Westinghouse Non-Proprietary Class 3

WCAP-16097-NP-A
Appendix 3, Revision 0
(Previously released as CENPD-396-NP, Appendix 3)

May 2003

Common Qualified Platform Digital Plant Protection System

Common Qualified Platform
Digital Plant Protection System

WCAP-16097-NP-A
Appendix 3, Revision 0

CENPD-396-NP-A
Appendix 3, 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 3. 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 3, Revision 1 has been modified as follows:

- On June 7, 2001, a document titled, "Westinghouse Nuclear Automation Basis for Change to CENPD-396-P, Appendix 3, Common Qualified Platform, Digital Plant Protection System" was provided to the NRC. This document addressed the simultaneous failure of the OM and MTP in the FMEA. Therefore, the FMEA table, Table A3.6-1, has been revised to include a new entry for both OM and MTP inoperable.
- The References to the Common Qualified Platform Topical Report and Software Program Manual have been updated.
- Correction of typographical errors.
- Minor document format changes were made.

TABLE OF CONTENTS

LIST OF ATTACHMENTS

LIST OF FIGURES

LIST OF TABLES

A3.0 DIGITAL PLANT PROTECTION SYSTEM (DPPS)

The purpose of this Digital Plant Protection System (DPPS) appendix is to provide the functional requirements and conceptual design of the DPPS.

The scope of this DPPS appendix includes implementation of both the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) based upon common-Q components. These requirements include DPPS functional design, testing, major Man Machine Interface functions, system block diagrams, and the interface with the Core Protection Calculators, Power Sources, Annunciators, Plant Computer, and other equipment.

This appendix addresses DPPS upgrades applicable to both the RPS and PPS generation of plants. For both RPS and PPS plants, it is possible to upgrade only the RPS, or only the ESFAS, or both the RPS and ESFAS. This appendix specifically addresses the most comprehensive case, namely that of replacing both the RPS and ESFAS. Considerations involved in replacing a subset of this equipment (RPS or ESFAS only) are also discussed, but to a lesser extent.

The scope of this Appendix is limited to replacement of the equipment located in the PPS cabinet and ESFAS Auxiliary Relay Cabinets (ARCs). Sensors and related signal conditioning equipment external to the PPS cabinet, and final actuated devices (trip circuit breakers, ESF valves, pumps and other equipment) are not to be altered by this DPPS upgrade, and are addressed only as an interface.

Brackets in this document indicate proprietary information. The bracket denoting the end of a proprietary segment in 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.

PPS/RPS Background

Philosophically, the Plant Protection System (PPS) is composed of both RPS and ESFAS functions. In the earlier Combustion Engineering (C-E) plants, the RPS and ESFAS were separate physical entities, with the RPS supplied by the NSSS Vendor, and the ESFAS typically falling within the Architect Engineer's scope of supply.

These earlier C-E plants with separate RPS and ESFAS implementations include:

- Palisades
- Fort Calhoun
- Millstone Unit 2
- Calvert Cliffs Units 1 and 2
- St. Lucie Units 1 and 2.

In this appendix, these plants, employing separate RPS and ESFAS implementations, are referred to as "RPS" plants.

C-E plants of more recent design combine the RPS and ESFAS functions into one common cabinet, referred to as a "PPS" cabinet. The PPS cabinet includes the bistable trip functions and two-out-of-four logic to initiate both the reactor trip and ESFAS function actuation. Plants employing a PPS cabinet also have two separate ESFAS cabinets which house the train A and Train B component actuation relays, as well as local indication, manual actuation, and selective two out of four actuation logic. These are designated Auxiliary Relay Cabinets (ARCs) Train A and Train B.

These more recent U.S. C-E plants with RPS and ESFAS implementations in a common PPS cabinet include:

- Arkansas Nuclear One-Unit 2 (ANO-2)
- San Onofre Units 2 and 3 (SONGS 2 and 3)
- Waterford Unit 3 (WSES-3)
- Palo-Verde Units 1, 2, and 3 (PVNGS).

In this appendix, these plants, employing a common RPS and ESFAS in a PPS cabinet are referred to as "PPS" plants.

In both the RPS and PPS generation of plants, fundamental RPS design features have remained essentially unchanged since the first CE plant (Palisades) was built. These features include four separate and redundant sensor and bistable channels providing outputs to six two-out-of-four coincidence matrices, whose output is provided to the RPS actuation devices that are

arranged in a selective two out of four logic. This configuration ensures that no single failure can either result in an inadvertent trip or prevent a legitimate trip from occurring. For all plants except Palisades and Fort Calhoun, this final selective two out of four logic is implemented using Reactor Trip Circuit Breakers (RTCBs) actuation devices. For the two plants listed, DC clutch power supplies are used in lieu of RTCBs, but the basic selective two-out-of-four configuration of initiation (K) relay inputs is identical for both designs. This similarity lends itself to a common DPPS replacement design.

For PPS-generation plants, the fundamental RPS design features were replicated for actuation of the ESFAS functions. This includes separate and redundant sensor and bistable channels providing outputs to six two-out-of-four coincidence matrices, whose output is provided to a selective two out of four logic. In the PPS plants, the sensor and bistable channels are sometimes shared with the RPS function. For example, Low Pressurizer Pressure provides both a reactor trip and an ESFAS actuation (SIAS, in this case). In the ESFAS, the final selective two out of four logic is implemented separately for each train, in the associated Train A or Train B ARC.

The ESFAS in RPS generation plants varies in implementation from plant to plant, but generally includes four sensor channels and a separate two out of four coincidence logic (sometimes multiple logic) for each function in each train. Thus, the ESFAS implementation in RPS-generation plants is not incompatible with that in the PPS-generation plants, though implementation details differ.

PPS/RPS CPC Implementation Differences:

The basic RPS implementation described above is applicable to the RPS design in all CE plants. Specific reactor trips and operating bypass functions do differ slightly from plant to plant, but these differences may be easily accommodated in the DPPS upgrade without any significant change to the fundamental design. For the purposes of this appendix, the intent is to replicate existing trip functions at each plant. Implementation of existing trips, presently based on analog hardware, with digital technology, offers the opportunity for significant enhancements to those trip functions. However, no changes to existing functions are proposed by this upgrade at this time. It is anticipated that setpoint changes will occur due to the absence of instrument drift considerations in digital hardware.

Although the most significant difference between "RPS" and "PPS" generation plants is the incorporation of the ESFAS into the latter, another significant difference between these generations of plants is in the implementation of the Core Protection Calculator (CPC) function. The CPCs provide protection from Anticipated Operational Occurrences (AOOs) which could violate plant Safety Limits associated with Departure from Nucleate Boiling Ratio (DNBR) and Local Power Density (LPD).

In the RPS generation of plants, this protection was afforded by two trip functions, the Thermal Margin/Low Pressure (TM/LP) and the Axial Power Distribution (APD) trips. The trip setpoints for these functions are somewhat complex variables, and are calculated in analog computers (analog core protection calculators) physically located in the lower part of the RPS cabinet. The implementation of the CPCs in these RPS plants is thus presently based upon analog technology, and though complex by the standards of other trip functions, is relatively straightforward, and lends itself well to implementation in a digital bistable processor without the need for any additional equipment. Thus, for the RPS plants, the CPC-based TM/LP and LPD trip functions will be implemented in the bistable processors in the DPPS upgrade.

[ ]

In the PPS generation of plants, the previously described protection is afforded by the Low DNBR and High Local Power Density (Hi-LPD) reactor trips. These are very complex functions as compared to their analog counterparts, and are calculated in separate stand-alone digital computers mounted in an Auxiliary Protective Cabinet (APC). The APC provides a contact input to the PPS cabinet for Low DNBR trip and pretrip, High LPD trip and pretrip, and CEA Withdrawal Prohibit (CPC-CWP). For the purposes of this appendix, it is assumed that the CPCs will remain separate from the PPS. Thus, these contact inputs to the PPS will continue to exist for the DPPS upgrade.

Remote Control Module

Each DPPS Channel shall communicate with a DPPS Remote Control Module (RCM) mounted in the Control Room. Plants have the option of retaining their existing RCM, implemented in hardware, or replacing this device with a standard Common-Q flat panel display-based RCM. For the purposes of this appendix, the flat panel-based RCM replacement is considered the standard design. The following discussion therefore applies to the flat-panel implementation.

[ ]

In RPS-generation plants, the RCM may be implemented in the RPS cabinet, since there is no RCM feature in the present design. In PPS-generation plants, the RCMs shall also monitor the status of the ESFAS trains.

[ ]

A3.1 FUNCTIONAL REQUIREMENTS

A3.1.1 Overview:

The DPPS shall fulfill functions of the existing PPS, RPS or ESFAS, as appropriate. For the purposes of this Appendix, the functional requirements for the 3410 Mwt class of plants shall be used as reference. These include ANO-2, SONGS 2 and 3, and WSES-3. For other plants, functional requirements are similar, and will be addressed by the plant-specific upgrade installation.

The following section lists functional requirements and design bases as delineated in Reference 1, "Functional Description for Plant Protection System", 00000-ICE-3201-Rev. 02, issued 03/02/76. The purpose of this section is to demonstrate the extent of DPPS upgrade compliance with basic PPS system requirements.

A3.1.1.1 General Functional Requirements (Reference 1, Section 2.1)

- "The PPS shall continuously monitor selected safety-related parameters such as neutron flux, reactor pressurizer pressure, steam generator pressure, and level etc,) in a reliable fashion, in order to assure a known plant status at all times except during refueling".

  The proposed DPPS installation shall comply with the above by reliably monitoring the same parameters and providing plant status information that is at least equivalent to the existing installation.

- "The PPS automatically initiates plant protective action in the form of actuation of appropriate systems whenever the monitored selected plant parameters reach predetermined levels where plant protection is required."

  The proposed DPPS installation shall comply with the above by actuating the same systems (RPS and ESFAS, as appropriate) subject to the same trip setpoint considerations as the present design. It is anticipated that setpoints may change somewhat because of reduced uncertainty associated with digital implementation, but compliance with established setpoint methodology as required by the Bases of NUREG 1432, "Standard Technical Specifications Combustion Engineering Plants" will be maintained. Though not specifically addressed in this Appendix, the versatility of a DPPS upgrade in accommodating more complex trip functions (e. g. variable setpoints vice fixed setpoints, compensation of neutron flux power for temperature (cold leg temperature shadowing), etc), makes it possible to more reliably and accurately monitor relevant variables, and provide protection as required.

- "The PPS provides alarms and, in some cases, limiting signals to control systems, whenever the monitored selected plant parameters approach the predetermined levels where plant protection would be required."

The proposed DPPS will provide the same alarms, and will provide additional diagnostic information in a user-friendly format, It will therefore be an enhancement over the existing system. The same limiting signal to control systems (i. e. the CEA Withdrawal Prohibit) will also be provided.

A3.1.1.2 Reactor Protection System Functional Requirements (Reference 1, Section 2.2)

- "The RPS shall consist of measurement channels, logic, and those circuits necessary to effect reliable and rapid reactor shutdown (reactor trip) if any one or a predetermined combination of the monitored conditions reach a limiting safety system setting. The system function is to protect the core and reactor coolant system pressure boundary.

"The measurement channels consist of sensors, signal conditioning equipment and trip bistables. These channels provide trip signals to the coincidence logic.

"A two-out-of-four coincidence of like trip signals is required to generate a reactor trip signal.

"The reactor trip signal opens the reactor trip circuit breakers, thus deenergizing the Control Element Drive Mechanism Coils, allowing the shutdown and regulating Control Element Assemblies (CEAs) to drop into the reactor core."

The proposed DPPS installation will satisfy all of the preceding requirements. Measurement channels are unaffected by the DPPS upgrade, as existing inputs will be used. The use of bistables feeding two-out-of-four coincidence logic remains, though existing hardware performing these functions will be replaced with digital bistable processors and local coincidence logic processors performing the same functions described above. The existing reactor trip circuit breakers, their configuration, and relationship to the CEDMCS will be unaffected by the DPPS upgrade.

[ ]

This appendix assumes either the four or eight RTCB configuration. In some cases (Palisades and Fort Calhoun) there may be four initiation contacts deenergizing clutch power supplies in lieu of RTCBs. In all cases,

the basic selective two out of four logic used in the initiation circuitry is the same.

- The RPS Provides trips for the following conditions:

1. High Linear Power Level Trip. This trip uses the average of the three ex-core linear subchannel flux signals. This trip function includes audible and visual pretrip indication.

   The proposed DPPS installation shall satisfy the above requirements for a high linear power level trip and pretrip. It should be noted that in some plants, the trip function is a variable high power trip. In the case of PVNGS, a rate limited function is employed on an increasing signal. In the RPS plants, the trip setpoint must be manually reset upwards as power level is increased. Minimum and Maximum trip setpoint values are also included. These trip function variations can be accommodated on a plant-specific basis.

2. High Logarithmic Power Level. This trip uses the wide range (logarithmic) ex-core channel output. A trip results when power increases above a preset value. The trip may be manually bypassed when power level rises above
   10^{-4} % RTP. This trip function includes audible and visual pretrip indication.

   The DPPS installation shall satisfy the above requirements for a high logarithmic power level trip, manual bypass capability, and pretrip indication. It should be noted that RPS-generation plants do not have a High Logarithmic Power Level trip. These plants do usually employ a "Rate of Change of Power-High" trip based upon wide range neutron flux indication. The rate of change of power is automatically bypassed when power level is below 1×10^{-4} % or above approximately 15 % power in these plants. The DPPS installation shall be capable of replicating this function for the RPS-based plants, including bypass operation.

3. High Local Power Density Trip. The High LPD trip is a contact input from the CPC channel. It ensures maintenance of the LPD safety limit during AOOs. This trip function includes audible and visual pretrip indication.

   For PPS-generation plants, the DPPS implementation shall accommodate the High LPD trip and Pretrip contact inputs from the CPC auxiliary protective cabinets. Though not explicitly stated in the functional requirement for this trip, the trip may be manually bypassed when below a preset power level as indicated by the ex-core wide range channel. This manual bypass feature shall also be accommodated in the DPPS design.

For RPS plants, the High LPD trip function does not exist. However, these plants usually employ an analogous High APD trip implemented in analog computer hardware. This trip is a function of the Axial Shape Index (ASI) and average channel ex-core power as indicated by the Power Range Nuclear Instrumentation (NI) safety channel. In the RPS-generation plants, this trip is implemented in the existing RPS cabinet without the use of external CPCs. Similarly, in the DPPS implementation, the High APD trip function shall be incorporated into the bistable processor trip algorithms, without requiring any additional CPC hardware. In the RPS plants, the APD-High trip is automatically bypassed when below a given power level (nominally 15%), as indicated by the power range nuclear instrumentation safety channel. This feature will be replicated in the DPPS. It should be noted that this automatic bypass feature is usually implemented with the same bistable responsible for bypassing the High Rate of Change of Power and Loss of Turbine reactor trips. In one RPS-generation plant, this bypass function has been separated from these other functions. In the DPPS design, it shall be possible to have separate bistable setpoints for each bypass function, if desired.

4. Low DNBR Trip. The Low DNBR trip is a contact input from the CPC channel. It ensures maintenance of the DNBR safety limit during AOOs. This trip function includes audible and visual pretrip indication.

   For PPS-generation plants, the DPPS implementation shall accommodate the Low DNBR trip and Pretrip contact inputs from the CPC auxiliary protective cabinets. Though not explicitly stated in the functional requirement for this trip, the trip may be manually bypassed when below a power level as indicated by the ex-core wide range channel. This manual bypass feature shall also be accommodated in the DPPS design.

   For RPS plants, the Low DNBR trip function does not exist. However, these plants usually employ an analogous Thermal Margin/Low Pressure (TM/LP) trip implemented in analog computer hardware. This trip is a function of RCS Pressure, the Axial Shape Index (ASI) and average channel ex-core power as indicated by the Power Range Nuclear Instrumentation (NI) safety channel, and Delta T power. In the RPS-generation plants, this trip is implemented in the existing RPS cabinet without the use of external CPCs. Similarly, in the DPPS implementation, the TM/LP trip function shall be incorporated into the bistable processor trip algorithms, without requiring any additional CPC hardware.

5. High Pressurizer Pressure Trip. The high pressurizer pressure trip function trips the reactor when RCS pressure reaches a high preset value. This trip function includes audible and visual pretrip indication.

   The proposed DPPS installation shall satisfy the above requirements for a high pressurizer pressure trip and pretrip. It should be noted that in the RPS-generation of plants, the high pressurizer pressure trip also provides a signal to open Power Operated Relief Valves (PORVs). PORVs do not exist at PPS-generation plants. In the DPPS implementation, the ability to open PORVs shall be retained for RPS generation plants.

6. Low Pressurizer Pressure trip. The low pressurizer pressure trip is provided to trip the reactor when measured pressurizer pressure falls to a low preset value. This trip function includes audible and visual pretrip indication.

   The proposed DPPS installation shall satisfy the above requirements for a low pressurizer pressure trip and pretrip. In the PPS generation of plants, this function trips the reactor and simultaneously initiates a Safety Injection Actuation Signal (SIAS). RPS-generation plants do not have an explicit Low Pressurizer Pressure trip, since this low pressure trip feature is a floor (minimum) setpoint in the TM/LP trip function. In the RPS-generation of plants, the ESFAS function is independent of the RPS. The DPPS implementation shall replicate all existing features on both generations of plants. Should the implementation be for an RPS and ESFAS upgrade in an RPS-generation plant, the option shall exist for simultaneous RPS trip and ESFAS actuation, as in the PPS generation of plant. It shall also be possible to retain separate RPS and ESFAS trips setpoints for this function.

7. High Steam Generator Water Level trip. This trip function trips the reactor when RCS steam generator level in either steam generator reaches a high preset value. This trip is equipment protective only, and is not required by the safety analysis. This trip function includes audible and visual pretrip indication.

   The proposed DPPS installation shall satisfy the above requirements for a high steam generator level trip and pretrip. In the PPS-generation of plants, there are presently two SG-specific high level trips. RPS-generation plants do not have High-SG level trips. The DPPS shall replicate existing functionality in both cases.

8. Low Steam Generator Water level Trip. This trip function trips the reactor when RCS steam generator level in either steam generator reaches a low preset value. This trip function includes audible and visual pretrip

indication. In many PPS-generation plants, this trip also serves as an input to the Emergency-Feedwater Actuation System (EFAS) logic. In some plants, the EFAS SG level trip input is derived from separate wide range SG level transmitters, and the EFAS actuation setpoint is significantly lower than the reactor trip setpoint. In the PPS-generation plants, the low SG water level trip includes two SG-specific trip functions. In the RPS-generation plants, the auctioneered lower of both SGs is provided to a single bistable trip unit.

The proposed DPPS installation shall satisfy the above requirements for a low steam generator level trip and pretrip, and shall replicate existing capabilities.

9. Low Steam Generator Pressure Trip. This trip function trips the reactor when steam generator pressure in either steam generator reaches a low preset value. This trip function may be manually reset by the operator to permit an orderly plant shutdown. This trip includes audible and visual pretrip indication. In PPS-generation plants, this trip also provides a Main Steam Isolation Signal (MSIS).

   In RPS generation plants, there is no capability to manually reset (decrease) the trip setpoint during system depressurization. However, there are provisions for manual bypass of the trip function as SG pressure is decreased.

   In the PPS-generation plants, the low SG water level trip includes two SG-specific trip functions. In the RPS-generation plants, the auctioneered lower of both SGs is usually provided to a single bistable trip unit.

   The proposed DPPS installation shall satisfy the above requirements for a low steam generator pressure trip and pretrip, and shall replicate existing capabilities, including setpoint reset (for PPS-generation plants), and system operating bypass (for RPS-generation plants).

10. High Containment Pressure trip. This trip function trips the reactor when containment pressure reaches a high preset value. This trip function includes audible and visual pretrip indication. In many PPS-generation plants, this trip also serves as an input to the Containment Isolation Actuation Signal (CIAS) and SIAS. In some cases, separate High Containment Pressure trips are employed for these ESFAS functions.

    The proposed DPPS installation shall satisfy the above requirements for a high containment pressure trip and pretrip.

11. Loss of Load (Loss of Turbine) trip. This trip function trips the reactor when the turbine trips above a preset power level. This trip is equipment protective and is not required for plant safety. The trip is automatically bypassed below a certain power level (15% to 55%, depending on the plant), consistent with steam bypass capability. PPS plants employing a reactor power cutback system do not have this trip function. Most RPS-generation plants use the same ex-core linear power safety channel bistable to provide this bypass as well as high-rate of change of power trip bypass and high APD trip bypass.

    The proposed DPPS installation shall satisfy the above requirements for a loss of load trip, including bypass feature. For RPS-generation plants, it shall be possible to separate the bypass functions for the loss of load, high rate of change of power, high APD trip functions.

12. Manual Actuation. A manual reactor trip is provided to permit the operator to manually trip the reactor. Actuation of two adjacent pushbuttons in the control room will cause interruption of the AC power to the CEDM power supplies. Two sets of trip pushbuttons are provided.

    The proposed DPPS installation shall retain this manual trip capability, as described above.

Other RPS Trips: There are several other plant-specific trip functions, such as the low flow trip (based upon SG primary side differential pressure), high seismic trip, (based upon seismic horizontal and vertical accelerometer contact inputs to the PPS) and low RCP Speed trip (for some RPS plants only) not specifically addressed in the Functional Description document. These plant-specific trips shall have their functionality replicated in the DPPS design.

Other RPS Trip Bypasses: In some cases, operating bypasses of installed trips have been made on a plant-specific basis that are not reflected in the Functional Description document. These include, for example, a low RCS temperature-dependent bypass permissive of the steam generator water level trips, and a low power bypass of the low flow trip. These plant-specific bypasses shall have their functionality replicated in any DPPS installation.

A3.1.1.3 Engineered Safety Features Actuation System Functional Requirements (Reference 1, Section 2.3)

- "The instrumentation and controls associated with the ESFAS shall consist of measurement channels, logic, and those circuits associated with the generation of each actuation signal.

"The measurement channels consist of sensors, signal conditioning equipment and trip bistables. The sensors monitor selected plant parameters and provide signals to the bistable trip devices. Trip signals are provided by the trip bistables if the monitored selected plant parameter reach (sic) predetermined setpoints. Two-out-of-four coincidence of like initiating trip signals from four independent measurement channels is required to generate actuation signals to the actuation devices associated with each individual actuated component in the ESFAS. Each actuation system logic, including test features, is similar to the logic for the reactor protective system.

"There is one actuation system for each of the ESF systems; each actuation system is identical except that specific inputs (and bypasses where provided) vary from system to system and the actuated devices are different..."

The proposed DPPS installation will satisfy all of the preceding requirements. Measurement channels are unaffected by the DPPS upgrade, as existing inputs will be used. The use of bistables feeding two-out-of-four coincidence logic remains, though existing hardware performing these functions will be replaced with digital bistable processors and local coincidence logic processors performing the same functions described above. The existing subgroup relays providing contact inputs to the various ESF component control circuits will most likely be replaced with new equivalent relays, though this is not a necessary requirement of the DPPS upgrade.

[ ]

- The ESFAS Provides trips for the following conditions:

  1. Safety Injection Actuation Signal (SIAS). This ESFAS function is typically initiated by two-out-of-four low pressurizer pressure or two-out-of-four high containment pressure signals. In the PPS plants the pressurizer pressure trip signal may be manually reset by the operator to permit an orderly plant shutdown. A manual bypass may be initiated below a predetermined pressurizer pressure trip function includes audible and visual pretrip indication.

     Parameters providing a SIAS differ somewhat from plant to plant. However, pressurizer pressure is common to all. In the RPS-generation plants there is no low pressurizer pressure reset capability. However, a manual SIAS block (bypass) is provided below a permissive pressurizer pressure setpoint to enable depressurization without initiating the SIAS function.

The proposed DPPS installation shall satisfy the above requirements for a SIAS actuation, including bypass or reset feature, modified as necessary to meet plant-specific requirements.

[ ]

2. Recirculation Actuation Signal (RAS). This ESFAS function is typically initiated by two-out-of-four low refueling water tank level signals. Unlike other ESFAS functions, some PPS plants do not include provisions for manual actuation of the RAS on the main control board, due to concern about premature actuation of this function.

   The proposed DPPS installation shall satisfy the above requirements for a RAS actuation, modified as necessary to meet plant-specific requirements. Implementation considerations for different plant generations are as described under the SIAS discussion.

3. Containment Isolation Actuation Signal (CIAS). This ESFAS function is typically initiated by two-out-of-four high containment pressure signals.

   In some plants, low pressurizer pressure or high containment radiation is also a CIAS initiator.

   The proposed DPPS installation shall satisfy the above requirements for a CIAS actuation, modified as necessary to meet plant-specific requirements.
   Implementation considerations for different plant generations are as described under the SIAS discussion.

4. Containment Cooling Actuation System (CCAS). Some PPS-generation plants employ a CCAS function. For other plants, containment cooling actuation is a subsidiary SIAS function. This function has the same inputs as the automatic SIAS (two out of four low pressurizer pressure or two-out-of-four high containment pressure), though it is provided with a separate manual trip capability from that provided for SIAS. For plants equipped with a CCAS function, pressurizer pressure bypass and setpoint reset use the same pushbuttons and switches provided for SIAS.

   The proposed DPPS installation shall satisfy the above requirements for a CCAS actuation for those plants with this feature.

5. Containment Spray Actuation System (CSAS). This function is initiated on a two out-of-four high-high containment pressure AND a simultaneous two-out-of-four SIAS.

Inputs to CSAS differ somewhat between plants. Because of the potential cleanup problem which would result from an inadvertent CSAS, most plants employ some interlocking feature requiring some aspects of an initiating signal, such as SIAS, in addition to High-High containment pressure. In RPS-generation plants, this interlocking may not be an explicit requirement for SIAS, but a functional mechanical interlock, such as having the SIAS start the containment spray pump, but requiring a CSAS on High-High containment pressure to open the spray header isolation valve.

The proposed DPPS installation shall satisfy the above requirements for a CSAS actuation, modified as necessary to meet plant-specific requirements.

6. Main Steam Isolation Signal (MSIS). The MSIS is actuated by two-out-of-four low steam generator pressure signals from each steam generator. The steam generator pressure signal may be manually reset by the operator to permit an orderly plant shutdown.

   Some plants employ additional inputs, such as high containment pressure or high containment radiation for this function. The ability to manually reset this setpoint downwards is restricted to the PPS generation of plants. In the RPS-generation, a manual block (bypass) is permitted when steam generator pressure is below a permissive setpoint.

   The proposed DPPS installation shall satisfy the above requirements for a MSIS actuation, modified as necessary to meet plant-specific requirements.

7. Emergency Feedwater Actuation Signal (EFAS). The EFAS initiates auxiliary feedwater on low water level to the intact steam generator (s) following a steam line break or loss of feedwater accident. It is initiated on a two out of four logic basis to a steam generator if that steam generator meets the conditions for either of the following:

   A. The steam generator's water level trip exists without the low steam generator pressure trip present.
   B. The steam generator's water level trip exists and this steam generator's pressure is greater than the pressure in the other by a predetermined differential pressure.

   EFAS-1 Logic pertains to SG 1, and EFAS 2 logic pertains to SG 2.

EFAS logic differs somewhat between plants. The above described "feed only good generator" (FOGG) logic is used only at the 3410 Mwt group of plants (ANO-2, SONGS 2 and 3, WSES 3). PVNGS uses a variation without the Low Pressurizer Pressure input. RPS-generation plants are more variable in EFAS design. In many cases, there is no FOGG logic, and low SG level is the only input. In these RPS plants, low SG level in either SG may feed both SGs.

The proposed DPPS installation shall satisfy the above requirements for a MSIS actuation, modified as necessary to meet plant-specific requirements.

8. Manual Actuation.

   Each of the ESFAS signals may be initiated from the control room by switches with the exception of RAS.

   There are plant-specific cases where RAS may be initiated from the control board.

   The proposed DPPS implementation shall retain the existing manual actuation capability.

A3.1.1.4 Remote Control Module Functions

Each DPPS channel shall communicate with a DPPS Remote Control Module (RCM) mounted in the Control Room. Plants have the option of retaining their existing RCM, implemented in hardware, or replacing this device with a standard Common-Q flat panel display-based RCM. For the purposes of this appendix, the flat panel-based RCM replacement is considered the standard design. The following discussion therefore applies to the flat-panel implementation.

[ ]

A3.1.1.5 Maintenance and Test Panel (MTP) Functions:

[ ]

A3.1.1.6 Interface and Test Processor (ITP) functions:

[ ]

A3.1.1.7 DPPS Channel Inputs:

[ ]

A3.1.1.7.1 Analog Inputs

[ ]

A3.1.1.7.4 Remote Shutdown Panel Contact Inputs:

[ ]

A3.1.1.8 DPPS Channel Outputs:

[ ]

A3.1.1.8.1 RPS Initiation Contact Outputs

[ ]

A3.1.1.8.2 DESFAS Initiation Contact Outputs

[ ]

A3.1.1.8.3 Other DPPS Contact Outputs:

Each DPPS channel and DESFAS train provides several contact outputs for a variety of purposes. These include:

1. Annunciation:

   - Trip/Pretrip Annunciation:
     Each trip or pretrip will have a DPPS-cabinet mounted annunciator output contact

   - Trip Channel Bypass:
     Trip Channel Bypass of any parameter in a given channel will be annunciated.

- Operating Bypass
  Each Operating Bypass (i. e. Low Pressurizer Pressure) will be annunciated. In the case of the High Log Power Bypass, annunciation will exist if the bypass permissive is available but the channel has not yet been bypassed. This latter feature prevents annunciation during normal (at power) plant operation, and is consistent with the present design.

- Trouble:
  The PPS trouble annunciator shall be expanded in scope from its present implementation to include a number of additional diagnostic-related conditions. The initiator for this annunciation will be indicated on the RCM and MTP. Detailed diagnostics on system failures are available on the MTP. The DESFAS shall be equipped with similar annunciation. Specific DESFAS failures may be diagnosed on the DESFAS MTP, as in the DPPS.

- Power Supply Trouble:
  Separate DPPS and DESFAS annunciation shall be retained for power supply trouble conditions.

- [ ]

2. CEA Withdrawal Prohibit

   There is one CWP contact output to the CEDMCS in the DPPS cabinet. The CWP contact is opened if there is a pretrip condition indicated in at least two of the four DPPS channels in High Pressurizer Pressure, or if the CPC-CWP input is received from two out of four channels. This is a non-safety related output not credited in the accident analysis. RPS plants have similar though slightly different initiators for this function .

3. CPC Trip Channel Bypass

   A contact output to the Core Protection Calculator is provided in each DPPS channel. This output is a permissive to enable CPC testing only if both the DNBR-Low and LPD-High trips are bypassed in that channel.

   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. However, in the present PPS/CPC design, a CPC Test

panel in the PPS performs the trip channel bypass interlock function and enables CPC or CEAC testing via a CPC/CEAC select switch if both the DNBR and LPD trips are trip channel bypassed. This Test Enable signal is transmitted from the PPS to the CPC or CEAC as a binary (contact) input.

4. Contact outputs to remote shutdown panel

- Low Pressurizer Pressure pretrip status to remote shutdown panel

  This output provides indication that the low pressurizer pressure trip should be manually reset during depressurization from the remote shutdown panel.

- Low SG pressure pretrip status to remote shutdown panel

  This output provides indication that the low SG pressure trip should be manually reset during depressurization from the remote shutdown panel

- Low Pressurizer pressure Bypass permissive and bypass status (bypass/no bypass)

  These contact outputs provide indication to the operator that RCS pressure is below the permissive setpoint, and provide bypass status

- Sequence of Events

  Each trip will have a means of indicating the trip sequence of events. In this appendix, the SOE will take the form of a dedicated contact output per trip, replicating the existing configuration.

A3.1.1.8.4 Indicator Analog Outputs

The following analog outputs (0 to 10 Vdc) are provided from the DPPS channel:

- Low Pressurizer Pressure Trip Setpoint
- Low Steam Generator Pressure 1 Trip Setpoint
- Low Steam Generator Pressure 2 Trip setpoint.

A3.1.1.9 Failure Modes:

The DPPS/DESFAS 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).

[ ]

A3.1.1.10 Human Machine Interface

[ ]

A3.1.1.11 Functional Diversity

[ ]

A3.1.1.11.1 DPPS Bistable Processor and Analog Input Signal Diversity

[ ]

TABLE A3.1-1: ANALOG INPUT SIGNAL ASSIGNMENTS

[ ]

A3.1.1.11.2 CPCs Functional Diversity

[ ]

A3.1.1.11.3 Bistable Trip Algorithm Software Diversity

[ ]

A3.1.1.11.4 LCL Algorithm Software Diversity

[ ]

A3.1.1.11.5 PPS Process Instrumentation Functional Diversity

[ ]

A3.1.2 PPS Functional Requirements Detail:

[ ]

A3.1.2.1 DPPS Design Basis:

[ ]

A3.1.2.1.1 Criteria and Requirements:

[ ]

A3.1.2.1.2 System Inputs:

[ ]

A3.1.2.1.3 Pretrip Indication:

[ ]

A3.1.2.1.4 Inadvertent Actuation

[ ]

A3.1.2.1.5 Measurement Channels

[ ]

A3.1.2.1.6 Channel independence and isolation:

[ ]

A3.1.2.1.7 Coincidence Logic

[ ]

A3.1.2.1.8 Trip Channel Bypass

[ ]

A3.1.2.1.9 Trip Paths

[ ]

A3.1.2.1.10 Safety-Non Safety Isolation

[ ]

A3.1.2.1.11 Manual Bypass Capability

[ ]

A3.1.2.1.12. Bypass Removal

[ ]

A3.1.2.1.13. Ground Isolation

[ ]

A3.1.2.1.14. Manual Reset after Initiation

[ ]

A3.1.2.1.15. Operator Display

[ ]

A3.1.2.1.16. Annunciation

[ ]

A3.1.2.2 System Requirements:

A3.1.2.2.1 Inputs:

[ ]

A3.1.2.2.2 DPPS Channel Outputs:

[ ]

A3.1.2.2.3 DESFAS Channel Outputs

[ ]

A3.2 SYSTEM DESCRIPTION

The DPPS is comprised of four redundant channels (A, B, C, and D as depicted on Figure A3.2-1 "DPPS Basic Block Diagram"), that perform the necessary bistable, coincidence, initiation logic and associated maintenance/test functions. The system includes four redundant Remote Control Modules located on the Main Control Room panels, one for each channel. Four redundant channels are provided to satisfy single failure criteria and improve plant availability.

A3.2.1 Overview

The Bistable Processors in each DPPS channel receives channelized process sensor analog inputs, discrete & analog signals from the Ex-Core detector system and discrete signals from the CPC to perform the Bistable Trip functions. Process input configuration is unchanged from the existing PPS design.

[ ]

FIGURE A3.2-1: PPS BASIC BLOCK DIAGRAM

[ ]

A3.2.2 Design Implementation

[ ]

FIGURE A3.2-2A: DPPS CHANNEL A BLOCK DIAGRAM

[ ]

FIGURE A3.2-2B: DPPS CHANNEL B BLOCK DIAGRAM

[ ]

FIGURE A3.2-2C: DPPS CHANNEL C BLOCK DIAGRAM

[ ]

FIGURE A3.2-2D: DPPS CHANNEL D BLOCK DIAGRAM

[ ]

FIGURE A3.2-3: DPPS/DESFAS TRAIN A BLOCK DIAGRAM

[ ]

A3.3 HARDWARE DESCRIPTION

The DPPS is composed of a four bay cabinet assembly which house the PLC equipment, Excore Neutron Flux Monitoring System (ENFMS) electronics chassis, maintenance and test equipment, internal power supplies, RPS and ESFAS initiation circuits, initiation relays, fiber optic isolation devices and other miscellaneous equipment.

The system includes four channelized Remote Control Modules (RCM) to be located on the plant Main Control Board.

The following sections provide an overview description of the DPPS.

A3.3.1 Mechanical

The four bay cabinet is consistent with existing PPS implementations. For new installations, there is also the option of using four single bay cabinets located either in four separate rooms or located together in one room, adjacent to each other. For the purposes of this appendix, it is assumed that a single four bay design will be utilized, consistent with existing RPS and PPS installations. See Figure A3.3-1 for typical cabinet layout.

Each cabinet bay is approximately 36 inches wide, 90 inches high and 54 inches deep. The cabinet design includes forced air cooling and is designed to be welded to floor embedments. The cabinet has front and rear access doors. A viewing window on the front door provides visibility of the controls and status information for ENFMS electronics and MTP display.

FIGURE A3.3-1: TYPICAL DIGITAL PLANT PROTECTION SYSTEM CABINET

[ ]

A3.3.2 Electrical

[ ]

A3.3.3 PLC Configuration

[ ]

A3.3.3.1. Bistable Processor:

[ ]

FIGURE A3.3-2: DPPS CHANNEL A CONFIGURATION BLOCK

[ ]

FIGURE A3.3-3: TYPICAL RPS INITIATION LOGIC

[ ]

A3.3.3.2. Local Coincidence Logic Processor:

[ ]

A3.3.3.3. PLC Extension Chassis

[ ]

A3.3.3.4. Cross Channel Communications High Speed Links

[ ]

A3.3.3.5. Maintenance and Test Panel

[ ]

A3.3.3.6. Interface and Test Processor

[ ]

FIGURE A3.3-4: INTERFACE AND TEST PROCESSOR BLOCK DIAGRAM

[ ]

A3.3.3.7. Communications Links and Networks

[ ]

FIGURE A3.3-5: INTERFACE BETWEEN DESFAS TRAIN ITPSAND DPPS ITPS

[ ]

FIGURE A3.3-6: DESFAS CONFIGURATION BLOCK DIAGRAM

[ ]

A3.3.4PLC Self -Test Diagnostics

A3.3.4.1. PLC I/O and CPU Modules:

[ ]

A3.3.4.2. Advant Fieldbus 100 Communication Modules:

[ ]

A3.3.5 AC 160 Description:

A3.3.5.1 Advant 160 General Description

[ ]

A3.3.5.2 Controller Subrack

A3.3.5.2.1 DPPS Channel

[ ]

A3.3.5.2.2 DESFAS Train

[ ]

A3.3.5.3 Input/Output Subrack

[ ]

A3.3.6 Power Supplies

A3.3.6.1 DPPS Power Supply

[ ]

A3.3.6.2 DESFAS Power Supply

[ ]

A3.4 SOFTWARE DESCRIPTION

[ ]

A3.4.1 PLC OPERATING SYSTEM SOFTWARE

[ ]

A3.4.2 APPLICATION PROGRAMMING TOOL SOFTWARE

[ ]

A3.4.3 BISTABLE PROCESSOR

[ ]

FIGURE A3.4-1: DPPS BISTABLE LOGIC BLOCK DIAGRAM

[ ]

FIGURE A3.4-2: FALLING TRIP BISTABLE LOGIC

[ ]

FIGURE A3.4-3: MANUALLY RESET VARIABLE SETPOINT

[ ]

FIGURE A3.4-4: RATE LIMITED VARIABLE SETPOINT

[ ]

FIGURE A3.4-5: OPERATING BYPASS LOGIC

[ ]

FIGURE A3.4-6: DISCRETE BISTABLE LOGIC

[ ]

FIGURE A3.4-7: TESTING BLOCK DIAGRAM

[ ]

A3.4.4 LCL PROCESSOR

[ ]

A3.4.5 MTP Processor

[ ]

A3.4.6 ITP Processor.

[ ]

A3.4.6.1 DPPS ITP Tests

[ ]

A3.4.6.2 DESFAS ITP Tests

[ ]

A3.4.6.3 ITP Modes

[ ]

FIGURE A3.4-8: ITP LOGIC BLOCK DIAGRAM

[ ]

3.4.7 HMI Software

[ ]

A3.5 SYSTEM INTERFACES

A3.5.1 DPPS System Interfaces

[ ]

A3.5.2 DPPS Cabinet Interface

[ ]

A3.6 FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

[ ]

A3.6.1 Assumptions

[ ]

A3.6.2 Definition of Terminology Used in the Analysis

[ ]

A3.6.3 Conclusions

[ ]

FIGURE A3.6-1: DPPS FMEA BLOCK DIAGRAM

[ ]

FIGURE A3.6-2: DESFAS FMEA BLOCK DIAGRAM

[ ]

TABLE A3.6-1: FAILURE MODES AND EFFECTS ANALYSIS

[ ]

A3.7 ALTERNATE CONFIGURATIONS

[ ]

FIGURE A3.7-1: COMMON-Q DPPS CONFIGURATION

[ ]

FIGURE A3.7-2: SEPARATE RPS/ESFAS CONFIGURATION

[ ]

FIGURE A3.7-3: DPPS WITH SINGLE PROCESSOR RACK/TRAIN

[ ]

FIGURE A3.7-4: DPPS WITH MULTIPLE ESFAS LCLS

[ ]

FIGURE A3.7-5: DPPS WITH DIVERSE BISTABLES

[ ]

A3.8 REFERENCES

1. "Functional Description for Plant Protection System", 00000-ICE-3201-Rev. 02, issued 03/02/76.
1. NUREG/CR6303-1994, "Methods for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems"
3. NRC Branch Technical Position BTSP HICB-19, "Guidance on Defense in Depth and Diversity in Digital Computer-based I&C Systems "
4. System 80+ final Safety Evaluation Report
5. NUREG 1432, "Standard Technical Specifications Combustion Engineering Plants", Revision 1, April, 1995.
6. "Software Program Manual for Common Q Systems", CE-CES-195-NP-A, Revision 2, May 2003.
7. Common Qualified Platform Topical Report, CENPD-396-P-A, Revision 2, May 2003.

A3.9 PROPOSED TECHNICAL SPECIFICATION CHANGES

The attached Technical Specification corrections are to be located in Standard Technical Specifications for Combustion Engineering Plants, NUREG 1432, Rev. 1. LCOs 3.3.1 "RPS Instrumentation-Operating (Digital)"; 3.3.2 "RPS Instrumentation-Shutdown"(digital)"; 3.3.4 "RPS Logic and Trip Initiation (digital); ESFAS Instrumentation (digital); and LC0 3.3.6, "ESFAS Logic and Manual trip" are affected.

The "digital" rather than analog versions of the NUREG LCOs were chosen for illustration, since the digital TS are much closer in format to the DPPS design than the existing analog versions.

The proposed changes are considered the minimum required to reflect the migration to a DPPS-based design for both the RPS and ESFAS functions. These TS reflect such major changes as the substitution of four LCL processors for the six existing coincidence matrix channels. Additional action statements were incorporated for cabinet high temperature alarm and excessive number of processor failures in a given period (12 hours). These are analogous to existing requirements imposed on the present CPC channels, which are also of a digital (computer-based) design.

[ ]

ATTACHMENT

To

Common Qualified Platform
Digital Plant Protection System

CENPD-396-NP-A
Appendix 3, Revision 2
May 2003

NUREG 1432, Revision 1
Standard Technical Specification
Markup Pages

(Pages 3.3-1 through 3.3-14, 3.3-19 through 3.3-31;
LCOS 3.3.1, 3.3.2, 3.3.4, 3.3.5, AND 3.3.6 (DIGITAL))

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