB)

The above listed CPC trip, pretrip, and CWP outputs to the PPS and analog outputs to the main control board are functionally identical to the outputs provided by the CPC in the present design.

A2.1.1.6 DNBR/LPD Trip Channel Bypassing during Periodic Testing:

Placing a CPC/CEAC channel in a periodic test mode shall only be possible if both the Low DNBR and High LPD trips are trip channel bypassed in the associated PPS channel. Trip channel bypassing these parameters within the PPS channel effectively bypasses the Low DNBR and High LPD trip contacts in that PPS channel, changing the RPS logic to a two out of three from the normal two out of four for these trip functions.

[ ]

The trip channel bypasses of the Low DNBR and High LPD trips shall be manually inserted in each channel from the PPS Bistable Control Panel, which shall communicate trip channel bypass status to the associated channel CPC MTP to enable CPC/CEAC testing. The trip channel bypasses shall allow for channel maintenance and surveillance testing at power per the requirements of IEEE Std. 338 and IEEE Std. 603, as augmented by USNRC Reg. Guide 1.22.

The interlock requiring trip channel bypassing of the DNBR-Low and LPD-High trips prior to initiation of CPC testing is functionally identical to the present design.

[ ]

A2.1.1.7 Operating Bypasses:

The operating bypass of the CPC channel shall be manually performed from the CPC OM or MTP when the Ex-core safety channel wide range neutron flux monitoring system indicates that power is low enough to warrant bypassing of the DNBR and LPD protection afforded by these trips. As in other operating bypasses performed in the PPS channel, the bypass is automatically removed when reactor power rises above the bypass permissive setpoint. The DNBR-Low and LPD-High pretrip signals shall be affected by the operating bypass in the same manner as the trip signal.

This operating bypass capability is functionally identical to that in the present design.

[ ]

A2.1.1.8 Failure Modes:

The CPC/CEAC system shall be designed for fail safe operation under component failure or loss of electrical power as defined in the Failure Modes and Effects Analysis (FMEA).

Since the proposed CPC channel implementation includes extensive hardware and software diagnostic capability, as well as redundant channel design features, the channel is fault tolerant to a great extent. Fault tolerance is discussed in Section A2.3.1.2.

A2.1.1.9 Human Machine Interface:

CPC/CEAC Human Machine Interface (HMI) shall be designed per accepted Human Factors Engineering (HFE) principles. Both the CPC and OM shall include display and diagnostic capabilities unavailable in the present design. HMI provisions are described in section A2.4.3.

A2.1.1.10 Functional Diversity:

[ ]

A2.1.2 CPC Functional Requirements Detail:

This section compares the functional design of the existing CPC/CEAC system with its proposed Common Q replacement. The proposed CPC/CEAC system shall meet or exceed the functional requirements of the existing system, as defined below.

The system requirements identified herein are defined to assure that the hardware/software configuration is compatible with the reactor protective algorithms. Requirements are specified in the area of input/output, protection program interaction, operator interface, and initialization. These requirements are derived from CPC Functional Design Requirements document, 00000-ICE-3208 Revision 08 (Reference 2.7.1).

A2.1.2.1 CPC Design Basis:

The Low DNBR and High Local Power Density trips, (1) assure that the specified acceptable fuel design limits on departure from nucleate boiling and centerline fuel melting are not exceeded during Anticipated Operational Occurrences (AOOs), and (2) assist the Engineered Safety Features Actuation System (ESFAS) in limiting the consequences of certain postulated accidents.

- The auxiliary trip feature of the CPCS, which opens the Low DNBR and High LPD trip contacts, will satisfy the following additional design bases:

[ ]

The replacement CPC/CEAC channels shall satisfy the above requirements by running safety-related protection algorithms functionally identical to those in the present CPC implementation. In the proposed implementation, a fatal CPC processor fault condition shall de-energize the CPC hardware watchdog timer, opening the Low DNBR and High LPD trip and pretrip outputs, as well as other outputs defined in Section A2.1.2.2.2. Test, maintenance, or initialization, shall force a "CPC Fail" condition, which shall open the Low DNBR and High LPD channel trip contacts.

The proposed CPC implementation has significant fault tolerance.

[ ]

These features are defined in the FMEA and described in Appendix section 2.3. Low DNBR and High LPD channel trips will be forced whenever a channel module or component failure is detected which would impact the ability of the channel to perform its safety-related function.

The following list of processor fault conditions is accommodated by the existing CPC implementation. The disposition of each condition in the proposed CPC implementation is addressed below:

[ ]

Response of the CPC channel to failure of the CEAC or Communications Processors is addressed in Section A2.3.1.2.1. The CPC processor and CEAC processor are each equipped with separate watchdog timers. The effect of CPC or CEAC watchdog timer timeout on the channel contact outputs is addressed in Section A2.1.2.2.2.

A2.1.2.1.1 CPC Timing:
The replacement CPC/CEAC channels shall have a response time consistent with that of the present CPC implementation, as defined in Appendix Section A2.1.2.2.4.

A2.1.2.2 System Requirements:

A2.1.2.2.1 Inputs:
The following table lists the CPC process input signals for each channel. The accuracy requirements given in the table reflect those in the present CPC implementation, and establish the maximum allowable uncertainty introduced by the conversion of input signals to internal binary format. The accuracy requirements are based upon the total uncertainties attributable to the following:

- Loading effects
- Reference voltage supply regulation
- Electrical noise
- Linearity
- A/D converter power supply sensitivity
- Quantization

Table A2.1.2-1
CPC PROCESS INPUT SIGNALS

[ ]

A2.1.2.2.2 Outputs:
The output signals for each CPC channel are listed in Table A2.1.2-2.

The two trip output signals are used in the Plant Protection System for DNBR and LPD reactor trips.

[ ]

All six contact outputs actuate operator alarms. The analog outputs for DNBR Margin, LPD Margin, and neutron flux power are required to drive analog meters that are monitored by the operator in the control room. The analog output for coolant mass flow rate is required for comparison of CPC calculated flow to measured flow during startup testing.

Table A2.1.2-2

CPC OUTPUT SIGNALS

Signal	Type	Range
Low DNBR Trip (Note 1)	Contact Output	0, 1 (logical)
Low DNBR Pretrip (Note 1)	Contact Output	0, 1 (logical)
High LPD Trip (Note 1)	Contact Output	0, 1 (logical)
High LPD Pretrip (Note 1)	Contact Output	0, 1 (logical)
CEA Withdrawal Prohibit (Note 1)	Contact Output	0, 1 (logical)
CPC Sensor Failure (Note 1)	Contact Output	0, 1 (logical)
DNBR Margin	Analog	0-10 (unitless)
LPD Margin	Analog	0-25 (KW/Ft)
Calibrated Neutron Flux Power	Analog	0-200 (% of rated power)
Core Coolant Mass Flow Rate	Analog	0-2 (fraction of design flow)

The first five conditions listed above are indicated or annunciated through the PPS interface. The sixth, CPC Sensor Failure, is annunciated from contacts within the CPC channel.

Annunciator Contact Outputs:

Provisions will be made within the CPC Channel to provide the following annunciator contact outputs:

[ ]

The CPC Fail annunciation requirement is derived from the existing CPC Functional Requirements. The CEAC Fail, CEAC Sensor Fail, and CEA Deviation output requirements are specified in the CEAC Functional Design Requirements document, 00000-ICE-3234, Revision 06, as identified in Appendix section A2.1.3. The requirement for CEAC Inoperable output is consistent with the present CPC implementation. Annunciation provisions for Operating Bypasses are required to comply with RG 1.47, as specified in the Common Qualified Platform Topical Report Section 4, Codes and Standards.

[ ]

A2.1.2.2.3 Program Structure:

The CPC design basis requires that the system calculate conservative, but relatively accurate, values of DNBR and peak linear heat rate. In order to achieve a

system time response sufficient to accommodate the limiting design basis events, additional dynamic calculations of DNBR and peak linear heat rate are required. The dynamic calculations must provide conservative estimates of DNBR and peak linear heat rate based on changes in the process variables between successive detailed calculations of DNBR and peak linear heat rate. The calculations of DNBR and peak linear heat rate must also be separated into different programs. The grouping of the detailed calculations must be such that the execution interval of each program reflects the time interval over which the dynamic adjustments to the parameters, calculated in that program, are valid.

The resultant protection software consists of four interdependent programs and one subroutine that is accessible to the first two programs

[ ]

The replacement CPCS shall run functionally identical CPC safety-related algorithms to the existing CPCS, so that program structure will remain unaffected. Software changes will be restricted to those required to reflect new hardware platform features, such as diagnostics and error handling, and backplane communications between CPC and CEAC in the proposed system. None of these changes will impact the safety-related aspects of CPC software.

In the existing CPCS, the TRIPSEQ Subroutine compares the minimum DNBR, quality margin, and peak local power density to their respective pretrip and trip setpoints. Whenever a setpoint is violated, the appropriate contact output is actuated.

[ ]

In the proposed CPCS, the above functionality will be replicated.

[ ]

A2.1.2.2.4 Program Timing and Input Sample Rates:
Execution of the four previously described programs is scheduled on a priority basis. The execution frequency of each protection program is fixed, based upon the required CPC time response. In addition, the more frequently executed programs are assigned a higher priority. The required execution frequencies are specified in Table A2.1.2-3.

[ ]

Communication among the protection programs must be controlled to assure that the output of a program is based on a consistent set of inputs. Therefore, it is necessary to ensure that the input to a program is not changed until after the

execution of the program is complete. The executive will be prohibited from interrupting a protection program while it is reading input from the output of another protection program. In addition, no protection program may be interrupted while it is transferring its output data or while a trip sequence routine is being executed.

Table A2.1.2-3
PROGRAM EXECUTION INTERVALS AND INPUT SAMPLING RATES

[ ]

A2.1.2.2.5 Operator Interface:
The reactor operator shall be informed of the status of a CPC channel by three mechanisms:

- The system generates alarms to alert the operator to abnormal events
- The operator interrogates the system using the OM or MTP to determine the current value of a particular parameter
- The operator reads one of three meters driven by the CPC analog outputs

The proposed CPCS will retain all of the above capabilities, and will display all of the same parameters.

[ ]

Some of these features are described below:

CPC Failed Sensor Stack:

The failed sensor stack logs CPC sensors out of range. Presently, up to six sensors are logged. When a sensor changes state the sensor ID is entered at the top of the stack, and all elements in the stack are shifted downwards one position, with the last entry discarded. Sensor out of range high, sensor out of range low, and sensor in range are each distinctively identified. For each failure, the time of sensor failure is also logged. In the present display it is necessary to scroll through 18 consecutive point IDs to obtain the preceding information.

[ ]

CPC Channel Tripped Snapshot:

In the present CPC design, when a trip is generated in a CPC channel a snapshot of CPC variables required for display is transmitted to a buffer, and made available using a teletype. An addressable constant is provided to reset (clear) the buffer. The value of the addressable constant is also a flag indicating the status of the buffer. A "1" indicates a full buffer, and a "0" indicates an empty buffer. Resetting the buffer PID from 1 to 0 clears the buffer. The snapshot is for the first trip after the buffer is cleared. An auto-restart shall not clear the buffer.

[ ]

A2.1.2.2.6 Operator Input:
The operator shall be able to change addressable constants using the OM or the MTP.

[ ]

It shall not be possible to modify any value not identified as an addressable constant.

A2.1.2.2.7 Initialization:
The CPC must be capable of initializing to steady state operation for any allowable plant operating condition.

[ ]

Until initialization is complete, all trip outputs must be set in a tripped state.

The proposed CPC design will also meet the above requirements.

A2.1.2.2.8 Interlocks and Permissives:
A means shall be provided to permit bypassing of the trip and pretrip contact outputs for a CPC channel when reactor power as indicated by the corresponding PPS flux power signal is less than 10^{-4} %. In addition, a means shall be provided to adjust the bypass setpoint up to at least 1 % power. The bypass shall be implemented such that it must be manually implemented at the input/output device for each CPC channel. A means, such as a key switch, must be provided to prevent initiation of the bypass by unauthorized personnel. The bypass must be automatically removed from each CPC channel when the PPS neutron flux signal indicates that power is above the bypass setpoint.

The proposed CPC design will also meet the above requirement.

A2.1.2.2.9 Algorithm Implementation:
The safety-related algorithms in the CPC channel will be functionally identical to those described in Reference 1.

It will be necessary to change some of the implementation details to accommodate the new platform, as described in this Appendix. However, these changes shall not negatively impact the functionality of safety-related CPC or CEAC algorithms.

A2.1.2.2.10 Testing Requirements:
The CPC shall be designed to permit periodic testing on demand. During testing, it shall be necessary to trip channel bypass the Low DNBR and High LPD reactor trip to enable operation of test software. Performance of CPC software testing will result in a CPC Fail condition, opening the Low DNBR and High LPD trip contacts.

A2.1.3 CEAC Functional Requirements Detail:

The system requirements identified herein are defined to assure that the hardware/software configuration is compatible with the reactor protective algorithms. Requirements are specified in the area of input/output, protection program interaction, operator interface, and initialization. These requirements are derived from CEAC Functional Design Requirements document, 00000-ICE-3234 Revision 06 (Reference 2.7.3).

[ ]

A2.1.3.1 CEAC Design Basis

The function of the CEAC is to scan all CEA positions, and, based upon any single CEA deviation within a CEA subgroup, to calculate the single CEA position-related penalty factors necessary to ensure that the CPCs calculate conservative approximations to the actual core peak LPD and DNBR during single CEA-related anticipated operational occurrences, which require CPC protection. The CEAC must also be capable of detecting a reactor power cutback event.

A2.1.3.2 Functional Design and Computer Design Requirements

A2.1.3.2.1 Inputs:
[ ]

The CEAC shall calculate the magnitude of CEA deviation penalty factors based upon CEA position sensor input data obtained from each RSPT. The components of the Penalty Factors are determined from the following data:

[ ]

The proposed CEACs shall retain the preceding program structure, and shall implement functionally identical safety-related algorithms.

A2.1.3.2.2 Outputs:
The existing output signals for each CEAC are listed in Table A2.1.3-1.

Table A2.1.3-1

CEAC OUTPUT SIGNALS

[ ]

A2.1.3.2.3 Program Structure:

[ ]

The proposed replacement CPCS shall meet the above criteria.

[ ]

A2.1.3.2.4 Program Timing and Input Sample Rates:

[ ]

The algorithm required for this purpose is time-oriented, with a calculation scheduling rate and update period that are compatible with overall CEAC/CPC system response requirements. The execution period is the maximum time in seconds from the time CEA RSPT sensors are scanned to the time the CEAC calculated outputs are updated with new information from that input scan and calculation. The calculations shall be scheduled in such a manner that the update requirements are met.

There are two CEAC update periods:

[ ]

A2.1.3.2.5 Program Interfaces

In the present design, communication between the CEAC output and the CPC must be rapid and simple, since each CEAC provides its output to all four CPC channels via a one-way isolated data link. The output to the CPCs must not change until after the execution of the CEACs has been completed.

[ ]

The proposed CEAC replacements will have the capability of transmitting the same information to the associated CPC channels.

[ ]

Thus, the format of the information transfer will change, as described in Section A2.1.3.2.2, though the content, as far as CPC/CEAC functionality is concerned, will remain the same.

A2.1.3.2.6 CEAC Failure Flags:

The CEAC Failure Flag, presently transmitted as part of the 16 bit buffer, is set true whenever either of the following conditions exists:

[ ]

CEAC processor faults resulting in CEAC failure are the same as those resulting in CPC failure, as described in Section A2.1.2.1.

Sensor validity checks (out of range, rate of change) are performed by the CEAC. If either check is failed the sensor failure flag is set.

A2.1.3.2.7 Case 2 Deviation Flag:
The CASE 2 Deviation Flag, presently transmitted as part of the penalty factor word, is set true whenever either or both of the following conditions exists:

[ ]

In the proposed CPC/CEAC implementation, the functionality of the Case 2 Deviation Flag will remain the same.

[ ]

A2.1.3.2.8 Reactor Power Cutback Flag:
The Reactor Power Cutback Flag, presently transmitted as part of the penalty factor word, is set true whenever the following conditions exist:

[ ]

In the proposed CPC/CEAC implementation, the functionality of the RPC Flag will remain the same.

[ ]

A2.1.3.2.9 Scaling Flag:
Presently, after the DNBR and LPD penalty factors have been calculated, the penalty factor is compared to set limits, and the scaling flag, part of the penalty factor word, applied.

In the proposed CPC/CEAC implementation, the functionality of DNBR and LPD penalty factor scaling will remain the same.

[ ]

A2.1.3.3 Operator Interface:

The reactor operator shall be informed of the status of a CEAC channel by three mechanisms:

1. The system generates alarms to alert the operator to CEA sensor failures or excessive CEA deviation.

2. The CEA Position Display (CEAPD) Monitor displays the position of the individual CEAs arranged into subgroups and control groups utilizing a bar graph representation, the floating point values of the two penalty factors, and a flag to indicate the cause of any alarms.

3. The CPC/CEAC OM or MTP can be used to display CEAC inputs, selected intermediate variables, and outputs.

The proposed CEACs will retain all of the above capabilities, and will display all of the same parameters.

[ ]

Some of these features are described below:

A2.1.3.3.1 CEAC Failed Sensor Stack

The failed sensor stack logs CEAC sensors (RSPTs) out of range. Presently, up to six sensors are logged. When a sensor changes state the sensor ID is entered at the top of the stack, and all elements in the stack are shifted downwards one position, with the last entry discarded. Sensor status (active/inactive) is identified. For each failure, the time of failure is also logged. In the present display it is necessary to scroll through 18 consecutive point IDs to obtain the preceding information.

[ ]

A2.1.3.3.2 CEAC Channel Trip Snapshot

A snapshot of CEA positions, penalty factors, and time of deviation occurrence is initiated by:

[ ]

The input CEA positions and resulting penalty factors are stored in a stack. A time tag is included in the stack. An addressable constant is provided to clear the buffer. The CEAC fail indication shall be saved through auto restarts.

[ ]

A2.1.3.3.3 CEAC Fail
CEAC Fail indication is transmitted to the CPC channel under the following conditions:

[ ]

In the proposed CPC/CEAC implementation, the functionality of CEAC Fail indication will remain the same.

[ ]

The CEAC Fail condition shall cause CEAC Trouble annunciation.

A2.1.3.3.4 Operator Input :
The Operator shall be able to change addressable constants from the Operator's Module. Addressable constants can only be changed when a manual interlock is satisfied. It shall not be possible to modify any value not identified as "addressable".

In the proposed CPC/CEAC implementation, the operator shall be able to change addressable constants from the OM or MTP.

[ ]

As in the present design, it shall not be possible to modify any value not identified as Addressable.

A2.1.3.4 Initialization:

The CEACs shall be capable of initializing to steady state operation for any allowable plant operating condition.

[ ]

Until initialization of a CEAC is complete, the CEAC failure flag shall be set.

A2.1.3.5 Testing Requirements:

The CEAC shall be designed to permit periodic testing of the CEAC penalty factor algorithm on demand. During testing, the CPC shall be informed that the CEAC is

in test. CEAC testing in the proposed CEAC implementation shall meet the functional requirements of the existing system.

Proposed testing implementation:

[ ]

A2.1.3.6 Algorithm Description:

The replacement CEAC safety-related algorithms shall be functionally identical to those in the existing CEAC system. It will be necessary to change some of the implementation details to accommodate the new platform, but the safety-related algorithms and timing requirements will not be altered.

[ ]

Figure A2.1-1
CPC Block Diagram

A2.2 SYSTEM DESCRIPTION

The CPC/CEAC system is comprised of four redundant channels (A, B, C, and D as depicted on Figure A2.1-1, "CPCS Block Diagram") that perform the necessary calculation, bistable, and maintenance/test functions. The system includes four redundant Operators Modules, one per CPC/CEAC channel, located on the Main Control Room panels. One CPC/CEAC channel is associated with each PPS channel, and provides Low DNBR trip and pretrip, High LPD trip and pretrip, and CWP discrete (contact) outputs to its associated PPS channel. Four redundant channels are provided to satisfy single failure criteria and improve plant availability.

The CPC/CEAC Processors in each channel receive channelized process sensor analog inputs, to perform the detailed DNBR and LPD calculations, and provide the associated bistable trip functions.

A2.2.1 Overview

The CPC System will be installed into the auxiliary protective cabinet (APC), physically separate from the PPS, as in the present CPC/CEAC system.

[ ]

A2.2.1.1 CPC/CEAC Processor Assembly Overview:

The CPC/CEAC processor assembly in each channel consists of two chassis:

1) The controller subrack, that contains the PM646 processors, global memory, communications, and RCP Speed Pulse Count input modules.

2) The I/O subrack, that contains the I/O modules.

[ ]

As described in the Functional Requirements section of this Appendix, Section A2.1, the channel inputs consist of hot and cold leg temperature, RCS pressure, RCP speed, and CEA position via RSPTs.

[ ]

CPC/CEAC processing of this CEA position input is functionally unchanged from that in the present design.

[ ]

Operator's Module Overview:

There are four CPC Operator's Modules, one for each channel, mounted in the main control room. The CPC OM is implemented using a Flat Panel Display System.

[ ]

Maintenance and Test Panel Overview:

There is one MTP in each CPC/CEAC channel, implemented using a Flat Panel Display System identical to that of the Operator's Module, used for diagnosing the system, providing electrically isolated communications to external systems, and displaying the same information as the Operator's Module. The MTP is local to the CPC processors and is the primary man-machine interface for routine maintenance and surveillance testing by plant technicians.

[ ]

Watchdog Timer:

The CPC and CEAC processor modules each contain an external Watchdog Timer Module (WDT). If the CPC or CEAC processor fails to refresh this module, the module will open its respective trip and annunciation output contacts.

The CPC WDT will cause the CPCS to generate Low DNBR and High Local Power Density channel trips to the PPS. This provides a failsafe condition should the CPCS computer system fail. Internal system diagnostics are contained within the AC160 as well. As described in Appendix section 2.2, the CPC Watchdog Timer module also opens the following contact outputs, placing them in an alarm state:

- DNBR Pretrip
- LPD Pretrip
- CWP
- CPC Trouble
- CPC Sensor Fail

The CEAC WDT will cause the CEAC processor to indicate alarm conditions for both CEAC outputs in that channel. As described in Appendix section A2.1.3.2.2, the CEAC Watchdog Timer module opens the following contact outputs, placing them in an alarm state:

- CEAC Trouble
- CEAC Sensor Fail
- CEA Deviation

[ ]

A2.2.2 CPC Design Implementation:

The CPC design implementation:

[ ]

The CPC architecture is designed to minimize potential single failures and improve system reliability. CPC equipment that performs safety-related functions is designed for simplicity to maximize system reliability and availability. This philosophy results in maximum system availability under single random failure conditions.

[ ]

The trip, pretrip, and CWP outputs to the PPS are channelized such that these outputs are provided only in the associated PPS channel.

[ ]

A2.3 HARDWARE DESCRIPTION

[ ]

Figure A2.3.1-1
Front View Of PM646 Processor Module

[ ]

A2.4 SOFTWARE DESCRIPTION

[ ]

Figure A2.4.2-1
AC160 Software Configuration Block Diagram

[ ]

A2.5 SYSTEM INTERFACES

[ ]

A2.6 FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

[ ]

The CPCS FMEA is documented in the Addendum to this Appendix .

A2.7 REFERENCES

The following list of references is specifically addressed in this Appendix.

A2.7.1 CPC Functional Design Requirements, 00000-ICE-3208, Revision 08

A2.7.2 CEAC Functional Design Requirements, 00000-ICE-3234, Revision 06

A2.7.3 Common Qualified Platform Topical Report, CENPD-396-P-A, Revision 2, May 2003.

A2.7.4 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603-1991

A2.7.5 IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Station Safety Systems, IEEE Std. 338-1987

A2.7.6 USNRC Regulatory Guide-Periodic Testing of Protection System Actuation Functions (Safety Guide 22), Regulatory Guide 1.22.

A2.7.7 Guidance on Defense-In-Depth and Diversity in Digital Computer Based I&C Systems, BTP HICB-19

A2.7.8 Methods for Performing Diversity and Defense In depth Analyses of Reactor Protection Systems, NUREG/CR-6303-1994

A2.7.9 Arkansas Nuclear One Unit 2 Safety Evaluation Report, Appendix D, Supplement 1, Docket No. 50-368.

A2.7.10 USNRC Regulatory Guide-Bypassed and Inoperable status Indication for Nuclear Power Plant Safety Systems, Regulatory Guide 1.47, Rev. 00

A2.7.11 IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384-1992

A2.7.12 IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE Std 379-1994

A2.7.13 USNRC Regulatory Guide-Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems, Regulatory Guide 1.53, Rev. 00

A2.7.14 USNRC Standard Review Plan for the Review of Safety Analysis reports for Nuclear Power Plants, Chapter 7, NUREG 0800-1997, Rev. 04

A2.8 PROPOSED TECHNICAL SPECIFICATION CHANGES

Insert A, Table 2.8-1, is to be located in Standard Technical Specifications for Combustion Engineering Plants, NUREG 1432, Rev. 1, LCO 3.3.1 "RPS Instrumentation-Operating (Digital)". Existing Conditions E, F, and G, will become Conditions I, J, and K.

[ ]

Table A2.8-1
PROPOSED LCO 3.3.1 INSERT A

[ ]

ATTACHMENT

To

Common Qualified Platform
Core Protection Calculator System

CENPD-396-NP-A
Appendix 2, Revision 2
May 2003

NUREG 1432, Revision 1
Standard Technical Specification
Markup Pages

(LCO 3.3.1 and 3.3.3, Digital)

(This entire attachment consists of information that is proprietary to Westinghouse Electric Co. Therefore, it is not included in this Non-Proprietary document.)

ADDENDUM

To

Common Qualified Platform
Core Protection Calculator System

CENPD-396-NP-A
Appendix 2, Revision 2
May 2003

Additional Information Regarding the
Westinghouse Common Qualified Platform
Core Protection Calculator System
CENPD-396-P, Appendix 2, Revision 1

This Addendum was provided to the USNRC as an Attachment to transmittal letter LTR-NRC-02-41, dated August 14, 2002

Attachment to LTR-NRC-02-41

Additional Information Regarding the Westinghouse Common Qualified Platform Core Protection Calculator System, CENPD-396-P, Appendix 2, Revision 1

Introduction:

The Common Qualified Platform-based Core Protection Calculator System (CPCS) has evolved from that presented in CENPD 396-P, Rev. 01, Appendix 2. The safety-related algorithms of the CPCS will remain the same as in the topical report submittal, as will the platform used to implement these algorithms. However, the configuration of the individual modules will be changed to enhance system performance. The following sections describe the configuration change and its rationale.

Revised CPCS Configuration

Figure 1.1 depicts the CPCS configuration as depicted in Figure 2.1-1 of the CPCS topical report appendix. Figure 1.2 depicts the revised configuration.

1.1 Physical Configuration Changes

The following changes to the CPCS configuration are depicted in Figures 1.1 and 1.2.

In the following description, the term "existing configuration" refers to the configuration as described in the topical report appendix. "Revised configuration" refers to the new CPCS configuration as it differs from that in the topical report appendix. "Legacy System" refers to the CPCS that is presently installed and operational at existing plants.

1.1.1. Number of Subracks and Disposition of Processors

[ ]

The revised configuration has several advantages over the existing CENPD 396P Appendix 2 configuration:

1.1.1.1 CEAC Redundancy

[ ]

1.1.1.2 Backplane Loading Considerations

[ ]

1.1.1.3 CPC Processor Allocation

[ ]

1.1.1.4 Analog Input Module Configuration

[ ]

1.1.1.5 CEAC to CPC Penalty Factor Transmission

[ ]

1.1.1.6 Channel Communications

[ ]

1.1.2 Power Supply Configuration

[ ]

1.1.3 OM and MTP ethernet connections

[ ]

1.1.4 Time Synchronization

[ ]

1.1.5 Processor Module Model

[ ]

1.1.6 Changes in Watchdog Timer Configuration.

The existing configuration employs a separate discrete watchdog timer module. The revised implementation employs a watchdog timer included within the PM646A processor. This WDT receives inputs from both the processor and communications sections of the PM646A such that if either fails to update the WDT within the prescribed time interval, the watchdog timer will time out, deenergizing an output relay which is accessed from the PM front panel. Relay contacts are configured to open (trip) the Low DNBR, High LPD trip and pretrip contacts, as well as the CWP signal to the PPS. This response is identical to the PPS.

2. Other Changes:

As the design has evolved, several additional changes have been made to the CPCS which are not apparent in an examination of Figures 1.1 and 1.2.

Appendix Section	Proposed
A2.1.1.3	[ ]
A2.1.1.3	[ ]
A2.1.1.3	[ ]
A2.1.1.3	[ ]
A2.1.2.1	[ ]
Table A2.1.2-2	Changed range of DNBR Margin meter output to 0 to 2 units rather than 0 to 10 units, at customer request. At full power, the DNBR margin is normally between 0 and 1.0, so the existing resolution is less than optimal. This affects meter display scaling only, and does not impact the safety related functions of the CPCS in any way. The resulting improved meter resolution will increase its usefulness during full power operation, when DNBR margins are the lowest, and DNBR margin monitoring is of the greatest concern.
A2.1.2.2.2	Refined conditions for annunciation. Additional annunciator digital outputs provided.
A2.1.2.2.2	[ ]
2.3	[ ]
A2.3.1.3	[ ]
A2.3.1.3	[ ]
A2.3.1.5	[ ] The AI685 module is referenced in the NRC SER for the Common Q platform.
A2.3.1.5	[ ]
A2.3.2.1	[ ]
A2.3.3.1	[ ]
A2.6	The FMEA is revised to reflect the new configuration and failure modes.
A2.8	Technical Specifications: Plant specific TS will be submitted, reflecting these changes.

Figure 1.1
(Existing Figure A2.1-1)

[

]

Figure 1.2
(Revised Figure A2.1-1)

[

]

REVISED CPC ARCHITECTURE
FAILURE MODE AND EFFECTS ANALYSIS

[

]