



Entergy Operations, Inc.
1340 Echelon Parkway
Jackson, MS 39213
Tel 601-368-5138

Ron Gaston
Director, Nuclear Licensing

10 CFR 50.90

W3F1-2020-0040

June 16, 2020

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Transmittal of Information for Fifth Partially Closed Presubmittal Meeting
with Entergy Operations, Inc. to Discuss a Planned License Amendment
Request for Digital Instrumentation and Control Modification at Waterford
Steam Electric Station, Unit 3 (EPID L-2019-LRM-0079)

Waterford Steam Electric Station, Unit 3
NRC Docket No. 50-382
Renewed Facility Operating License No. NPF-38

A partially closed meeting between Entergy Operations, Inc. (Entergy) and the U.S. Nuclear Regulatory Commission (NRC) staff is tentatively scheduled for the week of June 29, 2020. The purpose of this meeting is to discuss a planned license amendment request (LAR) for a digital instrumentation and controls (DI&C) modification at Waterford Steam Electric Station, Unit 3 (Waterford). The DI&C modification at Waterford will replace the existing instrumentation of the Core Protection Calculator (CPC) system and Control Element Assembly Calculator (CEAC) system with a digital system based on an NRC-approved licensing topical report. This will be the fifth partially closed presubmittal meeting between Entergy and the NRC on this topic.

Entergy will develop and submit this LAR in accordance with the guidance in NRC DI&C Interim Staff Guidance (ISG)-06, "Licensing Process," Revision 2 describing the Alternate Review Process (ARP). During the fifth presubmittal meeting, Entergy will discuss a draft version of the LAR with the NRC.

During a previous public meeting concerning this LAR, which was conducted on January 16, 2020, Entergy proposed to submit a draft version of the LAR in early June 2020 for initial review by the NRC, followed by a final presubmittal meeting.

In a subsequent public meeting (i.e., on March 19, 2020), the NRC indicated that conducting a brief initial review for this particular draft LAR would be acceptable due to the first-of-a-kind nature of the ARP. This is described in the NRC's summary of the March 2020 meeting, dated April 23, 2020 (ADAMS Accession No. ML20113E836).

The Enclosure to this letter and the following associated Attachments provide the draft LAR described above.

- Attachment 1 provides a draft version of the existing TS pages, marked-up to show the proposed changes.
- Attachment 2 provides draft revised (clean) TS pages.
- Attachment 3 provides, for information only, draft marked-up versions of existing TS Bases pages to show the proposed changes.
- Attachment 4 provides WCAP-18484-P, "Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System." This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.
- Attachment 5 provides the Westinghouse Affidavit in support of WCAP-18484-P. The Affidavit sets forth the basis on which the information may be withheld from public disclosure by the NRC and addresses, with specificity, the considerations listed in paragraph (b)(4) of Section 2.390 of the NRC's regulations.
- Attachment 6 provides a non-proprietary, redacted version of WCAP-18484-P.
- Attachment 7 provides the System Requirements Specification for the Common Q Core Protection Calculator System (00000-ICE-30158). This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.
- Attachment 8 provides the System Requirements Specification for the Waterford Core Protection Calculator System (WNA-DS-04517-CWTR3). This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.
- Attachment 9 provides the Failure Modes and Effects Analysis for the Common Q Core Protection Calculator System (00000-ICE-3338). This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.
- Attachment 10 provides the Failure Modes and Effects Analysis for the Waterford Core Protection Calculator System (WNA-AR-00909-CWTR3). This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.

- Attachment 11 provides the Core Protection Calculator System Primary Digital Components Qualification Summary Report for Waterford Unit 3 (EQ-QR-400-CWTR3). This attachment contains information proprietary to Westinghouse, which is supported by an Affidavit signed by Westinghouse, the owner of the information.
- Attachment 12 provides the Westinghouse Affidavit in support of Attachments 7, 8, 9, 10, and 11. The Affidavit sets forth the basis on which the information may be withheld from public disclosure by the NRC and addresses, with specificity, the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations.
- Attachment 13 provides a draft version of the Human Factors Engineering Analysis.
- Attachment 14 provides a draft version of the Vendor Oversight Plan (VOP) Summary.
- Attachment 15 provides a draft list of Regulatory Commitments, as discussed in DI&C ISG-06, Revision 2, subsection C.2.2.3.

As Attachments 4, 7, 8, 9, 10, and 11 contain information proprietary to Westinghouse, they are supported by Affidavits signed by Westinghouse (i.e., Attachments 5 and 12), the owner of the information. The Affidavits set forth the basis on which the information may be withheld from public disclosure by the NRC and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the NRC's regulations.

Accordingly, it is respectfully requested that the information which is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations.

Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavits should reference CAW-20-5031 and CAW-20-5040 and should be addressed to Camille T. Zozula, Manager, Infrastructure & Facilities Licensing, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

This letter contains no new regulatory commitments.

If there are any questions or if additional information is needed, please contact Paul Wood, Waterford Regulatory Assurance Manager, at (504) 464-3786.

Executed on the 16th day of June 2020.

Sincerely,



Ron Gaston

RWG/jls

Enclosure: Evaluation of the Proposed Change (DRAFT)

Attachments to Enclosure:

1. DRAFT Technical Specification Page Markups
2. DRAFT Clean Technical Specification Pages
3. DRAFT Technical Specification Bases Page Markups (Provided for Information Only)
4. WCAP-18484-P, "Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System, Proprietary
5. Westinghouse Letter CAW-20-5031, Affidavit, Proprietary Information Notice, and Copyright in support of WCAP-18484-P, (Attachment 4)
6. WCAP-18484-NP, "Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System," Non-Proprietary
7. Westinghouse Specification 00000-ICE-30158, Revision 14, "System Requirements Specification for the Common Q Core Protection Calculator System," Proprietary
8. Westinghouse Specification WNA-DS-04517-CWTR3, Revision 2, "Waterford 3 System Requirements Specification for the Core Protection Calculator System," Proprietary
9. Westinghouse Specification 00000-ICE-3338, Revision 0, "Failure Modes and Effects Analysis for the Common Q Core Protection Calculator System," Proprietary
10. Westinghouse Specification WNA-AR-00909-CWTR3, Revision 1, "Waterford 3 Failure Modes and Effects Analysis for the Core Protection Calculator System," Proprietary
11. Westinghouse Specification EQ-QR-400-CWTR3, Revision 0, "Core Protection Calculator System Primary Digital Components Qualification Summary Report for Waterford Unit 3," Proprietary
12. Westinghouse Letter CAW-20-5040, Affidavit, Proprietary Information Notice, and Copyright in support of 00000-ICE-30158, WNA-DS-04517-CWTR3 00000-ICE-3338, WNA-AR-00909-CWTR3, and EQ-QR-400-CWTR3, (Attachments 7, 8, 9, 10, and 11)
13. DRAFT Human Factors Engineering Analysis
14. DRAFT Vendor Oversight Plan (VOP) Summary
15. DRAFT List of Regulatory Commitments

cc: NRC Region IV Regional Administrator
NRC Senior Resident Inspector – Waterford Steam Electric Station, Unit 3
Designated State Official, Louisiana
NRC Project Manager – Waterford Steam Electric Station, Unit 3

Enclosure

W3F1-2020-0040

DRAFT
Evaluation of the Proposed Change

1. SUMMARY DESCRIPTION

2. DETAILED DESCRIPTION

1. System Design and Operation
2. Current TS Requirements
3. Reason for the Proposed TS Changes
4. Description of the Proposed TS Changes

3. DETAILED DESCRIPTION

1. DI&C-ISG-06 Alternate Review Process (ARP) LAR Contents
2. Licensing Technical Report (LTR)
3. Factory Acceptance Test/Site Acceptance Test (FAT/SAT) Description
4. Waterford System Engineer and Operations Actions Supporting TS SR Reduction

4. REGULATORY EVALUATION

1. Applicable Regulatory Requirements/Criteria
2. Precedent
3. No Significant Hazards Consideration Analysis
4. Conclusions

5. ENVIRONMENTAL CONSIDERATION

6. REFERENCES

7. ATTACHMENTS

1. SUMMARY DESCRIPTION

In accordance with 10 CFR 50.90, Entergy Operations, Inc. (Entergy) requests an amendment to Appendix A, "Technical Specifications" (TS) of Renewed Facility Operating License No. NPF-38 for Waterford Steam Electric Station, Unit 3 (Waterford). The proposed change will revise the Waterford TS in order to implement a planned digital modification at Waterford. The following TS sections are affected by this change:

- TS 2.2.1 Reactor Trip Setpoints
- TS 3.1.3 CEA Position
- TS 3.2.4 DNBR Margin
- TS 3.3.1 Reactor Protective Instrumentation
- TS 3.10.2 Moderator Temperature Coefficient, Group Height, Insertion, and Power Distribution Limits
- TS 6.8.1 Procedures and Programs
- TS 6.9 Reporting Requirements

The modification will replace the existing digital minicomputers of the Core Protection Calculator (CPC) system and Control Element Assembly Calculator (CEAC) system with a more reliable, digital system based on the Westinghouse Electric Company (Westinghouse) Common Qualified (Common Q) Platform. The Core Protection Calculator System (CPCS) is the combined CPC and CEAC. The Common Q platform has an NRC-approved topical report (Reference 11).

Waterford is the only nuclear site utilizing the original version of the CPCS. An Interdata 7/16 computer system is used in four channels of the CPCS. There are obsolescence concerns with the equipment due to limited spare parts availability. In addition, there are reliability concerns due to the identification of single point vulnerabilities in the system.

In Reference 1, Entergy submitted a letter-of-intent (LOI) to the U.S. Nuclear Regulatory Commission (NRC) that described a planned DI&IC license amendment request (LAR) for the CPCS modification at Waterford, indicating that the LAR would be developed and submitted in accordance with the Alternate Review Process (ARP) guidance in NRC DI&C Interim Staff Guidance (ISG)-06, "Licensing Process," Revision 2 (Reference 2). The LAR format and contents are consistent with the DI&C-ISG-06 guidance for the ARP.

Entergy plans to implement the digital upgrade modification to the CPC and CEAC systems at Waterford during the 24th refueling outage (RF24), which is scheduled for Spring 2022. In order to initiate and complete equipment fabrication and factory acceptance testing prior to the start of the refueling outage, Entergy requests approval of the proposed license amendment by August xx, 2021. The proposed changes will be implemented prior to start-up from RF24.

2. DETAILED DESCRIPTION

1. System Design and Operation

The Waterford Plant Protection System (PPS) is comprised of an Engineered Safety Features Actuation System (ESFAS) and a Reactor Protection System (RPS). The Core Protection Calculator System (CPCS) is part of the RPS.

The CPC/CEAC system issues two reactor trip signals to the RPS to protect the fuel design limits. These four independent Core Protection Calculators (CPCs), one in each protection channel, calculates departure from nucleate boiling ratio (DNBR) and local power density (LPD). The reactor trips provided by the CPCs are inputs to the RPS Coincidence and Initiation Logic. The CPC trips have a 2 out of 4 logic.

The calculations are performed in each CPC, utilizing the following input signals:

- Core inlet and outlet temperature,
- Pressurizer pressure,
- Reactor coolant pump speed,
- Excore nuclear instrumentation flux power (each subchannel from the safety channel),
- Selected (target) CEA position, and
- CEA subgroup deviation from the CEA calculators.

The DNBR and LPD calculation results are compared to trip setpoints for initiation of a low DNBR trip and a high LPD trip. These CPCS trip outputs become digital trip inputs to the corresponding RPS channel. The four channel RPS performs the 2 out of 4 coincidence logic on various reactor trip functions that include the CPC Low DNBR and High LPD. The CPCS is designed to initiate automatic protective action to assure that the specified acceptable fuel design limits (SAFDL) on DNBR and LPD are not exceeded during Anticipated Operational Occurrences (AOOs).

The High LPD Trip is to prevent the linear heat rate (kW/ft) in the limiting fuel pin in the core from exceeding the value corresponding to the centerline fuel melting temperature. This is to prevent exceeding the safety limit of peak fuel centerline temperature in the event of defined anticipated operational occurrences.

DNBR is the ratio of Critical Heat Flux to Actual Heat Flux. Critical heat flux (CHF) is that value of heat flux at which Departure from Nucleate Boiling (DNB) occurs. The Low DNBR trip is to prevent the DNBR in the limiting coolant channel in the core from exceeding the fuel design limit for the fuel cladding in the event of defined anticipated operational occurrences. In addition, this trip will provide a reactor trip to assist the Engineered Safety Features System (ESFS) in limiting the consequences of the steam generator tube rupture, steam line break and reactor coolant pump shaft seizure accidents.

CPC DNBR and LPD pre-trip alarms are initiated prior to the trip value to provide audible and visible indication of approach to a trip condition. These pre-trip functions have no direct safety function.

The CPC will also initiate DNBR and LPD trip outputs (i.e., Auxiliary trips) under the following conditions:

- CPC operating space limits are exceeded for the hot pin axial shape index, integrated one pin radial peak, maximum and minimum cold leg temperatures, and primary pressure (CPC Operating Space Trips).
- Opposing cold leg temperature difference exceeds its setpoint, which varies with power level (Asymmetrical Steam Generator Transient (ASGT) Trip).
- Reactor power exceeds the variable overpower trip setpoint. The trip setpoint is larger than the steady state reactor power by a constant offset. However, it is limited in how fast it can follow changes in reactor power. This provides protection from sudden power increases (Variable Overpower Trip)
- The maximum hot leg temperature approaches the coolant saturation temperature (Thot at saturation).
- The CPC system is not set in the normal operating configuration (CPC Failure).
- Reactor coolant pump shaft speed drops below its setpoint value for multiple pumps (Less than two RCPs running).

The CPCS/CEAC design basis functions are not changing as a result of this CPCS modification. All the design basis events in Chapter 15 and the reliance on the CPCS low DNBR and high LPD trips are unchanged.

The PPS/RPS performs a two out of four coincidence of like trip signals to generate a reactor trip signal. The use of four channels allows bypassing of one channel for maintenance while maintaining a two out of three channel trip.

The scope of this modification is the replacement of the CPCS including sensor terminations, replacement calculators (CPC and CEAC), alarm output termination, analog output terminations (Main Control Room (MCR) Indication), and output terminations to the PPS/RPS.

Excluded from the CPCS modification are:

- Sensors and their cabling to the CPCs
- Reactor Protection System
- CPC system Trip setpoints and outputs.

All functional requirements for DNBR and LPD trip output are unchanged.

2. Current TS Requirements

The following Technical Specifications (TS) sections are affected by this change:

2.2.1	Reactor Trip Setpoints
3/4.1.3.1	CEA Position
3.2.4	DNBR Margin
3/4.3.1	Reactor Protective Instrumentation
3/4.10.2	Moderator Temperature Coefficient, Group Height, Insertion, and Power Distribution Limits
6.8.1	Procedures and Programs
6.9	Reporting Requirements

TS 2.2.1 provides the list of reactor protective instrumentation setpoints in Table 2.2-1. None of the CPC-related setpoints are affected by the proposed changes, as discussed in section 2.4 below.

TS 3.1.3.1 provides the operability and alignment requirements for the Core Element Assemblies (CEAs) groups. Surveillance Requirement 4.1.3.1.1 specifies when the alignment checks are performed depending on CEAC operability status.

TS 3.2.4 provides requirements for monitoring DNBR Margin depending on the status of Core Operating Limits Supervisory System (COLSS) and CEACs.

TS 3.3.1 provides minimum operability requirements for the reactor protective instrumentation which includes CPCs and CEACs.

TS 3.10.2 provides the requirements for a special test exception permitting individual CEACs to be positioned outside of their normal group heights and insertion limits during the performance of select physics tests.

TS 6.8.1 is an administrative TS that governs modifications to CPCS software.

TS 6.9 is an administrative TS that governs reporting requirements.

3. Reason for the Proposed TS Changes

There are three aspects of the CPCS modification that drive the proposed changes:

2 to 8 CEAC Design Change

Many of the changes are due to the configuration change from having two CEACs shared across the four CPC channels to two dedicated CEACs in each of the four CPC channels. Some of the necessary changes are editorial, since currently the term "BOTH CEACs" applies to all CEAC capability and in the new configuration it does not. Having eight total CEACs also greatly reduces the operational impact of individual CEACs being inoperable.

Common Q Design

Due to the Common Q design, CPC features that are currently part of the Waterford TS are no longer applicable. For example, Surveillance Requirement (SR) 4.3.1.5 contains requirements for determining CPC or CEAC operability following three auto restarts. The upgraded CPCs will not have an auto restart function, thereby rendering this SR obsolete and no longer applicable.

Crediting Self-Diagnostics for TS Surveillance Requirement Elimination

The Common Q design also provides additional reliability and operational margin via the self-diagnostics. These self-diagnostics are continually monitoring the health of the hardware and software. Appendix B to the Licensing Technical Report (LTR) (Attachment 4) provides the justification to remove selected SRs.

4. Description of the Proposed TS Changes

Changes are proposed to the following Technical Specifications (TS) as described in the table below. TS markups are provided in Attachment 1.

2.2.1	Reactor Trip Setpoints
3.1.3.1	CEA Position
3.2.4	DNBR Margin
3.3.1	Reactor Protective Instrumentation
3.10.2	Moderator Temperature Coefficient, Group Height, Insertion, and Power Distribution Limits
6.8.1	Procedures and Programs
6.9	Reporting Requirements

TS Section	Proposed Change
TS 2.2.1 Table 2.1	The proposed changes to TS 2.2.1 are confined to Table 2.2-1. The changes are predominantly editorial to conform to the updated CPC-to-CEAC relationship, where two CEACs are provided in each CPC channel. The CPCs are the primary functional unit, possessing two trip functions, LPD-High and DNBR- Low. The culmination of the change is that the CPCs are Functional Unit 9, with the two trips listed. The former functional units 10, 14 and 15 are marked as "DELETED". Since the CEACs provide no direct trip function, they are not listed in the revised Table 2.2-1. However, since CEACs have operability and surveillance requirements they are included in Tables 3.3-1 and 4.3.1. None of the CPC-related setpoints are affected by the proposed changes.
TS 3.1.3.1 SR 4.1.3.1.1	The Surveillance Requirement 4.1.3.1.1 listed in TS 3.1.3.1 contains the only change to this TS. The operability requirements of the CEAs are not impacted.

TS Section	Proposed Change
	<p>The objective of the SR is also unchanged. The proposed change removes the current TS guidance on how often the SR should be performed depending on the operability condition of the CEACs. This guidance is redundant to the proposed TS 3.3.1 Action 6 statement which dictates when CEA position checks are performed depending on CEAC operability status. As described below, Action 6 directly stipulates performance of SR 4.1.3.1.1 on the same 4 hour frequency as is currently required.</p>
TS 3.2.4	<p>TS 3.2.4 is reformatted to resemble the PVNGS TS 3.2.4 wording, by grouping the four methods of monitoring DNBR depending on the status of the Core Operating Limit Supervisory System (COLSS). The PVNGS LCO wording was chosen because it concisely handles the eight CEAC configuration design and functionality impacts. It was previously reviewed and approved by the NRC, which is described in Section 4.2, "Precedent". The actions to take when the DNBR limit is not maintained are unchanged from the present Waterford TS 3.2.4.</p>
<p>TS 3.3.1 Table 3.3-1 including Table Notation</p>	<p>The Functional Unit designations are changed, similarly to Table 2.2-1 to put all the CPC subfunctions under Functional Unit 9, Core Protection Calculators (LPD – High, DNBR – Low and CEACs).</p> <p>The table requirements for the CPC, LPD, and DNBR are identical, and are listed as a single line entry. Notation "(h)" was added under the "Channels to Trip" column.</p> <p>The CEACs are included under Functional Unit 9 because each pair of CEACs directly supports one of the four CPC channels. Also, the "Total No. of Channels", "Channels to Trip", "Minimum Channels OPERABLE", and "Action" values were changed to reflect the eight CEAC configuration:</p> <ul style="list-style-type: none"> • Total No. of Channels – In the new CPC design, each of the four CPC channels houses a dedicated pair of CEACs. Therefore, there are four channels of CEACs, with two CEACs per Channel. Reference to notations "(g)" and "(i)" are also added. • Channels to Trip – CEACs cause trips by transmitting a high penalty factor (PF) to its associated CPC channel. It requires two CPC

TS Section	Proposed Change
	<p>channels to trip on either LPD – High or DNBR – Low to cause a reactor trip. Therefore, two separate channels of CEACs must send sufficiently high penalty Factor (PF) to their CPC to cause a reactor trip.</p> <ul style="list-style-type: none"> Minimum Channels Operable – A channel of CEAC is OPERABLE as long as one of the two CEACs in a CPC channel are OPERABLE. Therefore, requiring three channels as a minimum to be OPERABLE matches the CPC requirements and ensures single failure criteria is maintained or ACTIONS taken. Reference to notations “(g)” and “(i)” are also added. <p>Table 3.3-1, Table Notation, notes (g), (h), and (i) were added. These provide clarifying information concerning CEAC and CPC operability:</p> <ul style="list-style-type: none"> (g) There are two CEACS in each CPC channel. (h) Both Local Power Density – High and DNBR – Low must be OPERABLE for a CPC Channel to be OPERABLE. Both CEACs in an inoperable CPC channel are also inoperable.
<p>TS 3.3.1 Table 3.3-1 Action Statements</p>	<p><u>Action 6</u></p> <p>Action 6 is revised to accommodate the eight CEAC configuration, while maintaining essentially the same actions as the current TS, depending on the impact to CPCS functionality. A primary objective of the proposed changes to Action 6 is to ensure that all CEAC conditions of operability are included. For all of the actions described below, there is the option of declaring the associated CPC channel inoperable, which would invoke Actions 2 or 3, which are unchanged.</p> <p>The current Action 6 only contains two parts (one CEAC inoperable and both CEACs inoperable). In the proposed changes, considering the eight CEAC design, there are multiple combinations of potential CEAC inoperability, with varying impacts to CPCS functionality. To utilize the operational flexibility and redundancy offered by eight CEACs, while maintaining an understandable presentation of the Actions, the current two part Action 6</p>

TS Section	Proposed Change
	<p>is being revised to describe three CEAC operability conditions. The addition of a NOTE indicates that separate entries may be made for each CPC.</p> <p>Action “a” is new and reflects the robustness of the CPCS design such that up to two CPC channels maintain full capability with only a single CEAC OPERABLE in each. The action consists of ensuring the affected CPC channels does not use the input from the failed CEAC by manually setting the appropriate addressable constant. From a safety function perspective, the CPCS is fully capable of meeting all functional requirements. This is because the CEAs in each subgroup are monitored by redundant reed switch position transmitters (RSPT 1 and RSPT 2). CEAC 1 in each CPCS channel is identical and therefore redundant in four CPCS channels. It monitors all the CEA RSPT 1 signals to compute a penalty factor for the CPC in case there is a CEA deviation in a subgroup.</p> <p>Similarly, CEAC 2 in each CPCS channel is identical and therefore redundant in four CPCS channels. It monitors all CEA RSPT 2 signals to compute a penalty factor for the CPC in case there is a CEA deviation in a subgroup. If CEAC 1 or CEAC 2 is inoperable in a CPCS channel, the operable CEAC can still compute a CEA deviation penalty factor for the CPC using either RSPT 1 or RSPT 2 signals depending on the CEAC that is still operable in the channel.</p> <p>If two CPCS channels have 1 CEAC inoperable, the worst case scenario is that the same CEAC is inoperable in both CPCS channels. For example, if CEAC 1 is inoperable in both CPCS Channel A and Channel B, then the CPC in those channels rely solely on CEAC 2 to compute the CEA deviation penalty factor based on RSPT 2 signals. If we postulate an undetected error in one of the CEAC 2’s in Channel A or B, as required by IEEE 603, Clause 5.1, the 4-channel CPCS is still able to perform its safety function because it has 2 channels that have 2 operable CEACs (Channels C and D), and 1 channel with 1 operable CEAC. These three channels can calculate a CEA deviation penalty factor for the CPC.</p> <p>Should failures in the RSPTs occur that causes a CEAC to fail, this failure would cause CEAC failures to occur in all four CPCS channels which exceeds the condition of two CPCS channels having 1 CEAC inoperable. In the case of an undetected RSPT failure (e.g., RSPT1), this</p>

TS Section	Proposed Change
	<p>scenario affects 1 CEAC in all four CPCS channels. The other CEAC (e.g., CEAC 2) can still perform its safety function by generating a penalty factor based on the redundant RSPT signal (e.g., RSPT2).</p> <p>Action “b” is similar to the current TS action 6 for a single CEAC inoperable. It provides additional requirements when the third or fourth CPC channel experiences the inoperability of one of the two contained CEACs. Action “b.1” ensures the CPC channel does not use the input from the failed CEAC by setting the appropriate addressable constant. Action “b.2” is similar to the current action “6a” except instead of describing the 4-hour action similar to SR 4.1.3.1.1, it directs the performance of that SR.</p> <p>Action “c” is similar to the current set of “6c” actions, including specifying the 4-hour CEA position checks via performance of SR 4.1.3.1.1.</p> <p><u>Action 7</u></p> <p>Action 7 is being deleted since it is associated with Auto-restarts of the CEAC which is not a function of the upgraded system.</p>
TS 3.3.1 SR 4.3.1.3	SR 4.3.1.3 is modified to also exclude CPC and CEAC, along with neutron detectors, from REACTOR TRIP SYSTEM RESPONSE TIME testing. The response time assumptions of the CPCS Upgrade will be validated as part of the Site Acceptance Testing. Appendix B to the LTR provides the justification for this change.
TS 3.3.1 SR 4.3.1.4	SR 4.3.1.4 is no longer applicable, due to design changes, since isolation amplifiers and optical isolators are being replaced with fiber optic cabling which is qualified by Entergy, as described in LTR Section 6.2.2.19. The text of the SR is replaced with “DELETED”.
TS 3.3.1 SR 4.3.1.5	SR 4.3.1.5 is no longer applicable since the upgraded CPCS design, using the Common Q platform, does not include the auto restart feature. The text of the SR is replaced with “DELETED”.
TS 3.3.1 SR 4.3.1.6	SR 4.3.1.6 to perform a CHANNEL FUNCTIONAL TEST within 12 hours of receipt of a High CPC Cabinet Temperature alarm is being deleted. The basis for the removal of this SR is provided in Appendix B to the LTR

TS Section	Proposed Change
	<p data-bbox="594 296 1334 363">and is consistent with the safety evaluation presented in Reference 10 and summarized below.</p> <p data-bbox="594 401 1334 600">The requirement to perform testing upon receipt of a cabinet high temperature alarm is not necessary and does not meet the criteria provided in 10 CFR 50.36(c)(2)(i) for demonstration of “lowest functional capability or performance levels of equipment required for safe operation of the facility.” This is based on:</p> <ul style="list-style-type: none"><li data-bbox="594 638 1334 968">a. A high CPC cabinet temperature alarm does not indicate the lowest functional capability or performance level of a CPC or CEAC. These alarms (122 deg F) are actuated well below the qualification temperature of the CPCs and CEAC (140 deg F) and merely inform the Operations staff of a potential challenge to CPC/CEAC operability. Typically, only one of four channels is affected on high cabinet temperature since each cabinet has its own independent cooling system.<li data-bbox="594 1005 1334 1604">b. The existing SR requirement has no follow up requirements for continuous monitoring after the initial test to determine if functionality may be affected in the future with an existing high temperature condition. In contrast, the improved Common Q CPCS provides more extensive online diagnostics than the current CPCS and will continuously monitor and assess CPC/CEAC module functionality. These diagnostics address numerous failure conditions from many causes, temperature stress being only one such cause. Failures are flagged by pertinent error messages and a channel trouble alarm on the Operators Module (OM), Maintenance Test Panel (MTP) and remote annunciation. The improved CPCS design provides greater confidence in identifying and alarming on an actual loss of CPC/CEAC functionality.<li data-bbox="594 1642 1334 1938">c. Lastly, the existence of a high CPC cabinet temperature alarm does not directly relate to when the CPCS becomes inoperable. Recognizing that upon receipt of the high temperature alarm, the operators have an annunciator response procedure to assess the condition and respond appropriately. The new cabinet RTDs will be periodically calibrated per the site’s calibration procedures.

TS Section	Proposed Change
TS 3.3.1 SR 4.3.1.7	SR 4.3.1.7 is being added to perform a test on the CPC DNBR/LPD trip output contact interface to the PPS. As described in LTR Appendix B, this portion of the system does not get monitored by the CPCS self-diagnostics. The test will be performed at the frequency prescribed in the Surveillance Frequency Control Program.
TS 3.3.1 Table 4.3-1	<p>Table 4.3-1 is being changed to be consistent with the Functional Unit formatting changes described above for Tables 2.2-1 and 3.3-1, where the Core Protection Calculators are the designated Functional Unit 9, with Local Power Density – High, DNBR – Low, and CEACs listed as sub-functional units. The second change is that all entries for CHANNEL FUNCTIONAL TEST for all of the Functional Unit 9 lines are changed to “None”. LTR Appendix B provides the detailed justification that demonstrates that the self-diagnostics meet the requirements of 10 CFR 50.36 for the CPCS, except for the CPC DNBR/LPD trip output contacts which will be tested by the new SR 4.3.1.7. See also Section 3.4 below for Operations and site engineering actions.</p> <p>Table Notations (6) and (9) which describe elements of the CHANNEL FUNCTIONAL TEST are replaced with “DELETED”. The verification described in notation (9) is incorporated in the design of the upgraded CPCS as described in LTR Appendix B, P.B-41, Item 1.</p>
TS 3.10.2 SR 4.10.2.2	SR 4.10.2.2 is being revised to replace "Functional Unit 15" with "Functional Unit 9c".
TS 6.8.1	Administrative TS 6.8.1 (g) is being revised to conform to specification 5.4.1.f of NUREG-1432 Revision 4, “Standard Technical Specifications – Combustion Engineering Plants”. This change replaces the governing source document for modifications to the CPC software to the appropriate Common Q Software Program Manual and provides more substantive guidance for the control of CPC Type 1 addressable constants than the current site-specific guidance.
TS 6.9.1.11.1	Administrative TS 6.9.1.11.1 is being revised to conform with other proposed TS changes.

Attachment 2 contains the Clean TS pages reflecting incorporation of the changes described above.

Attachment 3 contains the TS Bases markups provided for information only.

3. TECHNICAL EVALUATION

The LAR is intended to address all of the DI&C-ISG-06 (Reference 2) content requirements for the Alternate Review Process (ARP). Enclosure B to DI&C-ISG-06, *Information Provided in Support of a License Amendment Request for a Digital Instrumentation and Control Modification*, provides a cross-reference to the descriptive material identified in the body of the DI&C-ISG-06 guidance document. This LAR addresses, as a minimum, items included in the Enclosure B "AR" column.

1. DI&C-ISG-06 Alternate Review Process (ARP) LAR Contents

DI&C-ISG-06 Section C.2 describes the ARP. Section C.2.1 provides guidance for ARP LAR contents. A prerequisite for requesting LAR review using the ARP is to use digital equipment which has a topical report previously approved by the NRC. There is also an expectation that the topical report vendor will develop the system. For the CPCS replacement, Entergy is proposing to use the Westinghouse Common Q digital platform. This platform has two NRC-approved topical reports for the application software development and for the digital equipment (References 7 and 11, respectively). The digital equipment topical report was recently re-reviewed by the NRC with an approval issued in January 2020. Thus, the equipment proposed for Waterford has been recently reviewed by the NRC. Note that LTR Section 6 (Attachment 4), which addresses DI&C-ISG-06 Section D.5, describes any differences between the Waterford system and that which is described in the NRC-approved topical reports. Westinghouse is contracted to develop the hardware and software system. The LTR addresses all of the Plant-Specific Action Items (PSAIs) and the remaining Generic Open Items (GOI) included in the most recent NRC approval for both topical reports.

There is a precedent for the CPCS design at Palo Verde Nuclear Generating Station Units 1, 2 and 3 (PVNGS). This is referred to as the reference design in the LAR and is described in LAR Section 4.2 below. The LTR describes the portions of the Waterford design that are similar to the PVNGS and have been previously reviewed by the NRC. The LAR includes the CPCS replacement project System Requirements Specification (SyRS) and Failure Modes and Effects Analysis (FMEA). Each of these project documents has a reference design document (Attachments 7 and 9), which has been previously reviewed by the NRC, and a "delta" document (Attachments 8 and 10) which describes differences for the Waterford project.

This is the pilot LAR for the ARP, and as such, this LAR is the first time a licensee has assembled the LAR content based on the DI&C-ISG-06 Revision 2 guidance. The ARP LAR is designed to be a single submittal provided to the NRC early in the project schedule. Thus, the LAR content is based on conceptual design, system requirements, and human-system interface requirements. Based on multiple NRC presubmittal meetings, Entergy believes the LAR contains sufficient "system design" information to demonstrate compliance with the regulatory requirements.

Both in DI&C-ISG-06 and in the public meetings held during its development, the NRC stressed the importance of licensees performing adequate vendor oversight of the digital platform vendor. The licensee has the primary responsibility to ensure that the vendor adheres to the lifecycle development process described in the LAR, NRC-approved vendor

topical reports, and other procurement information. Waterford has developed a Vendor Oversight Plan (VOP) to ensure Westinghouse compliance to the NRC-approved development process and other procurement information. The VOP, as currently executed, is used to ensure that the vendor executes the project consistent with the LAR. A summary of the project-specific VOP is included in LAR Enclosure Attachment 14.

Licensee Prerequisites

DI&C-ISG-06 Section C.2.2 describes the licensee prerequisites for use of the ARP. Item 1 states that the LAR should include a description of the licensee's VOP. The VOP, when executed must ensure that the vendor (1) executes the project consistent with the LAR, and (2) uses an adequate software QA program. As described above, the VOP summary is included in LAR Enclosure Attachment 14. The VOP describes the licensee interactions with the vendor throughout the entire system development lifecycle to ensure the software and system development is in accordance with the NRC-approved software development process (Reference 7).

Section C.2.2 Item 2 states that the LAR should contain a reference to an NRC-approved topical report. Item 2 has two subparts. To address subpart a. the Westinghouse Common Q platform has two NRC-approved topical reports (References 7 and 11). The CPCS application is within the scope of both topical reports. To address subpart b. Westinghouse will be using the NRC-approved Common Q Software Program Manual (SPM) (Reference 7) as the framework for the design and development of the WF3 CPCS replacement. This framework is a supplement to the Westinghouse 10 CFR 50 Appendix B Quality Assurance program to specifically address digital I&C safety system development.

Section C.2.2 Item 3 addresses licensee regulatory commitments (Attachment 15). This item has two subparts. Subpart a. states that the LAR should include regulatory commitments to complete the referenced topical reports' PSAIs. The LTR Sections 5 and 6 address the applicable PSAIs. In many instances, the PSAI response references vendor oversight. Through this LAR, Waterford will execute vendor oversight in accordance with the VOP. Based on one PSAI disposition, there is one regulatory commitment described in the Attachment 15 (i.e., SPM PSAI 5). Subpart b. states that the LAR should include regulatory commitments to complete lifecycle activities under the licensee's QA program similar to the activities a licensee would complete under a Tier 1, 2 or 3 licensing review. These activities are generically described in DI&C-ISG-06 Enclosure B. Based on an evaluation of the design activities completed at the time of LAR submittal and the activities covered by the VOP, no additional regulatory commitments are required.

2. Licensing Technical Report (LTR)

The LTR (Attachment 4) provides most of the LAR technical content. The LTR directly addresses the DI&C-ISG-06 Sections D.1 to D.8 subsections entitled "Information To Be Provided," which is delineated in the LTR Table of Contents. The various major section headings include "(D.x)". This parenthetical remark refers to the specific DI&C-ISG-06 sections with the x replaced with 1 to 8. Each section includes a description of compliance to the 10 CFR 50 Appendix A General Design Criteria or IEEE Std. 603 clauses or other regulatory requirements listed in the corresponding DI&C-ISG-06 section.

LTR Section 7 provides a compliance matrix describing LAR compliance to IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003 (References 12 and 15). The compliance matrix is based on the DI&C-ISG-06 example Table D-1, *IEEE Standards 603-1991 and 7-4.3.2-2003 Compliance/Conformance Table*.

LTR Appendix A contains draft FSAR markups. These markups are being provided for information only in support of the LAR review. Entergy engineering procedures will govern FSAR revisions as a result of LAR approval and equipment installation. NRC will receive the Waterford updated FSAR as part of the biennial submittal per 10 CFR 50.71.

LTR Appendix B provides the Failure Modes, Effects, Diagnostics Analysis (FMEDA) and other analyses to support TS SR elimination. This appendix addresses the NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP) Chapter 7 Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions," on self-test and surveillance test provisions. While the DI&C-ISG-06 Enclosure B AR column does not include a requirement for LAR inclusion of a FMEA, both the reference design and Waterford-specific FMEAs are included with the LAR (Attachments 9 and 10). These FMEAs are included to support review of the Appendix B FMEDA for TS SR elimination. The Waterford-specific FMEA is considered a "living document" per DI&C-ISG-06.

LTR Appendix C includes Endnotes providing references (e.g., Entergy documents, Westinghouse documents, etc.) for statements of fact within the LTR.

3. Factory Acceptance Test/Site Acceptance Test (FAT/SAT) Description

While not required by the DI&C-ISG-06 ARP content requirements, the NRC safety evaluation (SE) for the PVNGS precedent (Reference 10) describes the NRC's review of testing as part of the acceptability of the application-specific software. Since the conduct of the FAT and SAT are outside of the LAR review scope, the following description is included to provide NRC assurance of adequate testing.

Based on the Software Program Manual (SPM) for Common Q™ Systems (Reference 7), the purpose of the Factory Acceptance Test (FAT) is to demonstrate that the complete system is integrated and functional. The FAT will be conducted at the Westinghouse facilities prior to shipment of equipment to Waterford. The FAT will be performed as a manufacturing test to provide evidence that the system meets its requirements and provides confidence that the site installation and integration activities will be successful. The FAT test, together with the documentation of the prior Verification and Validation (V&V) activities (module tests, unit tests, software code reviews, integration testing, and system validation testing, etc.) demonstrate full compliance to the requirements.

The FAT will contain a comprehensive suite of tests that cover the Waterford-specific System Requirements Specification (SyRS) (Reference 8) functional requirements. The completeness of the FAT is demonstrated by:

- Waterford-specific system tests performed
- Reference design system validation testing, performed previously, that remains valid for those design aspects that are identical

- Waterford design system testing is based on regression analysis per the SPM and testing requirements are validated as part of the independent V&V and confirmed by Vendor Oversight Plan (VOP) (Reference 9) audits
- The minimum set of tests required for a FAT defined in the Common Q SPM, Exhibit 7-1

The FAT is performed to:

- Demonstrate that the system being delivered has been manufactured correctly
- Demonstrate (in conjunction with V&V) compliance to requirements for customer acceptance
- Reduce the risk associated with deferring compliance demonstration to the site activities (e.g., SAT, preoperational testing, etc.)
- Demonstrate aspects of the design that would not be practical once full integration is achieved due to limitations on interfaces that are connected in the plant.

For design changes introduced for the Waterford system, regression analysis shall be performed to determine what tests need to be repeated or introduced to maintain the level of system design validation achieved during the first of a kind system validation test program. The system validation tests required by the regression analysis may be performed on the deliverable equipment as a separate section of the FAT or performed on surrogate equipment consistent with the regression testing methods. These methods have been reviewed and approved by the NRC as part of the Westinghouse SPM, as confirmed by the VOP audits.

The following test items shall be included or demonstrated in the FAT:

- Safety Functions
- Communications
- Operability of Displays
- Diagnostics associated with hardware specific inputs (door alarms, temperature alarms, breaker status, etc.)
- Performance (accuracy, time response, etc.)

The Waterford CPCS FAT will include overall functional testing for the Single Channel components and the Four Channel components. In addition to the Single Channel FAT and the Four Channel FAT, there are IV&V design verification tests conducted at the module and unit level for the Waterford CPCS changes. The Four Channel FAT will include IV&V software and all associated connections.

The FAT results will be comprised of multiple reports that will include test anomalies and failures that were dispositioned and corrected. Waterford project team personnel will observe the FAT under the VOP.

The Site Acceptance Test (SAT) is considered a two-part test verifying correct functionality and performance after the system is installed at Waterford. The Waterford Common Q CPCS site acceptance testing will be performed and controlled in accordance with Entergy procedures, and include pre-installation and post-installation tests. The pre-installation

testing will include the tests considered to be the Site Acceptance Test (SAT). The primary intent of the SAT shall be to validate that the equipment was not damaged during shipment.

The SAT will include pre-installation testing at Waterford in the test area for the Single Channel and the Four Channel components after they are received on site. The Waterford test area will conform to all required Waterford procedures for software control and cyber security as part of a secure and controlled access area. The SAT is a reperformance of the applicable portions of the FAT, as part of receipt inspection, to ensure the full functionality of the delivered system. The SAT test procedures and reports are not complete at this time. The SAT is scheduled to be performed in March 2021 for the Single Channel, and November 2021 for the Four Channel systems. Westinghouse personnel are expected to be present during the SAT (in a support role only). Prior to performing the SAT, construction tests will be performed prior to initializing the CPC/CEAC system in the test area. Construction will include point to point (or scheme) checks, power and grounding checks, and an initial power-up check. After the SAT items are complete, dry runs of the CPCS post-installation tests will be performed to identify and correct any problems prior to the actual operability testing of the CPCS post-installation.

The post-installation tests will be conducted in two phases: post installation tests prior to declaring the CPCS operational, and tests to be performed after the CPCS is operational and the reactor is at power. Westinghouse personnel are expected to be present during the post-installation testing (in a support role only). The primary intent of the post-installation tests is to validate that the equipment was not damaged during installation and installed per the approved modification package. External system interface testing will be specified in the post-installation testing.

The post-installation tests prior to declaring the CPCS operable will include construction testing and functional testing. Construction tests will include point to point (or scheme) checks, power and grounding checks, and an initial power-up check. Functional testing will include annunciator operability, time response testing, channel calibration testing, channel interface testing, and system integrated tests.

The post-installation tests performed after declaring the CPCS operable are to ensure CEA movement, gather performance data, provide new baseline data, and to validate assumptions.

4. Waterford System Engineer and Operations Actions Supporting TS SR Reduction

As described in LTR Appendix B, the methodology to eliminate TS SRs leverages a precedent licensing action. Southern Nuclear Company (SNC) Vogtle Electric Generation Plant (VEGP) Units 3 and 4 requested a license amendment to eliminate a number of protection system TS SRs (Reference 13). The NRC approved this LAR in Reference 14. The NRC SE approved the removal of surveillance requirements related to the VEGP Units 3 and 4 Common Q-based safety system (i.e., the Protection and Safety Monitoring System (PMS)). As part of the NRC SE, the NRC described that

"...plant administrative controls will be implemented to assure continued monitoring of the PMS system to assure adequate operation of the system diagnostic function. In the

absence of the either divisional or system alarms, there will also be operator rounds and system engineer's monthly reports that evaluate and document the health, errors, and faults of system."

Waterford will also utilize operator rounds and system engineer activities to provide additional assurance that diagnostic faults are detected.

Post installation, CPCS operability will be verified using 1) the automated diagnostics credited in this LAR (i.e., as described in LTR Appendix B), 2) Technical Requirements Manual (TRM) 3/4.3.1, "Reactor Protective Instrumentation" and associated surveillance procedures; and 3) Waterford TS 6.5.1.8, "Surveillance Frequency Control Program (SFCP)". A failure of credited automated diagnostics to detect a fault will be either detected by other diagnostics in the system or by checker(s) of diagnostics. This condition will be alarmed and displayed on the main control room (MCR) operator modules (OM) and/or the main control room annunciators. Upon receipt of an alarm or abnormal conditions, the station operating procedures will require the operators to perform system checks and verify operability of the CPCS deviation / function. The procedure will direct the operator to dispatch a maintenance technician to determine the source of the alarm as needed.

Procedure changes made as part of the implementation will impact routine Operations and site engineering actions. The following actions will also provide assurance (defense-in-depth) that diagnostic faults are captured and investigated.

1. Conduct of Operations, Operations Shift Logs, and Control Room Shift Logs – During routine operator rounds and MCR activities, the following tasks will be performed by the operators:
 - Checking the OM's for Health Status, alarms and faults
 - Checking the OM's CPCS Channel System Event Log, as described in the LTR Section 3.2.7.2.4 (Attachment 4), for Health Status, alarms and faults
 - Checking the OM's for failed sensor stack
 - Checking MCR annunciators

The walkdowns and operator rounds are controlled by the plant procedures and the results are logged in accordance with plant procedures, which are continuously maintained and retrievable.

2. System Health Checks – Site engineers are required to establish and perform periodic system health monitoring and generate system health reports per Entergy procedures. Corrective actions are used to improve system health and the overall plant performance, safety and reliability. CPCS is a critical system which requires periodic system health monitoring and walk-down of the system. The CPC system checks include the following:
 - Failure trending of sub-components on CPC and CEAC circuit boards (as required)
 - CPC System Performance Indicator (PI) Trends – input instrument drift, sensor failures, system trips reviewed (various periodicities)
 - Review of trend data for CEAs including RSPTs and RSPT power supplies (weekly)
 - Walk-downs of the CPC system (quarterly)

System health reports are reviewed by systems engineering management and fleet subject matter experts. Required documentation, long range planning, and trending instruction are maintained in system notebooks. Issues are communicated, and adverse trends and issues not previously addressed (i.e., all alarms should have been addressed by Operations) are captured in condition reports.

4. REGULATORY EVALUATION

The Core Protection Calculator System (CPCS) replacement incorporates the fundamental design principles of redundancy, independence, deterministic behavior, and defense-in-depth and diversity while providing enhanced reliability and obsolescence management. The hardware and software development for the CPCS replacement complies with the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991 Clause 5.3 "Quality," and IEEE Standard 7-4.3.2-2003 Clause 5.3 "Quality," including the digital system development life cycle, in order to provide a high quality development process (References 12 and 15). The independent V&V effort for the replacement utilizes a process that complies with IEEE Standard 7-4.3.2-2003 Clause 5.3.3, "Validation and Verification" to ensure the replacement meets the specified functional requirements and criteria.

Therefore, Entergy concludes the proposed CPCS replacement project complies with the 10 CFR 50 regulations and associated regulatory guidance.

1. Applicable Regulatory Requirements/Criteria

The following regulations and guidance are applicable to the proposed CPCS replacement project installation:

- 10 CFR 50.36, "Technical Specifications." The criteria for limiting conditions for operation and surveillance requirements are in 50.36(c)(2) and (3), respectively.
- Paragraph 10 CFR 50.55a(a)(1), states that Structures, Systems, and Components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
- Paragraph 10 CFR 50.55a(h), "Protection and safety systems," approves the 1991 version of IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference including the correction sheet dated January 30, 1995.
- The following General Design Criteria (GDC) in Appendix A to 10 CFR Part 50 are addressed in the LTR (Attachment 4):
 - GDC 13, "Instrumentation and control"
 - GDC 21, "Protection system reliability and testability"
 - GDC 22, "Protective system independence"
 - GDC 23, "Protection system failure modes"

- GDC 24, "Separation of protection and control systems"
 - GDC 29, "Protection against anticipated operational occurrences"
- 10 CFR 50, Appendix A, GDC 10 requires that specified acceptable fuel design limits (SAFDLs) are not exceeded during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis (i.e., a 95/95 probability/confidence level criteria) that DNB will not occur on the limiting fuel rods, and by requiring that fuel centerline temperature stays below the melting temperature. The reactor core safety limits are established to preclude violation of these criteria. Automatic enforcement of the reactor core safety limits is provided by the reactor protection system (RPS), which includes a number of reactor trip functions, two of which are the DNBR - low and local power density (LPD) - high reactor trips. As part of the RPS, the CPCS generates a reactor trip signal when the DNBR or the LPD approach their specified limiting safety system settings. The reactor trips protect against violating core SAFDLs during AOO's. In meeting GDC 10, the replacement CPCS continues to satisfy these functional requirements.
- 10 CFR 50, Appendix A, GDC 20 requires that protection system functions shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety. The CPCS is designed to meet this GDC requirement. The WF3 design basis functions of the CPCS are unchanged as a result of this modification to the Common Q CPCS. These same CPCS design basis functions are found in the Common Q CPCS reference design (i.e., PVNGS CPCS).
- 10 CFR 50, Appendix A, GDC 25 provides protection system requirements for reactivity control malfunctions. It states that the protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods. The CPCS is designed to mitigate reactivity malfunctions as described in the WF3 FSAR, Chapter 15. The WF3 design basis functions of the CPCS are unchanged as a result of this modification to the Common Q CPCS. These same CPCS design basis functions are found in the Common Q CPCS reference design (i.e., PVNGS CPCS).
- Regulatory Guide 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems," November 2003 (ADAMS Accession No. ML033220006).
- Regulatory Guide 1.75, Revision 3, "Physical Independence of Electric Systems," February 2005 (ADAMS Accession No. ML13350A340).
- Regulatory Guide 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," June 1984 (ADAMS Accession No. ML003740271).

- Regulatory Guide 1.100, Revision 3, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," September 2009 (ADAMS Accession No. ML091320468).
- Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (ADAMS Accession No. ML102870022).
- Regulatory Guide 1.170, Revision 1, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013 (ADAMS Accession No. ML13003A216).
- Regulatory Guide 1.172, Revision 1 "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants," July 2013 (ADAMS Accession No. ML13007A173).
- Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003 (ADAMS Accession No. ML032740277).
- Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007 (ADAMS Accession No. ML070190294).
- NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," November 2012 (ADAMS Accession No. ML12324A013).
- NUREG-1764, Revision 1, "Guidance for the Review of Changes to Human Actions," September 2007 (ADAMS Accession No. ML072640413).
- DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms- Communications Issues (HICRc)," March 2007 (ADAMS Accession No. ML083310185).
- DI&C-ISG-06, "Task Working Group #6: Licensing Process," Revision 2, dated December 2018 (ADAMS Accession No. ML18269A259).
- The applicable portions of the following branch technical positions within NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Chapter 7, "Instrumentation and Controls," as follows:
 - Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer- Based Instrumentation and Control Systems"
 - Branch Technical Position 7-17, " Guidance on Self-Test and Surveillance Test Provisions"

- Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-In- Depth in Digital Computer-Based Instrumentation and Control Systems"

The Licensing Technical Report (Attachment 4) and other attachments contain project-specific compliance information for the above regulations and guidance.

2. Precedent

The Core Protection Calculator System (CPCS) at Waterford Steam Electric Station Unit 3 (Waterford) is being replaced with a new system based on the Common Qualified (Common Q™) Platform. This system is based on the reference design that is installed at the Palo Verde Nuclear Generating Station Units 1, 2, and 3 (PVNGS) that was reviewed and approved by the NRC (Reference 10). There are minor architectural changes from the reference design as a result of obsolescence and unique aspects of the Waterford plant compared to PVNGS. The Licensing Technical Report (Attachment 4) describes the Waterford Common Q CPCS and identifies where the implementation is the same as PVNGS to assist the NRC staff in their review of the LAR.

3. No Significant Hazards Consideration Analysis

In accordance with 10 CFR 50.90, Entergy Operations, Inc. (Entergy) requests an amendment to Renewed Facility Operating License (FOL) No. NPF-38, Appendix A, "Technical Specifications" (TSs) for Waterford Steam Electric Station, Unit 3 (Waterford). The proposed TS changes reflect the upgrade of the Waterford digital Core Protection Calculator System (CPCS), comprised of CPCs and Control Element Assembly Calculators (CEACs), with a new, more reliable digital system based on the NRC-approved Westinghouse Common Qualified (Common Q™) Platform.

The following Technical Specifications (TS) sections are affected by this change:

- 2.2.1 Reactor Trip Setpoints
- 3.1.3.1 CEA Position
- 3.2.4 DNBR Margin
- 3.3.1 Reactor Protective Instrumentation
- 3.10.2 Moderator Temperature Coefficient, Group Height, Insertion, and Power Distribution Limits
- 6.8.1 Procedures and Programs
- 6.9 Reporting Requirements

Entergy has evaluated whether a significant hazards consideration is involved with the proposed amendment by focusing on the three conditions set forth in 10 CFR 50.92, "Issuance of amendment," as discussed below:

1. Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No.

The probability of accidents occurring is not affected by the proposed amendment. The CPCS is not the initiator of any accident and does not interact with equipment whose failure could cause an accident. The CPCS provides reactor trips to the Reactor Protection System (RPS) for high local power density (LPD) and low departure from nucleate boiling ratio (DNBR). All design basis events, and the reliance on the CPCS low DNBR and high LPD trips will remain unchanged.

The consequences of accidents are not affected by the proposed amendment. The upgrade of the CPCS will change the existing system architecture in the area of CEAC processing by transitioning from two CEACs (i.e., providing input to four CPC channels) to eight CEACs (i.e., two in each CPC channel). Increasing the number of CEACs to eight will increase the availability of the CEAC processing. The CPCS functional design and design basis functions will not change as a result of the proposed amendment.

The availability of the upgraded CPCS system will be equal to or greater than the existing system and, as a result, the scram reliability will be equal to or better than the existing system. The requirements for response time and accuracy that are assumed in the Waterford Updated Final Safety Analysis Report (UFSAR) accident analysis will continue to be met. Therefore, the new CPCS will be capable of performing the same safety-related functions within the same response time and accuracy as the existing CPCS. No new challenges to safety-related equipment will result from the CPCS modification. Therefore, the proposed change does not involve a significant increase in the consequences of an accident previously evaluated.

Therefore, the proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The functional design of the CPCS system and the design basis functions will not change as a result of the CPCS modification. The components of the CPCS will be supplied to equivalent or better design and qualification criteria than is currently required for Waterford. The CPCS modification will not introduce any new operating modes, safety-related equipment lineups, accident scenarios, system interactions, or failure modes that would create a new or different type of accident. Failure(s) of

the system will have the same overall effect as the present design. Therefore, the upgraded CPCS will not adversely affect plant equipment.

The existing CPCS is implemented in computer-based hardware, therefore implementation of the NRC-approved Westinghouse Common Q™ platform represents a digital-to-digital upgrade. The original licensing basis for Waterford assumes a potential common cause failure of the CPCS. The replacement of the current digital CPCS with the Common Q™ platform does not change the Waterford licensing basis for defense-in-depth and diversity. Therefore, the proposed change does not result in any new common cause failure or any reduction in defense-in-depth and diversity.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any previously evaluated.

3. Does the proposed amendment involve a significant reduction in a margin of safety?

Response: No.

The proposed TS changes associated with the CPCS modification implement the constraints associated with eight CEACs, relative to the current design of two CEACs. This new design, as well as the implementation of the Westinghouse Common Q™ platform does not impact reactor operating parameters or the functional requirements of the CPCS. The CPCS will continue to provide reactor trips to the RPS for high LPD and low DNBR. All design basis events, and the reliance on the CPCS low DNBR and high LPD trips will remain unchanged.

Therefore, the proposed change does not involve a significant reduction in a margin of safety. Based on the above, Entergy concludes that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of no significant hazards consideration is justified.

4. Conclusions

In conclusion, based on the considerations discussed above, (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

5. ENVIRONMENTAL CONSIDERATION

The proposed change would change a requirement with respect to installation or use of a facility component located within the restricted area, as defined in 10 CFR Part 20, and would change an inspection or surveillance requirement. However, the proposed change does not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amounts of any effluents that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed change meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed change.

6. REFERENCES

- 6.1 Entergy Operations, Inc. (Entergy) letter to U.S. Nuclear Regulatory Commission (NRC), "Letter-of-Intent to Submit License Amendment Requesting Using Digital Instrumentation and Control Interim Staff Guidance-(ISG)-06, Revision 2 and Request for NRC Fee Waiver," (ADAMS Accession No. ML19137A082), dated May 16, 2019
- 6.2 U.S. NRC Digital Instrumentation and Control Interim Staff Guidance-(ISG)-06, "Licensing Process," Revision 2 (ADAMS Accession No. ML18269A259)
- 6.3 NUREG-1764, Guidance for the Review of Changes to Human Actions, Revision 1 (ADAMS Accession No. ML072640413), U.S. NRC
- 6.4 NUREG-0711, Human Factors Engineering Program Review Model, Revision 3, November 2012 (ADAMS Accession No. ML072640413), U.S. NRC
- 6.5 NUREG/CR-6400, Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience, January 1997, (ADAMS Accession No. ML072640413), U.S. NRC
- 6.6 Entergy-Westinghouse Contract #10575450-01 including Purchase Orders 10587546, 10591996
- 6.7 Software Program Manual for Common Q™ Systems, WCAP-16096-P-A, Revision 5, Westinghouse Electric Company LLC
- 6.8 System Requirements Specification for the Core Protection Calculator System, WNA-DS-04517-CWTR3, Revision 2, Westinghouse Electric Company LLC
- 6.9 Waterford Unit Steam and Electric Station Unit 3 Core Protection Calculator System Replacement Project Vendor Oversight Plan, Entergy document no. VOP-WF3-2019-00236, Revision 1
- 6.10 Palo Verde Nuclear Generating Station, Units 1, 2, and 3 – Issuance of Amendments on the Core Protection Calculator System Upgrade (TAC Nos. MB6726, MB6727 and MB6728) (ADAMS Accession No. ML033030363), U.S. NRC
- 6.11 Common Qualified Platform Topical Report, WCAP-16097-P-A, Revision 4, Westinghouse Electric Company LLC
- 6.12 IEEE Standard 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

- 6.13 Vogtle Electric Generation Plant Units 3 and 4 – Request for Licenses Amendment Regarding Protection and Safety Monitoring System Surveillance Requirement Reduction Technical Specification Revision (LAR 19-001), (ADAMS Accession No. ML19084A309), Southern Nuclear Company
- 6.14 Vogtle Electric Generating Plant Units 3 and 4 Safety Evaluation (LAR 19-001), (ADAMS Accession No. ML19297D159), U.S. NRC
- 6.15 IEEE Standard 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

7. ATTACHMENTS

- 1. Technical Specification Page Markups
- 2. Clean Technical Specification Pages
- 3. Technical Specification Bases Page Markups
- 4. Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System, WCAP-18484-P, Revision 0
- 5. Westinghouse Letter CAW-20-5031, Affidavit for Attachment 4
- 6. Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System, WCAP-18484-NP, Revision 0
- 7. System Requirements Specification for the Common Q Core Protection Calculator System, 00000-ICE-30158, Revision 14
- 8. System Requirements Specification for the Core Protection Calculator System, WNA-DS-04517-CWTR3, Revision 2
- 9. Failure Modes and Effects Analysis for the Common Q Core Protection Calculator System, 00000-ICE-3338, Revision 0
- 10. Failure Modes and Effects Analysis for the Core Protection Calculator System, WNA-AR-00909-CWTR3, Revision 1
- 11. Core Protection Calculator System Primary Digital Components Qualification Summary Report for Waterford Unit 3, EQ-QR-400-CWTR3, Revision 0
- 12. Westinghouse Letter CAW-20-5040, Affidavit for Attachments 7, 8, 9, 10, and 11
- 13. Human Factors Engineering Analysis
- 14. Core Protection Calculator System Replacement Project Vendor Oversight Plan (VOP) Summary
- 15. List of Regulatory Commitments

Enclosure, Attachment 1

W3F1-2020-0040

DRAFT
Technical Specification Page Mark-ups

TS Pages

2-3

3/4 1-20

3/4 2-6

3/4 3-1

3/4 3-2

3/4 3-3

3/4 3-4

3/4 3-6

3/4 3-7

3/4 3-10

3/4 3-11

3/4 3-12a

3/4 10-2

6-14

6-20

6-20a

3 Pages of INSERTS

TABLE 2.2-1
REACTOR PROTECTIVE INSTRUMENTATION TRIP SETPOINT LIMITS

FUNCTIONAL UNIT	TRIP SETPOINT	ALLOWABLE VALUES
1. Manual Reactor Trip	Not Applicable	Not Applicable
2. Linear Power Level - High		
Four Reactor Coolant Pumps Operating	$\leq 108\%$ of RATED THERMAL POWER	$\leq 108.76\%$ of RATED THERMAL POWER
3. Logarithmic Power Level - High (1)	$\leq 0.257\%$ of RATED THERMAL POWER (6)	$\leq 0.280\%$ of RATED THERMAL POWER (6)
4. Pressurizer Pressure - High	≤ 2350 psia	≤ 2359 psia
5. Pressurizer Pressure - Low	≥ 1684 psia (2)	≥ 1649.7 psia (2)
6. Containment Pressure - High	≤ 17.1 psia	≤ 17.4 psia
7. Steam Generator Pressure - Low	≥ 666 psia (3)	≥ 652.4 psia (3)
8. Steam Generator Level - Low	$\geq 27.4\%$ (4)	$\geq 26.48\%$ (4)
9. Local Power Density - High	≤ 21.0 kW/ft (5)	≤ 21.0 kW/ft (5)
10. DNBR - Low	≥ 1.26 (5)	≥ 1.26 (5)
11. DELETED		
12. Reactor Protection System Logic	Not Applicable	Not Applicable
13. Reactor Trip Breakers	Not Applicable	Not Applicable
14. Core Protection Calculators	Not Applicable	Not Applicable
15. CEA Calculators	Not Applicable	Not Applicable
16. Reactor Coolant Flow - Low	≥ 19.00 psid (7)	≥ 18.47 psid (7)

Replace with
INSERT A

Delete and
leave blank

Replace with
"DELETED"

W3F1-2020-0040
ATTACHMENT 1,
DRAFT
TECHNICAL SPECIFICATION PAGE MARK-UPS

9. Core Protection Calculators
 - a. Local Power Density - High
 - b. DNBR – Low

10. DELETED

REACTIVITY CONTROL SYSTEMS

SURVEILLANCE REQUIREMENTS

4.1.3.1.1 The position of each CEA shall be determined to be within 7 inches (indicated position) of all other CEAs in its group in accordance with the Surveillance Frequency Control Program except during time intervals when one CEAC is inoperable or when both CEACs are inoperable, then verify the individual CEA positions at least once per 4 hours.

4.1.3.1.2 Each CEA not fully inserted in the core shall be determined to be OPERABLE by movement of at least 5 inches in any one direction in accordance with the Surveillance Frequency Control Program.

Delete

POWER DISTRIBUTION LIMITS

3/4.2.4 DNBR MARGIN

LIMITING CONDITION FOR OPERATION

3.2.4 The DNBR margin shall be maintained by one of the following methods:

- Insert B →
- Replace with "1." →
- Replace with Insert C →
- Replace with "2." →
- Replace with Insert D →
- Replace with "1." →
- Replace with Insert E →
- Replace with "2." →
- a. Maintaining COLSS calculated core power less than or equal to COLSS calculated core power operating limit based on DNBR (when COLSS is in service, and either one or both CEACs are operable); or
 - b. Maintaining COLSS calculated core power less than or equal to COLSS calculated core power operating limit based on DNBR decreased by the amount specified in the COLR (when COLSS is in service and neither CEAC is operable); or
 - c. Operating within the region of acceptable operation specified in the COLR using any operable CPC channel (when COLSS is out of service and either one or both CEACs are operable); or
 - d. Operating within the region of acceptable operation specified in the COLR using any operable CPC channel (when COLSS is out of service and neither CEAC is operable).

APPLICABILITY: MODE 1 above 20% of RATED THERMAL POWER.

ACTION:

Replace with Insert F

- a. With the DNBR limit not being maintained as indicated by COLSS calculated core power exceeding the COLSS calculated core power operating limit based on DNBR, within 15 minutes initiate corrective action to reduce the DNBR to within the limits and either:
 1. Restore the DNBR to within its limits within 1 hour, or
 2. Reduce THERMAL POWER to less than or equal to 20% of RATED THERMAL POWER within the next 6 hours.
- b. With the DNBR limit not being maintained as indicated by operation outside the region of acceptable operation specified in the COLR with COLSS out of service, either:
 1. Restore COLSS to service within 2 hours, or
 2. Restore the DNBR to within its limits within the next 2 hours, or
 3. Reduce THERMAL POWER to less than or equal to 20% of RATED THERMAL POWER within the next 6 hours.

W3F1-2020-0040
ATTACHMENT 1,
DRAFT
TECHNICAL SPECIFICATION PAGE MARK-UPS

INSERT B

a. Core Operating Limit Supervisory System (COLSS) in Service:

INSERT C

when at least one Control Element Assembly Calculator (CEAC) is OPERABLE in each OPERABLE Core Protection Calculator (CPC) Channel; or

INSERT D

when the CEAC requirements of LCO 3.2.4.a.1 are not met.

b. COLSS Out of Service

INSERT E

OPERABLE Core Protection Calculator (CPC) Channel when at least one Control Element Assembly Calculator (CEAC) is OPERABLE in each OPERABLE CPC channel; or

INSERT F

OPERABLE Core Protection Calculator (CPC) Channel (with both CEACS inoperable) when the CEAC requirements of LCO 3.2.4.b.1 are not met.

3/4.3 INSTRUMENTATION

3/4.3.1 REACTOR PROTECTIVE INSTRUMENTATION

LIMITING CONDITION FOR OPERATION

3.3.1 As a minimum, the reactor protective instrumentation channels and bypasses of Table 3.3-1 shall be OPERABLE.

APPLICABILITY: As shown in Table 3.3-1.

ACTION:

As shown in Table 3.3-1.

SURVEILLANCE REQUIREMENTS

4.3.1.1 Each reactor protective instrumentation channel shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-1.

4.3.1.2 The logic for the bypasses shall be demonstrated OPERABLE prior to each reactor startup unless performed during the preceding 92 days. The total bypass function shall be demonstrated OPERABLE in accordance with the Surveillance Frequency Control Program during CHANNEL CALIBRATION testing of each channel affected by bypass operation.

4.3.1.3 The REACTOR TRIP SYSTEM RESPONSE TIME of each reactor trip function shall be demonstrated to be within its limit in accordance with the Surveillance Frequency Control Program. Neutron detectors are exempt from response time testing. Each test shall include at least one channel per function such that all channels are tested as shown in the "Total No. of Channels" column of Table 3.3-1.

Replace with Insert G

4.3.1.4 The isolation characteristics of each CEA isolation amplifier and each optical isolator for CEA Calculator to Core Protection Calculator data transfer shall be verified in accordance with the Surveillance Frequency Control Program during the shutdown per the following tests:

a. For the CEA position isolation amplifiers:

1. With 120 volts AC (60 Hz) applied for at least 30 seconds across the output, the reading on the input does not exceed 0.015 volts DC.

Replace with "DELETED"

**W3F1-2020-0040
ATTACHMENT 1,
DRAFT
TECHNICAL SPECIFICATION PAGE MARK-UPS**

INSERT G

Neutron detectors, Core Protection Calculators, and CEACs

INSTRUMENTATION

SURVEILLANCE REQUIREMENTS (Continued)

2. With 120 volts AC (60 Hz) applied for at least 30 seconds across the input, the reading on the output does not exceed 15.0 volts DC.

b. For the optical isolators: Verify that the input to output insulation resistance is greater than 10 megohms when tested using a megohmmeter on the 500 volt DC range.

Delete

4.3.1.5 The Core Protection Calculator System and the Control Element Assembly Calculator System shall be determined OPERABLE in accordance with the Surveillance Frequency Control Program by verifying that less than three auto restarts have occurred on each calculator during the past 12 hours.

4.3.1.6 The Core Protection Calculator System shall be subjected to a CHANNEL FUNCTIONAL TEST to verify OPERABILITY within 12 hours of receipt of a High CPC Cabinet Temperature alarm.

Replace with "DELETED" and
relocate to page 3/4 3-1

4.3.1.7 Perform a test on the CPC DNBR/LPD trip output through the contact interface to the PPS in accordance with the Surveillance Frequency Control Program.

Add new 4.3.1.7 and locate on page 3/4 3-1

THIS PAGE HAS BEEN DELETED

Add and
center on page

TABLE 3.3-1
REACTOR PROTECTIVE INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
1. Manual Reactor Trip	2 sets of 2	1 set of 2	2 sets of 2	1, 2	1
	2 sets of 2	1 set of 2	2 sets of 2	3*, 4*, 5*	8
2. Linear Power Level - High	4	2	3	1, 2	2#, 3#
3. Logarithmic Power Level-High					
a. Startup and Operating	4	2(a)(d)	3	2**	2#, 3#
	4	2	3	3*, 4*, 5*	8
b. Shutdown	4	0	2	3, 4, 5	4
4. Pressurizer Pressure - High	4	2	3	1, 2	2#, 3#
5. Pressurizer Pressure - Low	4	2(b)	3	1, 2	2#, 3#
6. Containment Pressure - High	4	2	3	1, 2	2#, 3#
7. Steam Generator Pressure - Low 4/SG		2/SG	3/SG	1, 2	2#, 3#
8. Steam Generator Level - Low	4/SG	2/SG	3/SG	1, 2	2#, 3#
9. Local Power Density - High	4	2(c)(d)	3	1, 2	2#, 3#
10. DNBR - Low	4	2(c)(d)	3	1, 2	2#, 3#
11. DELETED					
12. Reactor Protection System Logic	4	2	3	1, 2	5
				3*, 4*, 5*	8
13. Reactor Trip Breakers	4	2(f)	4	1, 2	5
				3*, 4*, 5*	8
14. Core Protection Calculators	4	2(c)(d)	3	1, 2	2#, 3# and 7
15. CEA Calculators	2	1	2(e)	1, 2	6 and 7
16. Reactor Coolant Flow - Low	4/SG	2/SG(c)	3/SG	1, 2	2#, 3#

Replace with
Insert H

Replace with "DELETED"

WATERFORD - UNIT 3

3/4 3-3

AMENDMENT NO. 44, 45, 46

W3F1-2020-0040
ATTACHMENT 1,
DRAFT
TECHNICAL SPECIFICATION PAGE MARK-UPS

INSERT H

9. Core Protection Calculators	4	2(c)(d)(h)	3	1,2	2#, 3#
a. Local Power Density - High					
b. DNBR – Low					
c. CEA Calculators	4 (g)(i)	2(e)	3 (g)(i)	1,2	6
10. DELETED					

TABLE 3.3-1 (Continued)

TABLE NOTATION

*With the protective system trip breakers in the closed position, the CEA drive system capable of CEA withdrawal, and fuel in the reactor vessel.

#The provisions of Specification 3.0.4 are not applicable.

**Not applicable above a logarithmic power of 10^{-4} % RATED THERMAL POWER.

- (a) The operating bypass may be enabled above the 10^{-4} % bistable setpoint and shall be capable of automatic removal whenever the operating bypass is enabled and logarithmic power is below the 10^{-4} % bistable setpoint. Trip may be manually bypassed during physics testing pursuant to Special Test Exception 3.10.3.
- (b) Trip may be manually bypassed below 400 psia; bypass shall be automatically removed whenever pressurizer pressure is greater than or equal to 500 psia.
- (c) The operating bypass may be enabled below the 10^{-4} % bistable setpoint and shall be capable of automatic removal whenever the operating bypass is enabled and logarithmic power is above the 10^{-4} % bistable setpoint. During testing pursuant to Special Test Exception 3.10.3, trip may be manually bypassed below 5% of RATED THERMAL POWER; the 10^{-4} % bistable setpoint may be changed to less than or equal 5% RATED THERMAL POWER to perform the automatic removal function.
- (d) Trip may be bypassed during testing pursuant to Special Test Exception 3.10.3.
- (e) See Special Test Exception 3.10.2.
- (f) Each channel shall be comprised of two trip breakers; actual trip logic shall be one-out-of-two taken twice.

- (g) There are two CEACs in each CPC channel.
- (h) Both Local Power Density- High and DNBR-Low must be OPERABLE for a CPC Channel to be OPERABLE.
- (i) Both CEACs in an inoperable CPC channel are also inoperable.

Add



TABLE 3.3-1 (Continued)

ACTION STATEMENTS

2. Pressurizer Pressure - High	Pressurizer Pressure - High Local Power Density - High DNBR - Low
3. Containment Pressure - (RPS) High	Containment Pressure - High Containment Pressure - High (ESF)
4. Steam Generator Pressure - Low	Steam Generator Pressure - Low Steam Generator ΔP 1 and 2 (EFAS 1 and 2)
5. Steam Generator Level	Steam Generator Level - Low Steam Generator ΔP (EFAS)
6. Core Protection Calculator	Local Power Density - High DNBR - Low
7. Logarithmic Power	Logarithmic Power Level - High Local Power Density - High ⁽¹⁾ DNBR - Low ⁽¹⁾ Reactor Coolant Flow - Low ⁽¹⁾

STARTUP and/or POWER OPERATION may continue until the performance of the next required CHANNEL FUNCTIONAL TEST. Subsequent STARTUP and/or POWER OPERATION may continue if one channel is restored to OPERABLE status and the provisions of ACTION 2 are satisfied.

ACTION 4 - With the number of channels OPERABLE one less than required by the Minimum Channels OPERABLE requirement, suspend all operations involving positive reactivity changes. *

ACTION 5 - With the number of channels OPERABLE one less those required by the Minimum Channels OPERABLE requirement, STARTUP and/or POWER OPERATION may continue provided the reactor trip breakers of the inoperable channel are placed in the tripped condition within 1 hour; otherwise, be in at least HOT STANDBY within 6 hours; however, one channel may be bypassed for up to 1 hour for surveillance testing per Specification 4.3.1.1.

ACTION 6 - a. With one CEAC inoperable, operation may continue for up to 7 days provided that at least once per 4 hours, each CEA is verified to be within 7 inches (indicated position) of all other CEAs in its group. After 7 days, operation may continue provided that Actions 6.b.1, 6.b.2, and 6.b.3 are met.

* Limited plant cooldown or boron dilution is allowed provided the change is accounted for in the calculated SHUTDOWN MARGIN.

⁽¹⁾ With the operating bypass enabled.

Replace with Insert I

INSERT I

ACTION 6 - Separate Actions may be entered for each CPC channel.

- a. With one CEAC inoperable in 1 or 2 CPC channels, either declare the associated CPC channel(s) inoperable; or set the "RSPT/CEAC Inoperable" addressable constant to the inoperable status within 4 hours.
- b. With one CEAC inoperable in 3 or 4 CPC channels, either declare the associated CPC channel(s) inoperable; or, operation may continue provided that:
 1. Within 4 hours the "RSPT/CEAC Inoperable" addressable constant(s) is set to the inoperable status.
 2. Operation may continue for up to 7 days provided that the position of each CEA is verified to be aligned with all other CEAs in its group by performing surveillance requirement 4.1.3.1.1 at least once per 4 hours.
 3. Operation may continue after 7 days provided that Actions 6.c.1, 6.c.2, and 6.c.3 are met
- c. With both CEACS inoperable in any CPC channel, either declare the associated CPC channel(s) inoperable; or, operation may continue provided that:
 1. Within 4 hours the DNBR margin required by Specification 3.2.4a (COLSS in service) or 3.2.4b (COLSS out of service) is satisfied and the Reactor Power Cutback System is disabled, and
 2. Within 4 hours:
 - a) All CEA groups are withdrawn to and subsequently maintained at the "Full Out" position, except during surveillance testing pursuant to the requirements of Specification 4.1.3.1.2 or for control when CEA group 6 may be inserted no further than 127.5 inches withdrawn.
 - b) The "RSPT/CEAC Inoperable" addressable constant in the CPCs is set to the inoperable status.
 - c) The Control Element Drive Mechanism Control System (CEDMCS) is placed in and subsequently maintained in the "Off" mode except during CEA motion permitted by a) above, when the CEDMCS may be operated in either the "Manual Group" or "Manual Individual" mode.
 3. At least once per 4 hours, all CEAs are verified fully withdrawn except during surveillance testing pursuant to Specification 4.1.3.1.2 or during insertion of CEA group 6 as permitted by 2.a) above, then perform surveillance requirement 4.1.3.1.1 at least once per 4 hours.

TABLE 3.3-1 (Continued)

ACTION STATEMENTS

	<p>b. With both CEACs inoperable, operation may continue provided that:</p> <ol style="list-style-type: none">1. Within 4 hours the DNBR margin required by Specification 3.2.4b (COLSS in service) or 3.2.4d (COLSS out of service) is satisfied and the Reactor Power Cutback System is disabled, and2. Within 4 hours:<ol style="list-style-type: none">a) All CEA groups are withdrawn to and subsequently maintained at the "Full Out" position, except during surveillance testing pursuant to the requirements of Specification 4.1.3.1.2 or for control when CEA group 6 may be inserted no further than 127.5 inches withdrawn.b) The "RSPT/CEAC Inoperable" addressable constant in the CPCs is set to the inoperable status.c) The Control Element Drive Mechanism Control System (CEDMCS) is placed in and subsequently maintained in the "Off" mode except during CEA group 6 motion permitted by a) above, when the CEDMCS may be operated in either the "Manual Group" or "Manual Individual" mode.3. At least once per 4 hours, all CEAs are verified fully withdrawn except during surveillance testing pursuant to Specification 4.1.3.1.2 or during insertion of CEA group 6 as permitted by 2.a) above, then verify at least once per 4 hours that the inserted CEAs are aligned within 7 inches (indicated position) of all other CEAs in its group.
ACTION 7 -	<p>With three or more auto restarts of one non-bypassed calculator during a 12-hour interval, demonstrate calculator OPERABILITY by performing a CHANNEL FUNCTIONAL TEST within the next 24 hours.</p>
ACTION 8 -	<p>With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement restore the inoperable channel to OPERABLE status within 48 hours or open the reactor trip breakers within the next hour.</p>

Delete

Replace with "DELETED"

TABLE 4.3-1

REACTOR PROTECTIVE INSTRUMENTATION SURVEILLANCE REQUIREMENTS

<u>FUNCTIONAL UNIT</u>	<u>CHANNEL CHECK</u>	<u>CHANNEL CALIBRATION</u>	<u>CHANNEL FUNCTIONAL TEST</u>	<u>MODES FOR WHICH SURVEILLANCE IS REQUIRED</u>
1. Manual Reactor Trip	N.A.	N.A.	SFCP and S/U(1)	1, 2, 3*, 4*, 5*
2. Linear Power Level - High	SFCP	SFCP(2,4), SFCP (3,4), SFCP (4)	SFCP	1, 2
3. Logarithmic Power Level - High	SFCP	SFCP(4)	SFCP and S/U(1)	2#, 3, 4, 5
4. Pressurizer Pressure - High	SFCP	SFCP	SFCP	1, 2
5. Pressurizer Pressure - Low	SFCP	SFCP	SFCP	1, 2
6. Containment Pressure - High	SFCP	SFCP	SFCP	1, 2
7. Steam Generator Pressure - Low	SFCP	SFCP	SFCP	1, 2
8. Steam Generator Level - Low	SFCP	SFCP	SFCP	1, 2
9. Local Power Density - High	SFCP	SFCP(2,4), SFCP(4,5)	SFCP, SFCP(6)	1, 2
10. DNBR - Low	SFCP	SFCP(7), SFCP(2,4), SFCP(8), SFCP(4,5)	SFCP, SFCP(6)	1, 2
11. DELETED				
12. Reactor Protection System Logic	N.A.	N.A.	SFCP(11) and S/U(1)	1, 2, 3*, 4*, 5*

Replace with INSERT J

**W3F1-2020-0040
ATTACHMENT 1,
DRAFT
TECHNICAL SPECIFICATION PAGE MARK-UPS**

INSERT J

9. Core Protection Calculators	SFCP	SFCP(2,4), SFCP(4,5)	None	1,2
a. Local Power Density – High	SFCP	SFCP(2,4), SFCP(4,5)	None	1,2
b. DNBR – Low	SFCP	SFCP(7), SFCP(2,4), SFCP(8), SFCP(4,5)	None	1,2
c. CEA Calculators	SFCP	SFCP	None	1,2
10. DELETED				

TABLE 4.3-1 (Continued)

REACTOR PROTECTIVE INSTRUMENTATION SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	CHANNEL FUNCTIONAL TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
13. Reactor Trip Breakers	N.A.	N.A.	SFCP(10,11), S/U(1)	1, 2, 3*, 4*, 5*
14. Core Protection Calculators	SFCP	SFCP(2,4), SFCP(4,5)	SFCP(9), SFCP(6)	1,2
15. CEA Calculators	SFCP	SFCP	SFCP, SFCP(6)	1, 2
16. Reactor Coolant Flow - Low	SFCP	SFCP	SFCP	1, 2

Replace with "DELETED"

Delete and leave blank

TABLE 4.3-1 (Continued)

TABLE NOTATIONS (Continued)

- (3) Above 15% of RATED THERMAL POWER, verify that the linear power subchannel gains of the excore detectors are consistent with the values used to establish the shape annealing matrix elements in the Core Protection Calculators.
- (4) Neutron detectors may be excluded from CHANNEL CALIBRATION.
- (5) After each fuel loading and prior to exceeding 70% of RATED THERMAL POWER, the incore detectors shall be used to determine or verify acceptable values for the shape annealing matrix elements used in the Core Protection Calculators.
- (6) This CHANNEL FUNCTIONAL TEST shall include the injection of simulated process signals into the channel as close to sensors as practicable to verify OPERABILITY including alarm and/or trip functions.
- (7) Above 70% of RATED THERMAL POWER, verify that the total RCS flow rate as indicated by each CPC is less than or equal to the actual RCS total flow rate determined by either using the reactor coolant pump differential pressure instrumentation or by calorimetric calculations and if necessary, adjust the CPC addressable constant flow co-efficients such that each CPC indicated flow is less than or equal to the actual flow rate. The flow measurement uncertainty is included in the BERR1 term in the CPC and is equal to or greater than 4%.
- (8) Above 70% of RATED THERMAL POWER, verify that the total RCS flow rate as indicated by each CPC is less than or equal to the actual RCS total flow rate determined by calorimetric calculations.
- (9) The CHANNEL FUNCTIONAL TEST shall include verification that the correct values of addressable constants are installed in each OPERABLE CPC.
- (10) In accordance with the Surveillance Frequency Control Program and following maintenance or adjustment of the reactor trip breakers, the CHANNEL FUNCTIONAL TEST shall include independent verification of the undervoltage trip function and the shunt trip function.
- (11) The CHANNEL FUNCTIONAL TEST shall be scheduled and performed such that the Reactor Trip Breakers (RTBs) are tested at least every 6 weeks to accommodate the appropriate vendor recommended interval for cycling of each RTB.

Replace with
"DELETED"

ADMINISTRATIVE CONTROLS

6.6 NOT USED

6.7 NOT USED

6.8 PROCEDURES AND PROGRAMS

6.8.1 Written procedures shall be established, implemented and maintained covering the activities referenced below:

- a. The applicable procedures recommended in Appendix A of Regulatory Guide 1.33, Revision 2, February 1978 and Emergency Operating Procedures required to implement the requirements of NUREG-0737 and NUREG-0737, Supplement 1, as stated in Generic Letter 82-33.
- b. Refueling operations.
- c. Surveillance and test activities of safety-related equipment.
- d. Not used.
- e. Not used.
- f. Not used.
- g. Modification of Core Protection Calculator (CPC) Addressable Constants, including independent verification of modified constants.

Replace with INSERT K

NOTES:

- (1) Modification to the CPC addressable constants based on information obtained through the Plant Computer - CPC data link shall not be made without prior approval of the On-Site Safety Review Committee.
- (2) Modifications to the CPC software (including algorithm changes and changes in fuel cycle specific data) shall be performed in accordance with the most recent version of CEN-39(A)-P, "CPC Protection Algorithm Software Change Procedure," that has been determined to be applicable to the facility. Additions or deletions to CPC Addressable Constants or changes to Addressable Constant software limits values shall not be implemented without prior NRC approval.

- h. Administrative procedures implementing the overtime guidelines of Specification 6.2.2e., including provisions for documentation of deviations.
- i. PROCESS CONTROL PROGRAM implementation.

INSERT K

g. Modification of core protection calculator (CPC) addressable constants.

These procedures shall include provisions to ensure that sufficient margin is maintained in CPC type I addressable constants to avoid excessive operator interaction with CPCs during reactor operation.

Modifications to the CPC software (including changes of algorithms and fuel cycle specific data) shall be performed in accordance with the most recent version of WCAP-16096-P-A, "CPC Protection Algorithm Software Change Procedure," which has been determined to be applicable to the facility. Additions or deletions to CPC addressable constants or changes to addressable constant software limit values shall not be implemented without prior NRC approval.

ADMINISTRATIVE CONTROLSINDUSTRIAL SURVEY OF TOXIC OR HAZARDOUS CHEMICALS REPORT

6.9.1.9 Surveys and analyses of major industries in the vicinity of Waterford 3 which could have significant inventories of toxic chemicals onsite to determine impact on safety shall be performed and submitted to the Commission at least once every 4 years.

6.9.1.10 A survey of major pipelines (≥ 4 inches) within a 2-mile radius of Waterford 3, which contain explosive or flammable materials and may represent a hazard to Waterford 3, including scaled engineering drawings or maps which indicate the pipeline locations, shall be performed and submitted to the Commission at least once every 4 years.

CORE OPERATING LIMITS REPORT COLR

6.9.1.11 Core operating limits shall be established and documented in the CORE OPERATING LIMITS REPORT prior to each reload cycle or any remaining part of a reload cycle for the following:

- 3.1.1.1 SHUTDOWN MARGIN – ANY CEA WITHDRAWN
- 3.1.1.2 SHUTDOWN MARGIN – ALL CEAS FULLY INSERTED
- 3.1.1.3 MODERATOR TEMPERATURE COEFFICIENT
- 3.1.2.9 BORON DILUTION
- 3.1.3.1 CEA POSITION
- 3.1.3.6 REGULATING AND GROUP P CEA INSERTION LIMITS
- 3.2.1 LINEAR HEAT RATE
- 3.2.3 AZIMUTHAL POWER TILT – T_q
- 3.2.4 DNBR MARGIN
- 3.2.7 AXIAL SHAPE INDEX
- 3.6.1.5 AIR TEMPERATURE, CONTAINMENT (Linear Heat Rate, 3.2.1)
- 3.9.1 BORON CONCENTRATION

6.9.1.11.1 The analytical methods used to determine the core operating limits shall be those previously reviewed and approved by the NRC as follows:

- 1) "Qualification of the PHOENIX-P/ANC Nuclear Design System for Pressurized Water Reactor Cores" (WCAP-11596-P-A), "ANC: A Westinghouse Advanced Nodal Computer Code" (WCAP-10965-P-A), and "ANC: A Westinghouse Advanced Nodal Computer Code: Enhancements to ANC Rod Power Recovery" (WCAP-10965-P-A Addendum 1) (Methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margins, 3.1.1.3 for MTC, 3.1.3.6 for Regulating and Group P CEA Insertion Limits, 3.2.4.b for DNBR Margin, 3.1.2.9 for Boron Dilution, and 3.9.1 for Boron Concentrations).
- 2) "CE Method for Control Element Assembly Ejection Analysis," CENPD-0190-A (Methodology for Specification 3.1.3.6 for Regulating and Group P CEA Insertion Limits and 3.2.3 for Azimuthal Power Tilt).

Replace "3.2.4.b"
with "3.2.4.a.2"

ADMINISTRATIVE CONTROLSCORE OPERATING LIMITS REPORT COLR (Continued)

- 3) "Modified Statistical Combination of Uncertainties, CEN-356(V)-P-A, Revision 01-P-A (Methodology for Specification 3.2.4.c and 3.2.4.d for DNBR Margin and 3.2.7 for ASI).

Replace "3.2.4.c" with "3.2.4.b.1"

Replace "3.2.4.d" with "3.2.4.b.2"
- 4) "Calculative Methods for the CE Large Break LOCA Evaluation Model," CENPD-132-P (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 5) "Calculative Methods for the CE Small Break LOCA Evaluation Model," CENPD-137-P (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 6) "Technical Manual for the CENTS Code," WCAP-15996-P-A, Rev. 1 (Methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margin, 3.1.1.3 for MTC, 3.1.3.1 for CEA Position, 3.1.3.6 for Regulating and Group P Insertion Limits, and 3.2.4.b for DNBR Margin).
- 7) "Implementation of ZIRLO Material Cladding in CE Nuclear Power Fuel Assembly Designs," CENPD-404-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).

Replace "3.2.4.b" with "3.2.4.a.2"
- 8) "Qualification of the Two-Dimensional Transport Code PARAGON," WCAP-16045-P-A (may be used as a replacement for the PHOENIX-P lattice code as the methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margins, 3.1.1.3 for MTC, 3.1.3.6 for Regulating and Group P CEA Insertion Limits, 3.2.4.b for DNBR Margin, 3.1.2.9 for Boron Dilution, and 3.9.1 for Boron Concentrations).
- 9) "Implementation of Zirconium Diboride Burnable Absorber Coatings in CE Nuclear Power Fuel Assembly Designs," WCAP-16072-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Tilt, and 3.2.7 for ASI).
- 10) "CE 16 x 16 Next Generation Fuel Core Reference Report," WCAP-16500-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, 3.2.4.b, 3.2.4.c and 3.2.4.d for DNBR Margin, and 3.2.7 for ASI).
- 11) "Optimized ZIRLO™," WCAP-12610-P-A and CENPD-404-P-A Addendum 1-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).

Replace with "3.2.4.a.2, 3.2.4.b.1 and 3.2.4.b.2"
- 12) "Westinghouse Correlations WSSV and WSSV-T for Predicting Critical Heat Flux in Rod Bundles with Side-Supported Mixing Vanes," WCAP- 16523-P-A (Methodology for Specification 3.2.4.b, 3.2.4.c and 3.2.4.d for DNBR Margin).
- 13) "ABB Critical Heat Flux Correlations for PWR Fuel," CENPD-387-P-A (Methodology for Specification 3.2.4.b, 3.2.4.c and 3.2.4.d for DNBR Margin and 3.2.7 for ASI).

Enclosure, Attachment 2

W3F1-2020-0040

DRAFT
Clean Technical Specification Pages

TS Pages

2-3
3/4 1-20
3/4 2-6a
3/4 3-1
3/4 3-2
3/4 3-3
3/4 3-4
3/4 3-6
3/4 3-7
3/4 3-7a (new)
3/4 3-10
3/4 3-11
3/4 3-12a
3/4 10-2
6-14
6-20
6-20a

TABLE 2.2-1
REACTOR PROTECTIVE INSTRUMENTATION TRIP SETPOINT LIMITS

<u>FUNCTIONAL UNIT</u>	<u>TRIP SETPOINT</u>	<u>ALLOWABLE VALUES</u>
1. Manual Reactor Trip	Not Applicable	Not Applicable
2. Linear Power Level - High		
Four Reactor Coolant Pumps Operating	≤ 108% of RATED THERMAL POWER	≤ 108.76% of RATED THERMAL POWER
3. Logarithmic Power Level - High (1)	≤ 0.257% of RATED THERMAL POWER (6)	≤ 0.280% of RATED THERMAL POWER (6)
4. Pressurizer Pressure - High	≤ 2350 psia	≤ 2359 psia
5. Pressurizer Pressure - Low	≥ 1684 psia (2)	≥ 1649.7 psia (2)
6. Containment Pressure - High	≤ 17.1 psia	≤ 17.4 psia
7. Steam Generator Pressure - Low	≥ 666 psia (3)	≥ 652.4 psia (3)
8. Steam Generator Level - Low	≥ 27.4% (4)	≥ 26.48% (4)
9. Core Protection Calculators		
a. Local Power Density - High	≤ 21.0 kW/ft (5)	≤ 21.0 kW/ft (5)
b. DNBR - Low	≥ 1.26 (5)	≥ 1.26 (5)
10. DELETED		
11. DELETED		
12. Reactor Protection System Logic	Not Applicable	Not Applicable
13. Reactor Trip Breakers	Not Applicable	Not Applicable
14. DELETED		
15. DELETED		
16. Reactor Coolant Flow - Low	≥ 19.00 psid (7)	≥ 18.47 psid (7)

W3F1-2020-0040
ATTACHMENT 2,
DRAFT REVISED (CLEAN)
TECHNICAL SPECIFICATION
PAGES

REACTIVITY CONTROL SYSTEMS

SURVEILLANCE REQUIREMENTS

4.1.3.1.1 The position of each CEA shall be determined to be within 7 inches (indicated position) of all other CEAs in its group in accordance with the Surveillance Frequency Control Program.

4.1.3.1.2 Each CEA not fully inserted in the core shall be determined to be OPERABLE by movement of at least 5 inches in any one direction in accordance with the Surveillance Frequency Control Program.

POWER DISTRIBUTION LIMITS

3/4.2.4 DNBR MARGIN

LIMITING CONDITION FOR OPERATION

3.2.4 The DNBR margin shall be maintained by one of the following methods:

- a. Core Operating Limit Supervisory System (COLSS) in Service:
 1. Maintaining COLSS calculated core power less than or equal to COLSS calculated core power operating limit based on DNBR when at least one Control Element Assembly Calculator (CEAC) is OPERABLE in each OPERABLE Core Protection Calculator (CPC) channel; or
 2. Maintaining COLSS calculated core power less than or equal to COLSS Calculated core power operating limit based on DNBR decreased by the amount specified in the COLR when the CEAC requirements of LCO 3.2.4.a.1 are not met.
- b. COLSS Out of Service
 1. Operating within the region of acceptable operation specified in the COLR using any OPERABLE Core Protection Calculator (CPC) channel when at least one Control Element Assembly Calculator (CEAC) is OPERABLE in each OPERABLE CPC channel; or
 2. Operating within the region of acceptable operation specified in the COLR using any OPERABLE Core Protection Calculator (CPC) channel (with both CEACS inoperable) when the CEAC requirements of LCO 3.2.4.b.1 are not met.

APPLICABILITY: MODE 1 above 20% of RATED THERMAL POWER.

ACTION:

- a. With the DNBR limit not being maintained as indicated by COLSS calculated core power exceeding the COLSS calculated core power operating limit based on DNBR, within 15 minutes initiate corrective action to reduce the DNBR to within the limits and either:
 1. Restore the DNBR to within its limits within 1 hour, or
 2. Reduce THERMAL POWER to less than or equal to 20% of RATED THERMAL POWER within the next 6 hours.

3/4.3 INSTRUMENTATION

3/4.3.1 REACTOR PROTECTIVE INSTRUMENTATION

LIMITING CONDITION FOR OPERATION

3.3.1 As a minimum, the reactor protective instrumentation channels and bypasses of Table 3.3-1 shall be OPERABLE.

APPLICABILITY: As shown in Table 3.3-1.

ACTION:

As shown in Table 3.3-1.

SURVEILLANCE REQUIREMENTS

4.3.1.1 Each reactor protective instrumentation channel shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-1.

4.3.1.2 The logic for the bypasses shall be demonstrated OPERABLE prior to each reactor startup unless performed during the preceding 92 days. The total bypass function shall be demonstrated OPERABLE in accordance with the Surveillance Frequency Control Program during CHANNEL CALIBRATION testing of each channel affected by bypass operation.

4.3.1.3 The REACTOR TRIP SYSTEM RESPONSE TIME of each reactor trip function shall be demonstrated to be within its limit in accordance with the Surveillance Frequency Control Program. Neutron detectors, Core Protection Calculators, and CEACs are exempt from response time testing. Each test shall include at least one channel per function such that all channels are tested as shown in the "Total No. of Channels" column of Table 3.3-1.

4.3.1.4 DELETED

4.3.1.5 DELETED

4.3.1.6 DELETED

4.3.1.7 Perform a test on the CPC DNBR/LPD trip output through the contact interface to the PPS in accordance with the Surveillance Frequency Control Program.

**W3F1-2020-0040
ATTACHMENT 2,
DRAFT REVISED (CLEAN)
TECHNICAL SPECIFICATION
PAGES**

THIS PAGE HAS BEEN DELETED.

I

TABLE 3.3-1
REACTOR PROTECTIVE INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
1. Manual Reactor Trip	2 sets of 2	1 set of 2	2 sets of 2	1, 2	1
2. Linear Power Level - High	2 sets of 2	1 set of 2	2 sets of 2	3*, 4*, 5*	8
3. Logarithmic Power Level-High	4	2	3	1, 2	2#, 3#
a. Startup and Operating	4	2(a)(d)	3	2**	2#, 3#
b. Shutdown	4	2	3	3*, 4*, 5* 8	
4. Pressurizer Pressure - High	4	0	2	3, 4, 5	4
5. Pressurizer Pressure - Low	4	2	3	1, 2	2#, 3#
6. Containment Pressure - High	4	2(b)	3	1, 2	2#, 3#
7. Steam Generator Pressure - Low	4	2	3	1, 2	2#, 3#
8. Steam Generator Level – Low	4/SG	2/SG	3/SG	1, 2	2#, 3#
9. Core Protection Calculators	4/SG	2/SG	3/SG	1, 2	2#, 3#
a. Local Power Density – High	4	2(c)(d)(h)	3	1, 2	2#, 3#
b. DNBR – Low					
c. CEA Calculators	4(g)(i)	2(e)	3(g)(i)	1, 2	6
10. DELETED					
11. DELETED					
12. Reactor Protection System Logic	4	2	3	1, 2	5
13. Reactor Trip Breakers	4	2(f)	4	3*, 4*, 5*	8
				1, 2	5
				3*, 4*, 5*	8
14. DELETED					
15. DELETED					
16. Reactor Coolant Flow - Low	4/SG	2/SG(c)	3/SG	1, 2	2#, 3#

TABLE 3.3-1 (Continued)

TABLE NOTATION

*With the protective system trip breakers in the closed position, the CEA drive system capable of CEA withdrawal, and fuel in the reactor vessel.

#The provisions of Specification 3.0.4 are not applicable.

**Not applicable above a logarithmic power of 10^{-4} % RATED THERMAL POWER.

- (a) The operating bypass may be enabled above the 10^{-4} % bistable setpoint and shall be capable of automatic removal whenever the operating bypass is enabled and logarithmic power is below the 10^{-4} % bistable setpoint. Trip may be manually bypassed during physics testing pursuant to Special Test Exception 3.10.3.
- (b) Trip may be manually bypassed below 400 psia; bypass shall be automatically removed whenever pressurizer pressure is greater than or equal to 500 psia.
- (c) The operating bypass may be enabled below the 10^{-4} % bistable setpoint and shall be capable of automatic removal whenever the operating bypass is enabled and logarithmic power is above the 10^{-4} % bistable setpoint. During testing pursuant to Special Test Exception 3.10.3, trip may be manually bypassed below 5% of RATED THERMAL POWER; the 10^{-4} % bistable setpoint may be changed to less than or equal 5% RATED THERMAL POWER to perform the automatic removal function.
- (d) Trip may be bypassed during testing pursuant to Special Test Exception 3.10.3.
- (e) See Special Test Exception 3.10.2.
- (f) Each channel shall be comprised of two trip breakers; actual trip logic shall be one-out-of-two taken twice.
- (g) There are two CEACs in each CPC channel.
- (h) Both Local Power Density-High and DNBR-Low must be OPERABLE for a CPC channel to be OPERABLE.
- (i) Both CEACs in an inoperable CPC channel are also inoperable.

TABLE 3.3-1 (Continued)

ACTION STATEMENTS

2.	Pressurizer Pressure - High	Pressurizer Pressure - High Local Power Density - High DNBR - Low
3.	Containment Pressure - (RPS) High	Containment Pressure - High Containment Pressure - High (ESF)
4.	Steam Generator Pressure - Low	Steam Generator Pressure - Low Steam Generator ΔP 1 and 2 (EFAS 1 and 2)
5.	Steam Generator Level	Steam Generator Level - Low Steam Generator ΔP (EFAS)
6.	Core Protection Calculator	Local Power Density - High DNBR - Low
7.	Logarithmic Power	Logarithmic Power Level - High Local Power Density - High ⁽¹⁾ DNBR - Low ⁽¹⁾ Reactor Coolant Flow - Low ⁽¹⁾

STARTUP and/or POWER OPERATION may continue until the performance of the next required CHANNEL FUNCTIONAL TEST. Subsequent STARTUP and/or POWER OPERATION may continue if one channel is restored to OPERABLE status and the provisions of ACTION 2 are satisfied.

ACTION 4 - With the number of channels OPERABLE one less than required by the Minimum Channels OPERABLE requirement, suspend all operations involving positive reactivity changes. *

ACTION 5 - With the number of channels OPERABLE one less those required by the Minimum Channels OPERABLE requirement, STARTUP and/or POWER OPERATION may continue provided the reactor trip breakers of the inoperable channel are placed in the tripped condition within 1 hour; otherwise, be in at least HOT STANDBY within 6 hours; however, one channel may be bypassed for up to 1 hour for surveillance testing per Specification 4.3.1.1.

* Limited plant cooldown or boron dilution is allowed provided the change is accounted for in the calculated SHUTDOWN MARGIN.

⁽¹⁾ With the operating bypass enabled.

TABLE 3.3-1 (Continued)

ACTION STATEMENTS

ACTION 6 - Separate Actions may be entered for each CPC channel.

- a. With one CEAC inoperable in 1 or 2 CPC channels, either declare the associated CPC channel(s) inoperable; or set the "RSPT/CEAC Inoperable" addressable constant to the inoperable status within 4 hours.
- b. With one CEAC inoperable in 3 or 4 CPC channels, either declare the associated CPC channel(s) inoperable; or, operation may continue provided that:
 1. Within 4 hours the "RSPT/CEAC Inoperable" addressable constant(s) is set to the inoperable status.
 2. Operation may continue for up to 7 days provided that the position of each CEA is verified to be aligned with all other CEAs in its group by performing surveillance requirement 4.1.3.1.1 at least once per 4 hours.
 3. Operation may continue after 7 days provided that Actions 6.c.1, 6.c.2, and 6.c.3 are met.
- c. With both CEACS inoperable in any CPC channel, either declare the associated CPC channel(s) inoperable; or, operation may continue provided that:
 1. Within 4 hours the DNBR margin required by Specification 3.2.4a (COLSS in service) or 3.2.4b (COLSS out of service) is satisfied and the Reactor Power Cutback System is disabled, and
 2. Within 4 hours:
 - a) All CEA groups are withdrawn to and subsequently maintained at the "Full Out" position, except during surveillance testing pursuant to the requirements of Specification 4.1.3.1.2 or for control when CEA group 6 may be inserted no further than 127.5 inches withdrawn.
 - b) The "RSPT/CEAC Inoperable" addressable constant in the CPCs is set to the inoperable status.
 - c) The Control Element Drive Mechanism Control System (CEDMCS) is placed in and subsequently maintained in the "Off" mode except during CEA motion permitted by a) above, when the CEDMCS may be operated in either the "Manual Group" or "Manual Individual" mode.
 3. At least once per 4 hours, all CEAs are verified fully withdrawn except during surveillance testing pursuant to Specification 4.1.3.1.2 or during insertion of CEA group 6 as permitted by 2.a) above, then perform surveillance requirement 4.1.3.1.1 at least once per 4 hours.

ACTION 7 - DELETED

ACTION 8 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement restore the inoperable channel to OPERABLE status within 48 hours or open the reactor trip breakers within the next hour.

TABLE 4.3-1

REACTOR PROTECTIVE INSTRUMENTATION SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	CHANNEL FUNCTIONAL TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
1. Manual Reactor Trip	N.A.	N.A.	SFCP and S/U(1)	1, 2, 3*, 4*, 5*
2. Linear Power Level - High	SFCP	SFCP(2,4),SFCP (3,4), SFCP (4)	SFCP	1, 2
3. Logarithmic Power Level - High	SFCP	SFCP(4)	SFCP and S/U(1)	2#, 3, 4, 5
4. Pressurizer Pressure - High	SFCP	SFCP	SFCP	1, 2
5. Pressurizer Pressure - Low	SFCP	SFCP	SFCP	1, 2
6. Containment Pressure - High	SFCP	SFCP	SFCP	1, 2
7. Steam Generator Pressure - Low	SFCP	SFCP	SFCP	1, 2
8. Steam Generator Level - Low	SFCP	SFCP	SFCP	1, 2
9. Core Protection Calculators	SFCP	SFCP(2,4),SFCP(4,5)	None	1, 2
a. Local Power Density - High	SFCP	SFCP(2,4),SFCP(4,5)	None	1, 2
b. DNBR - Low	SFCP	SFCP(7), SFCP(2,4), SFCP(8), SFCP(4,5)	None	1, 2
c. CEA Calculators	SFCP	SFCP	None	1, 2
10. DELETED				
11. DELETED				
12. Reactor Protection System Logic	N.A.	N.A.	SFCP(11) and S/U(1)	1, 2, 3*, 4*, 5*

TABLE 4.3-1 (Continued)

REACTOR PROTECTIVE INSTRUMENTATION SURVEILLANCE REQUIREMENTS

<u>FUNCTIONAL UNIT</u>	<u>CHANNEL CHECK</u>	<u>CHANNEL CALIBRATION</u>	<u>CHANNEL FUNCTIONAL TEST</u>	<u>MODES FOR WHICH SURVEILLANCE IS REQUIRED</u>
13. Reactor Trip Breakers	N.A.	N.A.	SFCP(10,11), S/U(1)	1, 2, 3*, 4*, 5*
14. DELETED				
15. DELETED				
16. Reactor Coolant Flow - Low	SFCP	SFCP	SFCP	1, 2

TABLE 4.3-1 (Continued)

TABLE NOTATIONS (Continued)

- (3) Above 15% of RATED THERMAL POWER, verify that the linear power subchannel gains of the excore detectors are consistent with the values used to establish the shape annealing matrix elements in the Core Protection Calculators.
- (4) Neutron detectors may be excluded from CHANNEL CALIBRATION.
- (5) After each fuel loading and prior to exceeding 70% of RATED THERMAL POWER, the incore detectors shall be used to determine or verify acceptable values for the shape annealing matrix elements used in the Core Protection Calculators.
- (6) DELETED
- (7) Above 70% of RATED THERMAL POWER, verify that the total RCS flow rate as indicated by each CPC is less than or equal to the actual RCS total flow rate determined by either using the reactor coolant pump differential pressure instrumentation or by calorimetric calculations and if necessary, adjust the CPC addressable constant flow co-efficients such that each CPC indicated flow is less than or equal to the actual flow rate. The flow measurement uncertainty is included in the BERR1 term in the CPC and is equal to or greater than 4%.
- (8) Above 70% of RATED THERMAL POWER, verify that the total RCS flow rate as indicated by each CPC is less than or equal to the actual RCS total flow rate determined by calorimetric calculations.
- (9) DELETED
- (10) In accordance with the Surveillance Frequency Control Program and following maintenance or adjustment of the reactor trip breakers, the CHANNEL FUNCTIONAL TEST shall include independent verification of the undervoltage trip function and the shunt trip function.
- (11) The CHANNEL FUNCTIONAL TEST shall be scheduled and performed such that the Reactor Trip Breakers (RTBs) are tested at least every 6 weeks to accommodate the appropriate vendor recommended interval for cycling of each RTB

ADMINISTRATIVE CONTROLS

6.6 NOT USED

6.7 NOT USED

6.8 PROCEDURES AND PROGRAMS

6.8.1 Written procedures shall be established, implemented and maintained covering the activities referenced below:

- a. The applicable procedures recommended in Appendix A of Regulatory Guide 1.33, Revision 2, February 1978 and Emergency Operating Procedures required to implement the requirements of NUREG-0737 and NUREG-0737, Supplement 1, as stated in Generic Letter 82-33.
- b. Refueling operations.
- c. Surveillance and test activities of safety-related equipment.
- d. Not used.
- e. Not used.
- f. Not used.
- g. Modification of core protection calculator (CPC) addressable constants.

These procedures shall include provisions to ensure sufficient margin is maintained in CPC type I addressable constants to avoid excessive operator interaction with CPCs during reactor operation.

Modifications to the CPC software (including changes of algorithms and fuel cycle specific data) shall be performed in accordance with the most recent version of WCAP-16096-P-A, "CPC Protection Algorithm Software Change Procedure," which has been determined to be applicable to the facility. Additions or deletions to CPC addressable constants or changes to addressable constant software limit values shall not be implemented without prior NRC approval.

- h. Administrative procedures implementing the overtime guidelines of Specification 6.2.2e., including provisions for documentation of deviations.
- i. PROCESS CONTROL PROGRAM implementation.

ADMINISTRATIVE CONTROLS

INDUSTRIAL SURVEY OF TOXIC OR HAZARDOUS CHEMICALS REPORT

6.9.1.9 Surveys and analyses of major industries in the vicinity of Waterford 3 which could have significant inventories of toxic chemicals onsite to determine impact on safety shall be performed and submitted to the Commission at least once every 4 years.

6.9.1.10 A survey of major pipelines (≥ 4 inches) within a 2-mile radius of Waterford 3, which contain explosive or flammable materials and may represent a hazard to Waterford 3, including scaled engineering drawings or maps which indicate the pipeline locations, shall be performed and submitted to the Commission at least once every 4 years.

CORE OPERATING LIMITS REPORT COLR

6.9.1.11 Core operating limits shall be established and documented in the CORE OPERATING LIMITS REPORT prior to each reload cycle or any remaining part of a reload cycle for the following:

- 3.1.1.1 SHUTDOWN MARGIN – ANY CEA WITHDRAWN
- 3.1.1.2 SHUTDOWN MARGIN – ALL CEAS FULLY INSERTED
- 3.1.1.3 MODERATOR TEMPERATURE COEFFICIENT
- 3.1.2.9 BORON DILUTION
- 3.1.3.1 CEA POSITION
- 3.1.3.6 REGULATING AND GROUP P CEA INSERTION LIMITS
- 3.2.1 LINEAR HEAT RATE
- 3.2.3 AZIMUTHAL POWER TILT – T_q
- 3.2.4 DNBR MARGIN
- 3.2.7 AXIAL SHAPE INDEX
- 3.6.1.5 AIR TEMPERATURE, CONTAINMENT (Linear Heat Rate, 3.2.1)
- 3.9.1 BORON CONCENTRATION

6.9.1.11.1 The analytical methods used to determine the core operating limits shall be those previously reviewed and approved by the NRC as follows:

- 1) "Qualification of the PHOENIX-P/ANC Nuclear Design System for Pressurized Water Reactor Cores" (WCAP-11596-P-A), "ANC: A Westinghouse Advanced Nodal Computer Code" (WCAP-10965-P-A), and "ANC: A Westinghouse Advanced Nodal Computer Code: Enhancements to ANC Rod Power Recovery" (WCAP-10965-P-A Addendum 1) (Methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margins, 3.1.1.3 for MTC, 3.1.3.6 for Regulating and Group P CEA Insertion Limits, 3.2.4.a.2 for DNBR Margin, 3.1.2.9 for Boron Dilution, and 3.9.1 for Boron Concentrations).
- 2) "CE Method for Control Element Assembly Ejection Analysis," CENPD-0190-A (Methodology for Specification 3.1.3.6 for Regulating and Group P CEA Insertion Limits and 3.2.3 for Azimuthal Power Tilt).

ADMINISTRATIVE CONTROLS

CORE OPERATING LIMITS REPORT COLR (Continued)

- 3) "Modified Statistical Combination of Uncertainties, CEN-356(V)-P-A, Revision 01-P-A (Methodology for Specification 3.2.4.b.1 and 3.2.4.b.2 for DNBR Margin and 3.2.7 for ASI).
- 4) "Calculative Methods for the CE Large Break LOCA Evaluation Model," CENPD-132-P (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 5) "Calculative Methods for the CE Small Break LOCA Evaluation Model," CENPD-137-P (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 6) "Technical Manual for the CENTS Code," WCAP-15996-P-A, Rev. 1 (Methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margin, 3.1.1.3 for MTC, 3.1.3.1 for CEA Position, 3.1.3.6 for Regulating and Group P Insertion Limits, and 3.2.4.a.2 for DNBR Margin).
- 7) "Implementation of ZIRLO Material Cladding in CE Nuclear Power Fuel Assembly Designs," CENPD-404-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 8) "Qualification of the Two-Dimensional Transport Code PARAGON," WCAP-16045-P-A (may be used as a replacement for the PHOENIX-P lattice code as the methodology for Specifications 3.1.1.1 and 3.1.1.2 for Shutdown Margins, 3.1.1.3 for MTC, 3.1.3.6 for Regulating and Group P CEA Insertion Limits, 3.2.4.a.2 for DNBR Margin, 3.1.2.9 for Boron Dilution, and 3.9.1 for Boron Concentrations).
- 9) "Implementation of Zirconium Diboride Burnable Absorber Coatings in CE Nuclear Power Fuel Assembly Designs," WCAP-16072-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Tilt, and 3.2.7 for ASI).
- 10) "CE 16 x 16 Next Generation Fuel Core Reference Report," WCAP-16500-P-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, 3.2.4.a.2, 3.2.4.b.1 and 3.2.4.b.2 for DNBR Margin, and 3.2.7 for ASI).
- 11) "Optimized ZIRLO™," WCAP-12610-P-A and CENPD-404-P-A Addendum 1-A (Methodology for Specification 3.1.1.3 for MTC, 3.2.1 for Linear Heat Rate, 3.2.3 for Azimuthal Power Tilt, and 3.2.7 for ASI).
- 12) "Westinghouse Correlations WSSV and WSSV-T for Predicting Critical Heat Flux in Rod Bundles with Side-Supported Mixing Vanes," WCAP- 16523-P-A (Methodology for Specification 3.2.4.a.2, 3.2.4.b.1 and 3.2.4.b.2 for DNBR Margin).
- 13) "ABB Critical Heat Flux Correlations for PWR Fuel," CENPD-387-P-A (Methodology for Specification 3.2.4.a.2, 3.2.4.b.1 and 3.2.4.b.2 for DNBR Margin and 3.2.7 for ASI).

Enclosure, Attachment 3

W3F1-2020-0040

DRAFT
Technical Specification Bases Page Markups
(Provided for Information Only)

TS Bases Pages

B 2-2a
B 3/4 3-1
B 3/4 3-1c
b 3/4 3-1d

SAFETY LIMITS AND LIMITING SAFETY SYSTEM SETTINGS

BASES

2.2.1 REACTOR TRIP SETPOINTS (Continued)

A Total Loop Uncertainty (TLU) is calculated for each RPS instrument channel. The Trip setpoint is determined by adding or subtracting the TLU from the Analytical Limit (add TLU for decreasing process value; subtract TLU for increasing process value). The Allowable Value is determined by adding an allowance between the Trip Setpoint and the Analytical Limit to account for RPS cabinet Periodic Test Errors (PTE) which are present during a CHANNEL FUNCTIONAL TEST. PTE combines RPS cabinet reference accuracy, calibration equipment errors (M&TE), and RPS cabinet bistable drift. Periodic testing assures that actual setpoints are within their Allowable Values. A channel is inoperable if its actual setpoint is not within its Allowable Value and corrective action must be taken. Operation with a trip set less conservative than its Trip Setpoint but within its specified Allowable Value is acceptable on the basis that the difference between each Trip Setpoint and the Allowable Value is equal to or less than the PTE allowance assumed for each trip in the safety analyses.

>(EC-18510, Ch. 64)

The DNBR - Low and Local Power Density - High are digitally generated trip setpoints based on Limiting Safety System Settings of 1.26 and 21.0 kW/ft, respectively. Since these trips are digitally generated by the Core Protection Calculators, the trip values are not subject to drifts common to trips generated by analog type equipment. The Allowable Values for these trips are therefore the same as the Trip Setpoints. The CPC power adjustment addressable constant BERR1 is used such that the CPC DNBR trip setpoint of 1.26 using the CE-1 critical heat flux correlation assures that the bounding safety limit DNBR of 1.24 for the WSSV-T and ABB-NV correlations will not be exceeded during normal operations and AOOs.

<(EC-18510, Ch. 64)

To maintain the margins of safety assumed in the safety analyses, the calculations of the trip variables for the DNBR - Low and Local Power Density -High trips include the measurement, calculational and processor uncertainties and dynamic allowances as defined in the latest applicable revision of CEN-305-P, "Functional Design Requirements for a Core Protection Calculator" and; CEN-304-P, "Functional Design Requirements for a Control Element Assembly Calculator."

>(EC-26338, Ch. 67)

The Core Protection Calculator, High Logarithmic Power (HLP), and Reactor Coolant System Flow use a single bistable to initiate both the permissive and automatic operating bypass removal functions. A single bistable cannot both energize and de-energize at a single, discrete value due to hysteresis. The CPC automatic bypass removal and permissive for the HLP trip bypass occur at the bistable setpoint (nominally 10^{-4} % power). However, the HLP automatic bypass removal and permissive for CPC trip bypass occur at the reset value of the bistable. Also, note if the bistable setpoint is changed as part of the Special Test Exception 3.10.3, the same dead band transition is applicable.

<(EC-26338, Ch. 67)

Replace with
INSERT A

**W3F1-2020-0040
ATTACHMENT 3,
DRAFT TECHNICAL SPECIFICATION BASES PAGE MARKUPS
FOR INFORMATION ONLY**

INSERT A

applicable revisions of 00000-ICE-30158, "System Requirements Specification for the Common Q Core Protection Calculator System," Appendix A, as augmented by WNA-DS-04517-CWTR3, "System Requirements Specification for the Core Protection Calculator System," Appendix A.

3/4.3 INSTRUMENTATION


BASES

3/4.3.1 and 3/4.3.2 REACTOR PROTECTIVE AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEMS INSTRUMENTATION

The OPERABILITY of the Reactor Protective and Engineered Safety Features Actuation Systems instrumentation and bypasses ensures that (1) the associated Engineered Safety Features Actuation action and/or reactor trip will be initiated when the parameter monitored by each channel or combination thereof reaches its setpoint, (2) the specified coincidence logic is maintained, (3) sufficient redundancy is maintained to permit a channel to be out of service for testing or maintenance, and (4) sufficient system functional capability is available from diverse parameters.

The OPERABILITY of these systems is required to provide the overall reliability, redundancy, and diversity assumed available in the facility design for the protection and mitigation of accident and transient conditions. The integrated operation of each of these systems is consistent with the assumptions used in the safety analyses.

Replace with
INSERT B

 The redundancy design of the Control Element Assembly Calculators (CEAC) provides reactor protection in the event one or both CEACs become inoperable. If one CEAC is in test or inoperable, verification of CEA position is performed at least every 4 hours. If the second CEAC fails, the CPCs will use DNBR and LPD penalty factors to restrict reactor operation to some maximum fraction of RATED THERMAL POWER. If this maximum fraction is exceeded, a reactor trip will occur.

→(LBDCR-14-003 Ch.78)

Table 3.3-1 ACTION 4 requires the suspension of all operations involving positive reactivity changes with the number of channels OPERABLE one less than required by the Minimum Channels OPERABLE requirement. With one of the two required minimum operable channels inoperable, it may not be possible to perform a CHANNEL CHECK to verify the sole remaining required channel is OPERABLE. Therefore, with one or more required channels inoperable, the logarithmic power monitoring function cannot be reliably performed. Consequently, the Required Actions are the same for one required channel inoperable or more than one required channel inoperable.

The (*) for ACTION 4 was added to allow small positive reactivity additions (i.e. temperature or boron fluctuations) necessary to maintain plant conditions. These activities may result in addition to the RCS of water at a temperature different than that of the RCS, may result in slight RCS temperature changes, and may require inventory makeup from sources that are at boron concentrations less than RCS concentration. Depending on core loading and time in core life, raising temperature may add positive reactivity and should be minimized when possible. This allowance is intended to give Operations flexibility to perform actions required to maintain plant conditions but should not be utilized to significantly change plant conditions.

←(LBDCR-14-003 Ch.78)

INSERT B

The redundancy design of the Control Element Assembly Calculators (CEAC) in each CPC channel (2 CEACs per CPC channel, 8 total CEACs) maintains CPC channel operability as long as one CEAC is OPERABLE in that CPC channel. Action 6c, discussed below, provides actions to maintain a CPC channel OPERABLE with both CEACs inoperable. At least 2 CPC channels must be OPERABLE to maintain reactor protection. Multiple CEACs may be Inoperable in different CPC channels. Actions associated with an inoperable CEAC ensure the affected CPC channel recognizes the condition. Separate actions may be entered for each CPC channel.

ACTION 6 provides requirements depending on the quantity and combination of inoperable CEACs across the four CPC channels. Action 6a allows for up to two CPC channels to have any one of its two CEAC channels inoperable. The affected CPC channels maintain full functionality as long as the failed CEAC is recognized by the CPC channel via the addressable constant setting.

Action 6b requires additional measures when three or four CPC channels are operating with only a single OPERABLE CEAC in each channel. With 3 or 4 CPC channels operating with only a single OPERABLE CEAC, the CEA position verifications ensure the assumptions for using the position values of the target CEAs in each channel remain valid.

Action 6c allows continued operation with both CEACs inoperable in any CPC channel(s) by imposing operational restrictions on CEA position, along with the periodic CEA position verification.

3/4 INSTRUMENTATION

BASES (Cont'd)

3/4.3.1 and 3/4.3.2 REACTOR PROTECTIVE AND ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION (Continued)

When one of the inoperable channels is restored to OPERABLE status, subsequent operation in the applicable MODE(S) may continue in accordance with the provisions of ACTION 19.

Because of the interaction between process measurement circuits and associated functional units as listed in the ACTIONS 19 and 20, placement of an inoperable channel of Steam Generator Level in the bypass or trip condition results in corresponding placements of Steam Generator ΔP (EFAS) instrumentation. Depending on the number of applicable inoperable channels, the provisions of ACTIONS 19 and 20 and the aforesaid scenarios for Steam Generator ΔP (EFAS) would govern.

Add Insert C

→(LBDCR 16-046, Ch. 86)

The Surveillance Requirements specified for these systems ensure that the overall system functional capability is maintained comparable to the original design standards. The periodic surveillance tests performed at the frequencies in the Surveillance Frequency Control Program are sufficient to demonstrate this capability. The frequency for the channel functional tests for these systems is controlled by the Surveillance Frequency Control Program.

←(LBDCR 16-046, Ch. 86)

→(LBDCR 16-046, Ch. 86)

Testing frequency for the Reactor Trip Breakers (RTBs) is controlled by the Surveillance Frequency Control Program. The RTB channel functional test and RPS logic channel functional test are scheduled and performed such that RTBs are verified OPERABLE in accordance with the Surveillance Frequency Control Program.

←(LBDCR 16-046, Ch. 86)

RPS\ESFAS Trip Setpoints values are determined by means of an explicit setpoint calculation analysis. A Total Loop Uncertainty (TLU) is calculated for each RPS/ESFAS instrument channel. The Trip Setpoint is then determined by adding or subtracting the TLU from the Analytical Limit (add TLU for decreasing process value; subtract TLU for increasing process value). The Allowable Value is determined by adding an allowance between the Trip Setpoint and the Analytical Limit to account for RPS/ESFAS cabinet Periodic Test Errors (PTE) which are present during a CHANNEL FUNCTIONAL TEST. PTE combines the RPS/ESFAS cabinet reference accuracy, calibration equipment errors (M&TE), and RPS/ESFAS cabinet bistable Drift. Periodic testing assures that actual setpoints are within their Allowable Values. A channel is inoperable if its actual setpoint is not within its Allowable Value and corrective action must be taken. Operation with a trip set less conservative than its setpoint, but within its specified ALLOWABLE VALUE is acceptable on the basis that the difference between each trip Setpoint and the ALLOWABLE VALUE is equal to or less than the Periodic Test Error allowance assumed for each trip in the safety analyses.

>(EC-26338, Ch. 67)

The Core Protection Calculator, High Logarithmic Power (HLP), and Reactor Coolant System Flow use a single bistable to initiate both the permissive and automatic operating bypass removal functions. A single bistable cannot both energize and de-energize at a single, discrete value due to hysteresis. The CPC automatic bypass removal and permissive for the

<(EC-26338, Ch. 67)

INSERT C

The CPC testing features are designed to allow for complete testing by using a combination of system self-checking and manual tests. Successful testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded. For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Software testing involves verifying that the software code has not changed and that the software code is executing. To the extent possible, CPC system testing will be accomplished with continuous system self-checking features in lieu of manual surveillance tests. Self-checking features include on-line diagnostics for the computer system and the hardware and communications tests. Faults detected by the self-checking features are alarmed in the main control room. These self-checking tests do not interfere with normal system operation. The performance of channel checks validates that the self-diagnostics are continuing to perform their self-checking functions.

3/4 INSTRUMENTATION

BASES (Cont'd)

3/4.3.1 and 3/4.3.2 REACTOR PROTECTIVE AND ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION (Continued)

>(EC-26338, Ch. 67)

HLP trip bypass occur at the bistable setpoint (nominally $10^{-4}\%$ power). However, the HLP automatic bypass removal and permissive for CPC trip bypass occur at the reset value of the bistable. Also note if the bistable setpoint is changed as part of the Special Test Exception 3.10.3, the same dead band transition is applicable.

<(EC-26338, Ch. 67)

The measurement of response time at the specified frequencies provides assurance that the protective and ESF action function associated with each channel is completed within the time limit assumed in the safety analyses. No credit was taken in the analyses for those channels with response times indicated as not applicable.

Response time may be verified by any series of sequential, overlapping, or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the topical report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

>(EC-26338, Ch. 67)

Insert D as new paragraph

← In the applicable logarithmic power modes, with the Logarithmic Power circuit inoperable or in test, the associated functional units of Local Power Density-High, DNBR-Low, and Reactor Coolant Flow-Low should be placed in the bypassed or tripped condition. With logarithmic power greater than $10^{-4}\%$ bistable setpoint and Local Power Density-High, DNBR-Low, and Reactor Coolant Flow-Low no longer bypassed (either through automatic or manual action), these functional units may be considered OPERABLE.

<(EC-26338, Ch. 67)

→(LBDCR 16-046, Ch. 86)

The Surveillance Frequency is controlled under the Surveillance Frequency Control Program.

←(LBDCR 16-046, Ch. 86)

TABLE 3.3-1, Functional Unit 13, Reactor Trip Breakers

The Reactor Trip Breakers Functional Unit in Table 3.3-1 refers to the reactor trip breaker channels. There are four reactor trip breaker channels. Two reactor trip breaker channels with a coincident trip logic of one-out-of-two taken twice (reactor trip breaker channels A or B, and C or D) are required to produce a trip. Each reactor trip breaker channel consists of two reactor trip breakers. For a reactor trip breaker channel to be considered OPERABLE, both of the reactor trip breakers of that reactor trip breaker channel must be capable of performing their safety function (disrupting the flow of power in its respective trip leg). The safety function is satisfied when the reactor trip breaker is capable of automatically opening, or otherwise opened or racked-out.

If a racked-in reactor trip breaker is not capable of automatically opening, the ACTION for an inoperable reactor trip breaker channel shall be entered. The ACTION shall not be exited unless the reactor trip breaker capability to automatically open is restored, or the reactor trip breaker is opened or racked-out.

W3F1-2020-0040
ATTACHMENT 3,
DRAFT TECHNICAL SPECIFICATION BASES PAGE MARKUPS
FOR INFORMATION ONLY

INSERT D

WCAP-18484-P, "Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System", Appendix B, "Elimination of Specific CPCS Technical Specification Surveillance Requirements" provides the basis and methodology for using allocated CPCS digital equipment response times in the overall verification of the channel response time for the CPCS. Response time verification for other equipment within the CPCS channel must be demonstrated by test as identified in the technical specifications."

Enclosure, Attachment 4

W3F1-2020-0040

WCAP-18484-P, Revision 0

**Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q
Core Protection Calculator System**

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 5

W3F1-2020-0040

**Westinghouse Letter CAW-20-5031, Affidavit, Proprietary Information Notice, and
Copyright in support of WCAP-18484-P
(Attachment 4)**

AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WCAP-18484-P, Rev. 0 be withheld from public disclosure under 10 CFR 2.390.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged, or as confidential commercial or financial information.
- (4) Pursuant to 10 CFR 2.390, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse and is not customarily disclosed to the public.
 - (ii) Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar technical evaluation justifications and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.

AFFIDAVIT

- (5) Westinghouse has policies in place to identify proprietary information. Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:
- (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.
 - (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage (e.g., by optimization or improved marketability).
 - (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
 - (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
 - (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
 - (f) It contains patentable ideas, for which patent protection may be desirable.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding is indicated in both versions by means of lower case letters (a) through (f) located as a superscript immediately following the brackets enclosing each item of information being identified as proprietary or in the margin opposite such information. These

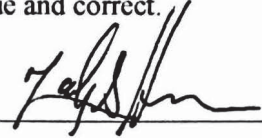
AFFIDAVIT

lower case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 4/6/2020



Zachary S. Harper, Manager
Licensing Engineering

Enclosure, Attachment 6

W3F1-2020-0040

WCAP-18484-NP, Revision 0

**Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q
Core Protection Calculator System**

Non-Proprietary

Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System

WCAP-18484-NP
Revision 0

Licensing Technical Report for the Waterford Steam Electric Station Unit 3 Common Q Core Protection Calculator System

Warren R. Odess-Gillett*
Licensing Engineering

April 2020

Reviewers: Allen C. Denyer*
CE Plant Safety Systems

Matthew A. Shakun*
Licensing Engineering

Approved: Zachary S. Harper*, Manager
Licensing Engineering

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066, USA

© 2020 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY

Revision	Author	Description	Completed
A	Warren Odess-Gillett	Revision A – First draft with open items	11/21/2019
B	Warren Odess-Gillett	1. Removed technical specification markups from this document. Entergy will include the technical specification markups in the LAR document. 2. Added new Appendix B, “Elimination of Specific CPCS Technical Specification Surveillance Requirements” 3. Incorporated Entergy comments from Revision A. 4. Rewrote Section 3.2.6 with safety analysis qualitative assessment 5. Closed all open items	2/21/2020
0	Warren Odess-Gillett	1. Incorporated Entergy comments	See PRIME

OPEN ITEMS

Item	Description	Status
	None	

TABLE OF CONTENTS

REVISION HISTORY	ii
LIST OF TABLES	vi
LIST OF FIGURES	vii
ACRONYMS AND TRADEMARKS	viii
1 INTRODUCTION	1-1
2 PLANT SYSTEM DESCRIPTION (D.1)	2-1
3 SYSTEM ARCHITECTURE (D.2)	3-1
3.1 EXISTING ARCHITECTURE (D.2.1)	3-1
3.2 NEW SYSTEM ARCHITECTURE (D.2.2)	3-5
3.2.1 CPC AC160 Controller	3-8
3.2.2 CEAC AC160 Controller	3-15
3.2.3 Power Supply	3-20
3.2.4 APC Multiplexer	3-21
3.2.5 HVAC Requirements	3-21
3.2.6 CPCS Design Function	3-22
3.2.7 Service/Test Functions	3-28
3.2.8 Separation and Independence	3-39
3.2.9 Cross Divisional Interfaces	3-41
3.2.10 Connections to Human-System Interfaces	3-42
3.2.11 Connections between Safety-Related Systems	3-42
3.2.12 Connections between Safety-Related and Non-Safety-Related Systems	3-42
3.2.13 Temporary connections	3-42
3.2.14 Interfacing with Supporting Systems	3-43
3.2.15 Physical Location of System Equipment	3-43
3.2.16 Communications	3-43
3.2.17 Failure Modes and Effects Analysis	3-57
3.2.18 Common Cause Failure (CCF)	3-60
3.2.19 Compliance to Applicable IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003	
Clauses	3-62
3.2.20 FSAR Changes	3-67
3.3 NEW SYSTEM FUNCTIONS (D.2.3 AND D.2.3.1)	3-68
3.3.1 Restoring CEA Rate of Change Lock-In	3-68
3.3.2 IEEE Std 603-1991 Clause 4 Compliance	3-69
3.3.3 IEEE Std 603-1991 Applicable Clauses for New System Functions	3-72
3.3.4 System Requirements Documentation (D.2.3.3 and D.2.3.3.1)	3-78
3.4 FUNCTION ALLOCATION (D.2.4 AND D.2.4.1)	3-82
3.5 SYSTEM INTERFACES (D.2.5)	3-83
3.5.1 CEA Position Cross Channel Communication	3-83
3.5.2 PPS Interface	3-83
3.5.3 Plant Annunciator System Interface	3-84

	3.5.4	OM and MTP Print Screen Interface	3-84
	3.5.5	Plant Monitoring System Interface.....	3-84
	3.5.6	CEAPD Interface.....	3-84
	3.5.7	MTP Time Synchronization Interface	3-85
	3.5.8	Support and Auxiliary System Interfaces	3-85
	3.5.9	Safety to Non-Safety Isolation Requirements	3-86
	3.5.10	IEEE Std 603 and IEEE Std 7-4.3.2 Relevant Clauses.....	3-86
3.6		FUNDAMENTAL DESIGN PRINCIPLES IN THE NEW ARCHITECTURE.....	3-92
	3.6.1	Redundancy (D.2.6.2.1).....	3-92
	3.6.2	Independence (D.2.6.2.2)	3-95
	3.6.3	Deterministic Behavior (D.2.6.2.3)	3-98
	3.6.4	Defense-in-Depth and Diversity (D.2.6.2.4)	3-100
	3.6.5	Simplicity of Design (D.2.6.2.5)	3-100
4		HARDWARE EQUIPMENT QUALIFICATION (D.3).....	4-1
5		I&C SYSTEM DEVELOPMENT PROCESSES (D.4).....	5-1
	5.1	COMMON Q SPM PLANT SPECIFIC ACTION ITEMS.....	5-2
	5.1.1	PSAI 1	5-3
	5.1.2	PSAI 2	5-3
	5.1.3	PSAI 3	5-5
	5.1.4	PSAI 4	5-5
	5.1.5	PSAI 5	5-5
	5.1.6	PSAI 6	5-6
	5.1.7	PSAI 7	5-6
	5.2	SYSTEM AND SOFTWARE DEVELOPMENT ACTIVITIES (D.4.2.1).....	5-7
	5.2.1	Plant and Instrumentation and Control System Safety Analysis (D.4.2.1.1)...	5-7
	5.2.2	Instrumentation and Control System Requirements (D.4.2.1.2)	5-7
	5.2.3	Instrumentation and Control System Architecture (D.4.2.1.3).....	5-8
	5.2.4	Instrumentation and Control System Design (D.4.2.1.4)	5-8
	5.2.5	Software Requirements (D.4.2.1.5).....	5-8
	5.2.6	Software Design (D.4.2.1.6).....	5-9
	5.2.7	Software Implementation (D.4.2.1.7).....	5-10
	5.2.8	Software Integration (D.4.2.1.8).....	5-11
	5.2.9	Instrumentation and Control System Testing (D.4.2.1.9).....	5-11
	5.2.10	Project Management Processes (D.4.2.2).....	5-12
	5.2.11	Software Quality Assurance Processes (D.4.2.3)	5-12
	5.2.12	Software Verification and Validation Processes (D.4.2.4).....	5-13
	5.2.13	Configuration Management Processes (D.4.2.5).....	5-13
6		APPLYING A REFERENCED TOPICAL REPORT SAFETY EVALUATION (D.5)	6-1
	6.1	COMMON Q PLATFORM CHANGES (D.5.1.1).....	6-1
	6.1.1	Common Q Platform Topical Report Revision	6-1
	6.2	RESOLUTION OF TOPICAL REPORT PLANT-SPECIFIC ACTION ITEMS (D.5.1.2).....	6-1
	6.2.1	Generic Open Items.....	6-2
	6.2.2	Plant-Specific Action Items	6-2

7	COMPLIANCE/CONFORMANCE MATRIX FOR IEEE STANDARDS 603-1991 AND 7-4.3.2-2003 (D.6)	7-1
8	TECHNICAL SPECIFICATIONS (D.7)	8-1
9	SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT (D.8)	9-1
	9.1 SECURE DEVELOPMENT ENVIRONMENT	9-1
	9.2 SECURE OPERATIONAL ENVIRONMENT.....	9-1
	9.2.1 Secure Operational Environment Vulnerability Assessment	9-2
10	REFERENCES	10-1
11	BIBLIOGRAPHY.....	11-1
	APPENDIX A WF3 FSAR MARKUPS	A-1
	APPENDIX B ELIMINATION OF SPECIFIC CPCS TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS.....	B-1
	APPENDIX C ENDNOTES	C-1

LIST OF TABLES

Table 3.2.1.1-1 CPC Program Execution Intervals and Input Sampling Rates.....	3-14
Table 3.2.2-1 Preferred Source for CEA Position Data	3-18
Table 3.2.2-2 CEAC Program Execution Intervals and Input Sampling Rates.....	3-20
Table 3.2.6-1 [.....]	^{a,c} 3-24
Table 3.2.16-1 DI&C-ISG-04-Compliance.....	3-45
Table 3.2.17.2-1 Window Watchdog Timer Actuation Summary	3-60
Table 3.3.3-1 ISG-06 System Requirements Document Content.....	3-79
Table 5.1.2-1 BTP 7-14 Documents.....	5-3
Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2.....	7-1
Table 9.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness	9-6
Table B.4-1. Annunciation Path FMEDAs.....	B-14
Table B.5-2. PM646A Communication Section (CS) Diagnostic Table.....	B-21
Table B.5-3. CI631 Communication Module Diagnostic Table.....	B-23
Table B.5-4. Backplane I/O Bus (BIOB) Diagnostic Table.....	B-24
Table B.5-5. Analog Input Module (AI688) Diagnostic Table.....	B-25
Table B.5-6. Digital Pulse Module (DP620) Diagnostic Table.....	B-26
Table B.6-1 PM646A Processing Module FMEDA.....	B-31
Table B.6-2 BIOB FMEDA.....	B-33
Table B.6-3 CI631 Communications Module FMEDA.....	B-34
Table B.6-4. Analog Input Modules (AI688) FMEDA.....	B-35
Table B.6.5. Digital Pulse Module (DP620) FMEDA.....	B-37
Table B.6.6. Digital Output Module (DO625) FMEDA.....	B-38
Table B.6.7. Interposing Relay Panel (IRP) FMEDA.....	B-38
Table B.7-1 [.....]	^{a,c} B-40
Table B.7-2. CPCS Components within Scope of TS RTT SR.....	B-43

LIST OF FIGURES

Figure 2-1. CPC Functional Block Diagram.....2-3

Figure 2-2 Existing CPC/CEAC Architecture Block Diagram2-4

Figure 2-3. Existing CPC/CEAC Channelization Diagram2-6

Figure 3.1-1. Existing CPC/CEAC Architecture Block Diagram3-1

Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram.....3-7

Figure 3.2.17-1 CPCS Channel B3-58

Figure B-1. Channel Fault Indication and Alarm Paths B-14

ACRONYMS AND TRADEMARKS

The following abbreviations and acronyms are defined to allow an understanding of their use within this document.

Acronym	Definition
ΔT_{cold}	Cold leg temperature difference
AI	Analog Input
AC	Alternating Current
AC160	Advant Controller 160
A/D	Analog to Digital [conversion]
AF100	Advant Fieldbus 100 (data bus within a CPC channel)
AO	Analog Output
AOO(s)	Anticipated Operating Occurrence(s)
APC	Auxiliary Protective Cabinet
AR	Alternate Review [process] (new process described in DI&C-ISG-06, Revision 2)
ASGT	Asymmetric Steam Generator Transient
ATWS	Anticipated Transient Without Scram
AUX CPC	Auxiliary CPC processor in the CPC AC160 controller
CCF	Common Cause Failure
CEA	Control Element Assembly
CEAC	CEA Calculator
CEACs	CEACs in multiple channels or referring to CEAC 1 and CEAC 2 in one channel
CEAPD	CEA Position Display

Acronym	Definition
CEAPDS	CEA Position Display System
CMRR	Configuration Management Release Report
COLR	Core Operating Limits Report
COLSS	Core Operating Limit Supervisory System
CONTRM	AC160 control module (i.e., periodic executable application in the PM646A)
CPCS	Core Protection Calculator System
CPCs	Core Protection Calculators in multiple channels (as distinguished from CEACs in each channel)
CPP	CEA Position Processor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Communication Section (see PS)
CWP	CEA Withdrawal Prohibit
DI(s)	Digital Input(s)
DNBR	Departure from nucleate boiling ratio
DO	Digital Output
EC	Engineering Change
ECT	EC Testing
ESFS	Engineered Safety Features System
EXLD	Excess heat removal due to secondary system malfunction
FAT	Factory Acceptance Test
FPD	Flat Panel Display

Acronym	Definition
FPDS	[Common Q] Flat Panel Display System
FE	Function Enable [key switch]
FICA	Fixed incore amplifier
FIDAS	Fixed Incore Detector Amplifier System
FMEA	Failure Modes and Effects Analysis
GDC	General Design Criteria
GOI(s)	Generic Open Item(s)
GUI	Graphical User Interface
HCD	Hold Coil Delay
HFP	Hot Full Power
HSI	Human System Interface
HSL(s)	High Speed Link(s)
HZP	Hot Zero Power
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
INOP	Inoperable
IRIG	Inter-range Instrumentation Group [time codes]
ISG	[NRC] Interim Staff Guidance
IRP	Interposing Replay Panel
kW/ft	Kilowatt per foot
LAR	License Amendment Request

Acronym	Definition
LOOP	Loss Of Offsite Power
LPD	Local power density
LTR	Licensing Technical Report
MCB	Main Control Board
MCR	Main Control Room
MSLB	Main Steam Line Break
MTP	Maintenance and Test Panel
MUX	Multiplexer
NI	Nuclear incore instrumentation
NRC	Nuclear Regulatory Commission
NRR	NRC Office of Nuclear Reactor Regulation
NSSS	Nuclear Steam Supply System
OEM	Original Equipment Manufacturer
OM	Operator's module
OMs	Operator's modules
OSS	Out of service
PA	Postulated Accident
PF	Penalty Factor
PMC	Plant Monitoring Computer
PPS	Plant Protection System
PS	<ol style="list-style-type: none"> 1. Processor Select [switch] 2. Processing Section (within the PM646A)

Acronym	Definition
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RCPSSSS	RCP Shaft Speed Sensing System
RDB	Reload Data Block
RE	Responsible Engineer
RPS	Reactor Protection System
RSE	Reusable Software Element
RSED	Reusable Software Element Description
RSPT	Reed Switch Position Transmitter
RTC	Real Time Clock
RTCB	Reactor Trip Circuit Breaker
RTD	Resistor Temperature Detector
RTM	Requirements Traceability Matrix
RTP	Rated Thermal Power
RTS	Return to Service
SAFDL	Specified Acceptable Fuel Design Limits
SDD	Software Design Description
SER	Safety Evaluation Report
SGTR	Steam Generator Tube Rupture
SHA	Software Hazards Analysis
SLB	Steam Line Break

Acronym	Definition
SLE	Software Load Enable [key switch]
SPM	Software Program Manual
SR	Surveillance Requirement
SRS	Software Requirements Specification
TE	Test Engineer
Tin/Tcold	Core inlet temperature (cold leg)
Tout/Thot	Core outlet temperature (hot leg)
TRIPSEQ	Trip sequence – a periodic executable application in the CPC PM646A (see CONTRM)
TS	Technical Specification(s)
Tsat	Saturation temperature
TSTF	<ol style="list-style-type: none"> 1. Technical Specification Task Force 2. Technical Specification Traveler Form
FSAR	Updated Final Safety Analysis Report
V&V	Verification and Validation
Vac	Volts alternating current
Vdc	Volts direct current
VOPT	Variable overpower trip
WDT	Watchdog timer
WF3	Waterford Steam Electric Station Unit 3
WWDT	Window watchdog timer

1 INTRODUCTION

The Core Protection Calculator System (CPCS) at Waterford Steam Electric Station Unit 3 (WF3) is being replaced with a new system based on the Common Qualified (Common QTM) Platform. This report supports the WF3 License Amendment Request (LAR) to be reviewed and approved by the United States Nuclear Regulatory Commission staff (NRC). This licensing technical report (LTR) follows aspects of the structure in revision 2 of DI&C-ISG-06, “Digital Instrumentation and Controls Licensing Process Interim Staff Guidance” (Reference 1). The aspects followed are those that pertain to the alternate review (AR) process as described in Section C.2 of DI&C-ISG-06 (Reference 1).

WF3 can use the information in this LTR to complete sections of the LAR that pertain to DI&C-ISG-06 Sections D.1 through D.8. Each section heading will include the corresponding DI&C-ISG-06 Section in parentheses (e.g., “Plant System Description (D.1)”).

2 PLANT SYSTEM DESCRIPTION (D.1)

The WF3 Plant Protection System (PPS) is comprised of an Engineered Safety Features Actuation System (ESFAS) and a Reactor Protection System (RPS). The Core Protection Calculator System (CPCS) is part of the RPS. The PPS cabinet includes the RPS Coincidence and Initiation Logic. The Auxiliary Protective Cabinet (APC) includes the CPCs and the CEACs. The CPC/CEAC system issues 2 of the 15 reactor trips in the RPS to protect the fuel design limits. These four independent Core Protection Calculators (CPCs), one in each protection channel, calculates departure from nucleate boiling ratio (DNBR) and local power density (LPD). The reactor trips provided by the CPCs are inputs to the RPS Coincidence and Initiation Logic, and the CPC trips have a 2 out of 4 logic. The calculations performed in each CPC utilize the input signals described later in this section. The DNBR and LPD calculation results are compared to trip setpoints for initiation of a low DNBR trip and the high LPD trip.¹ These CPCS trip outputs become digital trip inputs to the corresponding Plant Protection System (PPS) channel. The four channel PPS performs the 2 out of 4 voting logic on various reactor trip functions that include the CPC Low DNBR and High LPD. The CPCS is designed to initiate automatic protective action to assure that the specified acceptable fuel design limits (SAFDL) on DNBR and LPD are not exceeded during Anticipated Operational Occurrences (AOOs).²

The High LPD Trip is to prevent the linear heat rate (kW/ft) in the limiting fuel pin in the core from exceeding the value corresponding to the centerline fuel melting temperature. This is to prevent exceeding the safety limit of peak fuel centerline temperature in the event of defined anticipated operational occurrences.³

DNBR is the ratio of Critical Heat Flux to Actual Heat Flux. Critical heat flux (CHF) is that value of heat flux at which Departure from Nucleate Boiling (DNB) occurs.⁴ The Low DNBR trip is to prevent the DNBR in the limiting coolant channel in the core from exceeding the fuel design limit for the fuel cladding in the event of defined anticipated operational occurrences. In addition, this trip will provide a reactor trip to assist the Engineered Safety Features System (ESFS) in limiting the consequences of the steam generator tube rupture, steam line break and reactor coolant pump shaft seizure accidents.⁵

CPC DNBR and LPD pre-trip alarms are initiated prior to the trip value to provide audible and visible indication of approach to a trip condition.⁶ These pre-trip functions have no direct safety function.

The CPC will also initiate only the DNBR and LPD trip outputs which is known as an Auxiliary Trip under the following conditions:⁷

- a) CPC operating space limits are exceeded for the hot pin axial shape index integrated one pin radial peak, maximum and minimum cold leg temperatures, and primary pressure (CPC operating space Trips).
- b) Opposing cold leg temperature difference exceeds its setpoint, which varies with power level (Asymmetrical Steam Generator Transient (ASGT) Trip).
- c) Reactor power exceeds the variable overpower trip setpoint. The trip setpoint is larger than the steady state reactor power by a constant offset but is limited in how fast it can follow changes in reactor power. This provides protection from sudden power increases (Variable Overpower Trip (VOPT)).

- d) The maximum hot leg temperature approaches the coolant saturation temperature (T_{hot} at saturation or Quality Margin).
- e) The CPC system is not set in the normal operating configuration (CPC Failure).
- f) Reactor coolant pump shaft speed drops below its setpoint value for multiple pumps (Less than two RCPs running).

The Design Basis functions are not changing as a result of this CPCS upgrade. All the design basis events in Chapter 15 and the reliance on the CPCS low DNBR and high LPD trips are unchanged.⁸ The methodologies and algorithms used in low DNBR and high LPD processor calculations, including CEAC penalty factors, the treatment of raw data processing/filtering, and the treatment of bad data/faulted hardware in calculations, also remain unchanged.

The PPS/RPS performs a two out of four coincidence of like trip signals to generate a reactor trip signal. The use of four channels allows bypassing of one channel for maintenance while maintaining a two out of three channel trip.⁹

Each CPC receives the following inputs: core inlet and outlet temperature, pressurizer pressure, reactor coolant pump speed, excore nuclear instrumentation flux power (each subchannel from the safety channel), selected (target) CEA position, and CEA subgroup deviation from the CEA calculators. Input signals are conditioned and processed.¹⁰

The scope of the replacement is on the CPCS including sensor terminations, replacement calculators (CPC and CEAC), alarm output termination, analog output terminations (MCR Indication), and output terminations to the PPS/RPS.¹¹ Excluded from the modification are:

- Sensors and their cabling to the CPCs
- Reactor Protection System
- CPC system Trip setpoints and outputs. All functional requirements for DNBR and LPD trip output are unchanged

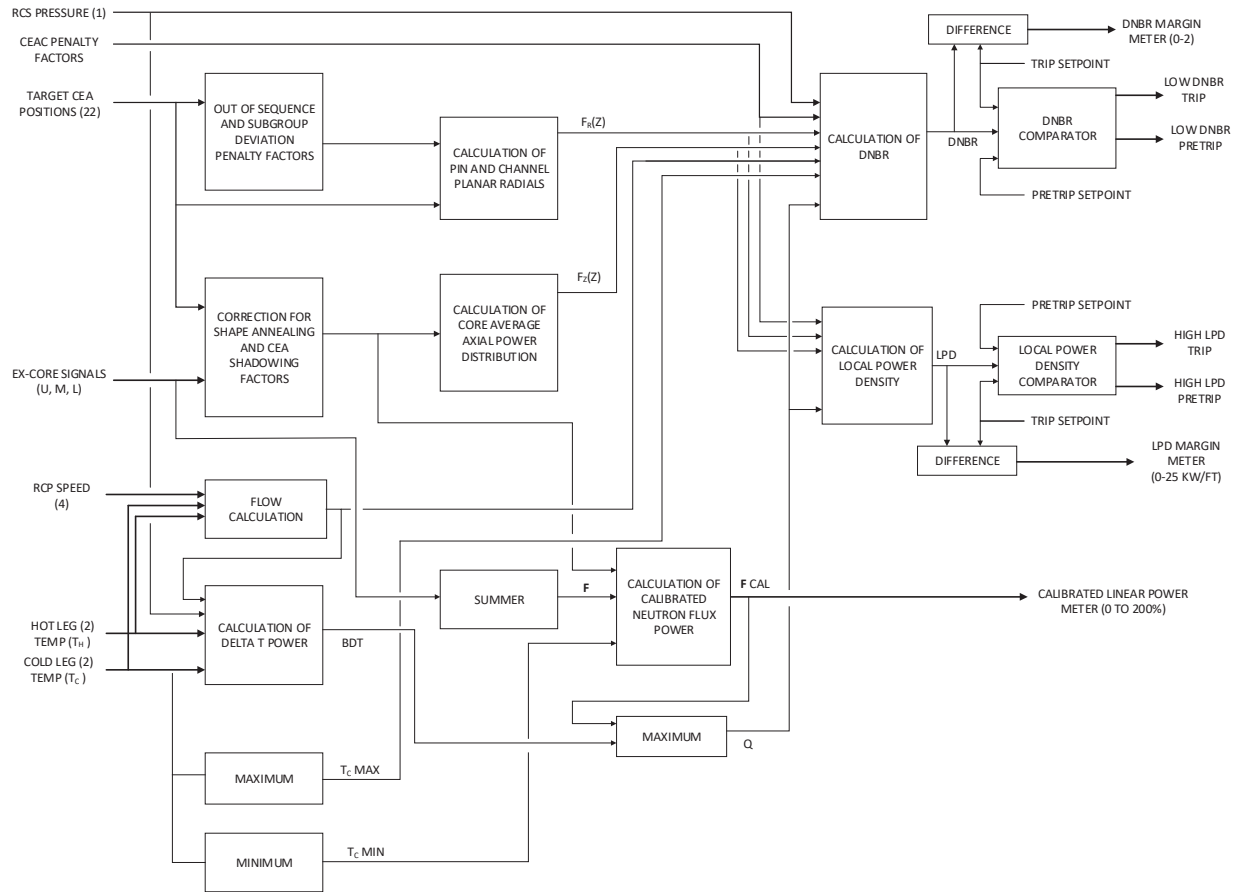


Figure 2-1. CPC Functional Block Diagram¹²

In the existing CPCS, the CPC in each channel receives one CEA position (target CEA) from each CEA Subgroup, which provides each CPC with one quarter of the CEA position inputs. The existing system has two independent CEAC calculators (CEACs), as part of the CPC System, to calculate individual CEA deviations from the position of the other CEAs in their subgroup.¹³ The position of each CEA is an input to the CEAC. These positions are measured by means of two redundant reed switch assemblies on each CEA. These redundant reed switch assemblies are not being changed as a part of the LAR. In the existing system each CEA is instrumented by redundant CEA reed switch position transmitters (RSPT) identified as RSPT1 and RSPT2 for each CEA.¹⁴ The RSPT1 inputs are monitored by CEAC 1 and the RSPT2 inputs are monitored by CEAC 2. CEAC 1 is located in Channel B and CEAC 2 is located in Channel C for the existing CPCS. One set of the redundant signals for all CEAs is monitored by one CEAC and the other set of signals by the redundant CEAC.¹⁵ In the new system, each channel will have a CEAC 1 and CEAC 2 calculator processing RSPT1 and RSPT2 signals, respectively, rather than just two CEAC calculators for all four CPCs.¹⁶

The CEAs are arranged into control groups that are controlled as subgroups of CEAs. The subgroups are symmetric about the core center. The subgroups are required to move together as a control group and should always indicate the same CEA group position. Each CEAC monitors the position of all CEAs within each control subgroup. Should a CEA deviate from its subgroup position, the CEACs monitor the event, sounds an annunciator, and transmit an appropriate deviation "penalty" factor to each CPC. This

will cause trip margins to be reduced. This assures conservative operation of the PPS, as any credible failure of a CEA reed switch assembly will result in an immediate operator alarm and conservative RPS trip margins.¹⁷

The CPC in each channel utilizes selected "target" CEA position reed switch signals as a measure of subgroup and group CEA position. The CPCs utilize single CEA deviation penalty factors from the CEACs to modify calculation results in a conservative manner should a deviating CEA be detected by either CEAC. The detailed signal paths of CEA position signals are shown in Figure 2-2 Existing CPC/CEAC Architecture Block Diagram.¹⁸

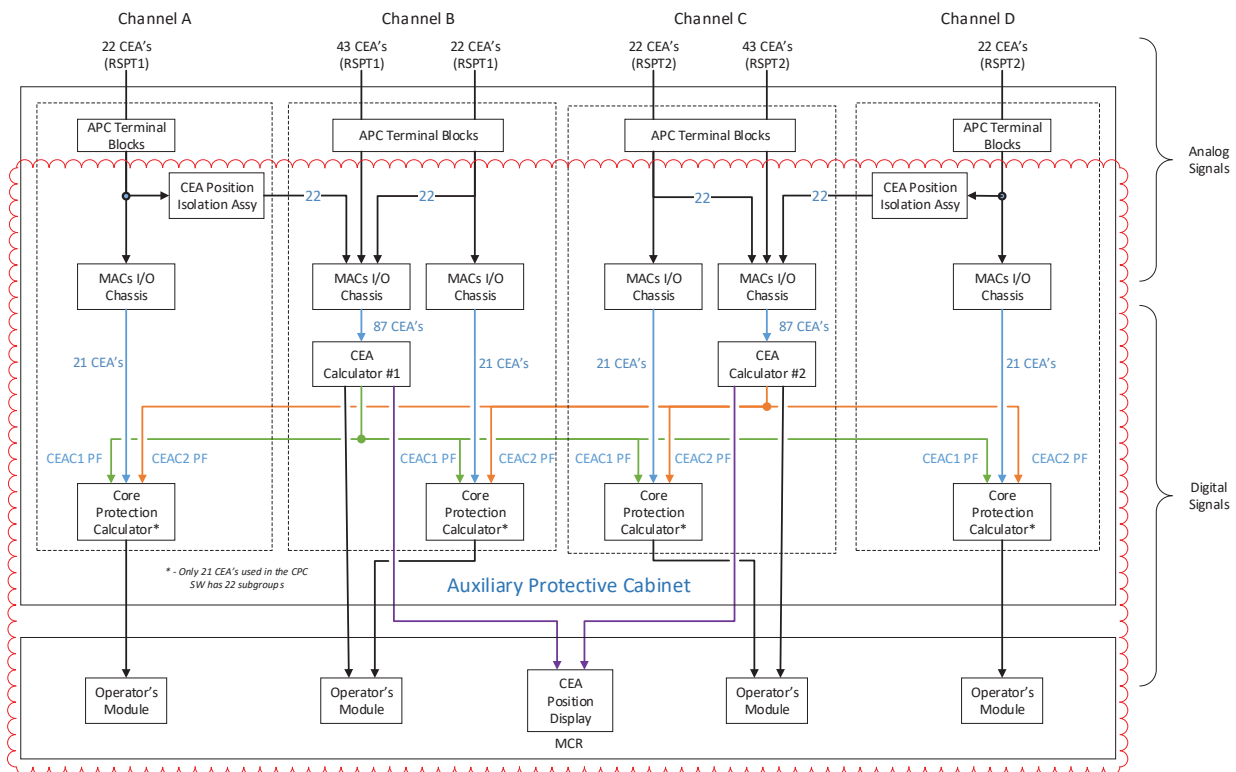


Figure 2-2 Existing CPC/CEAC Architecture Block Diagram¹⁹

The area within the red box in the figure is what will be replaced for the CPCS modification. It should be noted that the CEA Position Display in the main control room (MCR) is a non-safety display isolated from the two CEACs called the CEA Position Display (CEAPD). This part of the system is not included in the LAR. The plant modification for CEAPD will be performed under 10 CFR 50.59.

The following calculations are performed in the CPC (unless otherwise noted):

- a) CEA deviations and corresponding penalty factors:
 - 1) Single CEA deviation in a subgroup calculated by CEA calculators
 - 2) Subgroup deviations in a group calculated by CPCs

3) Groups out of sequence calculated by CPCs

- b) Correction of excore flux power for shape annealing and CEA shadowing
- c) Normalized reactor coolant flowrate from reactor coolant pump speed
- d) Core average Δ power from reactor coolant temperature and flow information
- e) Core average power from corrected excore flux power signals
- f) Axial power distribution from the corrected excore flux power signals
- g) Fuel rod and coolant channel planar radial peaking factors, selection of predetermined coefficients based on CEA positions
- h) DNBR
- i) Comparison of DNBR with a fixed trip setpoint
- j) Local power density compensated for thermal capacity of fuel
- k) Comparison of compensated local power density to fixed local power density setpoint
- l) CEA deviation alarm (CEA calculator)²⁰

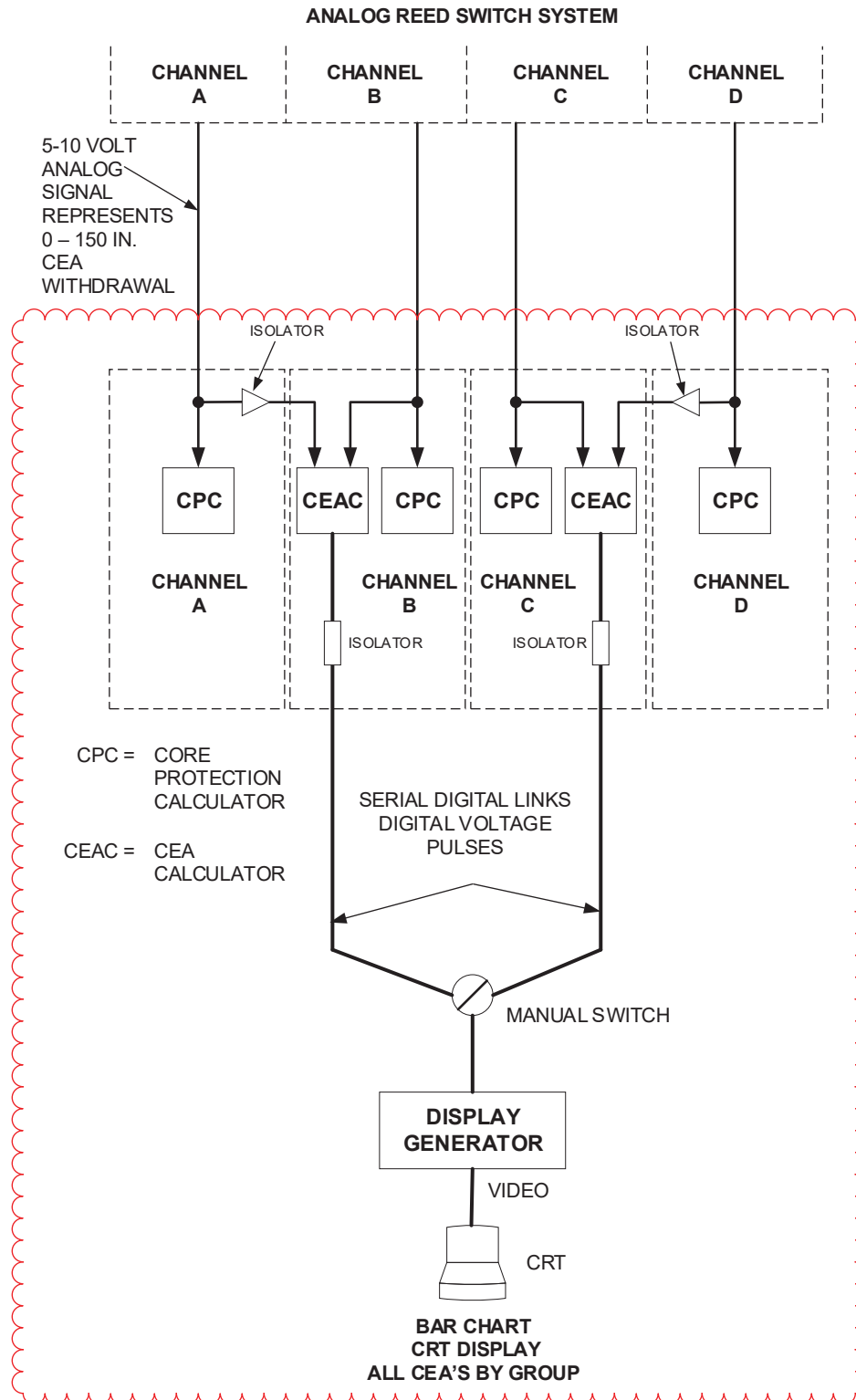
Figure 2-3. Existing CPC/CEAC Channelization Diagram²¹

Figure 2-2 Existing CPC/CEAC Architecture Block Diagram, shows four operator's modules (OMs) located on the Main Control Board (MCB). These are safety-related modules. Each OM receives data from each CPCS channel and facilitates changes to addressable constants. In Channels B and C, the OM has a select switch to choose which calculator to receive data from, the CPC or CEAC.²²

The CPCS has six (6) datalinks to the Plant Monitoring Computer (PMC) provided by four (4) datalinks for the CPCs (one from each channel), and two (2) datalinks from the CEACs (one from each CEAC). These datalinks are connected to the PMC through the APC Mux chassis. The CPC and CEAC data links are accomplished through interfacing a 16-bit parallel input card in the APC mux chassis to a 16-bit output card within the CPC and CEAC, respectively. The CPC and CEAC provides optically isolated Digital Outputs (16 bits) that are read by the APC Mux optically isolated digital input card (16 bits). The APC MUX communicates CPC and incore information to the PMC. The APC MUXs send their data to the PMC system over fiber optic serial communication links. This optic link provides electrical isolation from the APC MUX and the PMC system. The APC MUX sends the data when a data request is received from the PMC.²³

The APC Mux system receives inputs from the Fixed Incore Detector Amplifier System (FIDAS). The FIDAS converts the incoming Fixed Incore Detector Signals (0-10 μ Amps) into 0 to -10VDC signals for input to the APC Mux. WF3 contains 56 detector assemblies, each containing 5 rhodium detectors located at 15%, 30%, 50%, 70% and 90% of core height, plus one background detector. The FIDAS processes the 5 detector signals and 1 background signal per assembly and provides these six (6) 0 to -10VDC signals per assembly out to the APC Mux for processing, which is a total of 336, 0-10VDC signals. In total, this results in 56 detector assembly strings sending 280 detector signals and 56 background signals. These signals are split among the 4 APC channels, 14 detector assembly strings per channel that process 70 detector signals and 14 background signals.

The FIDAS provides two 0 to -10V outputs for each Incore detector signal, which are read by redundant APC Mux 1 and APC Mux 2 assemblies within each APC cabinet. Each APC Mux is identical with APC Mux 1 and APC Mux 2 communicating to the PMC network where the signals are available to both PMC A and PMC B.²⁴

The CPC/CEAC system, being part of the PPS/RPS, are periodically tested in accordance with the criteria described in IEEE Standard 338-1971. Test intervals and their bases are included in the technical specification documents (see Appendix A).²⁵

The existing CPCS requires analog to digital (A/D) conversion calibration as well as reference voltage calibration. The CPC/CEAC system performs both automatic and periodic testing. The automatic and periodic tests provide a means of checking, with a high degree of confidence, the operational availability of system input sensors and all devices used to derive the final system output signal.²⁶

Existing System - Automatic On-Line Testing²⁷

The automatic on-line testing consists of three separate checks: (1) internal self-checking of the input data, (2) internal self-checking of the calculator and (3) an external watchdog timer that monitors the execution of the cyclic scheduling mechanism. Although failures in the on-line system are expected infrequently, the automatic on-line testing is provided to assure high continuous system reliability beyond that provided in typical analog calculated trips.

The protection algorithms check the reasonability of input sensor data against predetermined maximum and minimum values. The CEAC checks raw CEA position data against high and low values for out of range conditions. These setpoints are part of the CPC database. The CEA position signals outside of this range are deemed unreasonable and a sensor failure flag is set. If a sensor is found to be out-of-range, the affected calculator generates the proper annunciation signal.

To provide a check on system software and to detect time frame overruns, an external "watchdog timer" is installed as part of the Data Input/Output (I/O) Subsystem. The watchdog timer lights the CPC or CEAC failure light at the Operator's Module (OM) directly.

For all other failures detected during automatic on-line testing, the affected calculator sets its outputs in the fail-safe state, such as "trip" for a CPC. If recovery from the failure is possible, the system maintains its outputs in the safe state and execute Auto-Restart, followed by initialization, followed by normal operation.

Further on-line testing capability is provided by continuous status indication and information read out from each Core Protection Calculator. Continuous displays of the following information is provided to the operator:

- a) DNBR margin
- b) Local power density margin
- c) Calibrated neutron flux power

Manual cross checking of the four channel displays can be made to assure the integrity of the calculator. The majority of the calculator failures result in anomalous indications from the failed channel that can be readily detected by the operator during cross checking.

Existing System - Periodic Testing²⁸

The CPC is periodically and routinely tested to verify its operability. A complete channel can be individually tested without initiating a reactor trip, and without violating the single failure criterion. The system can be checked from the sensor signal through the bistable contacts for low DNBR and high local power density in the Plant Protection System. Overlap in the checking and testing is provided to assure that the entire channel is functional.

The minimum frequencies for checks, calibration, and testing of the Core Protection Calculator System have been included in the Technical Specification documents (see Appendix A). Periodic testing of the DNBR/LPD Calculator system is divided into two major categories, (1) on-line system tests and (2) off-line performance diagnostic tests. Off-line testing is further subdivided into two categories, performance testing and diagnostic testing. Performance testing is used to check the numerical accuracy of the calculations. Diagnostic testing is used as an aid to troubleshooting whenever the performance tests or the on-line tests (interchannel comparisons) indicate the presence of a failure. Permanent mass storage units are used for storage of the test programs.

Existing System - On-line System Test²⁹

The on-line portion of the periodic testing consists of comparisons of like parameters among the four protective channels. Comparisons are made using the digital displays on the OM and the analog meters on the MCB. Comparisons of like analog and digital inputs give assurance that the analog and digital multiplexers and the A/D converters are functioning properly. These comparisons also give assurance that data are being properly entered into and retrieved from the data base. Comparisons of intermediate and final calculated parameters verify the performance of the protection algorithms and the analog display

meters on the control board. Calibration of the A/D converters is checked by displaying the reference voltage supplies which are connected to each CPC.

Existing System - Off-line Performance Test³⁰

Before off-line testing is initiated, the channel to be tested is bypassed at the plant protection system (PPS) and the trip logic is changed to two-out-of-three for the DNBR and LPD trips. Interlocks are incorporated in the PPS to prevent bypassing more than one channel at a time. To initiate off-line testing a key is required and only one key is provided. This ensures that only one channel can be placed in the test mode at a time. The performance test uses the CPC data base to verify numerical accuracy of the calculations. The data base is divided into three areas, namely, raw input data, filtered input data and calculated values. The raw data area contains the last samples of raw analog and digital data. The filtered data area contains averaged input data, filtered input data, past samples of input data needed for dynamic compensation, and dynamically compensated data. The calculated values area contains intermediate and final calculated values and calibration constants which are updated periodically. During performance testing, the permanent mass storage unit is used to load test inputs directly into the data base. For each set of test inputs, the expected calculated results are also loaded and compared with the values calculated by the protection algorithms. If agreement is achieved, the test program prints the expected results and the actual results on the Teletype and proceeds to the next set of test data. If agreement is not achieved, the test program halts at that point unless restarted by the operator. Dynamic effects in the calculations are tested by loading the filtered data area of the data base with test values representing past values of time varying inputs.

From the standpoint of the CPC software structure, the performance tests are virtually identical to the on-line functions. Only two differences exist from the normal functions of the calculators. First, the calculator outputs are in a fail-safe condition for the duration of the tests, and second, the algorithms use data derived from the permanent mass storage unit instead of the Data I/O subsystem. The algorithms themselves, however, do not recognize the data source or that they are executing in the test mode.

As a final check, the individual instructions in protected memory are compared with an image of the instructions stored on the permanent mass storage unit to ensure the integrity and demonstrate the "reliability" of the protection algorithms during the life span of the DNBR/LPD Calculator System.

Off-Line Diagnostic Tests³¹

After a given failure is detected by a performance test, on-line test, or on-line diagnostic, hardware diagnostic programs are provided to aid in locating (to the module level) and correcting malfunctions.

The CPCs and CEACs are digital computers. This modification is a digital-to-digital replacement of the existing CPC system.

3 SYSTEM ARCHITECTURE (D.2)

3.1 EXISTING ARCHITECTURE (D.2.1)

As described in Section 2, Plant System Description (D.1), the four independent CPCs, one in each protection channel, calculates departure from nucleate boiling ratio (DNBR) and local power density (LPD). These calculations are performed in each CPC, utilizing the input signals described in Section 2. The DNBR and LPD calculation results are compared to trip set-points for initiation of a low DNBR trip and the high local power density trip. These trip outputs become digital trip inputs to the Reactor Protection System (RPS). Among the other RPS trip functions, there are these two trip reactor functions: Low DNBR and High LPD.

The CPC/CEAC are 1970's vintage minicomputers. The CPC/CEAC system performs both automatic and periodic testing. The automatic and periodic tests provide a means of checking, with a high degree of confidence, the operational availability of system input sensors and all devices used to derive the final system output signal. The service/test functions of the existing CPCs is discussed in Section 2.

The four CPCs are separated into protection channels as depicted in Figure 3.1-1.

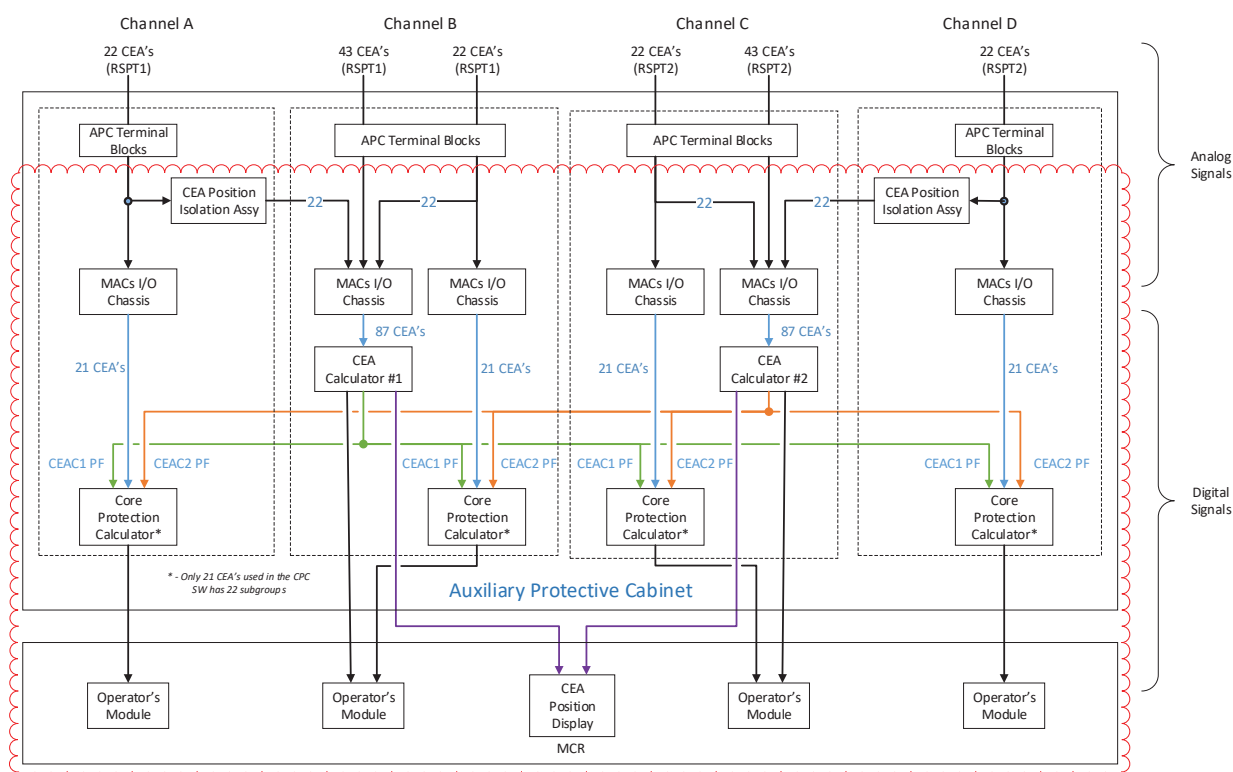


Figure 3.1-1. Existing CPC/CEAC Architecture Block Diagram

³²Prior to cycle 12 Waterford 3 had a total of 91 CEAs. Of this number, 83 were full length CEAs and 8 were partial length CEAs. The 83 full length CEAs consisted of 79 full length five element or 5-finger

CEAs, and 4 full length four element or 4-finger CEAs. The existing CPC system software lists a total of 91 CEAs, and the original CPCS had 23 RSPT signals in each channel assigned to the CPC. The Channel B and C CEAC calculators processed 68 RSPT signals in their respective channels and received 23 CEA's from channels A and D for a total RSPT complement of 91 CEA Positions. There were two modifications at WF3 that impacted this configuration. First CEA's 2 and 3 were part of subgroup 23 in the CPC which had only those two rods. Subgroup 23 in the CPC software was eliminated. However, these signals remain terminated in their respective channels and are sent to the CEAC for use in that calculator only.

The second modification was to replace eight part-length CEA's with full length CEA's and remove four full length four element or 4-finger CEA's (see Reference 23) which were assigned to subgroup 22, Shutdown group A. This resulted in reducing the number of CEA's to 87 from 91. During the refueling outage following cycle 11 (RF11), the following CEA changes were made under the direction of Engineering Request ER-W3-1999-0411-000.

The eight part-length CEAs (CEA numbers 28, 29, 30, 31, 32, 33, 34 and 35) were replaced with full-length five element (i.e., 5-finger) CEAs, and the four full-length four element, i.e., 4-finger CEAs (CEA numbers 88, 89, 90, and 91) were removed. The CEDM coil packs and pressure housings were not removed with the removal of the four CEAs. By not removing the coil packs the CEDM cooling air flow and cooling would not be impacted by the change. The control wiring to the coil packs was de-terminated. The RSPT wiring for CEA numbers 88, 89, 90, and 91 was de-terminated and the RSPT inputs into the CPC/CEACs for these CEAs which were in subgroup 22 were wired to subgroup 21 for RSPT inputs into the CPC/CEACs thus to simulate movement and eliminate the need for CPC software changes.

As a result of implementing the modification in this manner, the CPC and CEAC Software was not changed and still reflects 22 subgroups and 91 CEA's. The CPCS replacement will have 21 subgroups and a total of 87 CEA's to reflect the current CEA configuration.

The software changes that were made as documented in this engineering request were for the non-safety CEAPD System (CEAPDS) and the PMC. Per procedure EN-IT-104, the software change requests for these changes were SCR-WF3-2001-42 and SCR-WF3-2001-46. As stated above no CPCS software change was required.

Westinghouse letter (LTR-ME-01-1) covered the thermal hydraulic and mechanical assessment of the removal of (CEA numbers 88, 89, 90, and 91). The FSAR changes for the CEA modifications were incorporated with the Cycle 12 reload FSAR changes as documented in engineering request ER-W3-2002-0166-000.

The CPCS receives CEA position signals from the CEA RSPT signals. Each CEA has 2 RSPTs designated as RSPT1 and RSPT2. The RSPT signals for the removed CEA numbers 88, 89, 90 and 91 (Subgroup 22) are provided by RSPT signals from CEAs 81, 83, 85, 87 (Subgroup 21).

The current configuration of the CPCS has a total of 22 RSPT1 input signals terminated in the Channel A Auxiliary Protective Cabinet (APC). There are 21 RSPT1 inputs to be processed by the Channel A CPC and all 22 RSPT1 input signals are sent to CEAC 1 in Channel B. There is a qualified isolator between Channel A and Channel B to maintain separation between the two channels.

The current configuration of the CPCS has a total of 65 RSPT1 signals terminated in the Channel B APC. Twenty one (21) of these signals are processed by the Channel B CPC. All 65 RSPT1 inputs plus the 22 received from Channel A are processed by the Channel B CEAC No. 1. As a result, CEAC No. 1 reads 87 CEA positions.

The current configuration of the CPCS has a total of 65 RSPT2 signals terminated in the Channel C APC. Twenty one (21) of these signals are processed by the Channel C CPC. All 65 RSPT2 inputs plus the 22 RSPT2 signals received from Channel D are processed by the Channel C CEAC No. 2. As a result, CEAC No. 2 reads 87 CEA positions.

The current configuration of the CPCS has a total of 22 RSPT2 input signals terminated in the Channel D APC. There are 21 RSPT2 inputs to be processed by the Channel D CPC and all 22 RSPT2 input signals are sent to CEAC 2 in Channel C. There is a qualified isolator between Channel D and Channel C to maintain separation between the two channels.

The CPCs use their channelized set of CEA positions and channelized process inputs to calculate Low DNBR and High LPD. Each CPC uses 21 channelized RSPT signals for the DNBR and LPD calculations. These 21 CEAs are referred to as target rods.³³ The lines in Figure 3.1-1 between the CEACs and the CPCs (identified with "CEAC 1(2) PF") represents point-to-point serial links between each CEAC to each CPC to provide the CEAC penalty factor to each of the four CPCs. These data links are electrically isolated as they cross protective channel boundaries.³⁴ The CEACs are reading redundant CEA positions and execute a redundant penalty factor calculation. A CPC reads the two penalty factors from the two CEACs to apply the most conservative penalty factor to the calculations for Low DNBR and High LPD.³⁵

As shown in Figure 2-1, each CPC receives the following inputs: core inlet and outlet temperature, pressurizer pressure, reactor coolant pump speed, excore nuclear instrumentation flux power (each subchannel from the safety channel), selected CEA positions, and CEA deviation penalty factors from the CEA calculators.³⁶

Outputs of each CPC are:

- a) DNBR trip and pre-trip to the PPS/RPS
- b) DNBR margin to a safety-related recorder/indicator on the control board
- c) Local power density trip and pre-trip to the PPS/RPS
- d) Local power density margin to a safety-related recorder/indicator on the control board
- e) Calibrated neutron flux power to a safety-related recorder/indicator on the control board
- f) CEA withdrawal prohibit on DNBR or local power density pre-trip or CEA misoperation to the PPS and to CEA Rod Control from the PPS via a qualified isolator. The PPS interface to the CEA Rod Control is not part of the replacement CPCS scope.³⁷
- g) Control room alarms (e.g., CEAC FAIL)

As described in Section 2, each CPC drives an OM located on the control board. It is a safety-related module. From the four modules an operator can monitor all calculators, including specific inputs or calculated functions, and allow operators to change addressable constants. The OM for channels B and C are able to access the CEA calculators in those channels.

During periodic testing a mass storage unit is connected to the CPC channel to perform channel functional testing. This is a temporary connection and the CPC channel trip outputs are bypassed at the PPS during channel functional testing. Section 2 provides further description of the offline testing for the CPC.³⁸

All four channels of the CPC/CEAC system are installed in the Auxiliary Protective Cabinet (APC) in the control room area, where the channels are physically separated and isolated from each other. Each Channel in the APC Cabinet has two redundant APC Multiplexers (APC MUX). See Section 2 for the description of the APC MUX. This non-safety system will be replaced as part of the CPCS modification project, as described in Section 3.2.4, but under 10 CFR 50.59. It is described in the LAR to inform the NRC of the existence of this non-safety related system in the safety APC. The APC MUX in the APC is seismic Category I.³⁹

3.2 NEW SYSTEM ARCHITECTURE (D.2.2)

The major architectural change between the existing architecture and the new Common Q architecture is in the area of CEA processing. In the existing system, there are two CEACs total (CEAC 1 and CEAC 2) with CEAC 1 located in Channel B and CEAC 2 located in Channel C that receive the CEA RSPT signals from Channels A, B, C, and D. The CEACs located in Channel B and C distribute the penalty factors and other calculated results to the CPCs in Channels A, B, C and D. For the replacement CPCS, there are still four independent CPCs, but each CPC channel includes its own CEAC 1 and CEAC 2. The CEA RSPTs terminated in each channel will be connected to a CEA Position Processor (CPP) located in that channel, and these CPPs will distribute CEA position inputs to the corresponding CEAC 1 and CEAC 2 located in each channel. As in the existing system, the RSPT1 signals will provide CEA positions to CEAC 1, and the RSPT2 signals will provide CEA positions to CEAC 2. The existing architecture has only two CEACs shared by four CPC processors. Increasing the number of CEACs to eight (two in each channel) increases the availability of the CEAC processing.

Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram is a block diagram of the CPCs. In the existing CPCS, the four CPC channels (A through D) are mounted in the APC. The APC (CP-22) is constructed so that each channel is located in a separate cabinet section or bay that is physically separate from the other bays or sections which meets the requirements for channel separation.⁴⁰

The new Common Q CPCS hardware is mounted within the APC with one channel in each bay just like the existing system. For each channel the architecture of the new system includes the following:⁴¹

- CPC AC160 controller chassis (CPC Primary PM646A, CPC Auxiliary PM646A and associated I/O)
- CEAC 1 AC160 controller chassis (CEAC 1 PM646A, CEA Position Processor (CPP) 1 PM646A, and associated I/O)
- CEAC 2 AC160 controller chassis (CEAC 2 PM646A, CPP 2 PM646A and associated I/O)
- Redundant AF100 intrachannel buses connecting the three AC160 controllers (via a CI631 communication module), the OM, and the Maintenance and Test Panel (MTP). The AF100 bus is extended from the APC to the OM via fiber optic cable.
- One-way High Speed Links (HSLs) for each of the following:
 - CEA Position from redundant CPPs mounted in the CEAC controller chassis to the CEAC PM646A in all four channels
 - CEAC PM646As to CPC PM646A in each channel
 - CPC Primary PM646A to CPC Auxiliary PM646A in the same controller chassis
- Interposing Relay Panel (IRP) which houses the channel interposing relays for each channel digital output (DO) as well as the CPC watchdog timer (WDT) interposing relay and the MTP Test Enable relay.
- An MTP that houses a flat panel display (FPD), and provides isolation between the AF100 bus input and an optically isolated unidirectional Ethernet output connection from the MTP to a non-safety remotely mounted single board computer (SBC) for the UDP to TCP/IP Converter Assembly.
- An OM that consists of the Common Q FPDS, key switches, and AF100 bus optical modem.
- Power Supply Assembly, housing redundant RSPT Power Supplies (15 Vdc), relay power supplies (24 Vdc), and processor power supplies (24 Vdc)

The OM is mounted on the main control board outside the APC (also depicted in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram). The OM forms the primary graphical user interface (GUI) for the operator during normal system operation. The OM has its own power supply, and is provided with vital 120 Vac from the same bus as its associated CPC channel. The OM supports an optically isolated unidirectional Ethernet connection to support the OM “Printscreen” and Cyber Log functions to a non-safety remotely mounted single board computer (SBC) for the UDP to TCP/IP Converter Assembly.⁴²

a,c

Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram⁴³

The CEA Display in the upper right corner of Figure 3.2-1 and the APC MUX at the bottom of the figure are non-safety related systems and are not part of the License Amendment Request. That part of the plant modification will be made under the 10 CFR 50.59 process as part of the Engineering Change (EC).

3.2.1 CPC AC160 Controller

This controller includes the CPC PM646A primary processor module, used to implement the safety-related CPC algorithms. It also includes an auxiliary CPC PM646A processor used for non-trip related overhead functions, and a variety of I/O modules used to:

- process all required analog inputs with the exception of target CEA positions,
- generate analog outputs to MCB meters,
- generate digital trip signal outputs to the RPS/PPS
- generate digital alarm outputs via the IRP for plant annunciators (including new auxiliary trip pre-trip alarms)
- process all required digital input signals⁴⁴

The CPC PM646A processor module executes the safety-related algorithms which are functionally identical to those implemented in the existing CPC/CEAC system, as specified in Appendix A of Reference 2 as augmented by Reference 21. Functionally identical means that the algorithms in the upgraded CPCS will accomplish the same function within the same requirements for system time and accuracy⁴⁵. Changes to the CPC/CEAC applications program required by the new platform is restricted to enhancements, such as improved HMI⁴⁶ and error handling routines⁴⁷, and changes to adapt the application programs to the new platform without degrading the ability of the CPCs to perform their safety related function⁴⁸. These same changes were made as part of the Palo Verde CPCS replacement and was reviewed and approved by the NRC.⁴⁹

The CPC AC160 Controller consists of the following AC160 modules:

- One CI631 communications module

[

]a,c

- One PM646A Primary CPC processor module (PM646A)

[

]a,c

[
] ^{a,c}

- One PM646A Aux CPC processor module

The Aux CPC PM646A is located in the AC160 controller slot adjacent to the CPC Primary PM646A. It performs non-essential CPC functions such as storing trip buffer reports and failed sensor stacks, thus unburdening the primary CPC processor, which can more efficiently perform its safety-related trip functions. The primary CPC processor transmits information to the auxiliary CPC processor over one-way HSL.⁵²

- Two AI688 analog input (AI) modules

Two analog input (AI) cards redundantly provide the analog inputs used by the CPC PM646A, with the exception of Target CEA positions, which are received over HSL from the CEAC AC160 controllers in the channel. Each of the redundant analog input modules is capable of monitoring up to 16 inputs over the range of 0 to 10 Vdc. CPC Analog inputs to each card include:

- Hot Leg 1 Temperature (1 to 5 Vdc) – one input
- Hot Leg 2 Temperature (1 to 5 Vdc) – one input
- Cold Leg 1 Temperature (1 to 5 Vdc) – one input
- Cold Leg 2 Temperature (1 to 5 Vdc) – one input
- RCS Pressurizer Pressure (1 to 5 Vdc) – one input
- Upper Subchannel Ex-core NI input (0 to 10 Vdc) – one input
- Middle Subchannel Ex-core NI input (0 to 10 Vdc) – one input
- Lower Subchannel Ex-core NI input (0 to 10 Vdc) – one input
- APC Temperature –one input per AI module, not redundant. There are two separate temperature sensors monitoring APC temperature. Each of the AI cards in the CPC AC160 controller reads a separate sensor (i.e., temperature inputs are not redundant from the same sensor).⁵³

The above list of analog inputs thus encompasses all CPC channel analog inputs with the exception of CEA positions, which will be monitored by the CEA position Processors (CPPs) in the CEAC 1 and 2 AC160 controllers.⁵⁴

The Palo Verde CPCS used the Common Q AI685 Analog Input Card. This analog input card has been replaced with the Common Q AI688 Analog Input Card. It processes the same 0-10 Vdc signal and has been reviewed by the NRC as part of the 2013 update of the Common Q Topical Report (Reference 4).

- One DP620 pulse to frequency converter module

[

] ^{a,c}

[

]^{a,c} The RCP signal conditioning

system is not being changed as part of the EC.

- One AO650 analog output (AO) module

The AO module provides the 0 to 10 Vdc analog outputs for the following:

- DNBR Margin Indication on the Main Control Board (DNBR MARGIN), Scaled for 0 to 2 DNBR Units
- KW/ft Margin Indication on Main Control Board (LPD MARGIN), Scaled for 0 to 25 kW/ft
- Calibrated Nuclear Power Indicator/Recorder on MCB (PHICAL), Scaled for 0 to 200% Rated Thermal Power
- Core Total Flow – no indicator, used for startup testing (MASS FLOW), scaled for 0 to 2.0 fraction of rated flow

Note that the existing WF3 CPCS provides a 0-10V signal corresponding to 0-10 DNBR units. The DNBR trip setpoint is set to between 1.2 – 1.3 DNBR units thus the meter only uses 0 – 1.3 Vdc of the entire 10V range. Thus, changing to the above range provides much higher resolution on the meter for this indication.⁵⁶

A total of eight analog outputs are provided for use. One set of four outputs is sent to MCB indicators, as defined above. The second identical set is available for use if desired (for example, a hard wired analog input to the Plant Monitoring System). All of these values are provided to the Plant Monitoring Computer over the CPCS to PMC data link.⁵⁷

- One DI620 digital input (DI) module
 - DNBR and LPD trip channel bypass status from the PPS to enable CPC testing.

As in the existing design, trip channel bypass of the DNBR-Low and LPD-High trips in the PPS channel is a necessary precondition for performing channel CPC or CEAC testing. This DI provides trip channel bypass status to the CPC channel from the PPS to enable channel functional tests.

- Bypass permissive status (1E-4% power from the Ex-core Nuclear Instrumentation) used to enable DNBR/LPD operating bypass.

Bypass Permissive status from the PPS will be read as a CPC digital input. If the permissive is present, and the bypass has been inserted on the OM or MTP touch screen; a CPC Digital Output will be used to energize a hardware bypass relay. The hardware bypass relay contacts will short the Low DNBR and High LPD trip and pre-trip contacts when in bypass, effectively bypassing the trip and pre-trip functions, as in the present design.

Contacts from this hardware Bypass Relay shall also be used to provide bypass annunciation.

A second means of enabling this bypass relay will be implemented purely in hardware, using a locally (APC) mounted Bypass key lock switch in series with the 1E-4 % power permissive contact signal to energize the Bypass relay. Thus, as in the present design, it shall be possible to bypass a channel if power level is below the permissive setpoint even if that channel is Inoperable due to processor failure. If power rises above the permissive setpoint, the bypass will automatically be removed, as in the present CPC implementation.

- Op. Bypass Inserted Status

[] ^{a,c}

- Software Load Enable (SLE) Switch Status

This input reads the SLE switch. Placing this switch in the SLE position will result in Low DNBR and High LPD channel auxiliary trips.

- Power Supply Trouble:

Each power supply module within the power supply assembly contains features such as overvoltage, overcurrent, undervoltage, and short circuit protection. A contact output is monitored by the AC160 that indicates a problem with the power supply. In addition, there is a power supply cooling fan assembly which will provide a contact opening on power supply fan failure. The power supply alarm inputs to the DI module are as follows:

- PS Fan Failure
- Power Supply Failure (1 per module)⁵⁸

- One DO625 digital output (DO) module

One DO module is used to provide trip and annunciator output contacts for the following:

- Low DNBR Trip
- Low DNBR Pre-trip
- High LPD Trip
- High LPD Pre-trip
- Auxiliary Pre-trip Alarm
- CEA Withdrawal Prohibit (CWP)
- CPC Trouble
- CPC Fail
- Aux CPC Trouble
- CPC Test
- CPC Sensor Fail
- CEAC 1 Inoperable

- CEAC 2 Inoperable
- High Cabinet Temperature
- Operating Bypass

The final DO in the above list will be used to energize the DNBR/LPD Operating Trip Bypass relay when power is below the permissive setpoint.

The digital outputs operate interposing relays mounted on an Interposing Relay Panel (IRP) which provide electrical isolation between the DO modules and the output signals.

[

] ^{a,c}

3.2.1.1 CPC Application Program

The CPC Primary PM646A executes the CPC application program. [

] ^{a,c}

[

]^{a,c}

Table 3.2.1.1-1 CPC Program Execution Intervals and Input Sampling Rates shows the inputs and execution interval for each CPC application program.

Table 3.2.1.1-1 CPC Program Execution Intervals and Input Sampling Rates⁶¹

			a.c

3.2.1.2 Aux CPC Processor Application Program

There is a second PM646A in the CPC controller chassis. A high speed link (HSL) is connected between the CPC PM646A and the Aux CPC PM646A. The Aux CPC receives data from the CPC PM646A to formulate the trip buffer and failed sensor stack reports.⁶²

The Aux CPC does not perform any safety-related processing. There are two main functions of the Aux CPC application program: 1) format the trip buffer report and 2) format the fail sensor stack. These functions are a carryover from the legacy CPCS functionality and its implementation is identical to the Palo Verde CPCS replacement.⁶³

* This change from the original CPCS design has been reviewed and approved by the NRC for the Palo Verde CPCS replacement LAR.

The trip buffer is a snapshot of a specified number of variables that is “frozen” when a CPC trip occurs. The CPC processor feeds the Aux CPC with the values for the specified variables, and the Aux CPC processor formulates the data into a report for display on the OM and MTP.⁶⁴

The CPC PM646A provides the Aux CPC with the list of failed sensors for the failed sensor stack and formulates a report for display on the OM and MTP.⁶⁵

3.2.2 CEAC AC160 Controller

There are two CEAC AC160 Controllers referred to as CEAC 1 and CEAC 2. These AC160 controllers include the CEAC PM646A processor as well as CEA Position Processor (CPP) and supporting I/O modules. The CEAC processor calculates CEA deviation-related penalty factors based on CEA position input from all RSPT signals (RSPT1 for CEAC 1 and RSPT2 for CEAC 2) on all CEAs, and transmits these penalty factors to the CPC processor within the channel.⁶⁶

[

]^{a,c}

The CEAC 1 and 2 AC160 controller configurations are similar. Their differences are discussed in the description below. This implementation is nearly identical to the implementation of the Palo Verde CPCS. The one difference is the AI688 analog input module. The Palo Verde CPCS uses the AI685 analog input module. The AI688 analog input module was reviewed and approved by the NRC as part of the 2013 Common Q Topical Report update in 2013 (see Reference 4).

The CEAC AC160 controller includes the following AC160 modules:

- One CI631 communications module

[

] ^{a,c}

- One PM646A CEAC processor module

The CEAC processor module executes the CEAC algorithm. [

] ^{a,c}

The CEAC 1 PM646A executes the same safety-related application as the legacy (existing) CEA Calculator No. 1 in Figure 2-2 Existing CPC/CEAC Architecture Block Diagram. The CEAC 2 PM646A executes the same safety-related application as the legacy (existing) CEA Calculator No. 2 in Figure 2-2 Existing CPC/CEAC Architecture Block Diagram. This algorithm generates DNBR and LPD penalty factors in the event of detection of CEA deviations in a CEA subgroup. These penalty factors are transmitted over HSL to the CPC processor in the same channel. As in the legacy (existing) implementation, the CPC application selects the higher penalty factor from CEAC 1 or CEAC 2. The CEAC algorithms are defined in Appendix A of Reference 2.

The Common Q CEAC implementation also results in the need for the following additional software in the CEAC and CPC, beyond that in the legacy (existing) implementation:

- Target CEA Position transmission: The CPC channel no longer directly reads Target CEA positions using its own analog input modules. Target CEA positions are transmitted to the CPC from the CEAC over the same HSL as the DNBR and LPD penalty factor transmission. [

] ^{a,c}

- CEA Position sensor fail status is also transmitted to the CPC channel from the CEAC PM646A. This status is received by the CEAC from the CPP along with the CEA position and then passed on to the CPC PM646A via the HSL interface. CEA position sensor status is used in the CPC to establish validity of the target CEA position input. In the event that

the CEA position input to the CPC via the CEAC 1 data link should fail, the input via the CEAC 2 data link will be utilized by the CPC.

Transmission of Target CEA position via the CEAC HSL is regarded as a separate and distinct function from that of transmitting penalty factors. CEAC 1 in all four CPC channels always generates penalty factors based upon RSPT1 CEA position. CEAC 2 in all four channels always generates penalty factors based upon RSPT2 CEA position. However, transmission of Target CEA position to the CPC processor within a channel will be from the same RSPT source, whether the CEAC 1 or CEAC 2 data link is employed. In channels A and B, RSPT1 will provide Target CEA position signals. In channels C and D, RSPT2 will provide Target CEA position information. Thus, it is necessary for both CEACs in each channel to obtain target CEA position from their respective CPPs that are reading analog input modules. In the case of CEAC 1 this will be CPP 1, and for CEAC 2 this will be CPP 2.⁷¹

- Two PM646A CPP processor module

The CEA Position Processor (CPP) reads the RSPT channel hardwired inputs, converts the voltage inputs into CEA position values, detects input channel failures, and transmits the CEA position values over the HSL to a PM646A module in a CEAC AC160 controller chassis in all four CPCS channels. Table 3.2.2-1 Preferred Source for CEA Position Data defines the source of CEA position information for the two CEACs in each of the four CPC channels. [

] ^{a,c}

CPP 2 transmits the data to CEAC 1 via HSL since it is in a different controller chassis within the channel. [

] ^{a,c}

CPP 1 transmits the data to CEAC 2 via HSL since it is in a different controller chassis within the channel. [

] ^{a,c}

Table 3.2.2-1 Preferred Source for CEA Position Data⁷³

					a,c

A second function of the CPP is monitoring the target CEA positions within the CPC channel. Note that in channels A and B, Target CEA positions are based upon RSPT1, whereas in Channels C and D, it is based upon RSPT2.⁷⁴

[

]a,c

[

] ^{a,c}

- Two (channels A and D) or five (channels B or C) AI688 analog input (AI) modules

The CPCS design allows for up to 24 CEA positions (5 to 10 Vdc) to be monitored in channels A and D, and up to 73 CEA position inputs (5 to 10 Vdc) to be monitored in channels B and C. The analog input module is capable of monitoring up to 16 inputs over the range of 0 to 10 Vdc.⁷⁷

In both CEAC AC160 controller chassis, the 15 Vdc auctioneered RSPT power supply voltage is monitored by one analog input through voltage dividers so as not to exceed the range limit of the analog input module.⁷⁸

- One digital output (DO) module

The DO card is used to provide trip and annunciator output contacts for the following alarm and annunciation:

- CEA Deviation CEAC 1
- CEAC 1 Fail (or CEAC 2 Fail in the CEAC 2 AC160 Controller)
- CEAC 1 Sensor Fail (or CEAC 2 Sensor Fail in the CEAC 2 AC160 Controller)
- CPP 1 Trouble (or CPP 2 Trouble in the CEAC 2 AC160 Controller)
- CEAC 1 Trouble (or CEAC 2 Trouble in the CEAC 2 AC160 Controller)
- CEAC 1 Test (or CEAC 2 Test in the CEAC 2 AC160 Controller)

The digital outputs operate interposing relays mounted on an Interposing Relay Panel (IRP) which provide electrical isolation between the DO modules and the output signals.⁷⁹

3.2.2.1 CEAC Application Program

The CEAC PM646A executes the CEAC application program. [

] ^{a,c}

Table 3.2.2-2 CEAC Program Execution Intervals and Input Sampling Rates

a,c

3.2.3 Power Supply

The power supply powers the AC160 controllers, relays, and reed switch position transmitter circuits. Separate power supply modules are used for these different functions. All power supplies within a CPC channel receive AC power from the associated CPC channel Vital AC input power.

There are six power supplies in each CPC/CEAC channel. These consist of dual 24 Vdc auctioneered processor power supplies for the AC 160 processor equipment, a dual auctioneered 24 Vdc auxiliary power supply for output relays, and dual auctioneered 15 Vdc RSPT power supplies for CEA position input information.

Redundancy will be available for all power supply pairs using diode auctioneering which provides bumpless transfer upon module failure. Faults in one half of a redundant supply will not prevent the other from operating normally. Redundant modules can be replaced while the power supply remains energized without disturbing the powered system.

The power supply is configured so that it is not near its maximum loading to extend its life. Supplemental cooling is provided to extend the life of components.

Sufficient hold up time (20 milliseconds) is provided to allow momentary loss of external power due to bus transfer.

Each power supply has protection features for overvoltage and over current. Alarm contact outputs from the power supply modules are monitored by the CPC channel DI module. One DI is used for each power supply module.

The power supply assembly includes local monitoring features, such as lamps, to aid in diagnosing individual power supply problems.⁸²

3.2.4 APC Multiplexer

As described in Section 2, each channel in the existing APC has two redundant APC Multiplexers (APC MUX). These APC MUXs transmit the non-safety related Fixed Incore Detector Amplifier Systems (FIDAS) signals to the Plant Computer. Although the APC MUX data acquisition to the plant computer is a non-safety related function, the equipment resides in the safety-related APC and therefore needs to be qualified as an associated circuit in accordance with the WF3 licensing basis (NRC Regulatory Guide 1.75) (Reference 7).

The APC MUX is replaced with a non-safety chassis capable of accepting the 0 to -10Vdc incore detector signals from the incore amplifier and transmitting them via Ethernet to the plant monitoring computer (PMC). The replacement APC MUX provides its own Ethernet link separate from the CPC link to the PMC.⁸³

To meet the requirements of RG 1.75, the replacement APC MUX will go through equipment qualification to meet seismic DBE requirements for structural integrity and to meet EMC requirements to avoid EMI issues with the other safety-related equipment mounted in the APC.⁸⁴

3.2.5 HVAC Requirements

The CPCS is installed in the APC which is located in the main control room area. The HVAC heat load calculation (Reference 38) assumes the CPC heat load in the APC (CP-22) is:

- Channel A 2863 Watts
- Channel B 5171 Watts
- Channel C 4171 Watts
- Channel D 2863 Watts

POWER LOSS = 15,068 Watts

According to the Palo Verde CPCS Technical Manual (Reference 30), Section 2.1.1 specifies the typical power usage, and thus power consumption to be:

- Channels A/D: 463.6 Watts
- Channels B/C: 559.6 Watts

This represents a maximum of 16.2% of the assumed heat load in the HVAC heat load calculation for the CPCS. The architecture similarities between the Palo Verde CPCS and the Waterford CPCS replacements are such that should the heat load double for an unforeseen reason, the assumptions in the HVAC heat load calculation would not be affected.

The Waterford CPCS heat load calculation will be issued once the detailed hardware design is complete.

3.2.6 CPCS Design Function

The CPCS design functions are unchanged as a result of the CPCS upgrade using the Common Q Platform. The same design basis algorithms are used however the timing of some of the application programs were changed to accommodate the change in platform. This is identified in Table 3.2.1.1-1 CPC Program Execution Intervals and Input Sampling Rates. These changes were analyzed for the impact on response time in a timing analysis performed for the Palo Verde CPCS upgrade. The analysis concluded that the Common Q CPCS meets the design basis response time requirements for the Palo Verde Nuclear Generating Station.

Similar to Palo Verde, nuclear power plants typically allocate a “response time budget” for the I&C equipment portion of the safety system in their safety analysis. These budgets usually are conservative assumptions independent of the I&C equipment used and confirmed once by their safety analysis. In the case of WF3, the actual response time calculations of the legacy I&C CPCS equipment established the response time criteria (budget) in the safety analysis for the CPCS with no timing margin.

The WF3 CPCS Timing Analysis (Reference 55) documents the response time for the WF3 Common Q CPCS upgrade. [

] ^{a,c} As part of the normal fuel reload process, Waterford runs the safety analysis of record with the WF3 CPCS calculated response times to validate that acceptable margin is maintained. It is the fuel reload process performed under 10 CFR 50.59 that evaluates the results of the rerun of the safety analysis prior to core reload.

The estimate is documented in Reference 24. The basis of the estimate is the CEA rod drop time LAR submitted in 2015 that increased the CEA rod drop time in the safety analysis an additional 200 ms due to a hold coil delay that needed to be accounted for. The method used for the CPCS delay time estimate on thermal margin results is to take the thermal margin degradation of the CEA rod drop 200 ms delay and then extrapolate for the increase in CPCS response times. [

] ^{a,c}

In the case of the following DBE’s both the 200 millisecond increase in hold coil delay [^{a,c} resulted in no changes to the minimum DNBR or high LPD (peak linear heat rate):

- Increased Main Steam Flow (FSAR Section 15.1.1.3)
- Uncontrolled CEA Withdrawal from a critical condition (FSAR Section 15.4.1.3)

In the case of Asymmetric Steam Generator Transient (FSAR Section 15.9.1.1), the combination of the CPCS ΔT_{cold} trip in combination with the required overpower margin reserved in COLSS ensures that all the acceptance criteria ($DNBR \geq 1.24$ and $LHR \leq 21$ kw/ft) continue to be met. This conclusion was not impacted by the 200 milliseconds increase in hold coil delay time []^{a,c}.

The “0.8 sec HCD time” column is the margin degradation as a result of the 200 millisecond hold coil delay time. The next column to the right is the combination of this 200 millisecond delay []^{a,c}. AOR stands for the Safety Analysis of Record.

$$]^{a,c}$$
[illegible]

[illegible]

[illegible]

[

] ^{a,c}

3.2.7 Service/Test Functions

The Common Q CPCS is designed for fail safe operation under component failure or loss of electrical power as defined in the Failure Modes and Effects Analysis (FMEA) in Appendix 2 of the Topical Report, Reference 5. Sections 2.3.3, 2.4.2, 3.1.1.1.3, 3.1.1.4 and 3.1.1.7 of the CPCS System Requirements Specification (Reference 2 as augmented by Reference 21) provides the CPCS failure analysis.⁸⁵

The following list of processor fault conditions for the existing CPC implementation, describes how they are addressed for the Common Q CPCS:

[

] ^{a,c}

3.2.7.1 Maintenance and Test Panel (MTP)

Each CPC channel has an MTP. This panel is provided at the APC as the primary human system interface (HSI) for routine maintenance and testing by plant technicians. It is located in the APC, and uses a display screen. Many of the OM display functions are duplicated on the MTP. The MTP has a test mode to support maintenance testing.⁹¹ This functionality is identical to the Palo Verde CPCS replacement that was reviewed and approved by the NRC. The Palo Verde implementation included AI calibration as part of this function, but the AI688 cards do not require calibration and therefore are not included in this description.

The CPCS requires two input signals to go into test mode, PPS Test Enable and the MTP function Enable signals. The PPS Test Enable signal is generated by bypassing the DNBR and LPD signals at the PPS and provides the permissive signal for allowing the CPCS to be tested. The MTP has a Function Enable (FE) key switch that must be in the enable position in order to allow entering the Test Mode.⁹² Test Mode Displays are:

- Test Main Page⁹³

The Main Surveillance Test page provides status indicators showing which of the processors are in Test Mode. This will depend upon which of the tests have been initiated.

- CPC Functional Test⁹⁴

Note: This functional test screen is not to be confused with the technical specification periodic channel function test surveillance requirement, which is being eliminated.

Selecting the CPC Functional Test Icon forces entry into the CPC Test Mode, causing an auxiliary trip (DNBR/LPD channel trips), Channel Test indication, and CPC Test annunciation. A separate icon is used to exit from the CPC Functional Test. The auxiliary trip and associated indication/annunciation are cleared when the CPC Processor is no longer in Test Mode. The CPC remains in Test Mode until the functional tests are inactive (complete) and the Exit Functional test icon has been selected.

The Cabinet Temp DO Test is supported by an “On” icon, which initiates the cabinet temperature DO test by opening the alarm contact, and an “Off” icon which terminates the test, by restoring it to its pre-test position.

The DNBR and LPD Trip relay test is supported by buttons that allow the operator to change the state of the DNBR and LPD output trip contacts between “OPEN” and “CLOSED”.

- Load Addressable Constants⁹⁵

A “Load Addressable Constants” icon on the Test page supports loading of addressable constants into the CPC, CEAC 1, and CEAC 2 AC160 processors. A separate icon in proximity of the “Load Addressable Constants” icon is used to exit the Load Addressable Constants mode, clearing all associated trips, indication, and annunciation.

Depressing the Load Addressable Constants icon forces the CPC channel under test in a test mode, causing an auxiliary trip, and cause Channel Test indication, CPC Test, CEAC 1 Test, and CEAC 2 Test annunciation.

Addressable constants are loaded from removable media. This media is stored and secured using plant procedures. When the Addressable Constants are to be read in from removable media, the cyclic redundancy check (CRC), date, time, and channel identifier generated at time the addressable constants were saved is displayed. A prompt asks for verification that the data is correct, prior to permitting addressable constant load.

CPPs remain functional throughout this mode of operation, permitting normal CEA position transmission to all channels.

- Load Reload Data Block (RDB) Constants⁹⁶

Reload Data Block is in reference to fuel-dependent variables that need to be updated every refueling cycle. The Common Q CPCS replicates this functionality. The RDB block is loaded from removable media. This media is stored and secured using plant procedures. A “Load RDB” icon on the Test page supports loading of the RDB. A separate icon in proximity to the Load RDB icon is used to exit the RDB Load mode, clearing all associated trips, indication, and annunciation. Depressing the Load RDB icon forces the CPC channel in a test mode, causing an auxiliary trip, and cause Channel Test indication, CPC Test, CEAC 1 Test, and CEAC 2 Test annunciation. The CRC, Sequence, and Version of the RDB media is displayed. A prompt asks for verification that the data is correct, prior to permitting RDB load. CPPs remain functional throughout this mode of operation, permitting normal CEA position transmission to all channels.

The MTP is also used to load AC160 software. In order to load CPCS AC160 processor applications software it is necessary to place the two position SLE key-switch in the “SLE” position and select the destination AC160 processor (one of six) with the processor select (PS) switch. While the SLE switch is in the enable position, Low DNBR and High LPD trip contacts are opened in the affected channel.⁹⁷

The SLE switch can perform the following three functions:

[

] ^{a,c}

This functionality is identical to the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.2.7.2 OM/MTP Service/Test Functions

In addition to the MTP service and test functions described in Section 3.2.7.1, there are service/test functions that are both available on the OM as well as the MTP. These display functions are identical to those implemented for the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.2.7.2.1 Standard Display¹⁰²

The Standard Display Page emulates the existing OM interface, but with additional Tag Names for point ID values, to minimize training required to use the new displays. A “Find Tag Name” icon is provided on this display as an operator aid in associating tag names with Point IDs.

The “memory protect” keylock on the existing (legacy) display is eliminated. This function is addressed by the SLE interlock at the APC. The existing dedicated “Channel Bypass” switch and “Change Value” switches have had their functions combined into a common “Function Enable” key-lock switch mounted near the OM display.

The existing “Calculator Select” switch on the OM is eliminated. Instead of using this switch to display either CPC or CEAC point IDs, the point ID assignments have been changed by converting the three-digit point IDs of the existing CPCS to a four-digit Point ID. The first digit denotes the calculator.

The existing OM keypad, Point ID, Change Value, and Execute icons have been retained and have similar functionality in the new OM display. The replicated functions for the standard display include:

- Point ID Requests – Displays a value associated with a Point ID or addressable constant.
- Change Value Requests – Allows changing a value associated with a Point ID if it is classified as an addressable constant. The FE key switch must be in the enable position to allow this function.
- Operating Bypass Insertion and Removal – This replicates the existing CPCS function. This function can also be performed on a dedicated DNBR/LPD OP BYPASS display. Operating bypass of the CPC channel may only be performed when the power level, as sensed by the PPS Safety Channel Nuclear Instrumentation, is below the bypass permissive setpoint (nominally 1E-4%), and if the FE switch is placed in the “enable” position. The bypass permissive is provided from the PPS as a DI to the CPC channel. The FE switch position is a DI to the OM/MTP PC Node Box. Both DIs need to be true to allow this function to be performed.

In addition to the OM and MTP bypass capability described above, it is also possible to perform the bypass at the APC using a dedicated two position (OFF/BYPASS) key switch, independent of the “function enable” switches on the OM or MTP. This is to provide a hardware backup bypass capability in case the CPC channel is inoperable. This CPC hardware bypass switch must be left in the “bypass” position as long as the bypass is to be in effect. This is governed by administrative procedures. This function is identical to that implemented for the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.2.7.2.2 Nuclear Instrumentation (NI) Calibration Display¹⁰³

This display replaces the manual procedure for NI calibration. This display calibrates the NIs based on one of three off line sources of calorimetric power entered by the operator. The FE key switch must be in the enable position to allow this function. This is an identical function implemented for the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.2.7.2.3 System Status: CPCS System Health Page¹⁰⁴

The CPCS System Health Page includes a graphical depiction of the CPCS channel including all major components. This display is to facilitate diagnosis of CPCS system failures, at least to the module level. Alarm (or system error) conditions affecting one or more of the displayed components causes a color change of that component. The color shall remain in an alarm condition for the duration of the alarm condition.

[

] ^{a,c}

3.2.7.2.4 System Event List¹⁰⁵

The System event list provides one or more pages of dynamic alarm and status information. This list includes all CPCS channel current diagnostic failure (error) conditions. There is also a System Event Log that provides one or more pages of historical alarm and status information. It includes historical logging of the previous thirty diagnostic system failures. The log can be cleared with the FE key switch in the enable position.

3.2.7.2.5 CPC and CEAC Trip Buffer Displays¹⁰⁶

In the event of a Low DNBR or High LPD channel trip, the CPC trip buffer will be frozen at the time of trip [

] ^{a,c}. Similarly, the CEAC snapshot will be frozen on each of the following conditions:

- At least one of the CEAs in a subgroup with a deviation is between the top and bottom deadbands
- Multiple deviations in a subgroup
- Excessive number of input signal failures in a core quadrant
- Excessive number of deviations in a core quadrant (the is a subset of first condition)

When a snapshot is frozen, the current snapshot will depict data at the time of the freezing. [

] ^{a,c}

A print out of the CPC Trip Buffer and the CEAC snapshot can be initiated from this display.

3.2.7.2.6 Failed Sensor Stack¹⁰⁷

This display mimics the legacy (existing) CPC failed sensor stack. It displays the last twenty sensor failures. There are separate failed sensor stacks for the CPC, CEAC 1 and CEAC 2 AC160 controllers. This display also provides the means to clear the CEAC rate of change failure condition. The CEAC application program monitors for an excessive rate of change of CEA position. The rate of change failure latches and must be manually cleared via this display. The CEAC application program considers this a CEA failed sensor until the latch is cleared.

3.2.7.2.7 CRC/SysLoad

This page provides a dynamic display of the status of the PM646A CRC diagnostic and the processor loading. [

]a,c

[

] ^{a,c}

[

] ^{a,c}

[

] ^{a,c}

3.2.7.2.8 Trip Status Display

This display provides status indication for any trips, pre-trips or when a CWP alarm is present.¹¹⁸

3.2.7.2.9 FPD Status List

Each flat panel display (OM, MTP) contains a diagnostics page applicable to that display.¹¹⁹

3.2.7.2.10 Input Module Comparison¹²⁰

Provides one or more pages displaying dynamic analog input module values. Redundant module readings are displayed in a side by side format to facilitate comparison of the readings from each of the redundant modules.

The deviation between readings for each module is also displayed in a separate column to the immediate right of the two display columns. This column is provided to facilitate monitoring of the deviation magnitude between redundant inputs.

Redundant pairs include:

- The AI modules in CPCS processor slots 5 and 6, which redundantly provide analog inputs to the CPC processor, and the AI modules in the CEAC processors.
- Corresponding AI modules in both CEAC AC160 controllers. CEA positions are redundantly processed by AI modules in both CEAC AC160 controllers. AI module locations and channel assignments are identical in the two CEAC AC160 controllers. Therefore, the side by side display includes AI module readings from the corresponding AI modules in each of the two CEAC AC160 controllers.

3.2.7.2.11 Misc. displays of variables

These displays are based on context (e.g., plant mode or support an operator function like channel check).¹²¹

3.2.7.2.12 Dedicated Alarm Indication¹²²

The following alarm conditions are displayed on the OM and MTP. Note that it is possible to have several of these alarm icons illuminated simultaneously, if conditions dictate. For example, a processor module (PM646A) may detect a failure that will result in both a Channel TRBL and CPC Fail condition, each with a dedicated alarm icon.

All OM and MTP alarm icons will clear when the alarm condition clears, with the exception of the CPC Fail, CEAC 1 Fail, and CEAC 2 Fail alarms, which latch in, and must be manually reset by depressing the appropriate alarm icon. This is consistent with the existing CPCS functionality and the Palo Verde CPCS replacement. Resetting the alarm icons on either the OM or MTP will clear the alarm state at both locations.

For each of the alarm conditions, the system event list (Section 3.2.7.2.4) may be accessed on the OM or MTP. This page will provide diagnostic messages as to the alarm condition. In addition, the failed sensor stack (Section 3.2.7.2.6), and System health display (Section 3.2.7.2.3) may be used to provide diagnostic information.

The OM and MTP monitors all of the data packets being sent over the AF100 for indication that a data packet is not being updated. This can be the result of lost communication with the AC160 controller from where the data packet originated. Some alarm icons have multiple data packets associated with it that is used to determine the state of the alarm. The OM/MTP backlights an alarm icon with magenta when the OM/MTP detects a failed status on any data packet associated, as long as there is no alarm present on any of the data packets. If any of the "good" data packets associated with an Alarm icon contain an alarm value, the alarm value takes precedence over the failed status.

The CHAN TRBL alarm icon is displayed red when one of the AC160 controllers initiates a channel trouble alarm. The CHAN TEST alarm icon is red when one of the AC160 controllers imitates a channel test alarm.

The following Alarm icons are also present on the OM/MTP:

- CPC FAIL
- CPC SENS FAIL
- CEAC 1 (2) INOP*
- CEAC 1 (2) FAIL
- CEAC 1 (2) SENS FAIL
- CEAC 1 (2) CEA DEV

- * A CEAC can be manually put in the inoperable state (INOP) by the operator if the CEAC has failed. The CPC algorithm will use the last good penalty factor prior to this condition for selecting the maximum penalty factor between the two CEACs.

3.2.8 Separation and Independence

Each redundant CPC channel is electrically independent and isolated from adjacent channels, with the exception of the shared CEA position information through fiber-optically isolated HSL data links from the CEA Position Processors. This configuration of shared CEA position information is consistent with the current licensing basis described in the FSAR. It is also the exact same configuration for the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

The CPCS provides safety to non-safety communication through the Flat Panel Displays – OM and MTP. The OM and MTP contain a fiber optic modem and provide a single fiber transmit only link out of the CPCS channel. The fiber optical cabling provides electrical isolation to prevent external fault propagation back into the transmitting CPC channel. [

] ^{a,c} The destination devices are the Plant Monitoring Computer or CEAPDS or a printer to support the “Print screen” function. ¹²³

3.2.8.1 Interposing Relays

The trip, pre-trip, and CWP outputs to the PPS are channelized such that these outputs will be provided only in the associated PPS channel. CPC output contacts and associated field terminations to annunciators maintain separation from the PPS input/output contacts and other CPC channel equipment to prevent propagation of external faults into the CPC channel, as currently implemented in the existing CPCS. ¹²⁴

The interposing relays for the annunciator system are considered the Class 1E to non-1E isolation of these signals. The annunciator circuit is current limited to .002 A and 125 VDC. The IRP relay contacts are rated to switch a voltage of at least 200 V and the current rating is at least 0.200 A. The relay coil to contact isolation is of at least 1000 Vac. ¹²⁵

The following Interposing Relay Panel-mounted relays interface with the associated PPS channel, and are considered Class 1E on both the coil and contact side. The DNBR/LPD Trip and Pre-trip relays use one relay for output to the PPS, and one relay for output to the Input/Output Simulator. For the CWP relay, there is a second set of contacts that are currently spare, but may be used in the future to interface with the CPCS Input/output simulator for testing. Though the CWP relay is equipped with dual Form C contacts, only the normally open (Form A) contacts are used:

- DNBR Trip output to PPS (two Solid State Form A)
- DNBR Pre-trip output to PPS (two Solid State Form A)
- LPD Trip output to PPS (two Solid State Form A)
- LPD Pre-trip output to PPS (two Solid State Form A)

- CWP Output to PPS (two Form C)¹²⁶

The following IRP relay contacts are outputs to annunciator circuits. The second set of form C contacts on each relay are wired to connectors used to interface with the input/output simulator for testing.

Though the individual relays are equipped with dual Form C contacts, only the normally open (Form A) contacts are used:

- CPC Fail Annunciator (two Form C)
- CPC Trouble Annunciator (two Form C)
- CPC Test Annunciator (two Form C)
- CPC Sensor Fail Annunciator (two Form C)
- CEAC 1 Inoperable Annunciator (two Form C)
- CEAC 2 Inoperable Annunciator (two Form C)
- Aux CPC Trouble Annunciator (two Form C)
- CEA Deviation, CEAC 1 Annunciator (two Form C)
- CEA Deviation, CEAC 2 Annunciator (two Form C)
- CEAC 1 Fail Annunciator (two Form C)
- CEAC 2 Fail Annunciator (two Form C)
- CEAC 1 Trouble Annunciator (two Form C)
- CEAC 2 Trouble Annunciator (two Form C)
- CEAC 1 Sensor Fail Annunciator (two Form C)
- CEAC 2 Sensor Fail Annunciator (two Form C)
- CPP 1 Trouble Annunciator (two Form C)
- CPP 2 Trouble Annunciator (two Form C)
- CEAC 1 Test Annunciator (two Form C)
- CEAC 2 Test Annunciator (two Form C)
- Cabinet High Temperature (two Form C)
- Auxiliary Pre-trip Alarm (two Form C)¹²⁷

Three IRP Relays are used to perform operating bypass of the CPC channel. Each of the three relays has two form C contacts. Though the individual relays are equipped with dual Form C contacts, only the normally open (form A) contacts are needed in the bypass function. The relay used for annunciation utilizes the form A contact which will provide a closed contact when the relay is energized in an annunciate state:

- One relay is used to bypass the Low DNBR trip and pre-trip when the relay is energized. Two form C contacts are arranged in a form A configuration. Both the coil and contact are considered Class 1E.
- One relay is used to bypass the High LPD trip and pre-trip when the relay is energized. Two form C contacts are arranged in a form A configuration. Both the coil and contact are considered Class 1E.
- One relay is used to provide bypass annunciation when the relay is in an energized state. As such, the normally open (form A) contact is used. The second set of form C contacts on this relay are wired to connectors used to interface with the input/output simulator for testing. Only the normally open (form A) contact is used for this purpose. The relay contact is considered associated.¹²⁸

[

] ^{a,c}

The Test Enable MTP input (two form C) IRP relay is used to provide test enable low voltage input to the MTP when the Low DNBR and High LPD trips are in trip channel bypass in the PPS. Relay contacts are subject to low voltage (5 Vdc) and current. Dual form C relay contacts are used in a single Form A configuration.¹³⁰

3.2.9 Cross Divisional Interfaces

3.2.9.1 CEA Position Data

Each channel of the CPCS has two CEACs. The purpose of these two AC160 controllers is to calculate a PF multiplier to be used by the CPC algorithms based on CEA position deviations. CEAC 1 calculates the CEA position PF using the RSPT1 signals, and CEAC 2 calculates the CEA position PF using the RSPT2 signals.

In the existing (legacy) CPCS configuration there are four independent CPC channels that each contain a CPC. Then there are two CEACs (Channel B – CEAC 1, Channel C – CEAC 2) that calculate PFs associated with CEA rod positions and send the PFs and other related data to the individual CPCs via fiber optic data links. As a result, the legacy (existing) CPCS used cross channel (division) interfaces.

The CPCS replacement integrates the CEAC function into each CPCS channel. As a result, instead of providing the CEAC calculated results across channels, the CPCS replacement transmits CEA position data across channels so that each CPCS channel has a complete set of RSPT1 and RSPT2 signals for calculating CEAC PFs and other values within the channel.

The RSPT signals are channelized and read by each CPP in each channel redundantly (i.e., CPP 1 and CPP 2 in each channel read the same channelized RSPT signals). APC Channels A and B read RSPT1 signals and Channels C and D read RSPT2 signals. Each CPP then transmits these signals to the other 3 channels of the CPCS. The cross channel communication of the CEA position data is via the Common Q AC160 HSL through fiber optic modems that provide electrical isolation between channels. This is a secure, unidirectional communication protocol using fiber optic cable isolation that has been reviewed and approved by the NRC for cross channel communication (Reference 4).¹³¹

Section 3.2.8 discusses the safety to non-safety data communication interfaces for the OM and MTP.

This design is identical to the Palo Verde CPCS replacement implementation that has been reviewed and approved by the NRC (Reference 3).

3.2.10 Connections to Human-System Interfaces

There are two Human System Interfaces (HSIs) in each CPCS channel: MTP and OM. The MTP is primarily used for the service and test functions described in Section 3.2.7.1. It is located in the APC along with the AC160 controllers.

The OM is the primary HSI for the control room operator. It mimics many of the OM functions of the existing CPCS OM located in CP-7 on the main control board. These functions are described in Section 3.2.7.2.

The CPCS channel has a redundant AF100 bus that provides communication among the CPCS channel subsystems.¹³² The AF100 bus was reviewed and approved by the NRC and is described in Reference 4.

The OM AF100 uses a fiber optic interface because of its location outside the APC.¹³³

Section 3.2.8.1 discusses the hardwired interfaces to support the alarm annunciation of the CPCS channel.

3.2.11 Connections between Safety-Related Systems

The only external connection between the CPCS and other safety-related systems is the existing plant protection system. Those interfaces are hardwired using interposing relays as described in Section 3.2.8.1.

3.2.12 Connections between Safety-Related and Non-Safety-Related Systems

Section 3.2.8 discusses the OM, MTP and hardwired interfaces to non-safety-related systems.

3.2.13 Temporary connections

The CPCS design allows for the connection of an I/O simulator to support testing.¹³⁴ A single location is provided from which the CPCS I/O simulator may be connected to the CPCS for testing. Connection of the I/O simulator to the CPCS in this manner provides the following simulation and monitoring capabilities to the CPC channel:

- Simulate all externally sourced analog input values to the CPC and CEAC processor subracks
- Simulate all externally sourced digital inputs to the CPC processor subrack.
- Simulate CEA Position HSL inputs
- Monitor channel HSL outputs
- Monitor all CPCS digital outputs to the PPS
- Monitor all CPCS annunciator contact outputs, by means of a spare contact on each annunciator relay.
- Monitor all CPCS analog output channels.¹³⁵

Section 3.2.8.1 describes the IRP connections to the I/O simulator. The CPCS channel is put into Test by administrative procedure before connecting the I/O simulator to the CPCS channel.

3.2.14 Interfacing with Supporting Systems

The two supporting systems for the CPCS are the nuclear plant vital power and the main control room HVAC. Each CPCS channel receives plant power from the same vital instrument power supply used for the PPS as described in the WF3 FSAR Chapter 8. The PPS is supplied AC power from four inverters, two from each division, to supply power for the four measurement channels. A 120V uninterruptible ac system has been provided to supply the Plant Protection System control and instrumentation channels. The power supplies discussed in Section 3.2.3 convert the ac power into dc to power the described subsystems within the CPCS channel. The OM and MTP use AC power and so that power is provided directly from the 120V uninterruptible ac system.

Section 3.2.5 describes the HVAC requirements for the replacement CPCS.

3.2.15 Physical Location of System Equipment

The CPCS equipment is located in the existing APC replacing the legacy CPCS equipment. Only the OM is outside the APC and it is located on the main control board in the control room.

3.2.16 Communications

The data communications for the Common Q CPCS are:

[

] ^{a,c}

The Common Q Topical Report (Reference 4), Sections 4.4, 5.3.1.4, and 5.4.1.4 describe the functionality and capability of the AF100 bus. [

] ^{a,c} Topical report sections 4.5, 5.3.1.3, and 5.4.1.3 describe the functionality and capability of the HSL.

The Common Q Topical Report Section 5.6 addresses the compliance for the HSL communication protocol to the twenty communication criteria established in DI&C-ISG-04 (Reference 9). Table 3.2.16-1 DI&C-ISG-04-Compliance describes the difference in disposition of the criteria for the CPCS application. As stated in the topical report, in all cases the AF100 will not apply to the positions because the AF100 is contained within the channel. [

] ^{a,c}

Citations in the dispositions to section numbers are to the sections in this document unless a specific document is mentioned.

There is one inbound communication channel in the CPCS channel and that is the time synchronization data link using the inter-range instrumentation group (IRIG) input to the MTP in each channel. This input communication channel is fiber optically isolated.¹⁴⁰ This input is used to provide a common time reference for such functions as the print screen function, trip buffer report, and failed sensor stack.¹⁴¹ Time Synchronization is not required for the CPCS to perform its safety related functions. [

] ^{a,c}

The time synchronization aligns the MTP's clocks in all four channels. This is for the time stamping of the trip buffer report and other reports generated by the CPCS. This allows for comparing the trip buffer reports and determining the channel sequence for the trip thus simplifying the analysis of a trip. This function saves considerable operating costs without complicating the CPCS design. Without the time synchronization, operations would have to 1) look at the "time since restart" on each train and correlate to a real time clock, 2) determine the difference in time between channels, and 3) line up manually the trip buffer reports in each channel to determine the sequence of events.

The use of the IRIG interface is identical to the Palo Verde CPCS implementation that was reviewed and approved by the NRC. The NRC safety evaluation report for the Palo Verde CPCS, ML033030363, states, "The first component is an IRIG-B time card installed in the FPDS, that is used for time stamping events for the trip buffer and failed sensor stack. The card has been qualified (Seismic, EMI, environmental) to operate in the FPDS. The staff concludes that there is reasonable assurance that failure of this card does not adversely impact the safety functions operating in the CPCs or CEACs and, therefore, finds that the IRIG-B time card is appropriately used in the FPDS application."

Table 3.2.16-1 DI&C-ISG-04-Compliance also includes the disposition of the IRIG communication channel to the 20 criteria in DI&C-ISG-04.

a,c

[illegible]

[illegible]

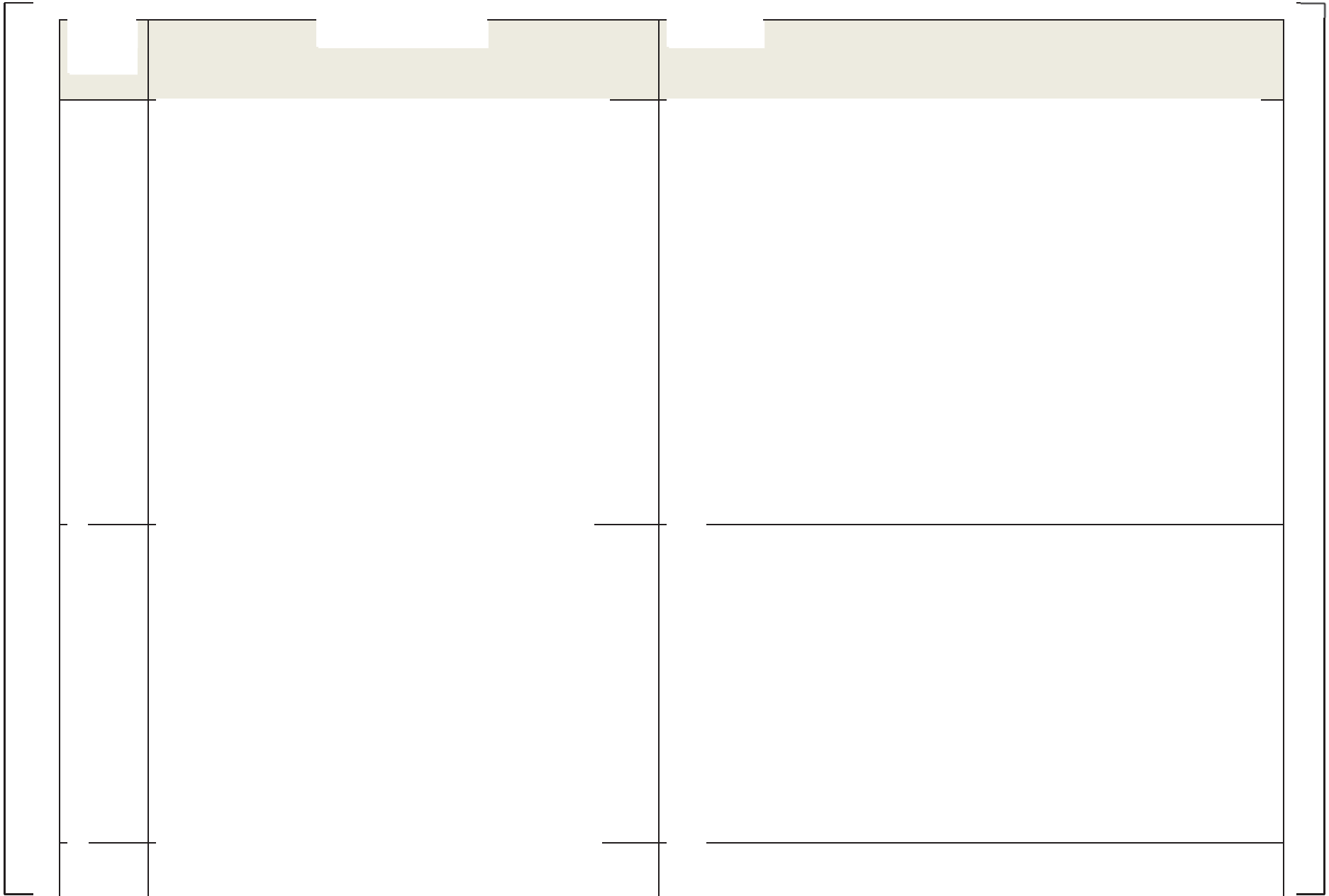
[illegible]

[illegible]

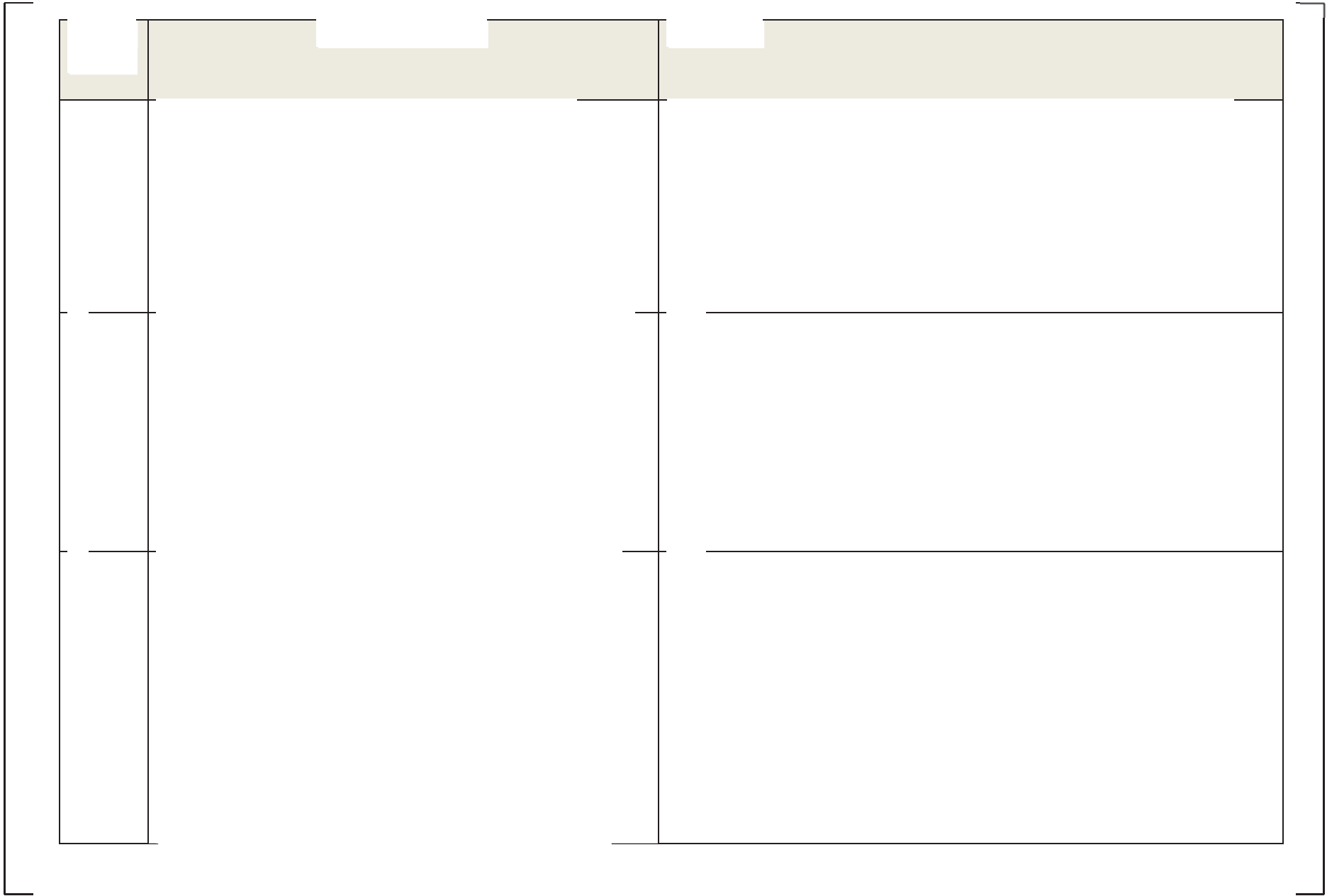
[illegible]

[illegible]

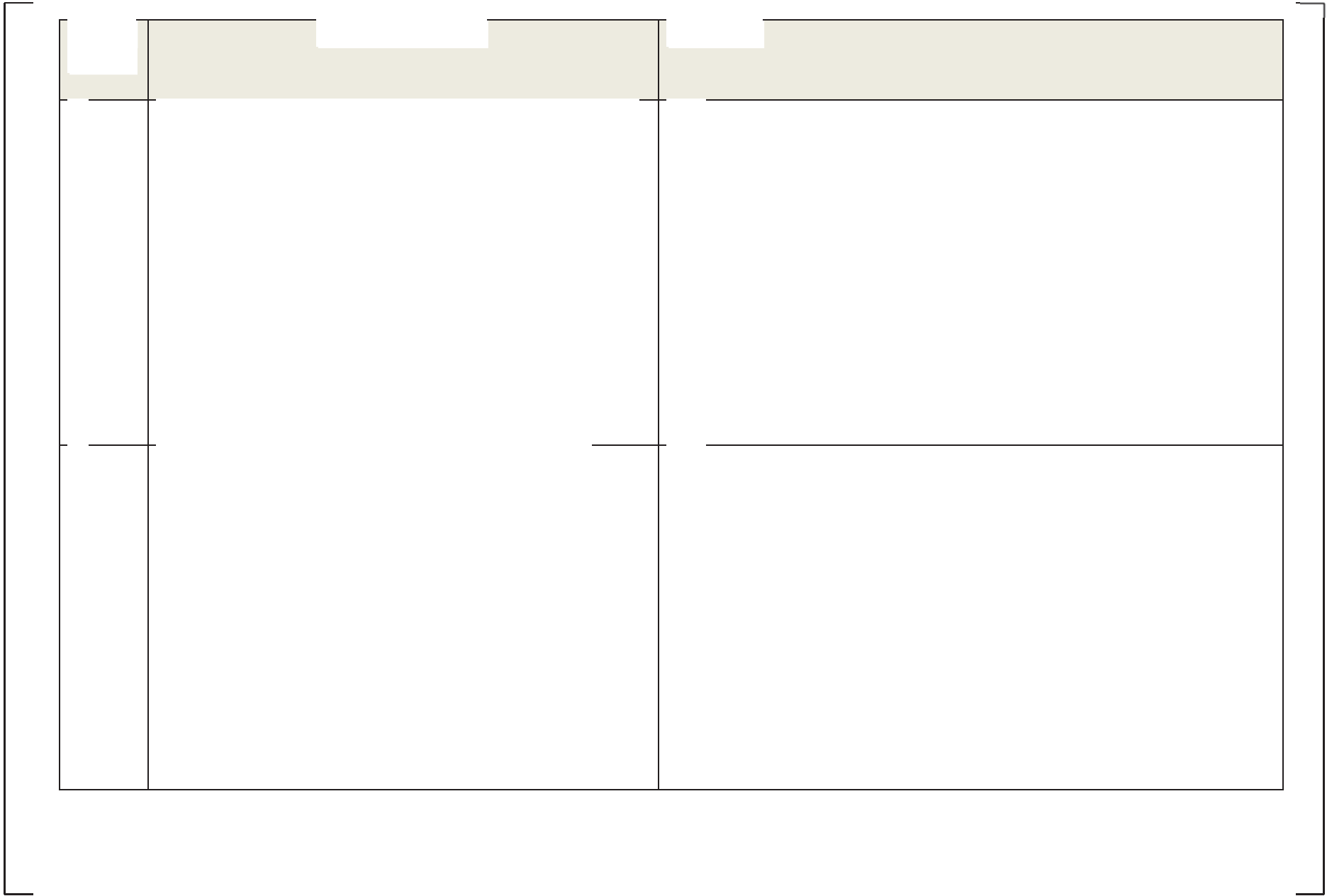
[illegible]



[illegible]



[illegible]



3.2.17 Failure Modes and Effects Analysis¹⁵⁸

The failure modes and effects analysis (FMEA) is a qualitative evaluation which identifies various failure modes which contribute to a system's unreliability. The FMEA identifies significant single failures and their effects or consequences on the system's ability to perform its functions.

The CPC system is designed so that any single failure in any channel will not prevent proper protective action of the other CPC channels, or inhibit operation of the PPS at the system level. The failure modes and effects analysis for this system shows that no single failure will defeat more than one of the four redundant CPC channels. The FMEA assumes that one of the four CPC channels is permanently bypassed, resulting in a two out of three PPS logic, as is consistent with plant Technical Specifications, LCO 3.3.1.

The FMEA addresses all credible outputs from the CPC/CEAC computers (e.g. communications failures, stalls, etc.), not all possible causes of the failure condition. At the hardware interface level, the FMEA bounds all cases by considering the worst case effects at the computer module outputs.

The CPCs possess several redundancy features to enhance channel reliability. Significant among these are redundant analog input monitoring by each CPC channel, and redundant CEA position transmission to the other three CPC channels. In order for a channel to remain operable, only one of the redundant signal paths (CPPs and associated HSL) need be operable. [

]^{a,c} In cases where all CEA position transmission from a channel is interrupted, such as upon loss of channel power, the presence or absence of redundant CPP links in other channels is irrelevant, since one channel will trip, and one CEAC will be rendered inoperable in the other operable channels. In cases where a failure impacts only one of the two redundant CPP links in the sending channel, the redundant link will maintain CEA position signal transmission to the applicable CEACs in the other channels, unless the receiving signal path is unavailable due to redundant link failure within the receiving channel. In this case, the CEAC in the receiving channel with the inoperable redundant link will be treated by the CPC as failed, due to loss of both sources of CEA position input. Other channels with both links operable will retain operability of the affected CEAC. These specific subsets are not addressed in this FMEA due to the numerous possible permutations of processor and link availabilities in all channels. However, all possible combinations are bounded by the case in which both redundant signal transmission paths are unavailable in the sending channel. In this case, one CPC channel is rendered inoperable, and one CEAC in the other three channels will fail. This is consistent with the response of the existing CPCS.

Figure 3.2.17-1 depicts Channel B of the CPCS architecture.

The diagram area is mostly blank, suggesting the content of Figure 3.2.17-1 CPCS Channel B is not visible or is a very faint image.

Figure 3.2.17-1 CPCS Channel B

3.2.17.1 Analog Input Module Failure Modes

Analog input failures are complicated by the overlaying of new failure modes attributable to analog input module error condition monitoring upon the failure modes as established in the existing CPCS. Generally, there has been no change to the manner in which the CPCS responds to sensor failures. That is, in the

existing CPC, a sensor out of range condition provides a sensor failure indication, and uses a fixed value in its calculations indicative of the out of range limit. In the CEAC, the last valid position of the sensor is used prior to the failure. In the CEAC, both range limits and rate of change of sensor input are used to establish a sensor failure condition.

In the replacement CPCS, all analog inputs will be redundantly processed by two analog input modules. For all inputs except CEA position, these two modules are in the CPC AC160 controller. For CEA positions, these modules are located in each of the two CEAC AC160 controllers.

Each analog input module is monitored for individual channel failures and module failures. The range of each analog input module input channel is 0 to 10 Vdc. If the input exceeds this range limit in either direction by greater than 10% of range (greater than 11.0 Vdc or less than -1.0 Vdc), the channel error terminal is set. In the CPC, if one or more individual channel error terminals are set, the same channels on the backup module will be used.

[

] ^{a,c}

The FMEA is documented in Reference 39.

3.2.17.2 Watchdog Timer¹⁵⁹

[

] ^{a,c}

[^{a,c} The DNBR and LPD Trip relays are solid state Form A (normally open) relays. These outputs are dedicated solid state relays outputs used for the Low DNBR trip and High LPD trip. In the case for the other PM646A WWDT outputs in other AC160 controllers, Table 3.2.17.2-1 Window Watchdog Timer Actuation Summary lists the reaction to these WWDT actuations. Note the IR for these outputs are standard relays with two DPDT contact outputs using the Form A configuration for actuation.

Table 3.2.17.2-1 Window Watchdog Timer Actuation Summary

a,c

3.2.18 Common Cause Failure (CCF)

Diversity requirements for software-based protection systems are explicitly stated in NRC Branch Technical Position BTP 7-19 and NUREG/CR6303. These documents impose CCF assumptions on software-based protection system designs which make it difficult to justify less than a CCF of all four protection channels, unless they differ significantly in implementation. CCF simply stated, is the concern that hidden defects (particularly in software) could cause the simultaneous failure of all redundant safety channels containing that defect, thus resulting in loss of the intended safety function.

The existing CPCS is implemented in computer-based hardware, so the change to the Common Q platform represents a digital-to-digital upgrade. The original licensing basis for WF3 assumes a potential CCF of the CPCS.¹⁶⁰ The replacements of the current digital CPCS with the Common Q platform does not change the WF3 licensing basis for defense in depth and diversity. The following description summarizes the original assessment for a digital CPCS and the coping strategy for a postulated beyond design basis CPCS CCF, and its application to WF3.

In practice, consequences of four channel CPC failure are significantly less severe than loss of all four PPS channels, since the CPCs provide only a small subset of the RPS trips. Since the WF3 PPS is analog, it is assumed that the remainder of the PPS is implemented in hardware diverse from that in the CPCs. Thus, the remaining PPS trips provide diverse actuations for the FSAR Chapter 15 Anticipated Operational Occurrences (AOOs) and accidents for which the CPCs are credited.

The NRC Safety Evaluation Report issued to ANO-2 (Reference 29), the first plant with digital CPCS, evaluated the diversity of the Core Protection Calculators, and found the design acceptable. This was reaffirmed by the NRC staff when they reviewed the Palo Verde CPCS replacements (Reference 3). The ANO-2 SER Appendix D, Supplement 1, "Design Basis" states the following:

Note: Clarifications and assessments of the NRC evaluation to the WF3 CPCS is summarized in italics within the quoted text.

"Because the core protection calculator system is a first of a kind design, the staff considered failure of the CPCs to perform its normal function. Backup trips and normal shutdown mechanisms were reviewed to assess the depth of protection provided. This extent of this review is beyond that normally performed for reactor protection systems.

"The CPCs provide the initial, but not the only trip, for the steam line break accidents, reactor coolant pump shaft seizure, and steam generator tube rupture. Increased fuel damage could occur for the above accidents with concurrent failure of the CPCs. However, analog backup trips on system pressure ... are available to provide reactor shutdown and mitigate the consequences of accidents. Failure of the CPCs, concurrent with any of the above incidents, is an extremely unlikely event.

"The CPCS is designed to initiate a trip for the following events:

- (1) Uncontrolled control element assembly (CEA) withdrawal from a critical condition.
- (2) CEA Misoperation
- (3) Uncontrolled boron dilution
- (4) Total and partial loss of reactor coolant forced flow
- (5) Excess heat removal due to secondary system malfunction
- (6) Steam Generator Tube Rupture with and without a concurrent loss of offsite power."

"Backup trips are available to limit the consequences of each of the above events, even with failure of the CPCS, except the CEA misoperation event.

"The CPCS provides a reactor trip for CEA deviation events where DNBR or peak linear heat rate limits are approached. Automatic reactor trips have not been provided in previous Combustion Engineering protection system designs for this event. In the unlikely event that a CEA deviation event which required a reactor trip occurred without a CPC-initiated trip, the operator would get alarms from the core operating limit supervisory system (COLSS) on CEA position and flux tilt similar to that in non-CE plants. Manual trip could then be initiated.

"For the other events the applicant has stated that the backup trips are:

- (1) CEA Withdrawal - high pressurizer pressure
- (2) Uncontrolled Boron dilution - high pressurizer pressure
- (3) Total or partial loss of flow-low reactor coolant flow, high pressurizer pressure*, low steam generator pressure, low steam generator water level. These trips are also available for loss of flow due to pump shaft seizure. **Although the PPS and CPCS share the same pressurizer pressure*

signals, loss of the CPCS due to a software CCF will not inhibit the PPS in performing its diverse protection function using the same pressurizer signal.

- (4) Excess heat removal - low steam generator water level, ~~high~~ low pressurizer pressure, and low steam generator pressure
- (5) Steam generator tube rupture-low pressurizer pressure"

During the NRC review of the Palo Verde CPCS replacement, the licensee responded to an NRC RAI regarding the credited manual trip for CEA misoperation, "The response time for operator action during a CEA misoperation event (Single Full-Length CEA Drop Event) is 900 seconds (15 minutes) as stated in Section 15.4.3 of the PVNGS UFSAR. Only the CEA insertion event is considered for CEA misoperation since a CEA withdrawal event is backed up by a high pressurizer pressure trip whereas a CEA insertion event has no backup automatic trip."

In the same SER for the Palo Verde CPCS replacement (Reference 3), the NRC staff "... considered failure of the digital trip system to perform its design function. Backup analog trips and/or inherent shutdown mechanisms limit the consequences of this type of failure for all but the CEA misoperation events. For CEA misoperation, a manual trip, similar to previous plants, is required but numerous alarms and indications are available to inform the operator of the event. We find the backup to the CPCs to be acceptable."

WF3 has the same response time for operator action during a CEA misoperation event (15 minutes, see Reference 33, NOTE.GEN.2).

3.2.19 Compliance to Applicable IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 Clauses

The licensing basis for WF3 is IEEE Std. 279, and this modification will not change the WF3 licensing basis. This licensing technical report and this section in particular, demonstrates compliance to the applicable clauses in IEEE Std 603-1991 and IEEE Std 7-4.3.2 for the new system architecture as identified in ISG-06 (Reference 1), Section D.2.2.1. In addition, IEEE Std 603 Clause 5.11 is addressed in this section.

3.2.19.1 IEEE Std 603-1991

3.2.19.1.1 IEEE Std 603-1991 Clause 5.1

IEEE Std 603-1991, Clause 5.1, Single-Failure Criterion states (in part):

The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 [5] provides guidance on the application of the single-failure criterion.[B21].

[

]^{a,c}

[

] ^{a,c}**3.2.19.1.2 IEEE Std 603-1991 Clause 5.7**

IEEE Std 603-1991, Clause 5.7, Capability for Test and Calibration states:

Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987 [3]. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

- (1) appropriate justification shall be provided (for example, demonstration that no practical design exists),*
- (2) acceptable reliability of equipment operation shall be otherwise demonstrated, and*
- (3) the capability shall be provided while the generating station is shut down.*

[

] ^{a,c}

3.2.19.1.3 IEEE Std 603-1991 Clause 5.8.1

IEEE Std 603-1991, Clause 5.8.1, Displays for Manually Controlled Actions states:

The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981 [9]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.

[
] ^{a,c}

3.2.19.1.4 IEEE Std 603-1991 Clause 5.8.2

IEEE Std 603-1991, Clause 5.8.2, System Status Indication states:

Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.

[

] ^{a,c}

3.2.19.1.5 IEEE Std 603-1991 Clause 5.8.3

IEEE Std 603-1991, Clause 5.8.3, Indication of Bypasses, states:

If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

5.8.3.1 This display instrumentation need not be part of the safety systems.

5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year; and (b) is expected to occur when the affected system is required to be operable.

5.8.3.3 The capability shall exist in the control room to manually activate this display indication.

[

] ^{a,c}**3.2.19.1.6 IEEE Std 603-1991 Clause 5.8.4**

IEEE Std 603-1991, Clause 5.8.4, Location, states:

Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

[

] ^{a,c}**3.2.19.1.7 IEEE Std 603-1991 Clause 5.11**

IEEE Std 603, Clause 5.11, Identification states:

In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

- (1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 [61] and IEEE Std 420-1982 [7].*
- (2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification,*
- (3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).*
- (4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.*
- (5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 (R1990) [8].*

[

] ^{a,c}**3.2.19.2 IEEE Std 7-4.3.2****3.2.19.2.1 IEEE Std 7-4.3.2 Clause 5.5.2**

IEEE Std 7-4.3.2, Clause 5.5.2, Design for Test and Calibration states:

Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change (e.g., setpoint change).

V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.

V & V, configuration management, and QA are not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

[

]^{a,c}

3.2.19.2.2 IEEE Std 7-4.3.2 Clause 5.5.3

IEEE Std 7-4.3.2, Clause 5.5.3, Fault Detection and Self-Diagnostics states:

Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.

The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.

If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:

- *Memory functionality and integrity tests (e.g., PROM checksum and RAM tests)*

- *Computer system instruction set (e.g., calculation tests)*
- *Computer peripheral hardware tests (e.g., watchdog timers and keyboards)*
- *Computer architecture support hardware (e.g., address lines and shared memory interfaces)*
- *Communication link diagnostics (e.g., CRC checks)*

Infrequent communication link failures that do not result in a system failure or a lack of system functionality do not require reporting.

When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

- a) Self-diagnostics during computer system startup*
- b) Periodic self-diagnostics while the computer system is operating*
- c) Self-diagnostic test failure reporting*

[

]^{a,c}

3.2.20 FSAR Changes

Appendix A provides draft FSAR markups to aid in the NRC review of the LAR.

3.3 NEW SYSTEM FUNCTIONS (D.2.3 AND D.2.3.1)

The Common Q CPCS replacement is not adding or modifying CPCS design basis functions except for adding new pre-trip alarms for the auxiliary trips.¹⁶³ The auxiliary trips are defined in the Common Q CPCS System Requirements Specification (Reference 2 as augmented by Reference 21), Appendix A, Section 3.2.5.4. The Common Q CPCS will continue to assure that the DNBR in the reactor core is greater than or equal to the minimum required. The Common Q CPCS will also continue to assure that the Local Power Density in the core does not exceed a value at which fuel centerline melting would occur for the list of design bases anticipated operational occurrences.¹⁶⁴

Chapter 15.0 of the WF3 Updated Final Safety Analysis Report (FSAR) presents analytical evaluations of the nuclear steam supply system (NSSS) response to postulated disturbances in process variables and to postulated malfunctions or failures of equipment. The assumptions for CPC performance, response time, and accuracy in Chapter 15.0 will continue to be met with the new system as described in Section 3.2.6.

The existing design functions of the CPCS are tabulated in the document CPCS Design Function Summary, Reference 32. These safety analysis design functions are not changing as a result of the CPCS replacement project. The following information is included:

- FSAR Events (AOOs/PAs relevant to the plant equipment discussed in the LAR)
- Credited Trip/Actuation Signals
- Variable(s) and ranges
- Nominal (100% RTP) Analytical Limit
- Number of Channels
- Coincidence Logic
- Automated Protection Function (all are reactor trip functions)
- Interlock / Permissive / Override and conditions for these functions
- Response Time Assumed in FSAR Event Analysis (note that the response times are modified from the legacy system as noted in Section 3.2.6 of this licensing technical report)

The service/test functions are different to accommodate the difference in hardware. These service and test functions are described in Section 3.2.7. Other non-design basis function changes from the existing CPCS are described below.

3.3.1 Restoring CEA Rate of Change Lock-In

The CPCS, when monitoring CEA positions, the CEAC program performs validity checks of the CEA input signal. These checks consist of 1) a range check to verify the CEA position is within the CEA operating band and 2) a rate of change check to verify CEA movement is reasonable.¹⁶⁵

The range check is a comparison of the CEA position to the lower and upper limit of the operating band and to lower and upper failed sensor setpoints, which are outside the operating band. If the CEA position is detected outside the failed sensor setpoints, the CEA is considered failed; but the failure can be automatically cleared if the position is detected inside the failed sensor setpoints.¹⁶⁶

[

] ^{a,c}

3.3.1.1 New CEA Rate of Change Reset

Correcting this coding deficiency in the replacement CPCS would allow the operators to manually reset the CEA position in the CEAC to the current good position (as validated by redundant position RSPT/Pulse Counter indication) without rebooting, thus reducing operational delays (see Section 3.2.7.2.6). There is no impact on DNBR and LPD. If the condition is due to the software lock-in, then continued group movement will create a deviation and generate a penalty. This would be a very conservative response. If the CEA position deviation is real, both CEACs will monitor it and respond accordingly.¹⁶⁸

3.3.2 IEEE Std 603-1991 Clause 4 Compliance

IEEE Std 603-1991 Clause 4 requires the plant design basis to be documented for the following criteria. For each criterion, the impact on the existing design basis for WF3 is indicated as a result of replacing the CPCS with the Common Q platform based system.

Clause 4.1: *The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.*

[

] ^{a,c}

Clause 4.2: *The safety functions and corresponding protective actions of the execute features for each design basis event.*

[

] ^{a,c}

Clause 4.3: *The permissive conditions for each operating bypass capability that is to be provided.*

[

] ^{a,c}

Clause 4.4: *The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable,*

the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.

[

]^{a,c}

Clause 4.5: *The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation.*

[

]^{a,c}

Clause 4.6: *For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.*

]^{a,c}

Clause 4.7: *The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.*

[

]^{a,c}

Clause 4.8: *The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).*

[

]^{a,c}

[

] ^{a,c}

Clause 4.9: *The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.*

[

] ^{a,c}

Clause 4.10: *The critical points in time or the plant conditions, after the onset of a design basis event, including:*

Clause 4.10.1: *The point in time or plant conditions for which the protective actions of the safety system shall be initiated.*

Clause 4.10.2: *The point in time or plant conditions that define the proper completion of the safety function.*

Clause 4.10.3: *The points in time or the plant conditions that require automatic control of protective actions.*

Clause 4.10.3: *The point in time or the plant conditions that allow returning a safety system to normal.*

[

] ^{a,c}

Clause 4.11: *The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.*

[

] ^{a,c}

[

] ^{a,c}

Clause 4.12: *Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).*

[

] ^{a,c}

3.3.3 IEEE Std 603-1991 Applicable Clauses for New System Functions

This section demonstrates compliance to the applicable clauses in IEEE Std 603-1991 for new system functions as identified in ISG-06 (Reference 1), Section D.2.3.1.

3.3.3.1 IEEE Std 603-1991 Clause 5.2

IEEE Std 603-1991, Clause 5.2, Completion of Protective Action states:

The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.

[

] ^{a,c}

3.3.3.2 IEEE Std 603-1991 Clause 5.5

IEEE Std 603-1991, Clause 5.5, System Integrity states:

The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

[

]^{a,c}

3.3.3.3 IEEE Std 603-1991 Clauses 5.7, 6.5, 6.5.1 and 6.5.2

IEEE Std 603-1991 Clause 5.7 is addressed in Section 3.2.19.1.2.

IEEE Std 603-1991 Clause 6.5.1 states:

Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

- (1) by perturbing the monitored variable,*
- (2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or*
- (3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.*

[

]^{a,c}

IEEE Std 603-1991 Clause 6.5.2 states: *One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:*

- (1) Checking the operational availability of sensors by use of the methods described in 6.5.1.*
- (2) Specifying equipment that is stable and retains its calibration during the post-accident time period.*

[

] ^{a,c}

3.3.3.4 IEEE Std 603-1991 Clause 5.8

This clause is addressed in Sections 3.2.19.1.3 through 3.2.19.1.6.

3.3.3.5 IEEE Std 603-1991 Clause 5.9

IEEE Std 603-1991 Clause 5.9, Control of Access states: *The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.*

[

] ^{a,c}

[

] ^{a,c}

3.3.3.6 IEEE Std 603-1991 Clause 5.10

IEEE Std 603-1991 Clause 5.10, Repair states: *The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.*

[

] ^{a,c}

3.3.3.7 IEEE Std 603-1991 Clauses 6.6 and 7.4

IEEE Std 603-1991 Clause 6.6, Operating Bypasses states: *Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

- (1) *Remove the appropriate active operating bypass(es).*
- (2) *Restore plant conditions so that permissive conditions once again exist.*
- (3) *Initiate the appropriate safety function(s).*

[

] ^{a,c}

[

] ^{a,c}**3.3.3.8 IEEE Std 603-1991 Clauses 6.7 and 7.5**

IEEE Std 603-1991 Clause 6.7, Maintenance Bypass states: *Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.*

EXCEPTION One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).

[

] ^{a,c}**3.3.3.9 IEEE Std 603-1991 Clause 6.8**

IEEE Std 603-1991 Clause 6.8.1, Setpoints states: *The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987 [18].*

[

] ^{a,c}

IEEE Std 603-1991 Clause 6.8.2, Setpoints states: *Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.*

[

] ^{a,c}

3.3.3.10 IEEE Std 603-1991 Clause 5.3

IEEE Std 603-1991 Clause 5.3 Quality states: *Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989 [16]).*

[

] ^{a,c}

IEEE Std 7-4.3.2-2003, Clause 5.4.2 **Qualification of existing commercial computers**, states: *NOTE-See Annex C for more information about commercial grade item dedication.*

The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B 16].

The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.

[

] ^{a,c}

3.3.4 System Requirements Documentation (D.2.3.3 and D.2.3.3.1)

Reference 2 is the CPCS System Requirements Document. It is the system requirements specification for the reference design for the Common Q CPCS. The reference design system requirements is based on two requirements documents that define the legacy CPCS functionality:

- Functional Design Requirements for a Core Protection Calculator (Reference 36) and
- Functional Design Requirements for a Control Element Assembly Calculator (Reference 37)

The Common Q CPCS reference design system requirements specification (Reference 2) was developed to migrate the functional requirements of References 36 and 37) to a Common Q CPCS architecture. The result was the Palo Verde CPCS implementation.

The existing Waterford CPCS is based on the same two functional design requirements documents (References 36 and 37). Therefore, the CPCS reference design is also applicable to the Waterford CPCS replacement plus additional changes to accommodate plant interface differences, requested licensee improvements, and changes in technology in the Common Q platform.

Reference 21 is the WF3 CPCS specific system requirements specification. This document includes additional system features and modifications to reflect the specific WF3 CPCS requirements. It describes the necessary clarifications, additions, changes, and modifications to Reference 2. The WF3 specific system requirements specification supplements Reference 2, and is used by both the hardware and software development teams as a source document for the design of the WF3 CPCS hardware and software.

[

] ^{a,c}

Table 3.3.3-1 ISG-06 System Requirements Document Content

a,c

The Reference 21 system requirements specification, Section 2.3.1.3 requires the software to be designed, developed and tested in accordance with the NRC-approved Common Q Software Program Manual (Reference 6). The hardware design requirements are defined in the Westinghouse 10 CFR 50 Appendix B Quality Assurance procedures. The Westinghouse NRC-approved Appendix B quality assurance

program is in accordance with NRC Regulatory Guide 1.28, Revision 4, with clarifications, alternatives, and exceptions defined in Appendix A of the NRC-approved QA manual.

Sections 2.3 and 2.4 of the CPCS system requirements specification (Reference 21) define the CPCS dynamic performance requirements including accuracy and response time. The functional requirements are in Appendix A of Reference 2.

Section 2.3.11 of Reference 21 defines the accuracy requirements for the input signals based on the total uncertainties attributable to:

- 1) loading effects
- 2) reference voltage supply regulation
- 3) electrical noise
- 4) linearity
- 5) A/D converter power supply sensitivity
- 6) quantization

The one interlock in the CPCS is the operating bypass function of the CPCS. It avoids a spurious reactor trip when power measured by the nuclear instrumentation is below the bypass permissive set point of 1E-4%. The requirements for the operating bypass function are defined in Reference 21, Sections 2.1.3.3.2, 2.2.1.4.1.3, and 2.7.

The Reference 21 system requirements specification defines the requirements for boundary interfaces with other systems in Section 4 and independence requirements in Section 2.3.9.

Since the CPCS replacement is a modification of a system that is already installed in the plant, the constraint is replacing the internal parts of the APC, so there is no additional physical constraints to be considered beyond the APC. There is also the constraint in regards to the control board in the main control room where the Common Q Flat Panel Display System will be installed to replace the existing Remote Operator Panel. The design of the parts will take into account fitting within the existing APC and control board space. So fitting in the existing cabinet and control board is the constraint. The Reference 2 system requirements specification and the Reference 21, WF3 system requirements specification define this as an installation constraint.

The CPCS system requirements specification (Reference 21) defines the operator and maintenance technician interface requirements in Sections 2.1.1.4 and 2.1.2.1.

The requirements for equipment qualification to environmental conditions is specified in Section 3.1.4 in Reference 21. That same section references out to the seismic and electromagnetic compatibility requirements in the Common Q Topical Report (Reference 4), Section 8.

The Reference 21 system requirements specification defines the service/test functions that will be deployed for the CPCS in Section 2.2.1.4.

3.4 FUNCTION ALLOCATION (D.2.4 AND D.2.4.1)

The allocation of design functions is described in Sections 3.2.1 and 3.2.2. The CPC logic is defined in Reference 21, Appendix A, Sections 3.2.1 – 3.2.5. This logic is executed in the CPC PM646A in the CPC AC160 controller.

The CEAC logic is defined in Reference 21, Appendix A, Section 3.2.6. This logic is executed in the CEAC PM646A in both CEAC AC160 controllers. CEAC 1 PM646A uses the RSPT1 signals, and CEAC 2 PM646A uses the RSPT2 signals.

The allocation of service/test functions is described in Section 3.2.7. Some of these functions are operator or technician initiated calibrations and tests. Other functions are reported status from the self-diagnostic functions within the AC160 controllers. These are described in Section 3.1.1.1.3 of the CPCS system requirements specification Reference 21.

The description of how the response time of the new design meets the response times credited in the accident analysis is found in Sections 3.2.1.1 and 3.2.6. The response time analysis includes the time delays associated with cross channel communications of the RSPT signals.

For the discussion on system interfaces, see Section 3.5.

3.5 SYSTEM INTERFACES (D.2.5)

This section will describe each of the CPCS channel external interfaces. The implementation of these interfaces is identical to the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.5.1 CEA Position Cross Channel Communication

Section 3.2.2 describes this cross channel communication using the unidirectional, fiber optically isolated HSL communication. Section 3.2.9.1 provides the justification for this cross channel communication. There is cross channel communication in the existing CPCS implementation. The replacement system increased the redundancy of the CEAC processors in the architecture and re-purposed the cross channel communication from communicating PFs to communicating CEA positions.¹⁹¹ The CPC trip function uses channelized target CEAs for the Low DNBR and High LPD trips. The cross channel CEA positions are used for calculating a PF to be applied to the algorithm in a conservative direction.

Section 3.2.16 demonstrates how communication hazards are controlled via HSL communication compliance to DI&C-ISG-04. These cross channel comparison communication paths have no external path (e.g., human contact point) to jeopardize the secure operating environment of the CPCS.

This cross channel CEA position communication function is identical to the Palo Verde CPCS replacement that was reviewed and approved by the NRC.

3.5.2 PPS Interface

The PPS interface is a hardwired interface as described in Section 3.2.8.1. It is the only external hardwired safety-related interface except for the safety-related indications on the control board. The purpose of the PPS interface is to provide the PPS with two trip inputs, Low DNBR and High LPD. It also provides a control rod withdrawal prohibit digital signal. CWP is initiated by the CPCS channel on the following conditions:

- Low DNBR Pre-trip
- High LPD Pre-trip
- CEA Group Out of Sequence
- Subgroup Deviation alarm
- Group P CEA Group excessive insertion
- CEA deviation or reactor power cutback input from the channel CEACs¹⁹²

The PPS two out of four coincidence logic for the CPCS trips protects the plant from spurious reactor trip due to a failure in a CPCS channel that spuriously actuates these hardwired trip signals (e.g., WWDT actuation on CPC PM646A failure).¹⁹³

The CPC receives the PPS operating bypass permissive signal (excore power < 10⁻⁴ % power) via a hardware digital input (see Section 3.2.1 discussion on the DI620 module).

The Test Enable signal is generated when the Low DNBR and High LPD trips are in trip channel bypass in the PPS. This signal drives an IRP relay and is read by the Digital Input card of the CPC AC160 Rack.

One of the IR's contact outputs (two form C contacts) is used to generate an MTP test enable input signal. The relay contacts are subject to low voltage (5 Vdc for the MTP and 24 Vdc for the DI card) and current.¹⁹⁴

These hardwired interface functions are identical to the existing CPCS implementation, and it is identical to the CPCS replacement at Palo Verde that was reviewed and approved by the NRC.

3.5.3 Plant Annunciator System Interface

The CPCS channel provides hardwired outputs to the plant annunciator system as described in Section 3.2.8.1. The implementation of these hardwired outputs is identical to the CPCS replacement at Palo Verde that was reviewed and approved by the NRC.

3.5.4 OM and MTP Print Screen Interface

This function allows the operator or technician to capture any screen displayed on the OM or MTP for printing external to the CPCS.¹⁹⁵ The MTP and OM transmit the screen capture file [

] ^{a,c}

3.5.5 Plant Monitoring System Interface

Each channel's MTP provides a unidirectional fiber optically isolated Ethernet data link to the plant computer [

] ^{a,c}

3.5.6 CEAPD Interface

Each channel's MTP provides a unidirectional fiber optically isolated Ethernet data link to the CEAPD [

] ^{a,c}

3.5.7 MTP Time Synchronization Interface

The existing CPCS includes no capability to provide time stamping of any display functions. In the legacy CPCS sensor failures are logged in hours since the last auto restart, rather than being keyed to a real-time clock.

The replacement CPCS includes time synchronization using an inter-range instrumentation group (IRIG) input to the MTP in each channel as described in Section 3.2.16

This communication is the only external communication coming into the CPCS channel.²⁰³ [

] ^{a,c}

Compliance to DI&C-ISG-04 is demonstrated in Table 3.2.16-1 DI&C-ISG-04-Compliance.

This implementation is identical to the implementation at Palo Verde for the replacement CPCS and was reviewed and approved by the NRC. The same implementation is running in the Common Q CPCS at Shin Kori Units 1-4 and Shin Wolsong Units 1 and 2.

3.5.8 Support and Auxiliary System Interfaces

There is no direct interface between the CPCS and the control room HVAC where the APC is located.²⁰⁹ Section 3.2.5 discusses the demonstration of compatibility of the replacement CPCS to the HVAC requirements in the control room.

Each channel of the CPCS is powered from the vital bus power supply system 1E inverter (Section 3.2.14). The CPCS complies with IEEE 603-1991 Clause 8.1 because it is using the existing WF3 vital power that meets its licensing basis for an electrical power source. IEEE 603-1991, Clause 8.2 does not apply because the CPCS only uses electrical power. The CPCS is compliant to IEEE 603-1991 Clause 8.3 via the trip channel bypass described in Section 3.2.8.1 (DI620 module discussion).

These interfaces are identical to the implementation of the Palo Verde CPCS that was reviewed and approved by the NRC.

3.5.9 Safety to Non-Safety Isolation Requirements

Data communications to non-safety systems use fiber optic cable to provide electrical isolation. The IRP relay provides electrical isolation to the non-safety annunciator system. The IRP relay contacts are rated to switch a voltage of at least 200 V and the current rating is at least 0.200 A.²¹⁰ The IRP is described in Section 3.2.8.1 and for digital data communications see Section 3.2.16.

3.5.10 IEEE Std 603 and IEEE Std 7-4.3.2 Relevant Clauses

The following clauses to IEEE Std 603-1991 and IEEE Std 7-4.3.2 are relevant to the discussion of system interfaces as identified in DI&C-ISG-06 (Reference 1), Section D.2.5.

3.5.10.1 IEEE Std 603 Clause 5.6.1

Clause 5.6.1, states: ***Independence Between Redundant Portions of a Safety System.*** *Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any design basis event requiring, that' safety function.*

[

] ^{a,c}

3.5.10.2 IEEE Std 603 Clause 5.6.2

Clause 5.6.2 states: ***Independence Between Safety Systems and Effects of Design Basis Event.*** *Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.*

[

] ^{a,c}

[
] ^{a,c}

3.5.10.3 IEEE Std 603 Clause 5.6.3

Clause 5.6.3 states: ***Independence Between Safety Systems and Other Systems.*** *The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.*

[

] ^{a,c}

3.5.10.3.1 IEEE Std 603 Clause 5.6.3.1

Clause 5.6.3.1 states: ***Interconnected Equipment Classification:*** *(1) Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems, Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.*

*(2) **Isolation:** No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.*

[

] ^{a,c}

3.5.10.3.2 IEEE Std 603 Clause 5.6.3.2

Clause 5.6.3.2 states: ***Equipment in Proximity***

*(1) **Separation:** Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981*

(2) **Barriers:** *Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.*

[

]^{a,c}

3.5.10.3.3 IEEE Std 603 Clause 5.6.3.3

Clause 5.6.3.3 states: ***Effects of a Single Random Failure.*** *Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 [51 for the application of this requirement.*

[

]^{a,c}

3.5.10.4 IEEE Std Clause 5.6.4

Clause 5.6.4 states: ***Detailed Criteria.*** *IEEE Std 384-1981 [6] provides detailed criteria for the independence of Class 1E equipment and circuits [B3].*

[

]^{a,c}

[
] ^{a,c}

3.5.10.5 IEEE Std 7-4.3.2 Clause 5.6

Clause 5.6 states: *In addition to the requirements of IEEE Std 603-1998, data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function.*

IEEE Std 603-1998 requires that safety functions be separated from nonsafety functions such that the nonsafety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and nonsafety software may reside on the same computer and use the same computer resources.

Either of the following approaches is acceptable to address the previous issues:

- a) Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements.*
- b) If barriers between the safety software and nonsafety software are not implemented, the nonsafety software functions shall be developed in accordance with the requirements of this standard.*

Guidance for establishing communication independence is provided in Annex E.

[

] ^{a,c}

3.5.10.6 IEEE Std 603 Clause 5.12

IEEE Std 603-1991 Clause 5.12 defines criteria for Auxiliary Features. The following sections describe compliance to the underlining subclauses 5.12.1 and 5.12.2.

3.5.10.6.1 IEEE Std 603 Clause 5.12.1

Clause 5.12.1 states: *Auxiliary supporting features shall meet all requirements of this standard.*

[

] ^{a,c}

[

] ^{a,c}

3.5.10.6.2 IEEE Std 603 Clause 5.12.2

Clause 5.12.2 states: *Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features shown in Fig 3 and an illustration of the application of this criteria is contained in Appendix A.*

[

] ^{a,c}

3.5.10.7 IEEE Std 603 Clause 5.14

Clause 5.14 states: ***Human Factors Considerations.*** *Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988 [12].*

[

] ^{a,c}

[

] ^{a,c}

3.5.10.8 IEEE Std 603 Clauses 8.1 - 8.3

These clauses are addressed in Section 3.5.8.

3.6 FUNDAMENTAL DESIGN PRINCIPLES IN THE NEW ARCHITECTURE

This section discusses how the CPCS replacement meets the four fundamental design principles: Redundancy, Independence, Deterministic Behavior, and Defense-in-Depth and Diversity, and the attribute Simplicity of Design.

3.6.1 Redundancy (D.2.6.2.1)

The replacement CPCS mirrors the existing CPCS redundancy by providing four independent channels of CPC that calculate and initiate trips for Low DNBR and High LPD. The replacement CPCS enhanced the redundancy of the CPCS by putting CEAC 1 and 2 AC160 controllers in each channel rather than relying on two CEACs in the existing CPCS. The safety-related data communications (i.e., AF100 bus and HSL) are redundant communication channels providing better availability of the CPCS.²¹⁴ The replacement CPCS enhanced redundancy within a channel by providing redundant AI688 modules to read the process inputs for the CPC (except for the RCP speed).²¹⁵ The replacement CPCS also provides redundant data acquisition within a channel for the CEA positions (CPP 1 and CPP 2, see discussion on the PM646A CPP Processor Module in Section 3.2.2).

Reference 39 is the Failure Modes and Effects Analysis (FMEA) for the WF3 CPCS that uses the redundancy of the system to meet IEEE Std 603-1991 single failure criterion. The FMEA is a bounding analysis. It postulates higher level failures that cover lower level failures that would have the same impact on the system.

The impact of WF3 plant failures on the CPCS are the same for both the existing CPCS and the replacement CPCS. The EQ Summary Report (Reference 35), documents the qualification of the CPCS equipment to mitigate against WF3 design basis events.

3.6.1.1 Relevant IEEE Std 7-4.3.2 Clauses

This section documents compliance to IEEE Std 7-4.3.2-2003 clauses deemed relevant by DI&C-ISG-06, Section D.2.6.2.1.2 (Reference 1).

3.6.1.1.1 IEEE Std 7-4.3.2 Clause 5.1

Clause 5.1 states: *No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B).*

IEEE Std 603-1991, Clause 5.1 is addressed in Section 3.2.19.1.1.

3.6.1.1.2 IEEE Std 7-4.3.2 Clause 5.15

Clause 5.15 states: **Reliability** NOTE-See Annex F for more information about the reliability criterion.

In addition to the requirements of IEEE Std 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.

[

] ^{a,c}

3.6.1.1.3 IEEE Std 7-4.3.2 Clause 6.7

IEEE Std 7-4.3.2-2003 does not have additional criteria for IEEE Std 603-1991 Clause 6. IEEE Std 603-1991 Clause 6.7 is addressed in Section 3.3.3.8.

3.6.1.1.4 IEEE Std 7-4.3.2 Clause 7.5

IEEE Std 7-4.3.2-2003 does not have additional criteria for IEEE Std 603-1991 Clause 7. IEEE Std 603-1991 Clause 7.5 is addressed in Section 3.3.3.8.

3.6.1.2 IEEE Std 379 Criteria

IEEE Std 603-1991 cites IEEE Std 379-1988 for guidance on the application of the single failure criterion. NRC Regulatory Guide 1.53 endorsed IEEE Std 379-2000. The following paragraphs address compliance to IEEE Std 379-2000.

Clause 5.1 addresses Independence and redundancy. [

] ^{a,c}

Clause 5.2 addresses non-detectable failures. [

] ^{a,c}

Clause 5.3 addresses Cascaded failures. [

] ^{a,c}

Clause 5.4 addresses Design basis events. [

] ^{a,c}

Clause 5.5 addresses Common-cause failures. [

] ^{a,c}

Clause 5.6 addresses Shared systems. [

] ^{a,c}

Clause 6 addresses Design analysis for single failure. [

] ^{a,c}

3.6.1.3 GDC 21

GDC 21 Protection System Reliability and Testability states: *The protection system shall be designed for high functional reliability and in service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.*

[

] ^{a,c}

3.6.1.4 GDC 24

GDC 24 Separation of Protection and Control Systems states: *The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.*

[

] ^{a,c}

[

] ^{a,c}

3.6.2 Independence (D.2.6.2.2)

The WF3 CPCS replacement maintains the independence of the existing CPCS. It provides for four functional and electrical CPCS channels that calculate and initiate Low DNBR and High LPD trip signals. For electrical independence see Section 3.2.8. For data communications functional and electrical independence see Section 3.2.16. This section describes the unidirectional communications between channels of the CPCS and between the CPCS and non-safety systems which meets the IEEE Std 384 criteria for independence of Class 1E equipment and circuits.

3.6.2.1 Relevant IEEE Std 7-4.3.2 Clauses

This section documents compliance to IEEE Std 7-4.3.2-2003 clauses deemed relevant by DI&C-ISG-06, Section D.2.6.2.2.2 (Reference 1).

3.6.2.1.1 IEEE Std 7-4.3.2 Clause 5.6

Clause 5.6 is addressed in Section 3.5.10.5

3.6.2.1.2 IEEE Std 7-4.3.2 Clause 5.11

Clause 5.11 states: *To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met:*

- a) *Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.*
- b) *Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.*
- c) *Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1998.*

[

] ^{a,c}

3.6.2.1.3 IEEE Std 7-4.3.2 Clause 6.3

IEEE 7-4.3.2 states that there are no additional requirements beyond IEEE Std 603 Clause 6. IEEE Std 603 Clause 6.3 Interaction Between the Sense and Command Features and Other Systems has two subclauses 6.3.1 and 6.3.2.

IEEE Std 603-1991 Clause 6.3.1 states: *Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:*

- (1) *Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:*
 - (a) *Channels that sense a set of variables different from the principal channels.*
 - (b) *Channels that use equipment different from that of the principal channels to sense the same variable.*
 - (c) *Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels. Both the principal and alternate channels shall be part of the sense and command features.*
- (2) *Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.)*

See Fig 5 for a decision chart for applying the requirements of this section.

[

]^{a,c}

IEEE Std 603-1991, Clause 6.3.2 states: *Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.*

[

]^{a,c}

3.6.2.2 RG 1.75

NRC Regulatory Guide 1.75 (RG 1.75) applies to one aspect of this license amendment. The APC MUX function that transmits the amplified fixed incore detector signals to the plant monitoring computer is a non-safety related system residing in the APC in close proximity to the CPCS. This equipment is considered an associated circuit as described in RG 1.75. As a result the APC MUX equipment is

qualified to Class 1E requirements to demonstrate that the non-safety related system will not adversely impact the safety related CPCS (see Sections 3.2.4 and 3.5.10.3.2).

3.6.2.3 Applicable 10 CFR 50 Appendix A General Design Criteria

The following sections address the GDCs listed in Reference 1, Section D.2.6.2.2.2 for the fundamental principle of Independence.

3.6.2.4 GDC 13 Instrumentation and Control

GDC 13 states: *Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.*

[

] ^{a,c}

3.6.2.5 GDC 21 Protection System Reliability and Testability

Compliance to GDC 21 is discussed in Section 3.6.1.3.

3.6.2.6 GDC 22 Protection System Independence

GDC 22 states: *The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.*

[

] ^{a,c}

3.6.2.7 GDC 23 Protection System Failure Modes

GDC 23 states: *The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the*

system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

[

]^{a,c}

3.6.2.8 GDC 24 Separation of Protection and Control Systems

CPCS compliance to GDC 24 is discussed in Section 3.6.1.4.

3.6.3 Deterministic Behavior (D.2.6.2.3)

The fundamental element for deterministic behavior of the CPCS is the AC160 PM646A controller and its cyclic execution of the application programs described in Sections 3.2.1.1 and 3.2.2.1. The cycle time of CPC and CEAC PF application programs are established to meet the response time requirements for the Chapter 15 events as described in Section 3.2.6.²²³ [

]^{a,c}

The WF3 CPCS timing analysis calculates the worst possible response time for each event in Chapter 15 of the FSAR (see Section 3.2.6).

3.6.3.1 Applicable IEEE Std 603 and IEEE Std 7-4.3.2 Clauses

The following sections address applicable clauses to IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 as described in Section D.2.6.2.3.2 of Reference 1.

3.6.3.1.1 IEEE Std 603 Clause 5.2

There is no corresponding Clause 5.2 in IEEE Std 7-4.3.2, and Clause 5.2 in IEEE Std 603 is addressed in Section 3.3.3.1.

3.6.3.1.2 IEEE Std 603 Clause 5.5 and IEEE Std 7-4.3.2 Clauses 5.5.1 – 5.5.3

Clause 5.5 in IEEE Std 603 is addressed in Section 3.3.3.2.

IEEE Std 7-4.3.2 Clause 5.5.1 states: ***Design for computer integrity.*** *The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. For example, input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes.*

If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function.

[

] ^{a,c}

IEEE Std 7-4.3.2 Clause 5.5.2 is addressed in Section 3.2.19.2.1.

IEEE Std 7-4.3.2 Clause 5.5.3 is addressed in Section 3.2.19.2.2.

3.6.3.1.3 IEEE Std 603 Clause 6.1

IEEE Std 603 states: ***Automatic Control.*** Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be, provided to automatically initiate and control those protective actions of 4.5.

[

] ^{a,c}

3.6.3.1.4 IEEE Std 603 Clause 6.2

IEEE Std 603 Clause 6.2 is criteria for Manual Control. [

] ^{a,c}

3.6.3.1.5 IEEE Std 603 Clause 7.1

Clause 7 in IEEE Std 603 is criteria on the execute or executive functions of the protective action. [

] ^{a,c}

3.6.3.2 Applicable 10 CFR 50 Appendix A General Design Criteria

This section describes CPCS compliance to the listed GDCs in Section D.2.6.2.3.2 in Reference 1.

3.6.3.2.1 GDC 13 Instrumentation and Control

GDC 13 is addressed in Section 3.6.2.4.

3.6.3.2.2 GDC 21 Protection System Reliability and Testability

GDC 21 is addressed in Section 3.6.2.5.

3.6.3.2.3 GDC 23 Protection System Failure Modes

GDC 23 is addressed in Section 3.6.2.7

3.6.3.2.4 GDC 29 Protection Against Anticipated Operational Occurrences

GDC 29 states: *The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.*

[

] ^{a,c}

3.6.4 Defense-in-Depth and Diversity (D.2.6.2.4)

Section 3.2.18 explains the licensing basis for why the existing defense in depth strategy for WF3 has not changed as a result of the replacement of the CPCS.

Reference 1 identifies GDC 13, 22 and 24 to be applicable to this fundamental principle. These GDCs are addressed in Sections 3.6.2.4, 3.6.2.6, and 3.6.2.8 respectively.

3.6.5 Simplicity of Design (D.2.6.2.5)

The design of the replacement system is very similar to the design of the existing CPCS. There are four independent CPCs that run the same application program [

^{a,c}. In the existing system, there are two CEACs that calculate a PF to steer the DNBR and LPD calculations into a conservative direction based on CEA deviations. However instead of two CEACs shared among the four CPC channels, each CPC channel now has its own CEAC 1 and CEAC 2. This change increases availability by replicating the CEAC 1 and CEAC 2 functions in each CPCS channel. By doing this, the CEA positions are shared among the four channels using fiber optically isolated, unidirectional HSLs. This design change is identical to the implementation at Palo Verde that was reviewed and approved by the NRC.

Another design change in the replacement CPCS is the used of an IRIG data link to synchronize time to a site wide standard clock. This significantly reduces WF3 staff burden when analyzing reports generated by the CPCS. The hazards for this data link are discussed in Sections 3.2.16 and 3.5.7. This design change is identical to the Palo Verde replacement CPCS that was reviewed and approved by the NRC.

3.6.5.1 IEEE Std 603 Clause 6.4

DI&C-ISG-06, Reference 1, identifies IEEE Std 603-1991, Clause 6.4 as relevant to this fundamental design attribute.

Clause 6.4 states: ***Derivation of System Inputs.*** *To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.*

[

]^{a,c}

4 HARDWARE EQUIPMENT QUALIFICATION (D.3)

The Common Q Platform Topical Report (Reference 4), Section 7, describes the equipment qualification methodology for the generic qualification of the Common Q Platform. The Common Q equipment is mounted in a test rack in the same manner as it will be mounted in an actual cabinet.

IEEE Std 603-1991, Clause 5.4 requires that *Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 [2] and IEEE Std 627-1980 [11].*

[

] ^{a,c}

IEEE Std 7-4.3.2, 2003, Clause 5.4.1 **Computer system testing**, states: *Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.*

[

] ^{a,c}

[

] ^{a,c}

5 I&C SYSTEM DEVELOPMENT PROCESSES (D.4)

Westinghouse will be using the NRC-approved Common Q Software Program Manual (SPM, Reference 6) as the framework for the design and development of the WF3 CPCS replacement. This framework is a supplement to the Westinghouse 10 CFR 50 Appendix B Quality Assurance program to specifically address digital I&C safety system development. Attributes of the framework as outlined in DI&C-ISG-06, Revision 2 (Reference 1), D.4.1 are:

- a. Create the concepts on which the system design will be based. For the WF3 CPCS there are three basic concepts upon which the WF3 CPCS system design is based.
 1. The WF3 CPCS system design is based on the design described in the Common Q Topical Report, Appendix 2 for the Core Protection Calculator System (Reference 5).
 2. The WF3 CPCS system design is based on the Palo Verde Common Q CPCS system design with minor modifications such as newer NRC-approved analog input modules (AI688 versus AI685).
 3. The WF3 CPCS system design concept is based on the existing WF3 CPCS system (e.g., four channel CPC, CEA configurations, etc.) as described in Section 2, Plant System Description (D.1).
- b. Translate these concepts into system requirements. The base system requirements for the WF3 CPCS is the CPCS System Requirements Specification (Reference 2), which have already been reviewed by the NRC as part of the Palo Verde CPCS replacement. These requirements are augmented by the WF3 CPCS System Requirements Specification (Reference 21) to document changed or new requirements specific to the WF3 CPCS replacement. These documents translate the concepts upon which the system design is based into system requirements.
- c. Allocate system requirements to system elements (e.g., software, hardware, and human-system interfaces). The base system requirements that are documented in CPCS System Requirements Specification (Reference 2) have already been allocated to system elements as part of the NRC-approved Palo Verde CPCS replacement. This represents the reference design for the WF3 CPCS replacement. Changed or revised requirements from the reference design is documented in the WF3 CPCS System Requirements Specification (Reference 21). These requirements are allocated to hardware, software, and other responsible groups in accordance with the requirements management plan.²²⁵ The independent V&V team assess the allocation of functions for completeness and correctness per the NRC approved Common Q SPM (Reference 6)²²⁶.
- d. Implement the design into hardware and software functions. As stated in c. above, the requirements traceability matrix documents the implementation of the system requirements into hardware and software functions in accordance with the NRC-approved Common Q SPM (Reference 6).
- e. Integrate system elements such as software and hardware. Westinghouse uses its testing methodology as described in the NRC-approved Common Q SPM (Reference 6), Section 7, that documents successive levels of testing to integrate the system elements (both software and hardware).
- f. Test the unit functions and the completed system to confirm that system requirements have been implemented correctly. The NRC-approved Common Q SPM (Reference 6), Section 7, describes the successive levels of testing up to a System Validation Test, and a Factory Acceptance Test to validate manufacturing. These last two tests may be combined in the case of WF3 because it is a

single NPP installation. The independent V&V team uses the RTM to trace testable requirements to test procedures and reports.

- g. Perform appropriate human factors engineering for the human-system interfaces throughout the development process. The WF3 CPCS has the benefit of operating experience with the CPCS operator's module and Maintenance and Test Panel. These displays have been in operation at the Palo Verde three nuclear units for at least 15 years. WF3 have engaged operations staff early in the project to familiarize them with the established display set so that operating procedures can be prepared in a timely manner to take advantage of the benefits of an improved human-system interface. None of the displays are necessary for the CPCS to perform its safety function but are used to assess status of the system, and configure and test the system when not in service.
- h. Analyze hazards and incorporate requirements that eliminate or mitigate identified hazards throughout the development process. The WF3 CPCS replacement has the benefit of extensive hazards analyses that have been performed on both the conceptual design (see the Failure Modes and Effects Analysis (FMEA) in the CPCS Topical Report Appendix, Reference 5), and on the Palo Verde CPCS replacement. A WF3 CPCS replacement FMEA is developed to eliminate or mitigate any additional hazards identified in that analysis. The WF3 CPCS documents a software hazards analysis (SHA) in accordance with the Common Q SPM (Reference 6) to eliminate or mitigate any software hazards identified in the analysis (see Reference 54).
- i. Perform V&V activities on work products throughout the development process. The WF3 CPCS development will undergo independent verification and validation (V&V) in accordance with the NRC-approved Common Q SPM (Reference 6).

The software life cycle process is governed by the NRC-approved Common Q SPM (Reference 6). Section 1.4.1 in the Common Q SPM defines the software life cycle to be:

- Concept
- Requirements Analysis
- Design
- Implementation or Coding
- Test
- Installation and Checkout
- Operation and Maintenance
- Retirement

The WF3 CPCS replacement project will be following this life cycle process. Any clarifications or exceptions (with justification) to the processes described in the NRC-approved Common Q SPM are documented in the WF3 CPCS Software Development Plan (Reference 25). There are other overarching processes such as Project Management, Verification and Validation (V&V), and Configuration Management. V&V and Configuration Management will be performed in accordance with the NRC-approved Common Q SPM (Reference 6). Project Management is discussed in Section 5.2.10.

5.1 COMMON Q SPM PLANT SPECIFIC ACTION ITEMS

The NRC documented seven Plant Specific Action Items (PSAIs) in the safety evaluation on the NRC-approved SPM (Reference 6). This section provides the dispositions for the seven PSAIs.

5.1.1 PSAI 1

As noted in Sections 3.2.1 and 3.2.3, WEC may choose to use alternatives to the SPM defined processes when performing Initiation phase activities for individual projects. These alternatives are required to be documented in the Project Quality Plan (PQP). This PQP should be reviewed to determine if alternatives to the SPM are being used for development of project specific software. When such alternatives are being used, the PQP should be evaluated to determine if the justifications for the use of alternatives to the SPM processes are acceptable.

The SPM states, “When the SPM refers to a PQP, it includes the Project Quality Plan and Project Plan (including the Software Development Plan) defined in the Westinghouse Quality Management System Procedures.” Any exceptions to the SPM would be documented in the WF3 CPCS Software Development Plan (Reference 25). The Software Development Plan also includes clarifications to particular items to make clear how certain aspects of the SPM are being fulfilled.

5.1.2 PSAI 2

The Common Q SPM only includes the Software Life Cycle Process Planning Documentation as outlined in SRP BTP 7-14, Section B.2.1. As such, the plant-specific documentation outlined in SRP BTP 7-14, Sections B.2.2, “Software Life Cycle Process Implementation,” and B.2.3, “Software Life Cycle Process Design Outputs,” is to be evaluated separately for any application that references the Common Q SPM.

The following table provides the cross reference between the documents listed in BTP 7-14 Sections B.2.2 and B.2.3 and the name of the Westinghouse WF3 CPCS corresponding document. If the document is complete, a document number will be cited, otherwise the document is produced later in the life cycle.

Table 5.1.2-1 BTP 7-14 Documents

<i>BTP 7-14 Document</i>	<i>Westinghouse Corresponding Document</i>
<i>B.2.2 Documents</i>	
Safety analyses	Software Hazards Analysis (Reference 54)
Verification and validation analysis and test reports	V&V Phase Summary Reports V&V Task Reports V&V Module Test Reports
Configuration management reports	Configuration Baseline Reports Configuration Management Release Reports
Testing Activities	Test Plan System verification test / FAT procedures and test reports

Table 5.1.2-1 BTP 7-14 Documents

<i>BTP 7-14 Document</i>	<i>Westinghouse Corresponding Document</i>
Requirements	CPCS System Requirements Specification (References 2 and 21) CPCS Software Requirements Specification
Design	Software Design Descriptions
Implementation	Software Release Records
Integration	V&V module and unit test reports (Unit tests may be part of the System Verification Test / FAT)
Validation	System Verification Test / FAT Reports
Installation	Technical Manual
Operations and maintenance	Technical Manual
<i>B.2.3 Documents</i>	
Software Requirements Specification	(See Requirements above).
Hardware and software architecture descriptions	Software Requirements Specification (for software architecture) Hardware Design Description (for hardware architecture)
Software design descriptions	(See Design above)
Code listings	Code resides on secure development environment and documented in Software Release Records.
Build documents	Various Westinghouse internal work instructions and CPCS Technical Manual
Installation configuration tables	Installation configuration tables reside on secure development environment and documented in Software Release Records.
Operations manuals	CPCS Technical Manual
Maintenance manuals	CPCS Technical Manual
Training Manuals	Separate training materials as part of a WF3 site training program.

5.1.3 PSAI 3

The Common Q SPM only addresses the vendor software planning processes for a Common Q-based system. For all activities in which the applicant or licensee assumes responsibility within a given project (including vendor oversight) for quality assurance, additional evaluations, audits or inspections must be performed to ensure that these licensee responsibilities are fulfilled.

Entergy has developed a vendor oversight plan that is summarized in the LAR to verify that Westinghouse is performing its activities in accordance with their quality assurance commitments. This verification is conducted by Entergy by way of evaluations, audits or inspections.

5.1.4 PSAI 4

Because the Common Q SPM does not address the criteria of BTP 7-14 Section B.3.1.8.4, "Software Operations Plan," an evaluation of compliance must be performed at the time of system development when the operational aspects of the system have been defined.

Westinghouse will develop a technical manual that includes the elements of a Software Operations Plan. As part of Entergy's vendor oversight activities as documented in the WF3 CPCS vendor oversight plan, Entergy will verify that the elements of BTP 7-14 for a Software Operations Plan is incorporated into the WF3 CPCS technical manual.

5.1.5 PSAI 5

Site acceptance testing and installation testing are not covered under the Common Q Software Test Plan because they are considered to be licensee actions that are to be addressed during the development of a Common Q based application. As such, a project specific, site acceptance and installation test plan should be developed and used to address these aspects of software test planning. Because the Common Q SPM does not address all aspects of the BTP 7-14 Section B.3.2.4 criteria, an evaluation of compliance must be performed at the time of system development when the site and installation testing activities have been defined.

Entergy's Engineering Change (EC) Process, EN-DC-115, (Reference 60) identifies testing including pre-installation testing, construction testing, functional testing, software V&V, additional post installation testing, and post return to service tests. The Responsible Engineer (RE) is responsible for preparing the EC testing requirements in accordance with EN-DC-115, with input from the Test Engineer (TE), Operations and other reviewers as applicable.

The EC Testing (ECT) is identified in the EC but is controlled outside of the EC process. The Engineering Change Process points to Entergy's Post Modification Testing and Special Instructions, EN-DC-117, (Reference 61) for the details for performing testing. Modification and special testing are controlled by this process, which creates the EC Test to perform post modification Functional Testing. This ECT format demonstrates that modified or affected systems, structures, or components will perform satisfactorily in service and satisfy design requirements. The ECT format may be used for Post Return to Service Testing. The TE is a qualified individual that is responsible for coordinating review and approval of ECT formatted tests. This includes reviewing and concurring with the ECT requirements developed by

the RE, in addition to the ECT development and performance, and Return To Service (RTS) for the EC. All ECT requirements are captured by at least one of the above types of tests.

The Post Modification Testing Philosophy, in general, is that the test for an EC should test the modification under all configurations, test not only what has been added by the EC, but also what has been deleted, test the EC thoroughly and at least one step beyond the interface to the equipment, which hasn't been modified, avoid testing by simulation when equipment may be operated safely, consider the use of the Simulator and other methods to aid in developing and validating the test procedure/instruction, and be sequenced to perform the most basic tests first, then proceed to perform more complex component and system level functional and acceptance tests.

Testing will be controlled with procedures or work orders that will use the ECT format. Many of the tests for the WF3 CPC replacement including the Site Acceptance Testing (SAT) will be performed with an ECT procedure due to the complexity of the testing.

Testing will be based on design requirements specified in the Westinghouse documents, as well as those specified in the ECT. Testing will also address license requirements associated with the WF3 Technical Specifications, which will include the approved changes for this modification. Testing will include hardware and software functional testing, verification of field inputs, post-installation testing, and integrated testing. Response time testing (RTT) will be performed for the two CPC trip signals to Reactor Protection System (RPS).

5.1.6 PSAT 6

A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q SPM.

Appendix 5 of the Common Q Topical Report (Reference 13) is the output document for the change process described in Reference 12. The document provides a summary of changes and then a detailed recording of analysis and/or qualification documents, and a conclusion statement on the status of the change relative to the NRC safety conclusions. Reference 13 can be audited by the NRC staff to achieve reasonable assurance that Westinghouse is maintaining the Common Q Platform within the bounds of the safety conclusions in the safety evaluation of the platform. It is also an activity documented in the Entergy vendor oversight plan to audit and confirm that adequacy of the analysis of platform changes.

See Section 6.1 for further details.

5.1.7 PSAT 7

Secure Development and Operational Environment – An applicant or licensee referencing the Common Q SPM for a safety-related plant specific application should ensure that a secure development and operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.

Section 9 describes how the CPCS replacement project will meet the requirements in NRC Regulatory Guide 1.152 for a Secure Development and Operational Environment.

The NRC-approved Common Q SPM (Reference 6) describes the Westinghouse Secure Development Environment. As part of the Entergy vendor oversight activities, Entergy will verify the secure development environment at Westinghouse meets the criteria in Section 12 of the SPM.

See Section 9.2 for the Secure Operational Environment vulnerability assessment and the correlation to system requirements.

5.2 SYSTEM AND SOFTWARE DEVELOPMENT ACTIVITIES (D.4.2.1)

The NRC-approved SPM (Reference 6), Section 4.3.2 describes the tasks and responsibilities for each life cycle phase. These tasks and responsibilities are applicable to the WF3 CPCS replacement project and will be followed. The detailed description of analyses, reviews and test activities for each life cycle phase are described in the SPM Sections 3 (Software Safety Plan), 4 (Software Quality Assurance Plan), 5 (Software V&V Plan), 6 (Software Configuration Management Plan), 7 (Software Test Plan), and 12 (Secure Development and Operational Environment Plan).

5.2.1 Plant and Instrumentation and Control System Safety Analysis (D.4.2.1.1)

As described in Section 3.3, there are no changes to the plant safety analysis associated with the WF3 CPCS replacement. [

]^{a,c} This is documented in the WF3 CPCS Software Development Plan (Reference 25). The independent V&V will be performed in accordance with the NRC-approved SPM for Protection class software for the AC160 controller software and for Important to Safety for the OM and MTP software.

5.2.2 Instrumentation and Control System Requirements (D.4.2.1.2)

The project input documents are collected and defined in a configuration baseline²²⁷. These documents include Entergy input documents along with Westinghouse CPCS product documents like the CPCS System Requirements Specification (Reference 2). The attributes of the System Requirements Specification (i.e., References 2 and 21) are described in Section 3.3.4. The WF3 CPCS replacement system requirements specification (Reference 21) is independently reviewed, traced to input documents identified in the configuration baseline, and approved.²²⁸ The configuration baseline is then revised to incorporate the WSES system requirements specification (Reference 21) for later system development life cycle activities.

A requirements traceability matrix (RTM) is created to trace the WF3 CPCS replacement system requirements to hardware and software design, implementation and test.²²⁹ The independent V&V performs a requirements traceability analysis (RTA) in accordance with the Common Q SPM (Reference 6) Section 5.4.5.3.

5.2.3 Instrumentation and Control System Architecture (D.4.2.1.3)

The WF3 CPCS replacement system requirements specification (Reference 21) defines the WF3 CPCS replacement system architecture. It is based on the NRC-approved Palo Verde CPCS replacement architecture. The technical elements described in Section 3.2 of this document are incorporated in the WF3 CPCS replacement system requirements specification (Reference 21). As described in Section 5.2.2, the WF3 CPCS replacement system requirements specification is independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

5.2.4 Instrumentation and Control System Design (D.4.2.1.4)

Both the CPCS system requirements specification and the WF3 CPCS replacement system requirements specification (References 2 and 21) also fulfill the role as the system design specification. Again, the WF3 CPCS replacement system requirements specification (Reference 21) is based on the CPCS system requirements specification (Reference 2), defining the differences in the system design from the NRC-approved Palo Verde CPCS replacement.

As stated earlier, the reference design for the WF3 CPCS replacement is documented in Reference 2. These requirements and their traceability have already been reviewed and approved by the NRC as part of the Palo Verde CPCS replacement. The WF3 delta requirements from the reference design are documented in Reference 21 and are traced bidirectionally using the requirements traceability matrix as described in the Common Q SPM (Reference 6), Section 5.4.5.3. The architecture and functional logic design in the reference design has already been traced to the design reference requirements as part of the Palo Verde CPCS replacement.²³⁰ The WF3 delta system requirements in Reference 21 include tracing to the architecture and functional logic designs.

DI&C-ISG-06 (Reference 1), D.4.2.1.4 states, “DI&C system safety analyses should be reviewed to identify hardware, software, or human-system interfaces that have the potential to cause a hazard or are credited to eliminate or mitigate hazards.” The WF3 CPCS FMEA (Reference 39) identifies the hardware and human-system interface hazards and their mitigation or elimination, and the WF3 CPCS SHA (Reference 54) identifies the software hazards and their mitigation or elimination.

As described in Section 5.2.2, the WF3 CPCS replacement system requirements specification is independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

5.2.5 Software Requirements (D.4.2.1.5)

The WF3 CPCS replacement software requirements specification (SRS) will be developed in accordance with the NRC-approved SPM (Reference 6), which states that the SRS complies in content but not format to IEEE Std 830-1998, “IEEE Recommended Practice for Software Requirements Specifications” as augmented by NRC Regulatory Guide 1.172, Rev. 1 (July 2013), “Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants”.

The allocation of CPCS reference design system requirements (Reference 2) to software have already been accomplished as part of the NRC-approved Palo Verde CPCS replacement. The WF3 delta

requirements from the reference design are documented in Reference 21. These are allocated to software as described in Section 5, item c and documented in the SRS.

The WF3 SRS is based on the NRC-approved Palo Verde CPCS replacement SRS (Reference 26) which documents additional or different requirements from the Palo Verde design. The WF3 replacement CPCS SRS completes the identification of the requirements for the software in the system. The SRS documents the requirements for the software in each subsystem (e.g., CPC processor, CEAC processor, CPP processor, etc.).

Information in the SRS include:

- Specific inputs and outputs, both those that are physical signals and information that is received from and supplied to human users and external data systems.
- Valid input ranges
- Output ranges, if they must be specifically limited
- Required HSI formats (only if not specified in the CPCS System Requirements Specification)
- Required sequences of operations (only if not specified in the CPCS System Requirements Specification)
- Functional processing of the data
- Timing requirements or constraints
- Response to abnormal conditions and error recovery
- Retention, use, and initialization of previous state information, where required
- Safety and security requirements
- Design constraints (e.g., adherence to the Common Q platform design restrictions in Reference 18)²³¹

Similar to the WF3 system requirements specification, the SRS is independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

In addition the RTM is updated showing the tracing of software requirements to the WF3 system requirements specification (Reference 21).²³²

An independent V&V team develops module and/or unit test procedures and conducts those tests. An independent test team develops system test plans and procedures, and conducts the system testing. The RTM traces the SRS requirements to either test or inspection documents for requirements validation.²³³

5.2.6 Software Design (D.4.2.1.6)

The software design description (SDD) decomposes the software requirements to document the design and implementation of software components, modules, and units used to implement the WF3 CPCS replacement system. The NRC-approved SPM (Reference 6) states that the SDD must comply with IEEE Standard 1016-1998 (Reaffirmed 2009), “IEEE Recommended Practice for Software Design Descriptions”.

There are a number of SDDs that document the complete detailed design of each software element of the system and how the software components are combined into the application program. [

]^{a,c} The WF3

SDDs will be based on the NRC-approved Palo Verde replacement CPCS SDDs, with new and changed design descriptions to address the WF3 CPCS replacement system requirements specification (Reference 21) and WF3 SRS. These SDDs describe the design of the WF3 application.

For the AC160 controller there are lower level software modules, referred to as Reusable Software Elements (RSE). These software modules are described in the SDDs and document their instantiation in the application. Many of these RSEs will remain unchanged since their usage in the NRC-approved Palo Verde CPCS replacement application software. The independent V&V team writes the module test procedures and test reports for these RSEs.²³⁵

[

]^{a,c}

The traceability of the WF3 SRS to the WF3 SDDs will be documented in the RTM to aid in the V&V of the adequate design implementation of the SRS requirements.²³⁶

The tools used to generate the WF3 CPCS replacement software are the same tools described in the Common Q topical report (Reference 4). The SPM (Reference 6), Section 3.3.10 defines the requirements for tools used for both development and V&V.

Similar to the WF3 system requirements specification, the SDDs are independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

5.2.7 Software Implementation (D.4.2.1.7)

The generation of the WF3 CPCS replacement application software and revised RSEs is governed by the requirements in the NRC-approved SPM (Reference 6), Westinghouse work instructions²³⁷, the Common Q coding standards (Reference 27), and the Common Q design restrictions (Reference 18).

The WF3 replacement CPCS application software is reviewed by the independent V&V team for correct implementation of the software requirements.

Each RSE set has a test procedure and test report generated by the independent V&V team. The WF3 replacement CPCS application software is tested by the independent test team. These tests are developed, performed and documented in accordance with the SPM (Reference 6), which leverages the guidance in IEEE Std 829, and was reviewed and approved by the NRC using the guidance in Regulatory Guide 1.170, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference 34).

The NRC-approved SPM (Reference 6) states that the RSE module testing shall be performed in accordance with the Test Plan (Section 7 in the SPM) which is in compliance with IEEE Standard 1008-1987 (Reaffirmed 2009), “IEEE Standard for Software Unit Testing”. The RSE testing includes internal state testing.

The RSEs and WF3 CPCS replacement software is under configuration control, is released using a software release record specifying the configuration baseline for which the software is released. The application software CMRR will identify the RSE libraries used for the application software.²³⁸

5.2.8 Software Integration (D.4.2.1.8)

Section 7 of the NRC-approved SPM (Reference 6) outlines the sequence of tests that define the integration process for the WF3 CPCS replacement system.

- RSE testing (or module testing) – this is the elemental level. The RSE is developed and tested independent of any application program by the independent V&V team.
- Unit testing – this is testing a function chart application in a PM646A processor module, in which RSEs and standard function blocks are instantiated to create the logic for the application. The OM and the MTP software are considered unit software. Often unit testing is combined with Integration and System Validation testing. Unit testing is conducted by either the independent V&V team or the independent test team.
- Integration Test – is an informal test in preparation for the System Validation Test. Any anomalies identified during integration testing are resolved before the System Validation Test, if practical. If not, the open anomaly is tracked during formal System Validation testing.
- System Validation Test – this is formal integration testing of the software and hardware performed by the independent test team. The System Validation Test traces the test cases to the WF3 CPCS replacement system requirements specification (Reference 21).

5.2.9 Instrumentation and Control System Testing (D.4.2.1.9)

Testing will be conducted in accordance with the Common Q SPM, Section 7 describing the levels of testing of the software modules and units (e.g., MTP and OM) culminating with an integrated system test. Section 7 of the SPM also describes the methodology for response time testing. Multiple runs of the DNBR and LPD trip functions will be conducted to demonstrate the system meets the response time requirements.

The testing includes the factory acceptance test (FAT) that is conducted on the deliverable WF3 CPCS. The Common Q SPM (Reference 6), Exhibit 7-1, lists the types of tests that will be conducted on the WF3 CPCS for FAT.

Both the independent V&V team and the independent test team execute the test plan in the SPM (Reference 6), Section 7 on a complete, integrated CPCS using a baseline version. The independent V&V team executes the module tests and the independent test team executes the system validation testing and FAT. The unit testing is either conducted by the independent V&V team or included in the system validation testing.

The RTM traces the test cases to the WF3 system requirements specification (Reference 21) which will include the requirements to mitigate or eliminate hazards identified in the FMEA and SHA.

The system test reports will identify the CPCS replacement system configuration baseline and software CMRRs that were tested. System test results are documented in a test report. The NRC-approved SPM (Reference 6) states that the test report shall comply with IEEE Standard 829-1998, "IEEE Standard for Software Test Documentation", Section 11.

Similar to the WF3 system requirements specification, the WF3 CPCS replacement system test plan and test documentation are independently reviewed, and approved; and stored under configuration control.

5.2.10 Project Management Processes (D.4.2.2)

The WF3 Project Plan (Reference 28) describes project management processes and project organization. It cites the Project Quality Plan that identifies the Westinghouse 10 CFR 50 Appendix B Quality Assurance procedures to be followed for the project. It describes the controls for identifying the project scope, determination of deliverables, lines of communication, formal and informal reviews, and interfaces with other internal and external organizations.

The WF3 Project Plan provides for the establishment, documentation, and maintenance of a schedule that considers the overall project, as well as interactions of milestones. It provides for risk management, including problem identification, impact assessment, and development of risk-mitigation plans for risks that have the potential to significantly affect system quality goals.

The establishment of quality metrics throughout the life cycle to assess whether the quality requirements of IEEE Std 603-1991, Clause 5.3, are being met, in keeping with the additional guidance from IEEE Std 7-4.3.2-2003, Clause 5.3 is achieved by performing the metric processes defined in the NRC-approved SPM (Reference 6), Section 4.5.2.4.

Adequate control of software tools to support system development and software V&V processes, in keeping with the additional guidance in IEEE Std 7-4.3.2-2003, Clause 5.3.2 is achieved by following the NRC-approved SPM (Reference 6), Section 6 Software Configuration Management Plan. The WF3 CPCS Software Development Plan (Reference 25) describes the use of the various tools used for the WF3 CPCS replacement.

Those tools used by the design team to develop the CPCS application are used in a manner such that defects not detected by the software tool will be detected by independent verification and validation activities. Those tools used by the independent verification and validation team have undergone a tool validation program that provides confidence that the necessary features of the software tool function as required.²³⁹

5.2.11 Software Quality Assurance Processes (D.4.2.3)

The WF3 CPCS replacement project will follow the software quality assurance plan in the NRC-approved SPM (Reference 6), Section 4.

5.2.12 Software Verification and Validation Processes (D.4.2.4)

The WF3 CPCS replacement project will follow the software V&V plan in the NRC-approved SPM (Reference 6), Section 5. Exhibit 2-1 in the SPM shows the independence requirements between the V&V and design team. The minimum requirement is that the independent V&V team and the design team shall report to two different directors in the organization. The Westinghouse current organization reporting structure for the independent V&V team and design team meets this requirement.²⁴⁰

5.2.13 Configuration Management Processes (D.4.2.5)

The WF3 CPCS replacement project will follow the software configuration management plan in the NRC-approved SPM (Reference 6), Section 6. The WF3 CPCS Replacement Project Configuration Management Plan (Reference 31) provides the project specific details for configuration management.

6 APPLYING A REFERENCED TOPICAL REPORT SAFETY EVALUATION (D.5)

The replacement CPCS is based on the Common Q Platform. Westinghouse has on record an NRC-approved topical report on the Common Q Platform (Reference 4). Currently Westinghouse has submitted a revision 4 of the topical report for NRC review and approval (Reference 24).

6.1 COMMON Q PLATFORM CHANGES (D.5.1.1)

Managing changes to a safety system platform after the initial NRC Safety Evaluation Report (SER), and how these changes are reviewed by the NRC in a timely fashion, has been a topic of concern for digital software-based safety systems. The Common Q Platform received its original SERs from the NRC's Office of Nuclear Reactor Regulation (NRR) that encompassed a) the Topical Report including closeout of generic open items (GOIs) in February 2003 and b) the Software Program Manual in September 2004. In February 2013 Westinghouse received an SER from the NRC on the updated version of the Common Qualified Platform Topical Report (Reference 4), and in November 2018, Westinghouse received an SER from the NRC on the updated Software Program Manual for Common Q Systems (Reference 6). Currently Westinghouse has submitted a revision 4 of the topical report for NRC review and approval (Reference 24).

There have been changes to the Common Q Platform since its approval in 2013. Westinghouse has a documented change process that evaluates platform changes. The process evaluates each change of the platform against the safety conclusions reached by the NRC in its safety evaluation report for the platform. This process is described in WCAP-17266-P, "Common Q Platform Generic Change Process" (Reference 12).

Appendix 5 of the Common Q Topical Report (Reference 13) is the output document for the change process described in Reference 12). The document provides a summary of changes and then a detailed recording of analysis and/or qualification documents, and a conclusion statement on the status of the change relative to the NRC safety conclusions. Reference 13 can be audited by the NRC staff to achieve reasonable assurance that Westinghouse is maintaining the Common Q Platform within the bounds of the safety conclusions in the safety evaluation of the platform.

6.1.1 Common Q Platform Topical Report Revision

The Common Q Platform Topical Report revision that applies to this licensing technical report and LAR is Revision 4 (see Reference 4)

6.2 RESOLUTION OF TOPICAL REPORT PLANT-SPECIFIC ACTION ITEMS (D.5.1.2)

The Common Q Topical Report (Reference 4) has two Generic Open Items (GOIs) and 24 Plant-Specific Action Items (PSAIs). PSAI 3 is closed and does not need to be addressed by licensees.²⁴¹ This section addresses each for the WF3 CPCS replacement. The Common Q Software Program Manual (Reference 6) also has PSAIs. These are addressed in Section 5.

6.2.1 Generic Open Items

Although the SER for the Common Q Topical Report lists 12 GOIs, all have been closed but two. These are addressed in this section.

6.2.1.1 GOI 8

GOI 8 states: *Westinghouse needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components. This is discussed in Section 4.4.4.3.2.*

This GOI refers to the loop controllers described in the Common Q Platform Appendix 4 (Reference 15). The loop controllers fulfill the function of a priority module as described in DI&C-ISG-04, Section 2 Command Prioritization (Reference 9). The replacement CPCS does not include loop controllers nor does it include a priority module function. Therefore this GOI does not apply to the replacement CPCS.

6.2.1.2 GOI 12

GOI 12 states: *Westinghouse has not yet concluded seismic, environmental and Electromagnetic Compatibility (EMC) qualification testing of the following Common Q platform hardware components:*

- *CI528W Communications Interface Module*
- *ATS-PCNB-007 – PC Node Box*
- *10160D05 Processor Module*
- *10160D06 Fiber Optic Module*
- *10160D07 Input / Output Module*
- *10160D08 Synchronization Module*
- *10160D09 Power Supply Module*

These hardware components are required to be tested and qualified for the specific plant conditions prior to being placed into operation within a safety system application.

The replacement CPCS does not use this equipment in the CPCS architecture, so this GOI does not apply to the replacement CPCS (this equipment is related to a new alternate Flat Panel Display System architecture under development and not deployed for the WF3 CPCS).

6.2.2 Plant-Specific Action Items

There are 25 PSAIs for the Common Q Platform Topical Report. One of these PSAIs, PSAI 3, has been resolved generically and therefore is not addressed here. The other 24 PSAIs are addressed in this section.

6.2.2.1 PSAI 1

PSAI 1 states: *Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements. See Section 4.1.1.1.2.*

The CPCS system requirements specification (Reference 2 and 21) Section 2.3.11 and 2.3.12 define the interface input and output requirements for the CPCS replacement. Aside from the number of CEAs and clarifications on accuracy, these are the same requirements for the Palo Verde CPCS replacement. The same I/O modules are used except for the analog input module. The Palo Verde CPCS replacements used the AI685 analog input module. The WF3 CPCS replacement uses the AI688 analog input module. The AI688 analog input module characteristics for the 0-1 vdc and 0-10 vdc meet the requirements of Reference 2, Section 2.3.11²⁴².

6.2.2.2 PSAI 2

PSAI 2 states: *A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The Review of the implementation of such a hardware user interface would be a plant-specific action item. See Section 4.1.2.*

The WF3 CPCS replacement is not using an alternative to the flat panel display system (FPDS) described in the Common Q Topical Report (Reference 4). Therefore, this PSAI does not apply to the WF3 CPCS replacement.

6.2.2.3 PSAI 4

PSAI 4 states: *Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. The licensee must also ensure that the plant specific common Q system configuration does not exceed the configuration used during platform qualification testing. See Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3.*

The Common Q test specimen was configured for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots. See Section 4.2.2.1.2.

The WF3 CPCS EQ Summary Report (Reference 35) analyzes the EQ of the components that make up the replacement CPCS and concludes that the testing and results encompass WF3 site requirements for the CPCS. The spare AC160 controller slots in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram, will be filled by the AC160 dummy module. Section 3.1.1.1 of the WF3 system requirements specification (Reference 21) defines the requirement to use dummy modules for unused AC160 controller slots.

6.2.2.4 PSAI 5

PSAI 5 states: *On the basis of its review of the Westinghouse software development process for application software, the NRC staff concludes that the Common Q software program manual SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the NRC staff or others to evaluate the quality of the design features upon which the safety determination will be based. When a license amendment process is used for implementation of a Common Q based safety system, the NRC staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant-specific basis. See Section 4.3.2.*

As stated in DI&C-ISG-06 (Reference 1) Section D.4.2, *Sections D.4.2.1.1 through D.4.2.1.4 address life cycle activities that are part of the NRC review scope. Sections D.4.2.1.5 through D.4.2.1.9 describe process evaluations that are part of the NRC review scope. The evaluation of the design outputs using the process described in Sections D.4.2.1.5 through D.4.2.1.9 are not within the scope of the LAR review. The licensee is responsible for ensuring vendor use of procedures and the acceptability of all vendor work products discussed in Sections D.4.2.1.1 through D.4.2.1.9.*

Section D.4.2.1.1 through D.4.2.1.4 represent the design life cycle phases respectively:

- Plant and Instrumentation and Control System Safety Analysis
- Instrumentation and Control System Requirements
- Instrumentation and Control System Architecture
- Instrumentation and Control System Design

It is understood that the licensee is responsible for ensuring vendor use of procedures and the acceptability of all vendor work products discussed in these phases. The NRC staff will also evaluate the implementation of the life cycle process and the software life cycle process design outputs for the CPCS replacement for these life cycle phases listed above. This represents the Common SPM life cycle phases 1) Concept and 2) Requirements Analysis (see Reference 6, Section 1.4.1).

As stated in DI&C-ISG-06 above, *Sections D.4.2.1.5 through D.4.2.1.9 are not within the scope of the LAR review.* Section D.4.2.1.5 through D.4.2.1.9 represent the design life cycle phases respectively:

- Software Requirements
- Software Design
- Software Implementation
- Software Integration
- Instrumentation and Control System Testing

This represents the Common Q SPM life cycle phases (see Reference 6, Section 1.4.1):

- Requirements Analysis
- Design
- Implementation or Coding
- Test

The WF3 vendor oversight plan describes how WF3 will verify Westinghouse use of procedures, and will verify the acceptability of Westinghouse work products to the requirements of the Common Q SPM.

6.2.2.5 PS AI 6

PSAI 6 states: *When implementing a Common Q safety system (i.e., PAMS, CPCS, or DPPS), the licensee must review the timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. See Sections 4.1.1.4 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.*

Section 3.2.6 describes how the response time criteria for the Common Q WF3 CPCS is created and how it will be demonstrated that the CPCS calculated response times maintain the safety margin for the plant. The Common Q SPM, Section 7, describes the testing to be performed on the replacement CPCS. The response time of the replacement CPCS will be validated to confirm the system meets the timing analysis results (see the Common Q SPM Exhibit 7-1). The accuracy requirements for the WF3 replacement CPCS are summarized in Section 3.3 and defined in the CPCS system requirements specification (Reference 2 and 21) Section 2.3.11. The accuracy requirements are validated by test as described in the Common Q SPM test plan Section 7.3.1.5 and Exhibit 7-1. The WF3 vendor oversight plan describes how the licensee will verify that Westinghouse properly propagates these requirements through the design, implementation, and test of the replacement CPCS.

6.2.2.6 PS AI 7

PSAI 7 states: *The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis. See Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 4.4.4.3.6 of Reference 3 for additional information on this item.*

The OM and MTP displays are summarized in Section 3.2.7. The requirements for these displays are specified in the CPCS system requirements specification (Reference 2), Section 2.2 and the WF3 specific CPCS system requirements specification (Reference 21). These displays have been reviewed by WF3 operations staff and modified accordingly to support their control room tasks.

In regards to access control, Section 3.3.3.5 describes how access control meets the criteria of IEEE Std 603-1991. These secure operational controls are similar to the controls implemented for the Palo Verde CPCS replacement and found to be acceptable from a human factors perspective.

6.2.2.7 PS AI 8

PSAI 8 states: *If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being*

replaced, and meets the functionality requirement applicable to those systems. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.

The CPCS system requirements (Reference 2) defines the functional and system requirements for the replacement CPCS to meet the same functionality of the existing CPCS. Reference 2 is the reference design system requirements, representing the Palo Verde CPCS implementation. The WF3 CPCS system requirements specification (Reference 21) defines those unique requirements for the WF3 CPCS replacement that differ from the Palo Verde replacement CPCS functional and system requirements.

6.2.2.8 PSAI 9

PSAI 9 states: Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the NRC staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.

WF3 is submitting a plant-specific request for license amendment with attendant justification for the replacement CPCS. The license amendment is following the guidance in DI&C-ISG-06 (Reference 1).

6.2.2.9 PSAI 10

PSAI 10 states: A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) must prepare its plant-specific model for the design to be implemented and perform the FMEA for that application. See Section 5.0 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.

The model for the WF3 CPCS replacement is defined in the CPCS system requirements specification (Reference 2) as augmented by the WF3 CPCS system requirements specification (Reference 21). The FMEA (Reference 39) for the WF3 CPCS replacement is summarized in Section 3.2.17.

6.2.2.10 PSAI 11

PSAI 11 states: A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in DI&C systems and meets the requirements of BTP 7-19. See Sections 4.1.6 of this SE as well as Sections 4.4.2.3, 4.4.3.3, and 4.4.4.3.3 of Reference 3 for additional information on this item.

The WF3 defense against common-mode failure (i.e., common cause failure) is addressed in Section 3.2.18.

6.2.2.11 PSAI 12

PSAI 12 states: A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing. See Section 4.4.3.3 of Reference 3 for additional information on this item.

As part of the CPCS replacement license amendment request, Entergy is proposing elimination of specific technical specification surveillance requirements including response time by crediting AC160 diagnostics. Appendix B - "Elimination of Specific CPCS Technical Specification Surveillance Requirements" provides the analysis and justification for this technical specification change. The WF3 CPCS is tested at the factory and during installation to confirm that the response time for the system is met. The methodology used is found in the Common Q SPM, Exhibit 7-1.

6.2.2.12 PSAI 13

PSAI 13 states, *The analysis of the capacity of the shared resources to accommodate the load increase due to sharing. Section 4.4.4.3.1 of Reference 3 for additional information on this item.*

This PSAI is in reference to the Common Q Topical Report Appendix 4 (Reference 15) that describes an architecture that integrates the functions of the plant protection system, core protection calculator system and the post accident monitoring system. The WF3 license amendment is only replacing the CPCS and not the plant protection system. This PSAI, regarding shared resources between the CPCS and other Common Q based systems, is not applicable to this license amendment.

6.2.2.13 PSAI 14

This PSAI states: *The licensee implementing Common Q applications must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items. See Section 5.0.*

The WF3 CPCS is a pre-TMI system that generates reactor trip signals for Low DNBR and High LPD trips. The OM for the CPCS is not used for any post accident monitoring. Once the reactor is tripped other systems are used for post accident monitoring.

6.2.2.14 PSAI 15

This PSAI states: *During the Software development process, the licensee must specify plant specific requirements for system automatic self-testing features that are needed to ensure proper functioning of the Common Q application during operation. See Section 4.1.1.3.*

The plant-specific requirements for system automatic self-testing features that are needed to ensure proper function of the Common Q application during operation is specified in the CPCS system requirements specification (Reference 2), Section 2.4.2.1 as augmented by WF3 CPCS system requirements specification (Reference 21). The service/test functions of the WF3 CPCS replacements are described in Section 3.2.7 in this document.

6.2.2.15 PSAI 16

This PSAI states: *A licensee implementing a Common Q DPPS shall ensure that no more than four processor modules are installed within a single AC160 controller. See Section 2.1.*

As shown in the architecture drawing of the four channel CPCS in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram, there are only two PM646A processor modules in a single AC160 controller.

6.2.2.16 PSAI 17

This PSAI states: *A licensee implementing a Common Q DPPS must ensure that all hardware components used for system development are approved for use in nuclear safety system class 1E applications and are listed in Table 1. See Section 2.1 for a discussion of the hardware components of the Common Q platform.*

Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram shows the following AC160 modules that will be used for the WF3 CPCS. They are listed below and all of them are listed on Table 1 of the safety evaluation. The product revision listed below are the current revisions of the modules. The Common Q record of changes document (Reference 13) assesses these later, qualified product revisions and the qualification references demonstrating that the product remains consistent with the safety conclusions in the NRC safety evaluation. Reference 13 is a living document that is continuously updated as revisions to modules are made.

AI688 – S600 Analog Input Module, PR: C

AO650 – S600 Analog Output Module, PR: B

CI527W – Communications Interface Module, PR: C

CI631 – Communications Interface Module, PR: H

DI620 – S600 Digital Input Module, PR: D

DO625 – S600 Digital Output Module, PR: B

DP620 – S600 Pulse Counter Module, PR: B

PM646A – Advant Controller 160 (AC160) Processor Module: PR: U

AC160 Base Software – Base Software, PR: 1.3/11

ACC Tool – Tool, PR: 1.7/1

The final equipment designation for the flat panel display system, power supply, and HSL fiber optic modems will be documented during the hardware design phase. The product revision levels for all Common Q platform equipment will be finalized at time of FAT for the CPCS. The Common Q Topical Report record of changes document (Reference 13) is a living document that is updated when platform changes are processed in accordance with Reference 12. WF3, via the vendor oversight plan, will compare the equipment part numbers to those listed in Table 1 of the safety evaluation. Where differences exist in part number or product revision, WF3 will review the topical report record of changes document (Reference 13) for adequate qualification documentation that demonstrate that the changes do not invalidate safety conclusions in the safety evaluation of the Common Q platform.

6.2.2.17 PSAI 18

This PSAI states: *The licensee implementing Common Q applications must ensure that administrative controls are put into place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions. The affected division of the Common Q safety system must be declared inoperable prior to implementation of setpoint changes. See Section 4.1.3.4.*

Table 3.2.16-1 DI&C-ISG-04-Compliance, Position 10 describes the administrative controls for changing setpoints in the WF3 CPCS replacement. WF3 procedures exist to declare a CPCS channel inoperable and put the CPCS channel in maintenance bypass when changing CPCS setpoints.²⁴³

6.2.2.18 PSAI 19

This PSAI states: *A licensee implementing a specific application based upon the Common Q platform must ensure that the serial communications link between the MTP and the Processor Module is disabled by means of a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A). Alternative means of disconnecting this serial communication link may be considered, however, any means of disabling this communication link which rely upon software logic would invalidate the DI&C-ISG-04 conformance safety conclusions in Section 4.1.3.4 Staff Position 1, Point 10 of this SE.*

The serial communications link between the MTP and the PM646A, referred to in this PSAI, is the programming cable that allows the MTP to load a new program into the PM646A. DI&C-ISG-04 compliance to the requirement that a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A) is addressed in Table 3.2.16-1 DI&C-ISG-04-Compliance, Position 10. [

]^{a,c} This is the same methodology used for the NRC-approved Palo Verde CPCS replacement.

6.2.2.19 PSAI 20

This PSAI states: *A licensee implementing an application based upon the Common Q platform that utilizes fiber optic cables to connect HSL's between safety divisions shall ensure that all plant specific environmental qualification requirements for this cabling are met. See Section 4.2.2.2.*

Fiber optic cable at WF3 is purchased to Entergy specification, SPEC-10-00001-MULTI, "73.55 Fleet Strategy Implementation – Fiber Optic Cable Common-Procurement Specification" (Reference 40) to ensure meeting the WF3 site environmental qualification requirements.

6.2.2.20 PSAI 21

This PSAI states: *A licensee implementing an application based upon the Common Q platform that includes implementation of HSL must perform a site specific analysis to quantify the impact of higher electromagnetic emissions on operation of locally mounted equipment. See Section 4.2.2.1.3.*

The WF3 equipment qualification summary report (Reference 35, Section 3.3) confirms that the electromagnetic emissions from the HSL do not adversely affect the operation of locally mounted equipment.

6.2.2.21 PSAI 22

This PSAI states: *A licensee implementing an application based upon the Common Q platform that uses AI685 modules configured for either RTD or Thermocouple input must ensure that the installation includes a metallic barrier in front of the module. See Section 4.2.2.1.3.*

The WF3 CPCS replacement uses the AI688 analog input module in place of the AI685 analog input module as shown in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram. Therefore this PSAI does not apply to the WF3 CPCS replacement.

6.2.2.22 PSAI 23

This PSAI states: *A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q platform hardware, software, or processes defined in the Common Q TR.*

The response to PSAI 17 (Section 6.2.2.16) addresses this PSAI.

6.2.2.23 PSAI 24

PSAI 24 states: *A licensee implementing an application based upon the Common Q platform that relies on the FPDS to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation.*

The OM and MTP do not perform safety critical functions. As defined in the Common Q SPM (Reference 6), safety critical functions are those functions that are “necessary to directly perform RPS control actions, ESFAS control actions, and safe shutdown control actions”. The MTP and OM functions are described in Section 3.2.7. None of these functions involve an RPS control action, ESFAS control action, or safe shutdown control action. Therefore, this PSAI does not apply to the WF3 CPCS replacement.

6.2.2.24 PSAI 25

This PSAI states: *A licensee implementing an application based upon the Common Q platform that relies upon the use of ITPs and the AF100 busses to provide separation between safety and non-safety signals must evaluate the plant-specific design against the independence criteria of IEEE 7-4.3.2-2003, Section 5.6.*

As shown in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram, the AF100 bus resides within one channel of the CPCS architecture. Only the unidirectional, fiber optically isolated HSL is used for CPCS interchannel communication.

7 COMPLIANCE/CONFORMANCE MATRIX FOR IEEE STANDARDS 603-1991 AND 7-4.3.2-2003 (D.6)

This section provides a compliance/conformance table for IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003. Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2 provides a summary of compliance and a cross reference to sections in this document that explain the compliance/conformance. The Compliance/Conformance column will have the following code:

- C: Complies
- PC: Partially Complies
- E: Exception
- N/A: Not applicable

Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
4.1	4*	Safety System Design Basis	C	3.3.2 Clause 4.1
4.2			C	3.3.2 Clause 4.2
4.3			C	3.3.2 Clause 4.3
4.4			C	3.3.2 Clause 4.4
4.5			C	3.3.2 Clause 4.5
4.6			C	3.3.2 Clause 4.6
4.7			C	3.3.2 Clause 4.7
4.8			C	3.3.2 Clause 4.8
4.9			C	3.3.2 Clause 4.9
4.10			C	3.3.2 Clause 4.10
4.11			C	3.3.2 Clause 4.11

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
4.12			C	3.3.2 Clause 4.12
5.1	5.1*	Single Failure Criterion	C	3.2.17 3.2.19.1.1
5.2	5.2*	Completion of Protective Action	C	3.3.3.1
5.3	5.3	Quality	C	3.3.3.10 5
	5.3.1	Software Development	C	5.2
	5.3.1.1	Software Quality Metrics	C	5.2.10
	5.3.2	Software Tools	C	5.2.10
	5.3.3	Verification and Validation	C	5.2.12
	5.3.4	Independent V&V Requirements	C	5.2.12
	5.3.5	Software Configuration Management	C	5.2.13
	5.3.6	Software Project Risk Management	C	5.2.10
5.4	5.4	Equipment Qualification	C	4
	5.4.1	Computer System Testing	C	4
	5.4.2	Qualification of Existing Commercial Computers	C	3.3.3.10 6.1
5.5	5.5	System Integrity	C	3.3.3.2
	5.5.1	Design for Computer Integrity	C	3.6.3.1.2
	5.5.2	Design for Test and Calibration	C	3.2.19.2.1
	5.5.3	Fault Detection and Self-Diagnostics	C	3.2.19.2.2
5.6	5.6	Independence	C	3.5.10.5

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
5.6.1		Between Redundant Portions of a Safety System	PC	3.5.10.1
5.6.2		Between Safety Systems and Effects of Design-Basis Event	C	3.5.10.2
5.6.3		Between Safety Systems and Other Systems	C	3.5.10.3
5.6.4		Detailed Criteria	C	3.5.10.4
5.7	5.7*	Capability for Testing and Calibration	C	3.2.19.1.2
5.8	5.8*	Information Displays	N/A – No specified criteria	N/A
5.8.1		Displays for Manually Controlled Actions	C	3.2.19.1.3
5.8.2		System Status Indication	C	3.2.19.1.4
5.8.3		Indication of Bypasses	C	3.2.19.1.5
5.8.4		Location	C	3.2.19.1.6
5.9	5.9*	Control of Access	C	3.3.3.5
5.10	5.10*	Repair	C	3.3.3.6
5.11	5.11	Identification	C	3.2.19.1.7 3.6.2.1.2
5.12	5.12*	Auxiliary Features	N/A – No specified criteria	N/A
5.12.1		Auxiliary Features	C	3.5.10.6.1
5.12.2		Other Auxiliary Features	C	3.5.10.6.2
5.13	5.13*	Multi-Unit Stations	N/A – The CPCS is not	N/A

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/ Conformance	Section(s)
			shared among multiple NPPs	
5.14	5.14*	Human Factors Considerations	C	3.5.10.7
5.15	5.15	Reliability	C	0 Clause 4.9 3.6.1.1.2
6.1	6*	Automatic Control	C	3.6.3.1.3
6.2		Manual Control	C	3.6.3.1.4
6.3		Interaction between the Sense and Command Features and Other Systems	N/A – No specified criteria	N/A
6.3.1		Requirements	C	3.6.2.1.3
6.3.2		Provisions	C	3.6.2.1.3
6.4		Derivation of System Inputs	C	3.6.5.1
6.5		Capability for Testing and Calibration	N/A – No Criteria	N/A
6.5.1		Checking the Operational Availability	C	3.3.3.3
6.5.2		Assuring the Operational Availability	C	3.3.3.3
6.6		Operating Bypasses	C	3.3.3.7
6.7		Maintenance Bypass	C	3.3.3.8
6.8		Setpoints	C	3.3.3.9
7.1-7.5	7*	Executive Features – Functional and Design Requirements	N/A – The CPCS only performs Sense and	N/A

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
			Command Features.	
8.1	8*	Electrical Power Sources	C	3.5.8
8.2		Non-electrical Power Sources	N/A – CPCS does not use non-electrical power sources	3.5.8
8.3		Maintenance Bypass	C	3.5.8

*The standard does not add additional criteria beyond that stated in IEEE Std 603-1991.

8 TECHNICAL SPECIFICATIONS (D.7)

WF3 is replacing the existing digital CPCS with a new, functionally equivalent, digital Common Q CPCS provided by Westinghouse Electric Power LLC. However, there will now be 8 CEACs instead of just two for the whole system. As a result, the technical specification changes will reflect improved operability capability than the existing CPCS. In addition, the technical specification changes will reflect elimination of certain surveillance requirements by crediting the CPCS diagnostics. The analysis for which surveillance requirements can be eliminated is in Appendix B of this document. The Entergy WF3 CPCS LAR provides the actual technical specification markups for WF3 as a result of the CPCS replacement. These proposed changes to the technical specifications continue to satisfy the requirements of 10 CFR 50.36.

9 SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT (D.8)

This section describes the secure development and operational environment of the CPCS meeting the guidance in both DI&C-ISG-06 (Reference 1) and RG 1.152 (Reference 17).

9.1 SECURE DEVELOPMENT ENVIRONMENT

The replacement CPCS is designed and developed by Westinghouse within their facility up to and including the FAT. Once FAT is completed, the CPCS is shipped to WF3 and stored until it is installed in the plant.

While the replacement CPCS is at the Westinghouse facility, it is designed and implemented using a secure development environment. The secure development environment is described in the Common Q SPM (Reference 6), Section 12.2.1.2. The NRC evaluated the secure development environment controls. Based on the NRC's review of the Westinghouse Common Q secure development environment as described in the Common Q SPM (Reference 6), the staff concluded that the described controls meet the requirements of RG 1.152 (Reference 17).

Entergy's vendor oversight plan will include verifying that Westinghouse complies with the requirements in the SPM for a secure development environment. This will address the NRC's Plant Specific Action Item 7 in their safety evaluation report for the SPM:

Secure Development and Operational Environment – An applicant or licensee referencing the Common Q SPM for a safety-related plant specific application should ensure that a secure development and operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.

9.2 SECURE OPERATIONAL ENVIRONMENT

The NRC stated in its safety evaluation in the Common Q Topical Report (Reference 4), *“Although application software is not within the scope of this review, platform features that contribute to the SDOE for the application are identified and discussed. Credit may be taken for the use of these security capabilities in establishing a secure operational environment for a plant specific safety-related application.”*

The replacement CPCS physical and logical access features are included in the system requirements (see Table 9.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness). The CPCS system requirements specification (Reference 2) as augmented by the WF3 system requirements specification (Reference 21) would normally have derived secure operational environment requirements from a vulnerability assessment as described in RG 1.152 (Reference 17). However, the CPCS system requirements specification (Reference 2) was developed prior to RG 1.152 specifying criteria for a secure operational environment. To meet the criteria of RG 1.152, a vulnerability assessment is included as part of the replacement CPCS LAR to confirm that the necessary secure operational environment requirements have been captured in Reference 2 and 21.

9.2.1 Secure Operational Environment Vulnerability Assessment

This assessment addresses the secure operational environment to address 1) deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system that may degrade its reliability, integrity or functionality during operations, and 2) the potential inability of the system to sustain the safety function in the presence of undesired behavior of connected systems as described in RG 1.152 (Reference 17).

The Common Q SPM (Reference 6), Section 12 includes the vulnerability assessment ensuring that the system is developed without undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely affect the reliable operation of the digital system. The NRC has reviewed these controls as part of the review of the Common Q SPM (see Safety Evaluation Report, Section 3.2.13, embedded in Reference 6).

9.2.1.1 CPCS System Architecture

The CPCS system architecture is depicted in Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram. It consists of the following components:

- AC160 – AC160 controllers perform the CPCS safety function (i.e., CPC and CEAC, see Sections 3.2.1 and 3.2.2).
- OM - The OM is in the control room and provides the operator with CPCS information (e.g. Low DNBR/High LPD Status, Post Trip Reports, etc.). The OM also allows the operator to adjust addressable constants and perform testing (see Section 3.2.7.2).
- MTP – The MTP is a local display system within the locked APC that provides system status information, adjustment for addressable constants, and provides for testing the CPCS. The MTP also provides an interface to an IRIG data link for time synchronization and a unidirectional, fiber optically isolated data link to the plant monitoring computer, CEAPD, and to a printer (see Section 3.5).
- AF100 – The AF100 bus is a network within a CPCS channel to allow the sharing of data between the AC160 controllers, the OM and the MTP. This network does not extend beyond the boundaries of the channel (see Sections 3.2.1 and 3.2.2).
- HSL – The HSL is a point to point data link which is used to communicate data within a channel when real time performance is critical (e.g., between CPC and CEAC AC160 controllers within a CPCS channel) and between channels (see Section 3.5.1).

9.2.1.2 CPCS Potential Vulnerability Assessment Process

A system's secure operational environment assessment addresses 1) the digital exposure along connectivity pathways for the system including direct and indirect connectivity, 2) the physical exposure of the system, including direct and indirect connectivity, 3) the effectiveness of the communication flow controls, and 4) the effectiveness of the access control and authorization mechanisms. As part of these assessments, vulnerabilities associated with inadvertent access or changes to a system are examined and failures or unpredictable behavior of connected systems are identified and addressed. This process identifies secure operational environment vulnerabilities associated with inadvertent access or changes to the system by performing an analysis of how the system's functions are accessed. Vulnerabilities related

to failures or unpredictable behaviors of connected systems are identified by examination of systems, networks, and communication systems that could be potential pathways for compromise.

This secure operational environment vulnerability assessment documents the controls that are in place as defined by the system requirements to mitigate the vulnerabilities identified.

9.2.1.3 Vulnerability Identification

Using Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram as a reference, digital connectivity pathways are assessed and potential vulnerabilities are identified.

Assessed interfaces to the replacement CPCS include:

- The replacement CPCS has an AF100 network interface for communication within a channel.
- The replacement CPCS has HSLs that can communicate within a channel and between channels.
- The MTP and OM support removable media to allow for saving and loading addressable constants.
- Each channel of the replacement CPCS has an OM in the control room. The OM provides the capability to change system addressable constants and activate the DNBR/LPD operating bypass. MTP and OM support removable media to allow for saving and loading addressable constants.
- Each channel of the replacement CPCS has an MTP. The MTP provides the capability to perform tests, change CPCS addressable constants, load Reload Data Block constants, and activate the DNBR/LPD operating bypass when operating under QNX.
- The MTP provides an interface to an IRIG data link for time synchronization
- The MTP provides a unidirectional, fiber optically isolated data link to the plant monitoring computer, CEAPD, and to a print server.
- Each AC160 controller, MTP, and OM provides a connection point for reprogramming or reconfiguring the CPCS.
- The MTP has the capability to reboot into Windows to allow the use of the Advant AC160 ACC tool for loading new applications to the processor modules in a channel. The system is in off line mode and tripped for these activities.

[

] ^{a,c}

9.2.1.4 Mitigating System Requirements

9.2.1.4.1 Safety System Independence Features

The following types of interfaces between the CPCS and external systems are summarized below along with independence features that protect the safety system from failures of external systems:

[

]^{a,c}

9.2.1.4.2 Compliance with IEEE Std 603-1991, Clause 5.9 Control of Access

Refer to Section 3.3.3.5 for compliance to IEEE Std 603-1991, Clause 5.9.

9.2.1.5 Summary of Vulnerabilities, Identified Controls, and Overall Effectiveness of Controls

Table 9.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness identifies the assessed interfaces, associated vulnerabilities, description of controls, assessment of effectiveness of controls, and references to system requirements for the controls. The requirements cited in Table 9.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness will be traced through the WF3 CPCS development life cycle for correct implementation through design, implementation and test, as required by RG 1.152 (Reference 17).

Table 9.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness

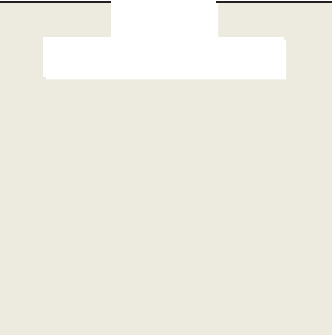
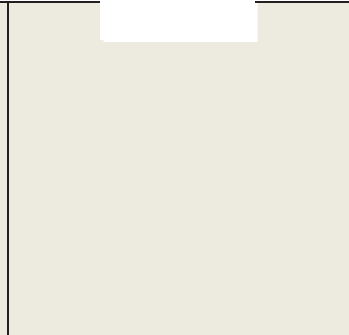
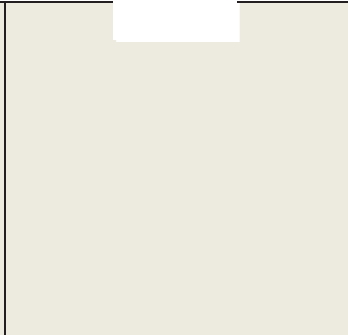
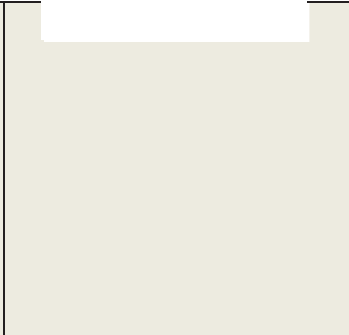
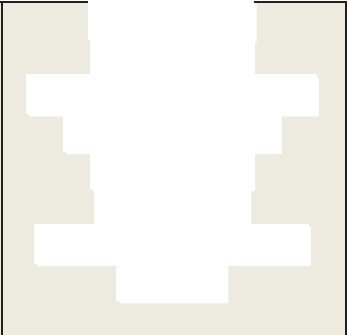
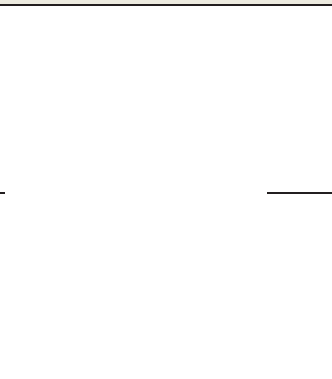
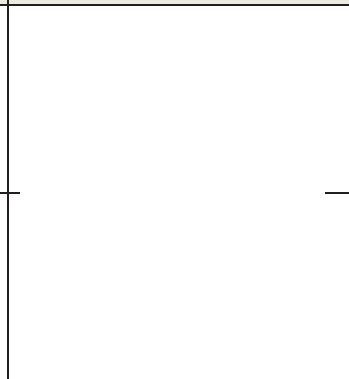
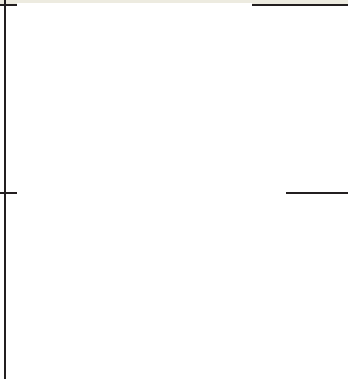
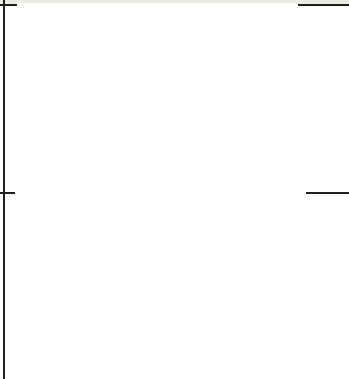
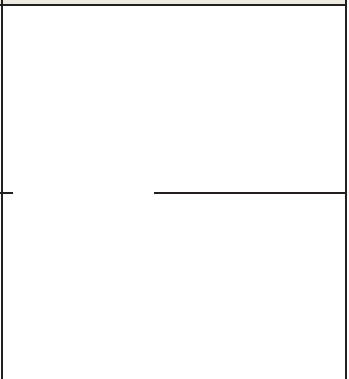
a,c

[illegible]

[illegible]

a,c

[illegible]

10 REFERENCES

1. DI&C-ISG-06, “Digital Instrumentation and Controls Licensing Process Interim Staff Guidance,” ML18269A259, Revision 2, United States Nuclear Regulatory Commission
2. System Requirements Specification for the Common Q Core Protection Calculator System, 00000-ICE-30158, Revision 14
3. Palo Verde Nuclear Generating Station, Units 1, 2, and 3 – Issuance of Amendments on the Core Protection Calculator System Upgrade (TAC Nos. MB6726, MB6727 and MB6728), ML033030363, US Nuclear Regulatory Commission
4. Common Qualified Platform Topical Report, WCAP-16097-P-A, Revision 4, Westinghouse Electric Company LLC
5. Common Qualified Platform Topical Report Appendix 2 Core Protection Calculator System, WCAP-16097-P-A Appendix 2, Westinghouse Electric Company LLC
6. Software Program Manual for Common Q™ Systems, WCAP-16096-P-A, Revision 5, Westinghouse Electric Company LLC
7. Physical Independence of Electric Systems, Regulatory Guide 1.75, Revision 1, US Nuclear Regulatory Commission
8. Control Panel 7 & 2 Cyber Security Door Lock Plan, ENT-WF3-CPC-115, March 17, 2020, Entergy Operations, Inc.
9. DI&C-ISG-04, Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance, ML083310185, Revision 1, United States Nuclear Regulatory Commission
10. S600 I/O Hardware Advant Controller 160 for Westinghouse Version 1.3 Reference Manual, 3BDS 005 740R501, Asea Brown Boveri
11. RPS/ESFAS Extended Test Interval Evaluation, CEN-327-A, May 1986, Combustion Engineering, Inc.
12. Common Q Platform Generic Change Process, WCAP-17266-P, Revision 1, Westinghouse Electric Company LLC
13. Common Qualified Platform Record of Changes, WCAP-16097-P Appendix 5, Revision 4, Westinghouse Electric Company LLC
14. AC160 Processor Module Stall Timers Not Activated as Described in Licensing Basis, Nuclear Safety Advisory Letter NSAL-17-2, Revision 1, Westinghouse Electric Company LLC
15. Common Qualified Platform Integrated Solution, WCAP-16097-P-A Appendix 4, Revision 0, Westinghouse Electric Company LLC
16. Guidance for the Review of Changes to Human Actions, NUREG-1764, Revision 1 (ML072640413), United States Nuclear Regulatory Commission
17. Criteria for Use of Computers in Safety System of Nuclear Power Plants, Regulatory Guide 1.153, Revision 3 (ML102870022), United States Nuclear Regulatory Commission
18. Application Restrictions for Generic Common Q Qualification, WNA-DS-01070-GEN, Revision 15, Westinghouse Electric Company LLC
19. Not used
20. Technical Specifications, NUREG-1117 (ML053130318 Appendix A), Waterford Steam Electric Station, Unit No. 3, Docket 50-382, Entergy Operations, Inc.

REFERENCES (cont.)

21. System Requirements Specification for the Core Protection Calculator System, WNA-DS-04517-CWTR3, Revision 2, Westinghouse Electric Company LLC
22. Core Protection Calculator (CPC) System Input Error Analysis, 00000-ICE-3672, Revision 5, Westinghouse Electric Company LLC.
23. WF3 Appendix K and PLCEA Replacement CPC Reload Data Block, LTR-TAS-01-20, Revision 0, Westinghouse Electric Company LLC
24. Waterford Unit 3 Common Q Implementation – Non-LOCA Evaluation of Updated CPCS Response Times, LTR-TA-20-4, Revision 0, Westinghouse Electric Company LLC
25. Software Development Plan for the Core Protection Calculator System Upgrade, WNA-PD-00594-CWTR3, Revision 0, Westinghouse Electric Company LLC
26. Software Requirements Specification for the Common Q Core Protection Calculator System, 00000-ICE-3233, Revision 9, Westinghouse Electric Company LLC.
27. Coding Standards and Guidelines for Common Q Systems, 00000-ICE-3889, Revision 16, Westinghouse Electric Company LLC
28. Project Management Plan for the Waterford 3 Core Protection Calculator Upgrade, GPEP-PMP-2019-000020, Revision 1, Westinghouse Electric Company LLC
29. Safety Evaluation Report related to operation of Arkansas Nuclear One, Unit 2, Supplement 1, NUREG-0308, Suppl. No. 1 (ML102850080), US Nuclear Regulatory Commission Office of Nuclear Regulation
30. Palo Verde Nuclear Generating Station Units 1, 2, & 3 Core Protection Calculator System Technical Manual, 14273-ICE-3460, Revision 4, Westinghouse Electric Company LLC
31. Configuration Management Plan for the Core Protection Calculator System Upgrade Project, WNA-PC-00069-CWTR3, Revision 1, Westinghouse Electric Company LLC
32. Waterford 3 Core Protection Calculator System Safety Function Table, LTR-TA-19-154, Revision 0, Westinghouse Electric Company LLC
33. WF3 Cycle 23 Final Safety Analysis Groundrules, NF-WTFD-18-5, Revision 0, Entergy Services, Inc.
34. Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.170, Revision 1, US Nuclear Regulatory Commission.
35. Core Protection Calculator System Upgrade Project Equipment Qualification Summary Report for Waterford Unit 3, EQ-QR-400-CWTR3, Revision 0.
36. Functional Design Requirements for a Core Protection Calculator, 00000-ICE-3208, Revision 08, Westinghouse Electric Company LLC
37. Functional Design Requirement for a Control Element Assembly Calculator, Requirements No. 00000-ICE-3234, Revision 6, Westinghouse Electric Company LLC
38. Control Room Heat Load (Normal and Station Blackout), ECE89-002, Revision 8, Entergy Operations, Inc.
39. Failure Modes and Effects Analysis for the Core Protection Calculator System, WNA-AR-00909-CWTR3, Revision 1, Westinghouse Electric Company LLC.
40. 73.55 Fleet Strategy Implementation Fiber Optic Cable Common-Procurement Specification, SPEC-10-00001-MULTI, Rev. 0, Entergy Operations, Inc.

REFERENCES (cont.)

41. Waterford 3 CPCS Reliability Block Diagram Analysis, WNA-AR-00913-CWTR3, Revision 0, Westinghouse Electric Company LLC.
42. Vogtle Electric Generation Plant Units 3 and 4 – Request for Licenses Amendment Regarding Protection and Safety Monitoring System Surveillance Requirement Reduction Technical Specification Revision (LAR 19-001), ML19084A309, Southern Nuclear Operating Company
43. Protection and Safety Monitoring System Technical Specification Surveillance Requirement Elimination, SV0-PMS-AR-001, Rev. 1, Westinghouse Electric Company, LLC.
44. Not used.
45. Final Quality Assessment and Justification Report, MOD 97-7771, Rev. 6, Westinghouse Electric Company, LLC.
46. Qualification of Category A I&C Self supervision and test functions FMEA, MOD 97-3184, Rev. 3, Westinghouse Electric Company, LLC.
47. AC160 Product Specification for AP1000 PMS, GBRA095801, Rev. E, Westinghouse Electric Germany, GmbH.
48. Evidence of Documentation for AC160 Platform Diagnostics, GIC-SSP-FSD-19-005, Rev. 1, Westinghouse Electric Company LLC.
49. Publicly Available – Vogtle Electric Generating Plant Units 3 and 4 Safety Evaluation (LAR 19-001), ML19297D159, United States Nuclear Regulatory Commission.
50. Description of Function HW - BIM2-2 ASIC, 3BSC140054D0060, Rev. 0, ABB Process Automation Corporation.
51. AI688M Analog Input 16Ch. (Main-board), 3BSE052212D0002, Rev. D, ABB Process Automation Corporation.
52. Description of Function HW CI627, 3BSE009799D0060, Rev. 0, ABB Process Automation Corporation.
53. Ceramic Capacitor Aging Made Simple, Johanson Dielectrics Inc., 2012
54. Software Hazard Analysis for the Core Protection Calculator System Upgrade Project, WNA-AR-00861-CWTR3, Rev. 0, Westinghouse Electric Company LLC.
55. Core Protection Calculator System Response Time Calculation, WNA-CN-00572-CWTR3, Revision 0, Westinghouse Electric Company LLC.
56. Reliability and Availability Analysis Methods, WNA-IG-00064-GEN, Rev. 3, Westinghouse Electric Company LLC.
57. Reliability Data Sheet, Advant Controller 160 Including S600 I/O, GKWF310708, Rev. 0, ABB Power Plant Control.
58. 2982786 PLC-OSC- 24DC/ 24DC/ 5/ACT Datasheet, Phoenix Contact.
59. Core Protection Calculator (CPC) System Input Processing Uncertainty Calculation for Waterford Unit 3, WNA-CN-00566-CWTR3, Revision 0, Westinghouse Electric Company LLC.
60. Engineering Change Process, Entergy Quality Related Procedure (includes instructions for IP-ENG-001, Standard Design Process), EN-DC-115, Rev. 27, Entergy Operations, Inc.
61. Post Modification Testing and Special Instructions, Entergy Quality Related Procedure, EN-DC-117, Rev. 14, Entergy Operations, Inc.

11 BIBLIOGRAPHY

1. Waterford-3 Comprehensive Checklist for Non-LOCA Transient Analysis with Revised CEA Drop Time Curve, CN-TDA-09-7, Revision 3, Westinghouse Electric Company LLC
2. WF3 Cycle 23 Core Operating Limits Report (per Section 1.1 of Reference 33)
3. WF3 Technical Requirements Manual, “Docket 50-382, Amendment 145 (per Section 1 of Reference 33)
4. Waterford-3 CPC and CEAC Data Base Document, 9270-ICE-3212, Revision 01, Westinghouse Electric Company LLC
5. Waterford-3 CPC Response Time Calculation, IC-03-040, Revision 05, Westinghouse Electric Company LLC
6. Functional Design Requirements for a Core Protection Calculator, 00000-ICE 3208, Revision 8, Westinghouse Electric Company LLC
7. Functional Design Requirements for a Control Element Assembly Calculator (CEAC), 00000-ICE 3234, Revision 6, Westinghouse Electric Company LLC
8. Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, “Common Qualified Platform” and Appendices 1, 2, 3, and 4, Rev. 01 (TAC No. MA1677), ML003740165, United States Nuclear Regulatory Commission.
9. Design and Life Cycle Evaluation Report on Previously-Developed Software in ABB AC160, I/O Modules and Tool, GKWF700777, Rev. 2, ABB Utility Automation, GmbH

APPENDIX A

WF3 FSAR MARKUPS

WSES-FSAR-UNIT-3

Insert: within each CPCS channel

Four independent core protection calculators (CPCS) are provided, one in each protection channel. Calculation of departure from nucleate boiling ratio (DNBR) and local power density is performed in each CPC, utilizing the input signals described below. The DNBR and local power density so calculated are compared with trip set-points for initiation of a low DNBR trip and the high local power density trip.

Replace with: Each CPC system channel

Two independent CEA calculators are provided as part of the CPC System to calculate individual CEA deviations from the position of the other CEAs in their subgroup.

Justification for deletion: CEAC CEA group deviations are now provided to the CPC via HSL within a channel

Each CPC receives the following inputs: core inlet and outlet temperature, pressurizer pressure, reactor coolant pump speed, excore nuclear instrumentation flux power (each subchannel from the safety channel), selected CEA position, ~~and CEA subgroup deviation from the CEA calculators~~. Input signals are conditioned and processed.

Insert: and

Additional temperature, pressure, flow and liquid level monitoring is provided, as required, to keep the operating personnel informed of plant conditions, and to provide information from which plant processes can be evaluated and/or regulated.

The plant gaseous and liquid effluents are monitored for radioactivity. Activity levels are displayed and off-normal values are annunciated. Area monitoring stations are provided to measure radioactivity at selected locations in the plant.

See Chapter 7 for further information.

1.2.2.4 Electric Power

Waterford 3 generates power at a nominal 25 kV. This is transformed up to 230 kV and enters the 230 kV switchyard through two overhead tie lines. Two start-up transformers, each supplied from one of the two overhead tie lines provide power for start-up, shutdown, reserve full load operation and preferred emergency shutdown service to the 6.9 kV and 4.16 kV auxiliary system buses. While the unit is in normal operation, these buses are normally supplied by two auxiliary transformers connected to the main generator 25 kV bus.

Redundant sources of offsite power are provided by seven separate transmission lines connected to the 230 kV switchyard. Any one of these lines together with either of the tie lines and its start-up transformer is capable of supplying the total emergency power requirements to ensure that no single failure of any active component can prevent a safe and orderly shutdown.

Redundant sources of onsite power are provided by two diesel generators, either of which is capable of supplying sufficient engineered safety features (ESF) loads to ensure safe shutdown and maintenance in a safe condition in the event of complete loss of offsite power.

The ESF redundant systems have been electrically and physically designed and segregated so that a single electrical fault or a single credible event will not cause loss of power to both sets of redundant essential electrical components.

See Chapter 8 for further information.

→(DRN 02-85, R11-A; 04-1444, R13-B)
Start of historical information.
←(DRN 04-1444, R13-B)

←(DRN 02-85, R11-A)

WSES-FSAR-UNIT 3

TABLE 1.7-1 (Sheet 47 of 47)

Revision 13-B (01/05)

ELECTRICAL, INSTRUMENTATION AND CONTROL DRAWINGS

<u>DRAWING & REVISION NUMBER</u>		<u>REVISION</u>	<u>PREPARED</u>	<u>PROPRIETARY</u>	<u>TITLE</u>
EBASCO	OTHERS	DATE	BY	INFO.	
5061	103-524312 Open		SEL		Block Diagram
5059	142-100067 Open		SEL		System Layout - Core Protection System (5 Shts.)
5062	144-100556 Open		SEL		Interconnection Diagram - Core Protection
5063	144-100556 Open		SEL		Calculator System (2 Shts.)
5064	149-100316	Open	SEL		Cable Assembly - External Operators
5066	149-100317	Open	SEL		Module Signal (5 Shts.)
5067	149-100318	Open	SEL		Cable Assembly - External CRT Signal
5068	149-100319	Open	SEL		CPC "A" Analog Inputs (19 Shts.)
5069	149-100320	Open	SEL		CPC "B" Analog Inputs (20 Shts.)
5070	149-100321	Open	SEL		CPC "C" Analog Inputs
					CPC "D" Analog Inputs (19 Shts.)
					CEAC "1" Analog Inputs (16 Shts.)
					CEAC "2" Analog Inputs

→(DRN 04-1444, R13-B)
End of historical information.
←(DRN 04-1444, R13-B)

To be updated with drawings reflecting the
Common Q CPCS architecture.

WSES-FSAR-UNIT-3

The DNBR limit includes the following allowances:

→ (EC-13881, R304)

1. NRC specified allowances for TORC code uncertainty.
2. Rod bow penalty as discussed in Section 4.3A.4.2 below.

→ (EC-9533, R302)

← (EC-9533, R302; EC-13881, R304)

4.3A.4.2 Effects Of Fuel Rod Bowing on DNBR Margin

→ (DRN 03-2058, R14; EC-9533, R302; EC-13881, R304)

Effects of fuel rod bowing on DNBR margin have been incorporated in the safety and setpoint analyses in the manner discussed in Reference 19. The penalty used for this analysis is valid for bundle burnups up to 33,000 MWD/T. This penalty is included in the 1.24 DNBR limit, applicable to both the ABB-NV and WSSV-T correlations.

← (EC-9533, R302; EC-13881, R304)

For assemblies with burnup greater than 33,000 MWD/T sufficient available margin exists to offset rod bow penalties due to the lower radial power peaks in these higher burnup batches. Hence the rod bow penalty based upon Reference 19 for 33,000 MWD/T is applicable for all assembly burnups expected.

← (DRN 03-2058, R14)

4.3A.5 REACTOR PROTECTION AND MONITORING

4.3A.5.1 Introduction

The Core Protection Calculator (CPC) System is designed to provide the low DNBR and high Local Power Density (LPD) trips to (1) ensure 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 System in limiting the consequences of certain postulated accidents. The CPCS is further described in subsection 7.2.1.1.2.5.

The CPC/CEAC in conjunction with the balance of the Reactor Protection System (RPS) must be capable of providing protection for certain specified design basis events, provided that at the initiation of these occurrences the Nuclear Steam Supply System, its sub-systems, components and parameters are maintained within operating limits and Limiting Conditions for Operation (LCOs).

4.3A.5.2 CPCS Software Modifications

The CPC/CEAC software for Waterford 3 was modified prior to Cycle 2. This modification implemented the CPC Improvement Program, including algorithms and plant specific data base changes, changes to the list of addressable constants and implementation of the Reload Data Block (RDB).

The Waterford 3 CPC/CEAC algorithms are the same as those implemented at SONGS-2 and -3 (Cycle 3) and at ANO-2 (Cycle 6) and described in References 21 and 22. The revised list of addressable constants are defined in Reference 23. The software modifications are described in References 23, 24, 25, and 29. All changes were implemented per the established software change procedures, References 26 and 27.

After Cycle x, the CPC system was replaced with one based on the Common Q Platform (see References 47 and 48). This modification changed the CPC system architecture such that now each CPC system channel has a CEAC 1 and CEAC 2. The same algorithms are used with the exception of the cycle times to accommodate the new architecture. The software was developed in accordance with Reference 49. The replacement is the same as that installed at the Palo Verde Nuclear Generating Station Units 1 - 3.

WSES-FSAR-UNIT-3

33. CEN-372-P-A, "Fuel Rod Maximum Allowable Gas Pressure," May 1990
34. CEN-386-P-A, "Verification of the Acceptability of a 1-Pin Burnup Limit of 60 MWD/Kg for Combustion Engineering 16 x 16 PWR Fuel," August 1992.
- (EC-13881, R304)
35. WCAP-16072-P-A, "Implementation of Zirconium Diboride Burnable Absorber Coatings in CE Nuclear Power Fuel Assembly Designs," August 2004.
- ←(EC-13881, R304)
- (DRN 03-270, R12-B)
36. ENEAD-01-P, Revision 0, "Qualification of Reactor Physics Methods for the Pressurized Water Reactors of the Entergy System," December 1993.
- ←(DRN 03-270, R12-B)
- (EC-9533, R302)
37. WCAP-11596-P-A, "Qualification of the PHOENIX-P/ANC Nuclear Design System for Pressurized Water Reactor Cores," June 1988
38. WCAP-10965-P-A, "ANC: A Westinghouse Advanced Nodal Computer Code," September 1986
39. WCAP-10965-P-A Addendum 1, "ANC: A Westinghouse Advanced Nodal Computer Code: Enhancements to ANC Rod Power Recovery," April 1989
40. WCAP-16045-P-A, "Qualification of the Two-Dimensional Transport Code PARAGON," August 2004
41. WCAP-16523-P-A, Rev. 0. "Westinghouse Correlations WSSV and WSSV-T for Predicting Critical Heat Flux in Rod Bundles with Side-Supported Mixing Vanes", August 2007.
42. CENPD-153-P, Revision 1-P-A, "Evaluation of Uncertainty in the Nuclear Power Peaking Measured by the Self-Powered, Fixed In-Core Detector System", May 1980.
- ←(EC-9533, R302)
- (EC-13881, R304, LBDCR 14-008, R038)
43. WCAP-16500-P-A, "CE 16x16 Next Generation Fuel Core Reference Report", August 2007.
44. WCAP-12610-P-A and CENPD-404-P-A Addendum 1-A, "Optimized ZIRLO™", July 2006.
45. CENPD-404-P-A, "Implementation of ZIRLO™ Material Cladding in CE Nuclear Power Fuel Assembly Designs," November 2001.
46. CENPD-387-P-A, "ABB Critical Heat Flux Correlations for PWR Fuel," May 2000.
- ←(EC-13881, R304, LBDCR 14-008, R308)
47. WCAP-16097-P-A, "Common Qualified Platform Topical Report", December 2019
48. WCAP-16097-P-A Appendix 2, "Common Qualified Platform Core Protection Calculator System", May 2013
49. WCAP-16096-P-A, "Software Program Manual for Common Q™ Systems", November 2018

WSES-FSAR-UNIT-3

- | | | |
|----|---|------|
| f) | Steam Bypass Control | (CE) |
| g) | Main Turbine Control | (E) |
| h) | Core Operating Limit Supervisory System | (CE) |
| i) | Plant Monitoring Computer | (E) |
| i) | Incore Instrumentation | (CE) |
| k) | Excore Neutron Flux Monitoring System | (CE) |
| l) | Reactor Power Cutback System | (CE) |
| m) | Plant Safety Parameter Display System | (E) |

A detailed description of these systems is given in Section 7.7.

7.1.1.7 Comparison

The Plant Protection System was designed and built by Combustion Engineering Inc. The system is functionally identical to the system provided for the ANO Unit 2 plant (AEC Docket No. 50-368) with the following exception;

→(EC-2800, R307)
 The number of CEAs is changed to 87. The corresponding change in the number of CEAs and CEA subgroups has resulted in minor changes in the CEA and CPC software for deviation logic.
 ←(EC-2800, R307)

The ESF Systems that are not part of the NSSS are similar in design to the ESF Systems used on the St Lucie #1 Nuclear Power Plant (Docket No. 50-335). In some systems specific instrument channels have been added or deleted depending on specific system requirements.

The major differences of these systems are described below:

- a) The Waterford 3 Containment cooling System uses two speed fans.
- b) The Waterford 3 Emergency Feedwater System is automatically initiated and has a different valving configuration.
- c) The Waterford 3 Shield Building Ventilation System uses no outside air, has somewhat different valving configuration and uses different set points and control although the functions of the systems are alike.

7.1.1.8 ATWS MITIGATING SYSTEMS

For detail description of ATWS Mitigating Systems (DRT, DEFAS, and DTTS) refer to Section 7.8.

WSES-FSAR-UNIT-3

protective parameters are measured with four independent process instrument channels. A detailed listing of the parameters measured is contained in section 7.5.

A typical protective channel, as shown on Figure 7.2-1, consists of a sensor and transmitter, instrument power supply and current loop resistors, indicating meter and/or recorder, and trip bistable/calculator inputs. The piping, wiring, and components of each channel are physically separated from that of other like protective channels to provide independence. The output of each process parameter transmitter is a current loop. Signal isolation is provided for plant monitoring computer inputs. Each channel is powered from a separate uninterrupted ac bus.

7.2.1.1.2.2 CEA Position Measurements

The position of each CEA is an input to the CPC/CEA calculator portion of the RPS. These positions are measured by means of two redundant reed switch assemblies on each CEA (Figure 7.2-2).

Each reed switch assembly consists of a series of magnetically actuated reed switches spaced at intervals along the CEA housing and wired with precision resistors in a voltage divider network. A magnet attached to the CEA extension actuates the adjacent reed switches, causing voltages proportional to position to be transmitted for each assembly. The two assemblies and wiring are physically and electrically separated from each other.

As is the case for the process instrument channels above, the wiring and components of each channel are physically and electrically separated from that of other like protective channels. Each channel is powered from a separate vital ac bus.

Each CEA is instrumented by redundant CEA reed switch position transmitters. One set of the redundant signals for all CEAs is monitored by one CEA calculator and the other set of signals by the redundant CEA calculator.

The CEAs are arranged into control groups that are controlled as subgroups of CEAS. The subgroups are symmetric about the core center. The subgroups are required to move together as a control group and should always indicate the same CEA group position.

Each CEA calculator monitors the position of all CEAs within each control subgroup. Should a CEA deviate from its subgroup position, the CEA calculators will monitor the event, sound an annunciator, and transmit an appropriate deviation "penalty" factor to the CPCs. This will cause trip margins to be reduced. This assures conservative operation of the RPS, as any credible failure of a CEA reed switch assembly will result in an immediate operator alarm and conservative RPS trip margins.

→ (DRN 01-1104; 02-1476)

The CEA calculators display the position of each regulating and shutdown CEA to the operator in a bar chart format on a cathode ray tube (CRT). Optical isolation is utilized at each CEA calculator output to the CRT display generator. The operator has the capability to select either CEA calculator for display.

← (DRN 01-1104; 02-1476)

Replace with: flat panel display

Replace with: between the CPC system output and the CEAPD

WSES-FSAR-UNIT-3

Physical and electrical separation of the preamplifiers and cabling between channels is provided.

The excore neutron flux monitoring safety channels are designed, manufactured, tested, and installed to the identical design, quality assurance and testing criteria as the remainder of the signal generating and processing equipment for the signals utilized by the RPS.

7.2.1.1.2.4 Reactor Coolant Flow Measurements

→(DRN 00-531, R11-A)

The speed of each reactor coolant pump motor is measured to provide a basis for calculation of reactor coolant flow through each pump. Two metal discs each with 44 uniformly spaced slots about its periphery are scanned by two proximity devices. The metal discs are attached to the pump motor shaft, one to the upper portion and one to the lower portion. Each scanning device produces a voltage pulse signal, the frequency of which is proportional to pump speed.

←(DRN 00-531, R11-A)

These signals are transmitted to the CPCs which compute the flowrate. Adequate separation between probes is provided.

The reactor coolant pump speed measurements are calibrated based on the average time between successive pulses at a given value of pump speed.

→(DRN 03-2081, R14)

The volumetric flowrates calculated for each pump are summed to give a vessel flow. The vessel flow is corrected for core bypass and density and the result is the core mass flowrate. At design, full-power conditions the sensitivity of reactor coolant density to changes in reactor coolant inlet temperature and RCS pressure is typically $-0.06935 \text{ lb}_m/\text{ft}^3 - \text{F}$ and $0.0006689 \text{ lb}/\text{ft}^3 - \text{psi}$, respectively. At any given reactor coolant volumetric flowrate, the percentage change in mass flowrate is equal to the percentage change in density from a given base density. Thus, for a design full power reactor coolant density, the above sensitivities are equivalent to a decrease of 0.15 percent in mass flowrate per degree increase in inlet temperature, and an increase of 0.0015 percent in mass flowrate per psi increase in primary coolant system pressure. The above sensitivities are used with the design, full-power mass flowrate in a manner that assures conservative calculated mass flowrate relative to the actual mass flowrate.

←(DRN 03-2081, R14)

The reactor coolant pump speed measurement system is designed, manufactured, tested, and installed to the identical design, quality assurance, and testing criteria as the remainder of the signal generation and processing equipment for signals utilized by the RPS.

7.2.1.1.2.5 Core Protection Calculators

Four independent CPCs are provided, one in each protection channel. Calculation of DNBR and local power density is performed in each CPC, utilizing the input signals described below. The DNBR and local power density so calculated are compared with trip setpoints for initiation of a low DNBR trip (Subsection 7.2.1.1.1.4) and the high local power density trip (Subsection 7.2.1.1.1.3).

Two independent CEA calculators are provided as part of the CPC system to calculate individual CEA deviations from the position of the other CEAs in their subgroup.

As shown in Figure 7.2-6, each CPC receives the following inputs: core inlet and outlet temperature, pressurizer pressure, reactor coolant pump speed, excore nuclear

Insert: in each CPC channel

WSES-FSAR-UNIT-3

f) CEA withdrawal prohibit on DNBR or local power density pretrip or CEA misoperation.

g) ~~Hot pin axial shape index (to control board indication)~~

Replace with: its respective CPC system channel

Replace with: is

Each calculator is mounted in the auxiliary protective cabinet with an operator's display and control module located on the main control board. From the four modules an operator can monitor all calculators, including specific inputs or calculated functions. The operators module ~~for channels B and C~~ are able to access the CEA calculators in ~~these channels~~.

Replace with: each CPC system channel

→
The system utilizes data links from ~~the CEA calculators and the CPCs~~ to the Plant Monitoring Computer. Each link is electrically isolated from the others and functions independently of the others. The Plant Monitoring Computer provides a backup monitoring capability in addition to the plant operating personnel by providing periodic comparisons of sensor channel inputs and checking of calculated results of the Core Protection Calculators.

Replace with: System

←
→
Failure of the Plant Monitoring Computer will in no way affect the operation of ~~the Core Protection Calculators~~. All data and control lines for each data link are optically isolated to assure that no failures at the Plant Monitoring Computer will affect the Core Protection ~~Calculators or the CEA Calculators~~. These optically isolated data links are designed such that open circuits, short circuits, or the application of the highest credible potential to the isolator output will not affect performing its intended function. Further, all data transfers are initiated by the Core Protection Calculators and data lines allow only one way data transfer from the Core Protection Calculators to the Plant Monitoring Computer.

Replace with: System

←
→
Data transmission is controlled by the CPC ~~Control Processing Unit and the resident programs in memory only~~ and is in no way dependent upon the status of the plant monitoring computer.

←
→
The optical link allows unidirectional data transmission to the plant monitoring computer. This feature, combined with the inherent isolation of the optical link, prevents the plant monitoring computer from affecting calculator operation.

←
→
No credit is taken for the operation of the Plant Monitoring Computer in determining the reliability of the Core Protection Calculators or in determination of the required interval for periodic testing.

7.2.1.1.2.6 Trip Generation

Except for the CPCs, and reactor trip on turbine trip, signals from the trip parameter process measurement loops are sent to voltage comparator circuits (bistables) where the input signals are compared to setpoint trip values. Whenever a channel trip parameter reaches the trip value, the channel bistable deenergizes the bistable output. The bistable output relay deenergizes trip relays. Outputs of the trip relays are in the trip logic (refer to subsection 7.2.1.1.3).

The trip bistable setpoints are adjustable from the PPS cabinet. Access is limited, however, by means of a key-operated cover and administratively controlled by Technical Specifications. In addition, each PPS door (front and rear) is provided with a key lock.

WSES-FSAR-UNIT-3

availability of system input sensors and all devices used to derive the final system output signal.

Automatic On-Line Testing

The automatic on-line testing consists of ~~three separate checks~~: (1) internal self-checking of the input data, (2) internal self-checking of the calculator and (3) ~~an external~~ watchdog timer that monitors the execution of the cyclic scheduling mechanism. Although failures in the on-line system are expected infrequently, the automatic on-line testing is provided to assure high continuous system reliability beyond that provided in typical analog calculated trips.

The protection algorithms will check the reasonability of input sensor data against predetermined maximum and minimum values. The CEA Calculator checks raw CEA position data against high and low values of +10 volts dc and +5 volts dc. Raw data which reads between 0 - 5 or 10 - 15 volts dc is deemed unreasonable. If a sensor is found to be out-of-range, the affected calculator will generate the proper annunciation signal.

To provide a check on system software and to detect time frame overruns, ~~an external "watchdog timer" is installed as part of the Data Input/Output Subsystem.~~

Add, "included along with other internal diagnostics."

The watchdog timer ~~will light the CPC or CEAC failure light at the Operator's Module directly.~~

Replace with, "timeout in the CPC or CEAC processor module will cause the CPC or CEAC FAIL indicator to turn red in the Operator's Module. In addition, a watchdog timer timeout in the CPC processor module will initiate a CPC channel trip."

For all other failures detected during automatic on-line testing, the affected calculator ~~will set its outputs in the fail safe state, such as "trip" for a CPC. If recovery from the failure is possible, the system will maintain its outputs in the safe state and execute Auto Restart, followed by initialization, followed by normal operation.~~

Replace with, "could possibly halt generating either a CPC or CEAC FAIL annunciation or channel trouble indication if the failure is detected in other processors in the CPC channel."

Further on-line testing capability is provided by continuous status indication and information read out from each Core Protection Calculator. Continuous displays of the following information is provided to the operator:

- a) DNBR margin
- b) Local power density margin
- c) Calibrated neutron flux power

Cross checking of the four channel displays can be made to assure the integrity of the calculator. The majority of the calculator failures will result in anomalous indications from the failed channel that can be readily detected by the operator during cross checking.

In addition, each protection channel is equipped with an Operator's Module which provides another level of assurance of the functional integrity of the calculator channels.

Periodic Testing

Add, "for those functions not covered by automatic testing."

The DNBR/LPD Calculator System is periodically and routinely tested to verify its operability. ~~A complete~~ channel can be individually tested without initiating a reactor trip, and without violating the single failure criterion. The system can be checked ~~from~~

WSES-FSAR-UNIT-3

~~the sensor signal~~ through the bistable contacts for low DNBR and high local power density in the Plant Protection System. Overlap in the checking and testing is provided to assure that the entire channel is functional.

The minimum frequencies for checks, calibration, and testing of the Core Protection Calculator system have been included in the Technical Specifications.

~~Periodic testing of the DNBR/LPD Calculator system is divided into two major categories, (1) on-line system tests and (2) off-line performance diagnostic tests. Off-line testing is further subdivided into two categories, performance testing and diagnostic testing. Performance testing is used to check the numerical accuracy of the calculations. Diagnostic testing is used as an aid to troubleshooting whenever the performance tests or the on-line tests (interchannel comparisons) indicate the presence of a failure. Permanent mass storage units will be used for storage of the test programs.~~

On-line System Test

The ~~on-line portion of the~~ periodic testing consists of comparisons of like parameters among the four protective channels. Comparisons are made using the digital displays on the Operator's Module and the ~~analog~~ meters on the control board. Comparisons of like analog and digital inputs give assurance that the analog and digital multiplexers and the A/D converters are functioning properly. These comparisons also give assurance that data are being properly entered into and retrieved from the data base. Comparisons of intermediate and final calculated parameters verify the performance of the protection algorithms and the ~~analog~~ display meters on the control board.

~~Calibration of the A/D converters is checked by displaying the reference voltage supplies which are connected to each calculator.~~

Off-line Performance Test

Periodic testing also tests the functionality of the DNBR and LPD contact outputs to the PPS, and the functionality of the Operating Bypass relay.

Before off-line testing is initiated, the channel to be tested is bypassed at the Plant Protection System and the trip logic is changed to two-out-of-three for the DNBR and local power density trips. Interlocks are incorporated in the Plant Protection System to prevent bypassing more than one channel at a time. To initiate off-line testing a key is required and only one key is provided. This ensures that only one channel can be placed in the test mode at a time.

~~The performance test uses the calculator data base to verify numerical accuracy of the calculations. The data base is divided into three areas, namely, raw input data, filtered input data and calculated values. The raw data area contains the last samples of raw analog and digital data. The filtered data area contains averaged input data, filtered input data, past samples of input data needed for dynamic compensation, and dynamically compensated data. The calculated values area contains intermediate and final calculated values and calibration constants which are updated periodically.~~

~~During performance testing, the permanent mass storage unit is used to load test inputs directly into the data base. For each set of test inputs, the expected calculated results are also loaded and compared with the values calculated by the protection algorithms. If agreement is achieved, the test program prints the expected results and the actual results on the Teletype and proceeds to the next set of test data. If agreement is not achieved, the test program halts at that point unless restarted by the operator. Dynamic effects in~~

WSES-FSAR-UNIT-3

~~the calculations are tested by loading the filtered data area of the data base with test values representing past values of time varying inputs.~~

~~From the standpoint of the calculator software structure, the performance tests are virtually identical to the on-line functions. Only two differences exist from the normal functions of the calculators. First, the calculator outputs are in a fail safe condition for the duration of the tests, and second, the algorithms use data derived from the permanent mass storage unit instead of the Data Input/Output subsystem. The algorithms themselves, however, do not recognize the data source or that they are executing in the test mode.~~

~~As a final check, the individual instructions in protected memory are compared with an image of the instructions stored on the permanent mass storage unit to ensure the integrity and demonstrate the "reliability" of the protection algorithms during the life span of the DNBR/LPD Calculator System.~~

Off-Line Diagnostic Tests

~~After a given failure is detected by a performance test, on-line test, or on-line diagnostic, hardware diagnostic programs are provided to aid in locating (to the module level) and correcting malfunctions.~~

7.2.1.1.9.4 Logic Matrix Test

This test is carried out to verify power operation of the six two-out-of-four logic matrices, any of which will initiate a bonafide system trip for any possible two-out-of-four trip condition from the signal inputs from each measurement channel.

Only the matrix relays in one of the six logic matrix test modules can be held in the energized position during tests. If, for example, the AB logic matrix hold pushbutton is held depressed, actuation of the other matrix hold pushbuttons will have no effect upon their respective logic matrices.

Actuation of the pushbutton will apply a test voltage to the test system hold coils of the selected four double coil matrix relays. This voltage will provide the power necessary to hold the relays in their energized position when deactuation of the bistable trip relay contacts in the matrix ladder being tested causes deenergization of the primary matrix relay coils.

The logic matrix to be tested is selected using the system channel trip select switch. Then while holding the matrix hold pushbutton in its actuated position, rotation of the channel trip select switch will release only those bistable trip relays that have operating contacts in the logic matrix under test. The channel trip select switch applies a test voltage of opposite polarity to the bistable trip relay test coils, so that the magnetic flux generated by these coils opposes that of the primary coil of the relay. The resulting flux will be zero, and the relays will release. A simplified diagram of this testing system is shown in Figure 7.2-9 using the AB matrix.

Trip action can be observed by illumination of the trip relay indicators located on the front panel and by loss of voltage to the four matrix relays, which is indicated by extinguishing indicator lights connected across each matrix relay coil. During this test, the matrix relay "hold" lights will remain on, indicating that a test

WSES-FSAR-UNIT-3

Table 7.2-5 (Sheet 3 of 119)

PLANT PROTECTION SYSTEM
FAILURE MODE AND EFFECTS ANALYSIS

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
Measurement Channel, Core Protection Calculators, Channel A (Typical), Figure 7.2-10 (cont.)							
Core Inlet Temperature Tcold (82) (cont.)	One spurious high	RTD opens network failure.	Decrease in ΔT power.	Annunciating.		Reactor trip logic for LO DNBR and HI PWR DENS is converted to 1-out-of-2.	
Reactor Coolant Pump Flow (84)	One spurious loss of transmission	Power supply or pulse amplifier failure. Mechanical damage to sensor.	Loss of data. LO DNBR channel trip possible.	Annunciating. Plant computer monitor and alarm. Trip status indication.	3-channel redundancy. (4th channel bypassed) channel in tripped mode.	Reactor trip logic for LO DNBR is converted to 1-out-of-2.	Sensor transmits pulses. Pulse rate related to flow. Operator can convert system to 1-out-of-2 trip logic for LO DNBR.
Measurement Channel, CEA Position Transmitters, Figure 7.2-10							
Non-target CEA Position (149)	Low	Shorted resistor, power supply malfunction.	Erroneous data input to one CEA calculator.	Annunciation, automatic sensor validity test. CEA deviation.	Add: in all four channels	A penalty factor is initiated in the CPC's (operating temperature margins reduced).	One CEA calculator will show CEA deviation to all CPC calculations. Possible reactor trip will occur.
	High	Shorted resistor, power supply malfunction.	Erroneous data input to one CEA calculator.	Annunciation, automatic sensor validity test. CEA deviation.	Add: in all four channels		
	Other than actual position	Shorted resistors, shorted reed switches, power supply malfunction.	Erroneous data input to one CEA calculator.	Annunciation. Automatic sensor validity test. CEA deviation.	Add: in all four channels		

WSES-FSAR-UNIT-3

Table 7.2-5 (Sheet 4 of 119)

PLANT PROTECTION SYSTEM
FAILURE MODE AND EFFECTS ANALYSIS

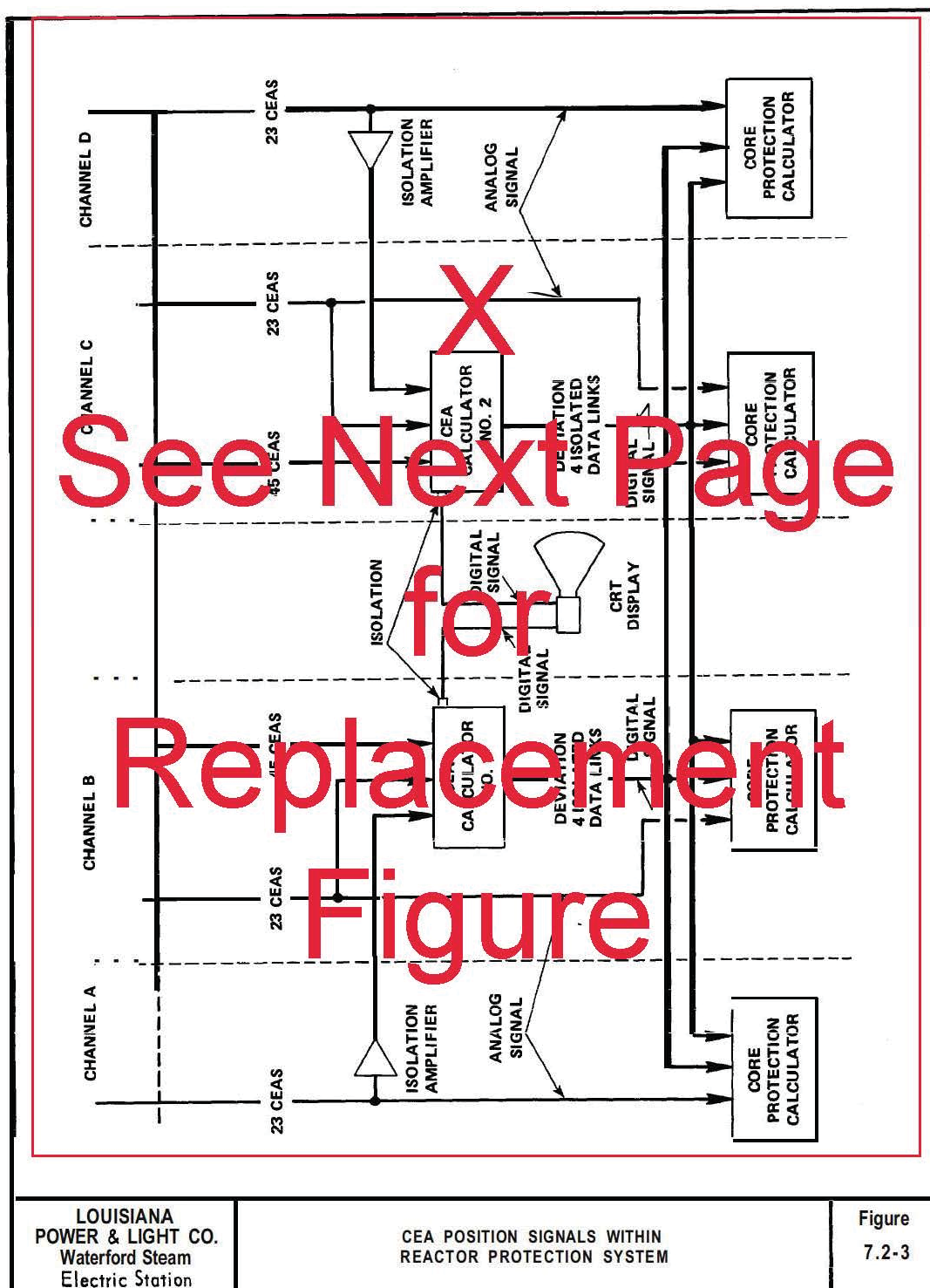
<u>Name</u>	<u>Failure Mode</u>	<u>Cause</u>	<u>Symptoms and Local Effects Including Dependent Failures</u>	<u>Method of Detection</u>	<u>Inherent Compensating Provision</u>	<u>Effect Upon PPS</u>	<u>Remarks and Other Effects</u>
Measurement Channel, CEA Position Transmitters, Figure 7.2-10 (cont.)							
Non-target CEA Position (149) (cont.)	Off scale	Broke wire, open resistor, electrical short, power supply malfunction.	Loss of data.	Annunciation, automatic sensor validity test.			
Target CEA Position (87)	Low	Shorted resistor, power supply malfunction.	Erroneous data input effects DNBR and LPD calculation.	Annunciation, automatic sensor validity test. 3-channel comparison.		Makes reactor trip logic for LO DNBR and HI PWR DENS 1-out-of-2.	Possible trip in one safety channel. Trip affected will show CEA deviation.
	High	Shorted resistor, power supply malfunction.	Erroneous data input to CPC calculator, and (one) CEA calculator.	Annunciation, automatic sensor validity test. CEA deviation.	Add: in all four channels		
	Other than actual position	Shorted resistor, shorted reed switches, power supply malfunction.	Erroneous data input to CPC's and (one) CEA calculator.	Annunciation, automatic sensor validity test. CEA deviation.	Add: in all four channels	Makes reactor trip logic	Possible trip in one safety channel. Trip affected will show CEA deviation
	Off scale	Broke wire, open resistor, electrical short, power supply malfunction.	Loss of data.	Annunciation, automatic sensor validity test. CEA deviation.			

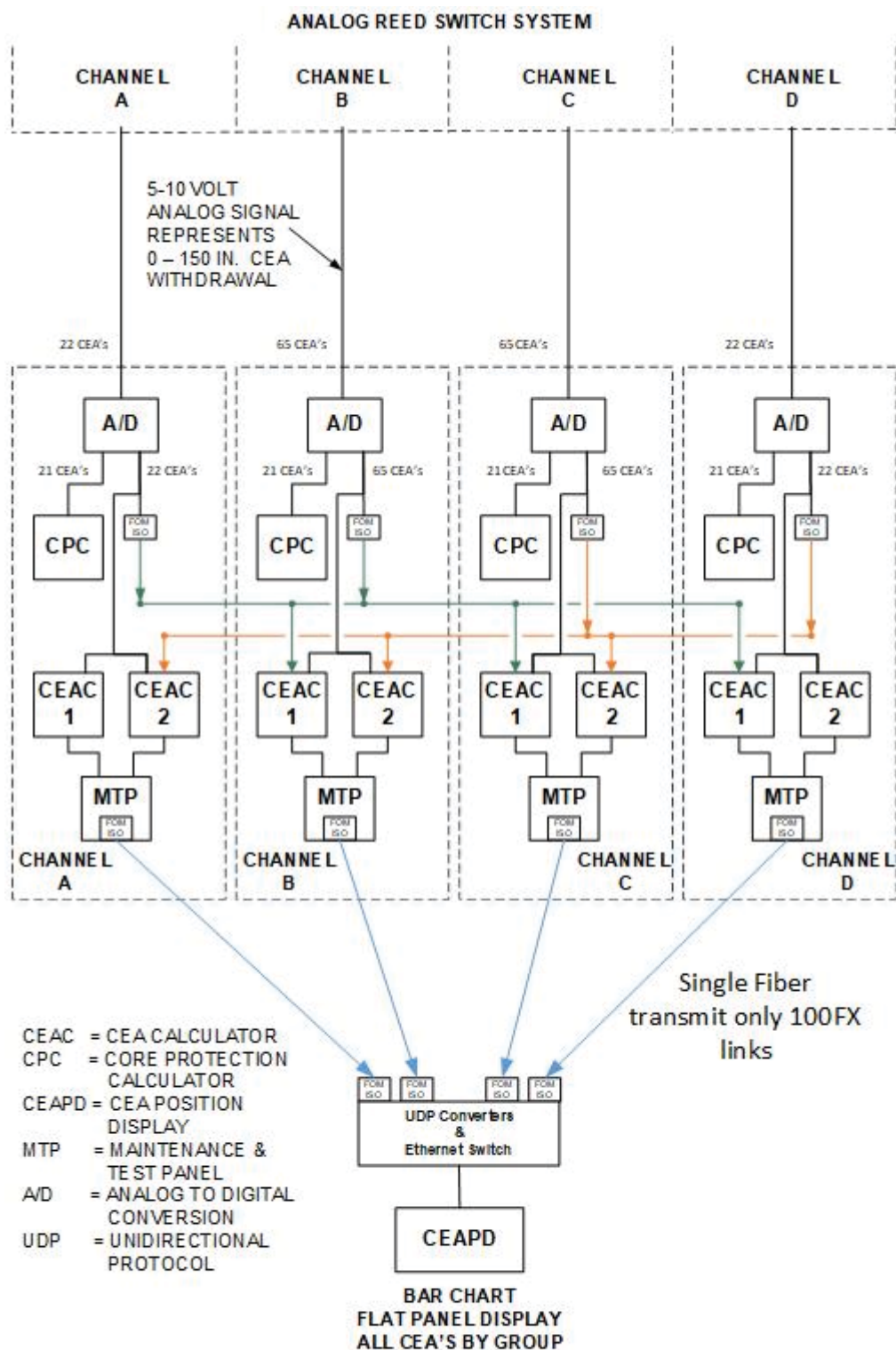
WSES-FSAR-UNIT-3

Table 7.2-5 (Sheet 5 of 119)

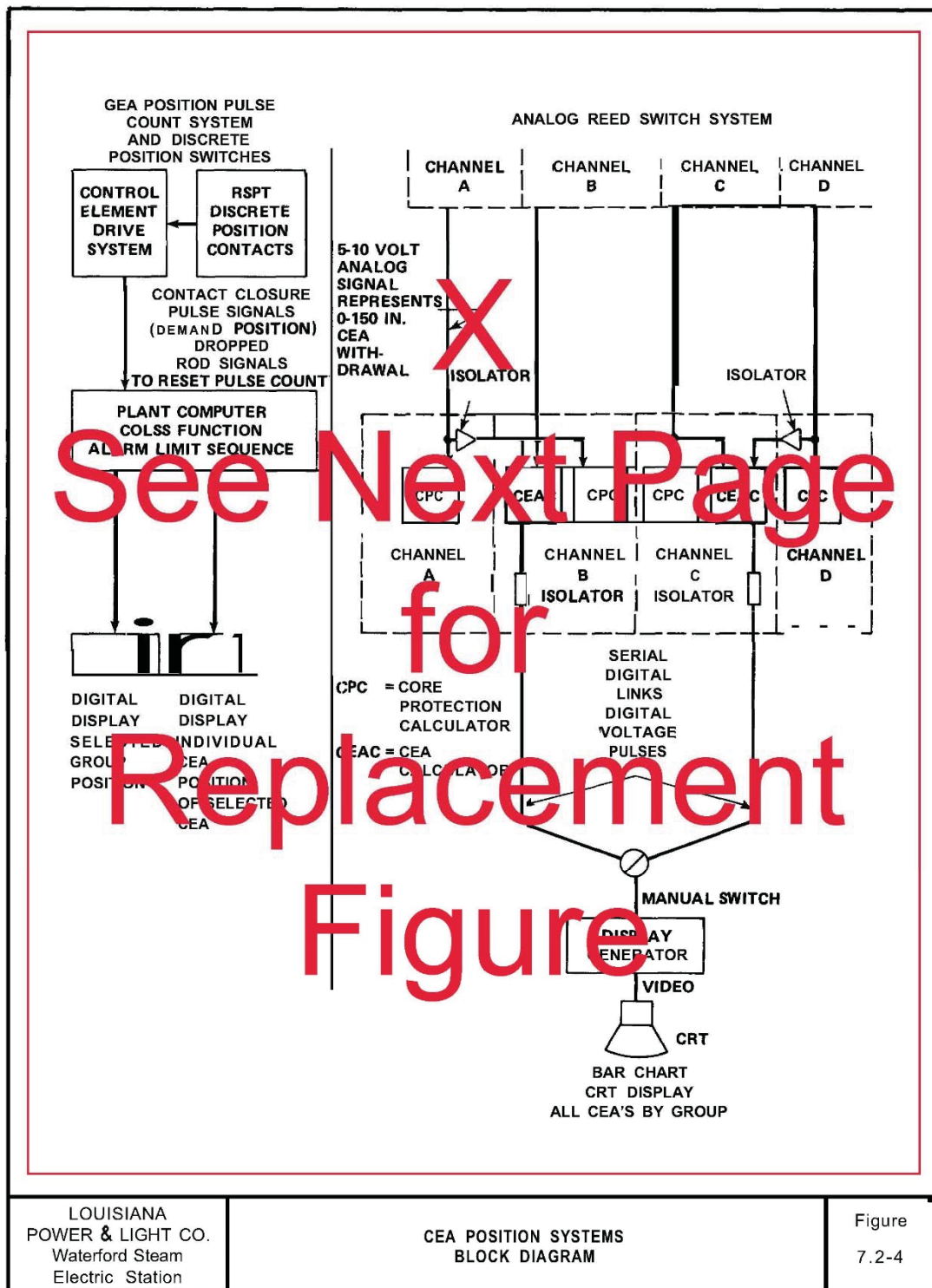
PLANT PROTECTION SYSTEM
FAILURE MODE AND EFFECTS ANALYSIS

<u>Name</u>	<u>Failure Mode</u>	<u>Cause</u>	<u>Symptoms and Local Effects Including Dependent Failures</u> Measurement Channel, Core Protection Calculator, Figure 7.2-10	<u>Method of Detection</u>	<u>Inherent Compensating Provision</u>	<u>Effect Upon PPS</u>	<u>Remarks and Other Effects</u>
Control Element Assembly Calculator (88)	No data output	Loss of ac power, input/output failure, Data link failure, Arithmetic, logic or memory failure.	Loss of CEA position display.	Annunciating alarm on CPC operator's module. Loss of CEA position display from failed CEAC watchdog timer.		Possible DNBR or LPD trip.	Add, in the one CPC channel that has the lost CEA Calculator.
	Erroneous data output	CEA position sensor failure, input/output failure, Data link failure, Arithmetic, logic or memory failure.	Erroneous calculated values. Possible DNBR or LPD trip.	Annunciating alarm on CPC operator's module. Comparison of CEA position displays.	With other channel in bypass state, CPC applies penalty factor of largest possible output from CEAC.	Possible DNBR or LPD trip.	
Core Protection Calculator (89)	Tripped	Loss of ac power, Input/output failure, Arithmetic, logic, or memory failure, Sensor failure.	Loss of control board displays.	Annunciating PPS alarm on channel trip. Three channel comparisons. Annunciating watchdog timer.	3-channel redundancy. 4th channel bypassed.	Reactor trip logic for DNBR, LPD and CWP is converted to 1-out-of-2.	Computer shuts down in orderly sequence upon loss of ac power and resumes normal operation when power is restored. System is converted to 1-out-of-2 logic for DNBR, LPD and CWP.
	Stays in untripped state	Input/output failure, Arithmetic, logic, or memory failure, Sensor failure	Erroneous calculated results.	3-channel comparisons. Annunciating watchdog timer.	3-channel redundancy. Trip channel bypass.	Reactor trip logic for DNBR, LPD and CWP is on coincidence of 2-out-of-2 remaining channels.	Computer shuts down in orderly sequence upon loss of ac power and resumes normal operation when power is restored. System must be converted by operator to 1-out-of-2 logic for DNBR,LPD,and CWP.





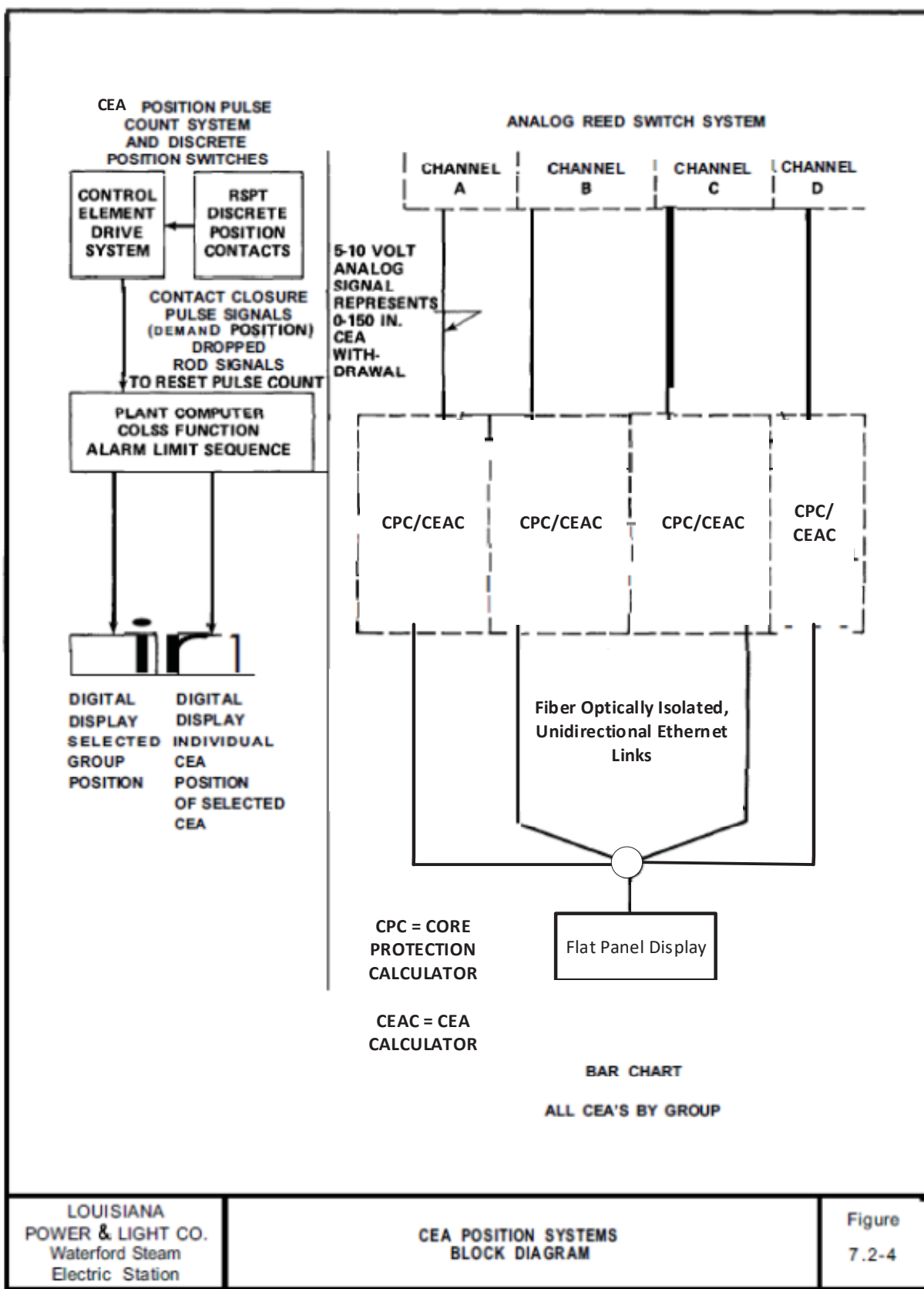
**Figure 7.2-3
CEA POSITION SIGNALS WITHIN
REACTOR PROTECTION SYSTEM**



LOUISIANA
POWER & LIGHT CO.
Waterford Steam
Electric Station

CEA POSITION SYSTEMS
BLOCK DIAGRAM

Figure
7.2-4



WSES-FSAR-UNIT-3

d) CEA Deviation Alarm

An alarm is provided to alert the operator in the event the deviation in position between the highest and lowest CEA in any group exceeds a predetermined allowable deviation.

e) Core Operating Limit Supervisory System (COLSS) Alarms

The pulse counting CEA Position Indication System provides input data to COLSS. These data are used in the COLSS power distribution calculations, and alarms are initiated in the event the affected COLSS limits are reached. The basis for the COLSS alarms and the use of the pulse count CEA position information is discussed in Section 7.7.

7.5.1.6.2

Reed Switch CEA Position Indication System

The Reed Switch CEA Position Indication System utilizes a series of magnetically actuated reed switches (Reed Switch Position Transmitters (RSPT)) to provide signals representing CEA position. Two independent reed switch position transmitters are provided for each CEA. The RSPT provides an analog position indication signal and three physically separate ~~discrete~~ reed switch position signals. The analog position indication system utilizes a series of magnetically actuated reed switches spaced at 1-1/2 in. intervals along the RSPT assembly and arranged with precision resistors in a voltage divider network. The RSPT ~~am~~ is mounted adjacent to the CEDM pressure housing, which contains the CEA extension shaft and actuating magnet. The analog output signal is proportional to the CEA position within the reactor core. The three discrete reed switch position signals are contact closure signals from three separately located reed switches. These signals are an upper electrical limit, a lower electrical limit and a rod drop contact.

CEA position information is provided to the ~~core protection calculator~~ (CPCS) directly ~~and also to the CEA calculators~~. The CEA calculators display the position of each regulating and shutdown CEA to the operator in a bar chart format on a dedicated CRT on the RTGB. The operator has the capability to select either CEA calculator for display. In addition, a backup readout is provided that can be utilized to read the output of any CEA analog reed switch position signal. The backup readout is a digital ~~meter~~ on the CPCs operator's module, from which the operator can address any analog position signal for display ~~on the digital meter~~. In addition to the displays, CEA deviation information is provided by the CEA calculators to the CPCs and a CEA deviation alarm. The CEA deviation alarm is provided to the plant annunciator system in the event a CEA calculator indicates that the difference between the highest and lowest CEA positions in a group exceeds a predetermined allowable deviation. The CEA deviation information is used in the CPCs determination of power distribution. The power distribution is then factored into the low DNBR and high local power density trip function. Pretrip alarms are initiated if the DNBR or local power density trip limits are approached. A pretrip alarm light is provided on the Plant Protection System control panel. Also, a pretrip alarm is provided to the plant annunciator system.

The three discrete CEA position switches provide signals (contact closure signals) to the Control Element Drive Mechanism Control System (CEDMCS) as shown in Figure 7.2-2. The signals are utilized to provide CEA limit indication on the RTGB and also to provide input

WSES-FSAR-UNIT-3

14.2.12.2.59.3 Test Method

- A. Verify the operation of each trip unit at the correct setpoint.
- B. Verify that the proper two-out-of-four logic will provide a trip signal to the reactor trip circuit breakers or an actuation signal to the Engineered Safety Features Actuation System (ESFAS).
- C. Verify the operation of the trip bypass features of any one channel.
- D. Verify that functional trip bypasses become automatically canceled when certain plant parameters exceed specified setpoints.
- E. Verify the proper tracking and reset functions of the setpoints for low pressurizer pressure and low steam generator pressure trips.
- F. Demonstrate the proper operation of testing equipment installed in the Plant Protection System.
- G. Verify the proper operation of the core protection calculator subsystem ~~and the control element assembly-calculator subsystem~~ through input/output tests as well as internal functioning test.
- H. Verify the proper operation of all protective devices, controls, interlocks, computer inputs, and alarms, using actual or simulated signals.
- I. Determine the Reactor Protection System trip response time by injecting signals into appropriate sensors or sensor terminals and measuring the elapsed time to achieve tripping of the reactor trip circuit breakers. Trip paths may be tested in several segments, with the total trip response time being the sum of the response times of the individual segments making up the entire trip path.

14.2.12.2.59.4 Acceptance Criteria

- A. The Plant Protection System performs as described in Sections 7.2 and 7.3.
- B. The measured Reactor Protection System trip response times are conservative with respect to the times used in the accident analysis (Chapter 15).

14.2.12.2.60 REACTOR REGULATING SYSTEM

14.2.12.2.60.1 Objective

To verify the proper operation of the Reactor Regulating System (RRS).

APPENDIX B

ELIMINATION OF SPECIFIC CPCS TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS

B.1 INTRODUCTION

B.1.1 Purpose

The purpose of this appendix is to provide the necessary analysis to justify the elimination of specific Technical Specification (TS) Surveillance Requirements (SRs) related to the CPCS. Based on NRC review, this will potentially culminate with the elimination of the need to perform specific surveillances on CPCS equipment based on the Common Q platform. This will lead to increased duration of plant operations with full CPCS redundancy and reduced operational and maintenance costs over the lifecycle of the CPCS.

The scope of this appendix is limited to Waterford-3 TS SRs that apply to the CPCS. SR candidates for elimination are outlined in Section B.1.3 of this appendix and are defined within Section 4.3.1 of the WF3 TS (Reference 20).

B.1.2 Background

TS establish requirements a nuclear facility must meet during operations. The basis for these specifications can be traced up to 10 CFR 50, “Domestic Licensing of Production and Utilization Facilities”, Section 36 “Technical Specifications”. Specifically relating to the safety system of a nuclear plant is 10 CFR 50.36(c)(ii)(A) which establishes limiting safety system settings for nuclear reactors.

To demonstrate that the CPCS is operable, which ensures that limiting conditions of operation (LCOs) are met, the TS stipulate various SRs (per 10 CFR 50.36(c)(3)). These SRs range from functional tests and calibrations, to visual inspections; and are performed on a periodic interval governed by the Waterford-3 Surveillance Frequency Control Program. The number of functions related to the CPCS coupled with the SR frequency, results in significant testing that is to be performed over the life of the CPCS.

In an effort to eliminate SRs in order to inherently increase the safety of the plant through reducing the duration of how long the CPCS is at less than full redundancy, Westinghouse has produced this appendix detailing the analyses necessary to justify the elimination of certain SRs. These SR eliminations take full advantage of the Common Q platform self-diagnostic features, something not accounted for in the Waterford-3 TS. The elimination of SRs will also reduce the burden on operations and maintenance personnel, as well as the generation and preservation of procedures related to SR testing.

The methodology to eliminate TS SRs in this appendix leverages ML19084A309, “Vogtle Electric Generation Plant Units 3 and 4 – Request for Licenses Amendment Regarding Protection and Safety Monitoring System Surveillance Requirement Reduction Technical Specification Revision (LAR 19-001)” (Reference 42). This reference received an NRC safety evaluation (ML19297D159, Reference 49)

which approves the removal of surveillance requirements related to the Vogtle 3&4 Common Q based safety system (the Protection and Safety Monitoring System).

B.1.3 Scope of Analysis

The scope of SRs analyzed within this appendix are limited to SRs that are related to the CPCS and can be eliminated within the implemented Common Q equipment (as well as the IRP, which is described in Section 3.2.8.1). This simplifies to Channel Functional Tests related to the CPCS (which include the LPD and DNBR trip functions), response time testing on the trip functions implemented within the CPCS, on top of other SRs solely applicable to the current WF3 CPCS. Specially, the WF3 TS (Reference 20) SRs subject for elimination are:

- SR 4.3.1.1 (Channel Functional Testing of the CPCS portion of the SR) which states:
“Each reactor protective instrumentation channel shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-1.”

Note: This includes TS Table 4.3-1 Note 9, which states, “The CHANNEL FUNCTIONAL TEST shall include verification that the correct values of addressable constants are installed in each OPERABLE CPC.”

- SR 4.3.1.3 (CPCS portion of the SR) which states:
“The REACTOR TRIP SYSTEM RESPONSE TIME of each reactor trip function shall be demonstrated to be within its limit in accordance with the Surveillance Frequency Control Program. Neutron detectors are exempt from response time testing. Each test shall include at least one channel per function such that all channels are tested as shown in the "Total No. of Channels" column of Table 3.3-1.”
- SR 4.3.1.4 which states that, “each CEA isolation amplifier and each optical isolator for CEA Calculator to Core Protection Calculator data transfer shall be verified in accordance with the Surveillance Frequency Control Program during the shutdown.”
- SR 4.3.1.5 which states:
“The Core Protection Calculator System and the Control Element Assembly Calculator System shall be determined OPERABLE in accordance with the Surveillance Frequency Control Program by verifying that less than three auto restarts have occurred on each calculator during the past 12 hours.”
- SR 4.3.1.6 which states:
“The Core Protection Calculator System shall be subjected to a CHANNEL FUNCTIONAL TEST to verify OPERABILITY within 12 hours of receipt of a High CPC Cabinet Temperature alarm.”

B.2 INDUSTRY STANDARDS AND REGULATORY GUIDANCE

The following regulations, industry standards, and regulatory guidance are applicable to periodic testing during normal plant operations and therefore related to this effort:

- 10 CFR 50 (specifically Section 36, Section 55a, and Appendix A)
- IEEE 279-1971
- IEEE 338-1971
- BTP 7-17

These regulations and standards are discussed in the following sections. IEEE 338-2012 is also discussed below, though not endorsed by the NRC, to provide context as to the current industry position regarding self-diagnostics and how they relate to surveillance testing.

B.2.1 10 CFR 50

10 CFR 50 contains several regulations related to manual surveillance testing requirements. These are summarized as follows:

1. 10 CFR 50, Section 36, “Technical Specifications” – 10 CFR 50.36 establishes the need for TS to verify the operability of select systems and components in the plant. The TS are derived from the analyses and evaluations included in the safety analysis report. The TS include, in part, limiting conditions for operation and SRs. When a limiting condition for operation of a nuclear reactor is not met, the licensee is required to shut down the reactor or follow any remedial action permitted by the TS until the condition can be met. SRs are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility will be within safety limits, and that the LCOs will be met.
2. 10 CFR 50, Section 55a, “Codes and Standards” – Paragraph h of this section establishes the requirement to meet IEEE 603-1991. IEEE 279-1971 is a predecessor to this standard, one that is discussed in more detail below in Section B.2.2.
3. 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants” – There are two General Design Criteria (GDC) applicable to this effort:
 - GDC 18, “Inspections and Testing of Electric Power Systems,” requires (in part) that electric power systems important to safety be designed to permit periodic testing, including periodic testing of the performance of the components of the system and the system as a whole.
 - GDC 21, “Protection System Reliability and Testability,” requires (in part) that the protection system be designed to permit its periodic testing during reactor operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.
4. 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants” – Criterion XI, “Test Control”, requires (in part) that a test program be established to ensure that all testing, including operational testing required to demonstrate that systems and components will perform satisfactorily in-service, is identified and performed in accordance with written test procedures.

B.2.2 IEEE 279

IEEE 279-1971, “IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations” requires that the protection system to have certain capabilities regarding testing. Specifically, Section 4.10 “Capability for Test and Calibration”, requires the protection system to have the capability for testing and calibration during power operations while retaining the capability of the safety systems to accomplish their safety functions. This section does not state that the protection system needs to use these features as part of a testing program, but just that they are available.

B.2.3 IEEE 338

IEEE 338-1971, "Trial-use Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Protection Systems" provides minimum requirements for the safety-related functional performance and reliability of the protection system for nuclear power generating station safety systems. Included within this set of requirements are those related to the capability for testing the protection system.

The scope of periodic testing is defined within this standard as including functional tests and checks, calibration verification, and time response measurements, as required, to verify the protection system performs to meet its defined safety function. However, what is not defined is how to determine what should be included within the manual surveillance program. Instead, the standard provides guidance for those tests within the surveillance program. Even though the self-diagnostics are not part of the surveillance program, they do support the basis of the standard (i.e., IEEE 338-1971, Section 4) in that they continuously and periodically check the system to verify operability.

IEEE 338-2012, “IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems,” Section 5.4.3, though not currently endorsed by the NRC or included in the WF3 licensing basis, does provide a basis for eliminating periodic surveillance tests as evidenced by the following statement, “Digital control/protection systems or equipment that have a mechanism to continuously verify proper digital processing are exempt from periodic testing provided:

- a) Input interfaces are tested either automatically or manually.
- b) Output interfaces are tested either automatically or manually.
- c) Any malfunction that may affect design assumptions is alarmed in the control room.”

B.2.4 BTP 7-17

NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition”, Branch Technical Position (BTP) 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” provides NRC review guidance into periodic surveillance testing and self-diagnostic features for a digital system. This BTP acknowledges the use of automatic self-testing as an appropriate method to perform periodic surveillance tests. Additionally, BTP 7-17 states, “Self-test functions should be verified during periodic functional tests.” This statement will be assessed in relation to this Appendix in the evaluation section below.

B.2.5 Evaluation/Conclusion

Although historically industry and regulatory standards have required periodic surveillance testing during normal operations for safety systems, exceptions have been allowed. Specifically:

- **IEEE 279-1971:** Requires protection systems to have the capability to test. However, the approach taken in this appendix is to not to eliminate the capability for manual testing to be performed on a protection system, but instead credit self-diagnostics in order to eliminate the need to perform SRs. The self-diagnostics being credited within the SR elimination analysis (Section B.5 of this appendix) are automatic tests that are performed within the CPCS at an interval significantly shorter than the current SR interval. These proposed Tech Spec modifications for elimination of SRs result in improved safety system availability and reduced potential for human error.
- **IEEE 338-1971:** This activity proposes the removal of several Tech Spec surveillances due to self-diagnostic test coverage. These self-diagnostics will not be part of the surveillance program, and therefore, the requirements in IEEE 338-1971 are not directly applicable. Additionally, this standard is written specifically for analog systems, resulting in guidance that does not explicitly address self-diagnostic testing features.
- **IEEE 338-2012:** Though not endorsed by the NRC, this standard provides an exception to periodic surveillance tests based on being able to continuously verify proper digital processing. This shows how the industry has adapted IEEE 338 for digital systems.
- **BTP 7-17:** Acknowledges automatic self-testing as an appropriate substitute to periodic surveillance tests. However, an important caveat is Acceptance Criterion 3 which states that “self-test functions should be verified during periodic functional tests.” It is not possible to test self-diagnostics as part of surveillance testing because it would require creating destructive faults within the I&C system, such as Random-Access Memory (RAM) errors. Therefore, this acceptance criterion is addressed as follows:
 - Software-based diagnostics are confirmed to be functional by Cyclic Redundancy Checks (CRCs) of the system software and are not subject to random failure. The CRC diagnostic is described in WCAP-16097-P-A (Reference 4). A CRC number is generated when the firmware is qualified and released. The CRC diagnostic compares the run-time calculated CRC of the system software to the qualified release CRC number and if it is different, then it is possible that a hardware failure may have impacted the operation of the firmware-based diagnostics. This will result in a CPC FAIL alarm and operator notification (See Section B.4 for more details). The NRC Safety Evaluation Report (SER) for the Common Q Topical Report states, “Any changes made to AC160 software will also affect the CRC checksum value which is continually monitored by the safety application which will activate a system alarm.” In the case of the CPCS, that system alarm is the CPCS FAIL Alarm.
 - The CRC diagnostic is monitored to be completed within the allotted cycle time (discussed in more detail in Section B.3.1.2). If it is not, then the CPC FAIL alarm will be annunciated.

[

] ^{a,c}

In summary, the elimination of SRs by crediting self-diagnostics meets the underlying NRC regulations. Although some of these standards/guidance documents assume a testing program is in place (which will continue to be the case for some items related to the CPCS), others allow for exceptions to testing given that designated criteria are met justifying the change. This appendix will demonstrate that the self-diagnostics being credited in lieu of an SR are adequate which will make some SRs unnecessary. Therefore, the intent of the standards/regulations will be met even when SRs are eliminated.

B.3 INTRODUCTION TO COMMON Q SELF-DIAGNOSTICS

B.3.1 Overview

There are two types of self-diagnostics which are used to detect faults in the CPCS. These are:

- AC160 Platform Self-Diagnostics – implemented in hardware and firmware by the equipment manufacturer (ABB).
- Application Self-Diagnostics – specific software design by Westinghouse for the CPCS application.

B.3.1.1 AC160 Platform Self-Diagnostics

The AC160 platform self-diagnostics have been designed, implemented, design tested, configuration controlled and produced under the same processes as the AC160 equipment that implements the CPCS safety functions. Westinghouse has subjected this equipment to equipment qualification testing and uses the same quality processes to commercially dedicate, assemble, and test this equipment as the other CPCS safety equipment, since most of the platform self-diagnostics are integral to the equipment that performs the safety functions. This platform software qualification was done for the Oskarshamn 1 RPS Modification (O1 MOD) Project, and summarized in MOD 97-7771, “Final Quality Assessment and Justification Report” (Reference 45). This report summarizes the methodologies and results of qualification activities for the AC160 for use as a Category A I&C system (synonymous with Class 1E in the U.S.) for the O1 MOD project. The results of this report were discussed with the NRC staff during the licensing of the Common Q platform. The NRC also reviewed this document as part of their review of LAR 19-001 for Vogtle 3&4 (Reference 42).

MOD 97-7771 (Reference 45) references MOD 97-3184, “Qualification of Category A I&C Self Supervision and Test Functions FMEA” (Reference 46). This report postulates failures of the platform self-supervision and documents their effects. Section 6 of this reference summarizes the results of self-supervision FMEA.

The platform is described in WCAP-16097-P-A (Reference 4). Section 5.4 of WCAP-16097-P-A describes system diagnostics including the passive monitoring that includes the use of self-diagnostics and the MTP/OM to monitor system operation and provide indication of detected faults. This topical report has been reviewed and approved by the NRC.

B.3.1.2 Guaranteed Completion of AC160 Self-Diagnostics

[

] ^{a,c}

[

] ^{a,c}

B.3.1.3 Application Self-Diagnostics

The application self-diagnostics of the CPCS will be developed, implemented, and subjected to Independent Verification & Validation (IV&V) under the processes described in WCAP-16096-P-A, “Software Program Manual for Common Q Systems,” (Reference 6) which has been reviewed and approved by the NRC.

B.3.1.4 Self-Diagnostic Online Testing

There are two PM646A Processor Module self-diagnostics that provide on-line self-testing. These are the [

] ^{a,c} both of which are discussed in the Common Q platform topical report (Reference 4). These diagnostics include on-line self-testing to verify that these diagnostics are performing as designed.

Since the platform self-diagnostics are embedded in the safety system equipment, it is not feasible to periodically test these functions without significant disassembly of the equipment and the use of specialized test equipment, which would compromise the integrity of the safety system equipment being tested in this manner. The evaluations of the self-diagnostics that are described and evaluated in this appendix have shown that there are multiple self-diagnostics with a level of diversity for the detection of each postulated fault.

B.3.1.5 Single Failure Criteria

In evaluating the single failure criteria, it is necessary to consider single failures together with all other identifiable, but non-detectable failures that may be present in the system. In the current regulatory framework, failures not detected by self-diagnostics are expected to be detected by a surveillance test. With the methodology for eliminating SRs within this appendix, the diagnostics must cover these postulated failure modes. This is done by starting with Waterford-3 CPCS FMEA (WNA-AR-00909-CWTR3, "Failure Mode and Effects Analysis for the Core Protection Calculator System," Reference 39), which shows that the CPCS is single failure tolerant. The Failure Modes, Effects, and Diagnostics Analyses (FMEDAs) listed in Section B.6 are based mostly on the failure modes outlined in SV0-PMS-AR-001, "Protection and Safety Monitoring System Technical Specification Surveillance Requirement Elimination" (Reference 43), which contains the underlying analysis for Vogtle 3&4 LAR 19-001 (Reference 42). These tables demonstrate diagnostic coverage for the aforementioned failure modes. By doing so, it is established that the CPCS will still be single failure tolerant. Note that the Waterford-3 CPCS FMEA (Reference 39) was compared with the FMEDAs listed in Section B.6 to ensure that the failure modes outlined in these tables are bounding.

B.3.2 Qualification of AC160 Self-Diagnostics

B.3.2.1 Common Q Topical Report – NRC Safety Evaluation

The Common Q Platform diagnostics were developed under a robust process that was reviewed by the NRC. In 2000, the NRC issued a safety evaluation report (ML003740165, Bibliography 8) on the Common Q Topical Report (CENP-396-P, Rev. 01 which is the predecessor to WCAP-16097-P-A, Reference 4). In that report the NRC acknowledged receipt of Westinghouse document GKWF700777, "Design and Life Cycle Evaluation Report on Previously-Developed Software in ABB AC160, I/O Modules and Tool Software" (Bibliography 9) in support of the commercial dedication of the AC160.

The safety evaluation report states that the, "AC160 PDS [Previously Developed Software] is composed of the AC160 software, S600 I/O Module(s) software, and ABB Tool software. The evaluation is based on the requirements specified in International Electrotechnical Commission (IEC) standard IEC-60880, "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC 60880 is referenced in IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations". IEC 60880 is comparable to IEEE 7-4.3.2-2003, and the staff has found standard IEC 880 to be an acceptable equivalent."

The Design and Lifecycle Evaluation (DLCE) applies to all aspects of the PDS including the system software that executes the nuclear application program and the diagnostics integrated with the system software. In other words, the same software quality approach applied to both aspects of the system software. The results of this report were discussed with the NRC staff during the licensing of the Common Q platform. The NRC also reviewed this document as part of their review of LAR 19-001 for Vogtle 3&4 (Reference 42).

B.3.2.2 Platform Differences Since Initial NRC Review and Palo Verde CPCS

The only module not used in the Oskarshamn Reactor Protection System (the basis for the original NRC review) or the Palo Verde CPCS, but is used in the Waterford-3 CPCS configuration and included in this analysis is the AI688 analog input module. This module has been reviewed by the NRC in 2019 via topical report WCAP-16097-P-A (Reference 4). The results of this report were discussed with the NRC staff during the licensing of the Common Q platform. This module was also included in the NRC staff review of LAR 19-001 for Vogtle 3&4 (Reference 42).

The PM646A firmware has changed since the original qualification (based on the Oskarshamn Reactor Protection System) and since the Palo Verde CPCS. Both installations used PM646A firmware version 1.3/4. There have been improvements to the diagnostic functions since this version which are taken credit for in this report. For example, in PM646A version 1.3/4 it is not possible to store setpoint data onto the PM646A Flash Programmable Read-only Memory (FPRM). It is now a feature of the PM646A firmware and it is described in the Common Q Topical Report WCAP-16097-P-A (Reference 4). As a result, an alternate method of verifying that the setpoints have not inadvertently changed is deployed for the use in some Common Q based safety systems. This method of verifying setpoints is described in WCAP-16097-P-A (Reference 4) which was reviewed and approved by the NRC staff.

It's important to note that the NRC staff reviewed PM646A firmware version 1.3/9 for the Vogtle 3&4 LAR 19-001 (Reference 42). Although the WF3 CPCS is using version 1.3/11, the differences between the two revision levels have no impact on this report (except for an improved version of the overload and high-load self-diagnostics, see PS-9 and PS-10 in Table B.5-1).

B.3.2.3 Southern Nuclear Company LAR 19-001

Southern Nuclear Company (SNC) submitted a Licensing Amendment Request (LAR) (ML19084A309, "Vogtle Electric Generation Plant Units 3 and 4 – Request for Licenses Amendment Regarding Protection and Safety Monitoring System Surveillance Requirement Reduction Technical Specification Revision (LAR 19-001)", Reference 42) for the Vogtle 3&4 AP1000 Nuclear Power Plants in 2019 which involved crediting the PMS (Safety I&C System based on Common Q) self-diagnostics to eliminate Tech Spec SRs. Many of the diagnostics tables and FMEDAs, which were accepted by the NRC, were used within in this appendix. In their Safety Evaluation Report (ML19297D159, Reference 49), the NRC staff made the following statements regarding crediting PMS (Common Q and CIM self-diagnostics) for eliminating TS SRs.

- **Benefits of Self-diagnostics vs. Manual Testing:** The NRC staff agreed with the position that the method of crediting self-diagnostics reduces risks associated with manual testing. Specifically, the staff states in the SER that, "The current manual SRs require the PMS division under test to be in bypass mode resulting in less than full redundancy. Whereas, the PMS self-diagnostic functions execute continuously and do not require the PMS channel under test to be bypassed. In addition, automatic self-diagnostic minimizes risks associated with potential human errors in performing manual surveillance tests. Considering these factors, the NRC staff concludes that the removal of manual SRs for the channel check, COT, ALT, and ALOT could potentially reduce the risk associated with the PMS manual surveillance testing." Note that COT, ALT, and ALOT are PMS surveillances that together, cover the protection path for trip signals (similar to the Channel Functional Tests).
- **Qualifications of Self-diagnostics:** The NRC staff reviewed various aspects of the self-diagnostics including the qualification and documentation relating to these functions. The qualifications of these self-diagnostic functions, which are documented within this appendix, were found to be acceptable. Within the SER, the NRC staff stated, "the staff finds that that Common-Q diagnostic functions credited in the SNC LAR, were developed, tested, qualified, and will be maintained using rigorous processes in accordance with Appendix B requirements, and provide reasonable assurance for the detection of platform-level faults for the Common-Q based PMS."
- **Adequacy of Self-diagnostics for Detecting Faults:** The NRC staff agreed that the Common Q and application self-diagnostics are an adequate substitute for manual surveillance testing. Specifically stated in the SER, "the staff concludes that the self-diagnostic functions are able to detect most PMS hardware faults, and are designed to initiate a division fault alarm to alert the operator to respond as directed by the alarm response procedure. The self-diagnostics continuously assess the health of all digital processor and communication components and are therefore substantially more effective in detecting hardware faults than are the PMS manual

surveillances currently specified for detecting hardware faults by exercising each safety logic pathway.”

B.3.2.4 Conclusion on Qualification Status of Diagnostics

In summary, the AC160 diagnostics were commercially dedicated to the same standards as the rest of the AC160 system software and have been reviewed by the NRC staff in their application to justify eliminating and extending surveillance test frequencies.

B.4 CPCS CHANNEL FAULT INDICATION/ANNUNCIATION PATH

Annunciation is necessary to alert operators when a fault is detected by self-diagnostics within the CPCS. There are multiple ways that the operator can be informed of a CPCS fault. These are:

[

] ^{a,c}

There are various alarm signals that are generated from the CPC and CEAC processors, some of which are used to indicate a fault within the system. These alarms are indicated on the OMs and MTPs (as described in Section 3.2.7.2.12), as well as transmitted to the MCR for annunciation via the Interposing Relay Panel. The following alarms (described in more detail within WNA-DS-04517-CWTR3, Reference 21) indicate a fault within the CPCS that requires the attention of operations:

[

] ^{a,c}

The AC160 platform and application software self-diagnostics function to detect these conditions which generate the aforementioned alarms. When this occurs, the alarm signal is sent from the corresponding CPC or CEAC to the [

] ^{a,c} These paths are shown in Figure B-1 below.

a,c

Figure B-1. Channel Fault Indication and Alarm Paths**Indication and Alarm Path FMEDAs**

[

]a,c

Table B.4-1. Annunciation Path FMEDAs

a,c

CPCS Annunciation via the IRP

[

] ^{a,c}

MTP and OM Diagnostics and Indication

[

] ^{a,c}

CEAPD and PMC Interface

[

] ^{a,c}

Summary

The annunciation of CPCS faults is assured by self-diagnostics for the entire communication path (with the exception of the DO625 and IRP outputs which will still be cycled via the CPCS Output Test). These diagnostics are sufficient to replace the need to test the annunciation features previously performed during surveillance testing.

B.5 SELF-DIAGNOSTIC FUNCTIONS

Section B.6 of this appendix contains the FMEDA tables which demonstrate that postulated failure modes of the CPCS equipment can credit the platform/application self-diagnostics to eliminate TS surveillance testing. The diagnostics being credited to cover these failure modes are contained within the various tables within this section, and are distinguished by the Common Q equipment (or application software) that the self-diagnostics reside in.

It is important to note that there is more than one self-diagnostic capable of detecting each failure mode within the FMEDA tables within Section B.6, due to the sequential processing of digital functions. This characteristic of a digital system provides multiple lines of fault detection for postulated failures. There are levels of diversity between self-diagnostics detecting failures on the equipment in which the platform software is included and the self-diagnostics on equipment that is monitoring the component where the failure is postulated. There is also diversity provided between the self-diagnostics within the platform software, and those which are implemented in the application software.

B.5.1 AC160 Self-Diagnostics

The AC160 platform self-diagnostics are implemented in the hardware and firmware of the platform equipment. In the same manner as all the other platform equipment, the self-diagnostic functions have been designed, implemented, tested and configuration controlled by the platform equipment supplier and has been commercially dedicated by Westinghouse consistent with Westinghouse's Commercial Grade Dedication process. The platform self-diagnostics have a large installed base in Nuclear Power Plants in the U.S., South Korea, China, and Europe.

[

]^{a,c}

The platform self-diagnostics are described in the tables below. These tables were derived from the Vogtle 3&4 LAR 19-001 (Reference 42). To simplify the self-diagnostic evaluation, each type of platform self-diagnostic to be used within this analysis is assigned a designator for the platform equipment where it has a primary self-diagnostic function. The self-diagnostic designators are:

- PS-N, where PS refers to the Processing Section of the PM646A processor module and N is the line number for a specific diagnostic (see Table B.5-1).
- CS-N, where CS refers to the Communication Section of the PM646A processor module and N is the line number for a specific diagnostic (see Table B.5-2).
- CI-N, where CI refers to the CI631 communications module and N is the line number for a specific diagnostic (see Table B.5-3).
- B-N, where B refers to the BIOB and N is the line number for a specific diagnostic (see Table B.5-4).
- AI-N, where AI refers to the AI688 analog input cards and N is the line number for a specific diagnostic (see Table B.5-5).

- DP-N, where DP refers to the DP620 pulse input cards and N is the line number for a specific diagnostic (see Table B.5-6).

[

]^{a,c}

Additional information on the AC160 platform self-diagnostics is provided in WCAP-16097-P-A (Reference 4) and GBRA095801, “AC160 Product Specification for AP1000 PMS,” (Reference 47). It’s also worth noting that GIC-SSP-FSD-19-005, “Evidence of Documentation for AC160 Platform Diagnostics” (Reference 48), which is cited in the tables below (provides details regarding the documentation of testing performed AC160 diagnostics) was created for a separate analysis. However, this document still applies to this analysis since the diagnostics listed in the tables within this section are contained within GIC-SSP-FSD-19-005. The NRC staff reviewed the aforementioned documents as part of their review of LAR 19-001 for Vogtle 3&4 (Reference 42).

Table B.5-1. PM646A Processing Section (PS) Diagnostic Table

c

[illegible]

Table B.5-1. PM646A Processing Section (PS) Diagnostic Table (cont.)

c

[illegible]

Table B.5-1. PM646A Processing Section (PS) Diagnostic Table (cont.)

Table B.5-1. PM646A Processing Section (PS) Diagnostic Table (cont.)

[illegible]

Table B.5-2. PM646A Communication Section (CS) Diagnostic Table

C

[illegible]

Table B.5-2. PM646A Communication Section (CS) Diagnostic Table (cont.)

C

Table B.5-3. CI631 Communication Module Diagnostic Table

C

[illegible]

Table B.5-4. Backplane I/O Bus (BIOB) Diagnostic Table

a,c

Test		Test		Test		Test		Test	
1	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
2	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
3	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
4	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
5	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
6	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
7	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
8	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
9	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
10	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
11	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
12	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
13	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
14	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
15	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
16	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
17	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
18	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
19	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
20	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
21	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
22	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
23	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
24	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
25	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
26	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
27	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
28	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
29	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
30	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
31	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
32	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
33	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
34	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
35	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4		4		4		4		4
36	1	2	1	3	1	4	1	5	1
	2		2		2		2		2
	3		3		3		3		3
	4								

Table B.5-5. Analog Input Module (AI688) Diagnostic Table

a,c

Test Step		Test Result		Test Action		Test Result		Test Action																		
1. Perform a visual inspection of the AI688 module for any physical damage or loose connections.	Pass	No physical damage or loose connections are present.		Proceed to the next test step.		No physical damage or loose connections are present.		Proceed to the next test step.																		
	Fail	Physical damage or loose connections are present.		Repair or replace the damaged components or tighten the loose connections.		Physical damage or loose connections are present.		Repair or replace the damaged components or tighten the loose connections.																		

Table B.5-6. Digital Pulse Module (DP620) Diagnostic Table

a,c

B.5.2 Application Diagnostics

The application software contains self-diagnostic functions that are carried out within the CPC and CEAC PMs as well as the OM and MTP. There are many self-diagnostic functions that monitor the system for errors [

] ^{a,c}

[

] ^{a,c}

B.6 FAILURE MODES, EFFECTS, AND DIAGNOSTIC ANALYSES

The evaluations of the suitability of the self-diagnostics to replace the manual Tech Spec SRs are documented by the FMEDA Tables within this section (one table for each CPCS component that is currently covered by manual surveillances). The FMEDAs use the failure modes outlined in SV0-PMS-AR-001, “Protection and Safety Monitoring System Technical Specification Surveillance Requirement Elimination” (Reference 43) as a basis (except for Tables B.6-6 and B.6-7, which were derived within this analysis). For each fault postulated in Reference 43 relating to the CPCS components within the FMEDA tables, the self-diagnostics capable of detecting the type of fault are identified. Additionally, the WF3 CPCS application-specific FMEA (WNA-AR-00909-CWTR3, Reference 39) was analyzed to ensure all failure modes associated with the LPD/DNBR trip paths were enveloped by those within the FMEDA tables in Reference 43 (and Tables B.6-6 and B.6-7 which were constructed in this analysis). Where there was not overlapping coverage, the failure mode from Reference 39 was added to the FMEDA tables within this section with a note denoting that it is not from the application-specific FMEA. The following FMEDA tables were developed:

- PM646A FMEDA – Table B.6-1
- BIOB FMEDA – Table B.6-2
- CI631 FMEDA – Table B.6-3
- AI688 FMEDA – Table B.6-4
- DP620 FMEDA – Table B.6-5
- DO625 FMEDA – Table B.6-6
- IRP FMEDA – Table B.6-7

The module FMEDA tables document the evaluation of diagnostic coverage for postulated module faults. The format of the FMEDA tables is as follows.

[

]^{a,c}

[

] ^{a,c}

Table B.6-1 PM646A Processing Module FMEDA

Table B.6-1 PM646A Processing Module FMEDA

[illegible]

Table B.6-1 PM646A Processing Module FMEDA (cont.)

a,c

Table B.6-2 BIOB FMEDA

a,c

Table B.6-3 CI631 Communications Module FMEDA

a,c

Table B.6-4. Analog Input Modules (AI688) FMEDA

a,c

Table B.6-4. Analog Input Modules (AI688) FMEDA (cont.)

a,c

					Analog Input Modules (AI688)			FMEDA
					Failure Mode	Failure Mechanism	Failure Rate (per 10 ⁶ hours)	

Table B.6.5. Digital Pulse Module (DP620) FMEDA

Table B.6.5. Digital Pulse Module (DP620) FMEDA

[illegible]

Table B.6.6. Digital Output Module (DO625) FMEDA

						a,c	

Table B.6.7. Interposing Relay Panel (IRP) FMEDA

						a,c	

B.7 TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENT MAPPING

The general approach to showing TS SRs can be eliminated can be summarized as follows:

- The Common Q components (and the IRP) that are tested by current manual Tech Spec SRs are identified.
- The failure modes for these components are identified (see FMEDAs in Section B.6).
- The platform and application software self-diagnostics are then mapped to the failure modes (see FMEDAs in Section B.6)
- If all failure modes for all components within the test envelope the current manual Tech Spec SRs are covered by the Common Q self-diagnostics or an existing test, then that surveillance test can be eliminated as a requirement for the CPCS based off of the Common Q platform.

There are some deviations from this general methodology when the analysis involves response time testing. These deviations are described in more detail within the corresponding sub-section within Section B.7.3. Section B.7.1 contains the analysis for the elimination of SR 4.3.1.1 (Channel Functional Testing of the CPCS portion of the SR), Section B.7.2 contains the analysis for the elimination of SR 4.3.1.3 (CPCS portion of RTT SR), and Sections B.7.3 – B.7.5 contain the justifications behind the elimination of SRs 4.3.1.4 – 4.3.1.6 respectively.

B.7.1 CPCS Channel Functional Test SR Elimination

The CPC and CEAC subracks are required to be tested [

] ^{a,c}

[

a,c

[illegible]

[

$$\mathbb{J}^{a,c}$$

Based on the above analysis, the Channel Functional Test SRs performed on the CPCS can be eliminated. Furthermore, there are two additional items worth discussing.

[

] ^{a,c}

B.7.2 CPCS RTT SR Elimination

The foundation for the RTT SR elimination analysis consists of the following two notions:

- The system and application diagnostics that are being credited in this report to eliminate other SRs in this appendix, although only designed to test the operability of the system, would still capture failures of the CPCS that would result in slower response times.
- Portions of the CPCS actuation paths are tested under other SRs not eliminated within this appendix.

Based on these, only failures that cause a response time delay, but have no functional effect on the component, will be considered. These failures are those that will either effect the CONTRM (i.e., the control module structure PC element used for execution control of modules within a PC program) cycles in the PMs or hardware failures that result in response time delays. Therefore, to eliminate RTT SRs, it must be demonstrated that both the CONTRM cycle time and hardware are covered by diagnostics.

NOTE: It's important to note that the following two assumptions were made during the development of this section:

1. The excore nuclear instrumentation processing equipment can be response time tested independently of the CPCS.
2. The scope of RTT for the LPD and DNBR trips begins at the input modules to the CPCS and ends at the output to the PPS.

B.7.2.1 Methodology

The methodology to be used to eliminate RTT is as follows:

1. Determine all RTT paths tested under WF3 TS (Reference 20) SR 4.3.1.3 related to the CPCS.:
 - a. Table 4.3-1, Function 9 "Low Power Density – High"
 - b. Table 4.3-1, Function 10 "DNBR – Low"
 - c. Table 4.3-1, Function 14 "Core Protection Calculators"
 - d. Table 4.3-1, Function 15 "CEA Calculators"

Once all paths are determined, the scope of the components that make up the functional paths for response time testing can be determined.

2. Analyze the components identified in Step 1 for potential failures that could generate delays in response time. For identified failures, diagnostics will be discussed which will be credited to ensure the response time will not continue to degrade to a point that would be qualitatively worse than the current frequency of checking the response time of the system (any given division is only response time tested every 4th refueling outage). This will be done by analyzing the components in three groups:
 - a. Input Modules
 - b. Processing and Communication Components
 - c. Output Modules

This captures the subrack portion of the actuation paths which constitutes the scope of this SR elimination task. This methodology and most of the analysis that follows is derived from the RTT elimination portion of SNC LAR 19-001 (Reference 42). The NRC staff reviewed that analysis for the Vogtle 3&4 PMS and provided the following conclusion in their SER (ML19297D159, Reference 49), “the NRC staff finds the methodology presented in the LAR for use of PMS racks’ allocated times acceptable because it satisfies the applicable requirements of 10 CFR 50.55a(h).” It’s important to note that although RTT of the PMS rack was eliminated from the Vogtle 3&4 TS, the SRs remain as a result of this effort. This was an implementation decision since the SRs cover more than just the PMS rack. Within the WF3 TS, the RTT SR applicable to the CPCS (SR 4.3.1.3) invokes the CPCS via Table 4.3-1. Therefore, this Appendix will eliminate the CPCS portion of the RTT SR by explicitly stating within SR 4.3.1.3 that the CPCS is excluded from being applicable to the SR.

B.7.2.2 Response Time Paths

In order to eliminate the RTT SRs related to the CPCS (identified in methodology step 1), these components that comprise the trip paths need to be determined. Table B.7-2 provides the list of components that needs to be analyzed per the identified paths using Figure 3.2-1 and the detailed architecture described in the WF3 CPCS SyRS (WNA-DS-04517-CWTR3, Reference 21).

Table B.7-2. CPCS Components within Scope of TS RTT SR

Type of Component	CPCS Rack Components within SR Paths
Input Modules	- AI688 - DP620
Processing/Communication	-PM646 - BIOB - CI631 - HSL
Output Modules	- DO625 - IRP ¹

Note:

1. The IRP does not contain Common Q components but is part of the CPCS portion of the LPD/DNBR trip paths and thus included in this analysis.

B.7.2.3 Input Module Analyses

Input Module Scope

The input modules utilized within the RT actuation paths are listed below, along with a synopsis as to whether they should be included in the RTT elimination analysis.

1. **AI688 Input Modules** – The AI688 is a high-level analog input module used in the CPCS to process 4-20 mA, 0-10 VDC and 0-1 VDC inputs. []^{a,c}

[

]^{a,c}

AI688 Analysis

[

]^{a,c}

DP620 Analysis

The FMEDA for this type of input device is defined in Table B.6.5 “Digital Pulse Module (DP620) FMEDA”. [

]^{a,c}

Input Filter Analysis

An important discussion revolves around the fact that the aforementioned input cards contain [

]^{a,c}

[]^{a,c}

Time-degradation of capacitors leads to the capacitance of the devices to degrade (reduce) over time [

] ^{a,c}

B.7.2.4 Processing/Communication Component Analysis

Processing/Communication Component Scope

Processing within the CPC and CEAC racks is performed within the PM646A processing modules. These modules communicate with each other via the BIOB and the CI631 (which contains the Global Memory for the subrack). Communication from subrack to subrack is done via HSLs. These components that comprise the Processing/Communication portions of the RTT SR paths are summarized below along with a synopsis as to whether they should be included in the RTT elimination analysis.

1. **PM646A Processing Module** – Component failures that do not result in a functional failure captured by diagnostics used to eliminate other SRs [

] ^{a,c}

2. **CI631 Communication Module** – The Global Memory stored on the CI631 is used to share information among PMs. [

] ^{a,c}

3. **Backplane I/O Bus (BIOB)** – The backplane connects the PMs with the CI631 and I/O modules. [

] ^{a,c}

4. **High-Speed Link (HSL)** – [

] ^{a,c}

[]^{a,c}

PM646A Analysis

The FMEDA for this device is defined in Table B.6-1 “PM646A Processing Module FMEDA”. [

] ^{a,c}

CI631 Analysis

The FMEDA for this device is defined in Table B.6-3 “CI631 Communications Module FMEDA”. [

] ^{a,c}

B.7.2.5 Output Module Analysis

The only Common Q based output module used in the protection path of the CPCS is the DO625. This module has 16 solid-state output channels. [

] ^{a,c}

Similarly, the IRP is included in the output module analysis since it is included in the CPCS response time paths due to the interface it provides with the CPCS and the PPS. [

] ^{a,c}

B.7.3 CEA Isolation Amplifier and Optical Isolator Operability (SR 4.3.1.4 Elimination)

The existing CPCS contains isolation amplifiers and optical isolators between the CEAC and the CPC racks. These will no longer exist in the Common Q implementation of the CPCS, resulting in this surveillance no longer having any applicability in the WF3 TS. Therefore, this SR can be eliminated.

B.7.4 CPC and CEAC Operability (SR 4.3.1.5 Elimination)

Determining operability by verifying the auto-restart count of the CPCS doesn't apply to the Common Q platform. [

] ^{a,c}

B.7.5 CPCS Operability Following High Temperature Alarm (SR 4.3.1.6 Elimination)

[

] ^{a,c}

B.8 CONCLUSIONS

The evaluations within Sections B.7.1 – B.7.5 show that the respective surveillances analyzed can be eliminated based on the AC160 platform and application software self-diagnostic functions, as well as overlapping test coverage and in some cases, due to the Common Q architecture. This is summarized as follows:

1. **SR 4.3.1.1 (Channel Functional Testing of the CPCS portion of the SR)** – The channel functional tests for the LPD and DNBR trip functions are no longer required based on ability of self-diagnostic functions to detect failures within the trip path, []^{a,c}
2. **SR 4.3.1.3 (CPCS portion of the SR)** – Response time testing of the CPC/CEAC racks and related functions is no longer required. This includes the LPD/DNBR trip path portion of the IRP which is included in Section B.7.2.5.
3. **SR 4.3.1.4 (CEA Isolation Amplifier and Optical Isolator Operability SR)** – This SR was tailored to a feature of the legacy CPCS architecture which will no longer exist in the Common Q CPCS implementation. As a result, this SR is no longer required.
4. **SR 4.3.1.5** – This SR was dependent on the legacy CPCS auto-restart feature that does not exist in the Common Q CPCS []^{a,c}. As a result, this SR is no longer required to ensure operability of the CPCS based on self-diagnostics being credited to confirm operability of the system.
5. **SR 4.3.1.6** – This SR is no longer required to ensure operability of the CPCS after receipt of a high-cabinet temperature alarm []^{a,c}.

APPENDIX C ENDNOTES

-
- ¹ Waterford FSAR Section 1.2.2.3.2
- ² Waterford Plant Protection System design basis document, W3-DBD-12
- ³ Waterford FSAR Section 7.2.1.1.1.3 and 00000-ICE-3208, Rev 8, Section 2.1.b
- ⁴ Waterford FSAR Section 4.4.4.1
- ⁵ Waterford FSAR Section 7.2.2.2.4
- ⁶ Waterford FSAR Section 7.2.2.1
- ⁷ Waterford FSAR Section 7.2.1.1.1.4, CPCS Functional Design Requirements 00000-ICE-3208, Section 4.2.9
- ⁸ CPCS System Requirements Specification, 00000-ICE-30158 Appendix A represents the CPCS design basis algorithms. The revision changes over time to Appendix A are not related to CPCS design basis functions (see revision descriptions in the document). WSES-3 specific CPCS System Requirements Specification, Reference 21, only modifies Appendix A to add pre-trip alarms for auxiliary trips.
- ⁹ Waterford FSAR Section 1.2.2.3.2
- ¹⁰ Waterford FSAR Section 1.2.2.3.2
- ¹¹ Entergy Purchase Specification SPEC-18-00005-W, Rev. 0, Paragraph 1.6.3.5
- ¹² Waterford FSAR Figure 7.2-6
- ¹³ Waterford FSAR Section 7.2.1.1.2.5
- ¹⁴ Waterford FSAR Section 7.5.1.6.2
- ¹⁵ Waterford FSAR Figures 7.2-3 and 7.2-4
- ¹⁶ WSES-3 specific CPCS System Requirements Specification, Reference 21, Figure 2.1-1
- ¹⁷ Waterford FSAR Section 7.2.1.1.2.2
- ¹⁸ Waterford FSAR Section 7.2.1.1.2.2
- ¹⁹ Waterford FSAR Sections 4.1 and 7.1.1.7, Table 1.7-1 and Figure 7.2-3, modified to correct CEA quantities and to add equipment detail from existing CPCS technical manual
- ²⁰ Waterford FSAR Section 7.2.1.1.2.5
- ²¹ Waterford FSAR Figure 7.2-4
- ²² Waterford FSAR Section 7.2.1.1.2.5
- ²³ Existing CPCS Technical Manual
- ²⁴ APC Interface Specification, WNA-DS-04519-CWTR3
- ²⁵ Waterford FSAR Section 7.1.2.5
- ²⁶ Waterford FSAR Section 7.2.1.1.9.3
- ²⁷ Waterford FSAR Section 7.2.1.1.9.3
- ²⁸ Waterford FSAR Section 7.2.1.1.9.3
- ²⁹ Waterford FSAR Section 7.2.1.1.9.3
- ³⁰ Waterford FSAR Section 7.2.1.1.9.3
- ³¹ Waterford FSAR Section 7.2.1.1.9.3
- ³² Waterford Engineering Changes, ER-W3-1999-0411-000, ER-W3-1999-0411-002, and ER-W3-2002-0166-000
- ³³ Waterford FSAR Section 7.2.1.1.2.2
- ³⁴ Waterford FSAR Section 7.2.1.1.2.5
- ³⁵ Refer to Section 2 citation for source for this repeated information
- ³⁶ Refer to Section 2 citation for source for this repeated information
- ³⁷ Waterford FSAR Section 7.2.1.1.2.5
- ³⁸ Waterford FSAR Section 7.2.1.1.9.3, Periodic Testing
- ³⁹ Waterford FSAR Section 7.2.1.2(j)
- ⁴⁰ CPCS SyRS 00000-ICE-30158, Section 1.1
- ⁴¹ CPCS SyRS 00000-ICE-30158, Section 2.1
- ⁴² CPCS SyRS 00000-ICE-30158, Section 2.1
- ⁴³ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Figure 2.1-1
- ⁴⁴ CPCS SyRS 00000-ICE-30158, Section 2.1.1.1

-
- ⁴⁵ Reference 3, Section 3.3.2
- ⁴⁶ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4
- ⁴⁷ CPCS SyRS 00000-ICE-30158, Sections 2.2.1.4.13 – 16, 2.2.1.4.21, 2.2.1.4.23
- ⁴⁸ CPCS SyRS 00000-ICE-30158, Section 2.4.1.2.1.2
- ⁴⁹ Reference 3
- ⁵⁰ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.1
- ⁵¹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.2
- ⁵² CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.3
- ⁵³ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.4, AI688 identified in WSES-3 CPCS Hardware Design Description (HDD) WNA-DS-04650-CWTR3, Section 2.1.1.1
- ⁵⁴ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.4.1
- ⁵⁵ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.5; module number specified in WSES-3 CPCS HDD WNA-DS-04650-CWTR3, Section 2.1.2.6
- ⁵⁶ Entergy Purchase Specification SPEC-18-00005, Section 5.1.1.8
- ⁵⁷ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.6 and WSES-3 CPCS SyRS WNA-DS-04517-CWTR3 R-DS-04517-10083
- ⁵⁸ CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10084; module number specified in WSES-3 CPCS HDD WNA-DS-04650-CWTR3, Figures 2.1-2A – 2.1-2D
- ⁵⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.8; module number specified in WSES-3 CPCS HDD WNA-DS-04650-CWTR3, R-DS-04650-10006
- ⁶⁰ CPCS SyRS 00000-ICE-30158, Section 2.4.1.2.1.2
- ⁶¹ CPCS SyRS 00000-ICE-30158, TABLE 2.4.1.2-1
- ⁶² CPCS SyRS 00000-ICE-30158, Sections 2.2.1.5.2.2.4, and 3.1.1.1.1.5.1, and Table 3.1.1.1.7-1
- ⁶³ CPCS SyRS 00000-ICE-30158, Section 2.1.1.1
- ⁶⁴ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.4
- ⁶⁵ CPCS SyRS 00000-ICE-30158, Sections 2.1.2.1.7.4, 2.2.1.4, and 2.2.1.4.17
- ⁶⁶ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3
- ⁶⁷ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.3 and 3.1.1.1.1.4
- ⁶⁸ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.2.1
- ⁶⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.3 and 3.1.1.1.1.4
- ⁷⁰ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.1
- ⁷¹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.2
- ⁷² CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.3 and 3.1.1.1.1.4.3
- ⁷³ CPCS SyRS 00000-ICE-30158, Table 2.1.1-1
- ⁷⁴ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.3 and 3.1.1.1.1.4.3
- ⁷⁵ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.2.1, 3.1.1.1.1.3.3, 3.1.1.1.1.4.2, and 3.1.1.1.1.4.3
- ⁷⁶ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.3 and 3.1.1.1.1.4.3
- ⁷⁷ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.4.1
- ⁷⁸ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.4.2
- ⁷⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.3.5
- ⁸⁰ CPCS SyRS 00000-ICE-30158, Table 2.4.1.2-1
- ⁸¹ CPCS SyRS 00000-ICE-30158, Table 2.4.1.2-1
- ⁸² CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.10, as augmented by WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, R-DS-04517-10125
- ⁸³ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Figure 2.1-3
- ⁸⁴ Waterford FSAR Section 7.5a III. E
- ⁸⁵ CPCS SyRS 00000-ICE-30158, Section 2.3.3
- ⁸⁶ CPCS SyRS 00000-ICE-30158, Section 2.4.2.2.1
- ⁸⁷ CPCS SyRS 00000-ICE-30158, Section 2.4.2.2.1
- ⁸⁸ CPCS SyRS 00000-ICE-30158, Section 2.4.2.2.2
- ⁸⁹ Common Q Topical Report CPCS Appendix 2, Section A2.1.2.1 F.
- ⁹⁰ Common Q Topical Report CPCS Appendix 2, Section A2.1.2.1 G.
- ⁹¹ CPCS SyRS 00000-ICE-30158, Sections 1.1 and 2.1.1.4
- ⁹² CPCS SyRS 00000-ICE-30158, Section 2.2.1.3
- ⁹³ CPCS SyRS 00000-ICE-30158, Section 2.2.2.4.6

-
- ⁹⁴ CPCS SyRS 00000-ICE-30158, Section 2.2.2.4.1
- ⁹⁵ CPCS SyRS 00000-ICE-30158, Section 2.2.2.4.4
- ⁹⁶ CPCS SyRS 00000-ICE-30158, Section 2.2.2.4.5
- ⁹⁷ CPCS SyRS 00000-ICE-30158, Section 2.2
- ⁹⁸ CPCS SyRS 00000-ICE-30158, Section 2.2.3.5 and 2.4.2.2.7
- ⁹⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.3.13.10
- ¹⁰⁰ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.8
- ¹⁰¹ CPCS SyRS 00000-ICE-30158, Section 2.2.3.6
- ¹⁰² CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.1
- ¹⁰³ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.12 and 2.2.1.4.12.2
- ¹⁰⁴ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.13
- ¹⁰⁵ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.14
- ¹⁰⁶ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.4
- ¹⁰⁷ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.17
- ¹⁰⁸ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.21
- ¹⁰⁹ Many in this list are descriptions of what is not implemented in the CPCS. The descriptions are background information, but the important fact is that the listed restriction is met by not including the design element in the CPCS design that can be verified by analyzing the CPCS architecture. Where a restriction is software based, then a citation to the Common Q Application Restrictions Document (Reference 18) is made. Therefore citations to these descriptions for what is not in the CPCS design is not included.
- ¹¹⁰ Reference 18, Restriction S122
- ¹¹¹ Reference 18, Restriction S57:12
- ¹¹² The Palo Verde CPCS Software Design Descriptions (SDDs) were reviewed to validate that the OPT: enhanced PCDB is not used. The Palo Verde CPCS application code was reviewed to validate that neither the STEP or SEQ PC element is used
- ¹¹³ Reference 26, Section 2.7.2
- ¹¹⁴ Reference 18, Restriction S5
- ¹¹⁵ Reference 18, Restriction S4
- ¹¹⁶ Reference 18, Restrictions S13-14
- ¹¹⁷ Reference 26, Section 2.7.2
- ¹¹⁸ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.22
- ¹¹⁹ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.23
- ¹²⁰ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.16
- ¹²¹ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.3
- ¹²² CPCS SyRS 00000-ICE-30158, Section 2.2.1.5
- ¹²³ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirements R-DS-04517-10074 - 78
- ¹²⁴ CPCS SyRS 00000-ICE-30158, Section 2.3.9.3
- ¹²⁵ WNA-DS-04650-CWTR3 Section 2.1.1.7.1, R-DS-04650-10009
- ¹²⁶ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6.1
- ¹²⁷ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6.2
- ¹²⁸ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6.3
- ¹²⁹ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6.4
- ¹³⁰ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6.5
- ¹³¹ CPCS SyRS 00000-ICE-30158, Section 2.1.1.2 and 2.1.3.1.1
- ¹³² CPCS SyRS 00000-ICE-30158, Section 2.5.1.2
- ¹³³ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.7
- ¹³⁴ CPCS SyRS 00000-ICE-30158, Section 1.1
- ¹³⁵ CPCS SyRS 00000-ICE-30158, Section 2.1.1.8
- ¹³⁶ CPCS SyRS 00000-ICE-30158, Section 2.1.3.1.1
- ¹³⁷ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10008
- ¹³⁸ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10008
- ¹³⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.2.1
- ¹⁴⁰ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.6
- ¹⁴¹ CPCS SyRS 00000-ICE-30158, Section 2.1.1.4.3.7
- ¹⁴² CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.9.14

- ¹⁴³ Common Q Topical Report, Reference 4, Section 4.5
- ¹⁴⁴ Common Q Topical Report, Reference 4, Section 5.2.1.1.1 and CPCS SyRS 00000-ICE-30158, Section 2.1.1.1
- ¹⁴⁵ Common Q Topical Report, Reference 4, Section 5.2.1.2.2
- ¹⁴⁶ Common Q Topical Report, Reference 4, Section 5.2.1.2.1, Base Software, Communication Section Software Description
- ¹⁴⁷ Common Q Topical Report, Reference 4, Section 5.2.1.2.1, Base Software, Task Scheduler (Tick ISR) and Advant Controller 100 Series – System Manual, Figure 16-1.
- ¹⁴⁸ Advant Controller 100 Series System Software Manual, Chapter 16
- ¹⁴⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.6
- ¹⁵⁰ The MTP and AC160 are two different computer systems and thus run asynchronously.
- ¹⁵¹ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.9.14
- ¹⁵² CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.21
- ¹⁵³ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.1.6
- ¹⁵⁴ Software Design Description for the Common Q Generic Flat Panel Display Software, 00000-ICE-30157, Rev. 26, Section 5.6.7
- ¹⁵⁵ AC160 Product Specification for the AP1000 PMS, GBRA095801 Rev. E, Table 15
- ¹⁵⁶ CPCS SyRS 00000-ICE-30158, Section 2.2.1.3
- ¹⁵⁷ Software Design Description for the Common Q Generic Flat Panel Display Software, 00000-ICE-30157, Rev. 26, Section 4.5.13
- ¹⁵⁸ Failure Modes and Effects Analysis for the Common Q Core Protection Calculator System, 00000-ICE-3338, Revision 0
- ¹⁵⁹ CPCS SyRS 00000-ICE-30158, Section 2.1.1.5
- ¹⁶⁰ Waterford FSAR Section 7.2.1.1.8
- ¹⁶¹ CPCS SyRS 00000-ICE-30158, Section 2.3.3
- ¹⁶² CPCS SyRS 00000-ICE-30158, Section 2.1.3.3.1.1
- ¹⁶³ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Section A.2
- ¹⁶⁴ CPCS SyRS 00000-ICE-30158, Appendix A, Section 1.2
- ¹⁶⁵ CPCS SyRS 00000-ICE-30158, Appendix A, Section 3.2.6.1.1
- ¹⁶⁶ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.17.2 and Appendix A, Table A8
- ¹⁶⁷ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.17.2 and Appendix A, Table A8
- ¹⁶⁸ CPCS SyRS 00000-ICE-30158, Appendix A, Table A8
- ¹⁶⁹ CPCS SyRS 00000-ICE-30158, Section 3.1.4
- ¹⁷⁰ CPCS SyRS 00000-ICE-30158, Table 3.1.4-1
- ¹⁷¹ CPCS SyRS 00000-ICE-30158, Section 2.2.1.5.2.1.1
- ¹⁷² System Operating Procedure Core Protection Calculator System, OP-004-006
- ¹⁷³ CPCS SyRS 00000-ICE-30158, Section 2.2
- ¹⁷⁴ See LTR Sections 3.2.8.1, 3.2.9, 3.2.11, 3.2.12, and 3.2.16
- ¹⁷⁵ CPCS SyRS 00000-ICE-30158, Section 2.1.1.5
- ¹⁷⁶ CPCS SyRS 00000-ICE-30158, Section 3.1.1.1.3.13.7 and Appendix A, P. A39, variable NPASMX
- ¹⁷⁷ CPCS SyRS 00000-ICE-30158, Section 2.3.3.3.4
- ¹⁷⁸ CPCS SyRS 00000-ICE-30158, Section 2.1.1.8
- ¹⁷⁹ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4.12.2
- ¹⁸⁰ Cyber Security Physical Access Requirements for Critical Digital Assets, Section 5.4, EN-IT-103-07, Entergy Operations Inc. The keys for the cabinets are stored in a cyber security locker and a cyber control log is kept of the keys in EN-IT-103-07 Att. 9.1
- ¹⁸¹ CPCS SyRS 00000-ICE-30158, Section 2.3.2.2
- ¹⁸² CPCS SyRS 00000-ICE-30158, Section 2.3.2.1
- ¹⁸³ CPCS SyRS 00000-ICE-30158, Section 2.2.1.3
- ¹⁸⁴ CPCS SyRS 00000-ICE-30158, Sections 2.2.1.4.12.2, 2.2.2.2 and 2.2.2.3
- ¹⁸⁵ CPCS SyRS 00000-ICE-30158, Section 2.2
- ¹⁸⁶ WCAP-16097-P-A, Section 5.6.10
- ¹⁸⁷ WCAP-16097-P-A, Section 5.2.1.2.1 *Slow Background Task*, and 00000-ICE-3239 Section 3.2.24
- ¹⁸⁸ Section 3.2.7.2.7 in this document, and CPCS SyRS 00000-ICE-30158, Sections 2.2.1.4.21 and 2.4.2.1.2
- ¹⁸⁹ Reference 30 only identifies the AI685 analog input module requiring calibration. The new AI688 for the WSES-3 CPCS will use the AI688 analog input module that does not require calibration.

-
- ¹⁹⁰ System Operating Procedure Core Protection Calculator System, OP-004-006
¹⁹¹ Figure 2-2 Existing CPC/CEAC Architecture Block Diagram in this document
¹⁹² WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10012
¹⁹³ FSAR Section 7.2.2.2
¹⁹⁴ CPCS SyRS 00000-ICE-30158, Sections 2.3.9.6.5 and 3.1.1.1.3.13.10
¹⁹⁵ CPCS SyRS 00000-ICE-30158, Section 2.2.1.4
¹⁹⁶ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04157-10009
¹⁹⁷ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10008
¹⁹⁸ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10075
¹⁹⁹ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10008
²⁰⁰ CPCS SyRS 00000-ICE-30158, Sections 2.5.1.4.2 and 3.1.1.1.1.6, and WNA-DS-04683-CWTR3, Sections 1.2 and 2.1
²⁰¹ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirements R-DS-04517-10074 and R-DS-04517-10075
²⁰² See ²⁰⁰
²⁰³ See Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document
²⁰⁴ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Figure 2.1-2
²⁰⁵ 00000-ICE-30157 Section 4.5.13
²⁰⁶ CPCS SyRS 00000-ICE-30158, Section 2.3.2
²⁰⁷ 00000-ICE-30157 Section 4.5.13
²⁰⁸ Advant Controller 100 Series System Software Manual, Chapter 16
²⁰⁹ See Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document
²¹⁰ CPCS SyRS 00000-ICE-30158, Section 2.3.9.6
²¹¹ CPCS SyRS 00000-ICE-30158, Section 2.2.1.5.2.1.1
²¹² See Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document
²¹³ See Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document
²¹⁴ See Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document
²¹⁵ CPCS SyRS 00000-ICE-30158, Section 2.1.3.1.3
²¹⁶ FSAR Section 4.11
²¹⁷ CPCS SyRS 00000-ICE-30158, Table 3.1.1.1.7-1, Note 1
²¹⁸ Section 3.5 in this document.
²¹⁹ WCAP-16097-P-A, Section 5.2.1.1.1 Diagnostic Functions
²²⁰ Section 3.5 in this document.
²²¹ CPCS SyRS 00000-ICE-30158, Table 2.3.11-1
²²² Section 3.2.17.2 in this document
²²³ Section 3.2.6 in this document
²²⁴ 00000-ICE-30165
²²⁵ WNA-RM-00015-CWTR3 WSES-3 CPCS Requirements Management Plan, Section 1.4.2. The engineering organization is delineated by system design, hardware design, and software design.
²²⁶ WCAP-16096-P-A SPM Section 4.6.2.2.1
²²⁷ WNA-BR-00379-CWTR3
²²⁸ WNA-RTM-00076-CWTR3
²²⁹ WCAP-16096-P-A SPM, Definition for RTM
²³⁰ 00000-ICE-37755
²³¹ Reference 26 in this document.
²³² WCAP-16096-P-A SPM, Section 4.6.2.1
²³³ WCAP-16096-P-A SPM, Exhibit 5-1
²³⁴ Based on Palo Verde CPCS SDDs - 00000-ICE-30106 – 08, 11, 29, 40,65-66
²³⁵ WCAP-16096-P-A SPM, Exhibit 5-1
²³⁶ WCAP-16096-P-A SPM, Section 5.5.4.1 and 5.5.4.2
²³⁷ There are a multitude of Westinghouse internal work instructions. One example is WNA-WI-00053-GEN, Custom PC Element Compile and Link Work Instructions
²³⁸ Reference 25 in this document and Configuration Management Implementation Guideline WNA-IG-00109-GEN
²³⁹ WCAP-16096-P-A SPM, Sections 2.1.1.3 and 3.3.10
²⁴⁰ Westinghouse can provide an organization chart at time of review
²⁴¹ Reference 4 in this document, PSAI 6.3
-

²⁴² AI688 description in Reference 10 of this document.

²⁴³ System Operating Procedure Core Protection Calculator System, OP-004-006

²⁴⁴ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10050

²⁴⁵ WSES-3 CPCS SyRS WNA-DS-04517-CWTR3, Requirement R-DS-04517-10051

²⁴⁶ Locked cabinet: CPCS SyRS 00000-ICE-30158, Section 2.3.2.1; Secure location: APC in the main control room; Procedural Controls: Cyber Security Physical Access Requirements for Critical Digital Assets, EN-IT-103-07, Revision 7, Entergy Operations, Inc.; and Control of Portable Digital Media Connected to Critical Digital Assets, EN-IT-103-01, Revision 13, Entergy Operations, Inc.

²⁴⁷ Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document.

²⁴⁸ Figure 3.2-1 Common Q CPC/CEAC Architecture Block Diagram in this document.

²⁴⁹ Sections 3.5.4, 3.5.5, and 3.5.6 in this document.

Enclosure, Attachment 7

W3F1-2020-0040

Westinghouse Specification 00000-ICE-30158, Revision 14

**System Requirements Specification for the Common Q
Core Protection Calculator System**

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 8

W3F1-2020-0040

Westinghouse Specification WNA-DS-04517-CWTR3, Revision 2

System Requirements Specification for the Core Protection Calculator System,

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 9

W3F1-2020-0040

Westinghouse Specification 00000-ICE-3338, Revision 0

**Failure Modes and Effects Analysis for the Common Q Core
Protection Calculator System**

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 10

W3F1-2020-0040

Westinghouse Specification WNA-AR-00909-CWTR3, Revision 1

Failure Modes and Effects Analysis for the Core Protection Calculator System

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 11

W3F1-2020-0040

Westinghouse Specification EQ-QR-400-CWTR3, Revision 0

**Core Protection Calculator System Primary Digital Components
Qualification Summary Report for Waterford Unit 3**

Proprietary

Proprietary Information - Withhold from Public Disclosure Under 10 CFR 2.390

Enclosure, Attachment 12

W3F1-2020-0040

Westinghouse Letter CAW-20-5040

**Affidavit, Proprietary Information Notice, and Copyright in support of 00000-ICE-30158,
WNA-DS-04517-CWTR3 00000-ICE-3338, WNA-AR-00909-CWTR3, and EQ-QR-400-CWTR3
(Attachments 7, 8, 9, 10, and 11)**

AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of 00000-ICE-30158, Revision 14, WNA-DS-04517-CWTR3, Revision 2, c, Revision 0, WNA-AR-00909-CWTR3, Revision 1, EQ-QR-400-CWTR3, Revision 0 be withheld from public disclosure under 10 CFR 2.390.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged, or as confidential commercial or financial information.
- (4) Pursuant to 10 CFR 2.390, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse and is not customarily disclosed to the public.
 - (ii) Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar technical evaluation justifications and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.

AFFIDAVIT


- (5) Westinghouse has policies in place to identify proprietary information. Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:
- (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.
 - (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage (e.g., by optimization or improved marketability).
 - (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
 - (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
 - (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
 - (f) It contains patentable ideas, for which patent protection may be desirable.
- (6) The attached submittal contains proprietary information throughout, for the reasons set forth in Sections 5 (a) and (c) of this Affidavit. Accordingly, a redacted version would be of no value to the public.

AFFIDAVIT

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 06/08/2020



Zachary S. Harper, Manager
Licensing Engineering

Enclosure, Attachment 13

W3F1-2020-0040

DRAFT
Human Factors Engineering Analysis

1. HFE Introduction

Per DI&C-ISG-06 Section B.1.4 (Reference 1), a human factors evaluation is required when a licensee is changing main control room or other interface for which operations and maintenance will be interacting. DI&C-ISG-06 references the following for human factors engineering (HFE) considerations:

- IEEE Standard 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* (IEEE Std 603) (Reference 2)
- NUREG-1764, *Guidance for the Review of Changes to Human Actions* (NUREG-1764) (Reference 3)
- NUREG-0800 Chapter 18, *Standard Review Plan Human Factors Engineering* (NUREG-0800 Chapter 18) (Reference 4), and
- NUREG-0711, *Human Factors Engineering Program Review Model* (NUREG-0711) (Reference 5)

HFE considerations are integrated into the requirements, development, and design of the Core Protection Calculator System (CPCS) modification. This is to ensure that HFE products facilitate the safe, efficient, and reliable performance of operations, maintenance, tests, inspections, and surveillance tasks.

The LTR (Attachment 4) addresses IEEE Std 603, Clause 5.14, *Human Factors Considerations*, in Section 3.5.10.7. IEEE Std 603, Clause 5.14, requires that human factors be considered at the initial and subsequent stages of the design process to assure that functions allocated can be successfully accomplished. The Operator's Module (OM) and Maintenance Test Panel (MTP) displays for the Waterford CPCS are similar to the Palo Verde Nuclear Generating Station (PVNGS) CPCS implementation. The differences are a result of Operator and Maintenance feedback catering the displays to Waterford-specific needs. The PVNGS displays were approved by the NRC and developed with input from PVNGS nuclear control room operator staff. The displays support existing operating procedures for the existing CPCS to avoid unnecessary operational changes. In some cases, the displays ease the burden of the operator by allowing the operator to see multiple indications or trends at one time.

The LTR (Attachment 4) addresses NUREG-1764 which provides NRC guidance for reviewing changes to human actions based on risk importance. A graded, risk-informed approach is used to determine the level of NRC human factors engineering review. The CPCS does not include any manual actions associated with Waterford UFSAR Chapter 15 event mitigation or event initiation, and therefore the risk level of the Human-System Interface (HSI) changes in accordance with NUREG-1764 is low.

The NUREG-0800 Chapter 18, Section III, *Acceptance Criteria*, is based on meeting the relevant requirements of select regulations. It states the following, "The regulatory guidance provided in NUREG-0711 addresses all the human factors elements of these requirements."

The following assessment addresses the review elements identified in NUREG-0711, providing evidence that human factors engineering has been integrated into the CPCS modification.

2. HFE Program Management

This change does not impact Waterford's HFE Program Management. The CPCS modification is evaluated under the established plant modification and Human Factors Evaluation processes and procedures (References 6 and 7), which include the following HFE considerations:

- Evaluating operator impacts during installation, normal operation, maintenance, and abnormal/emergency operation
- Planning and scheduling of work to minimize disruptions
- Coordinating training and procedure updates with the modification as discussed below
- Providing maintenance and operator training on the new system prior to installation
- Involving Operations and Maintenance department representatives throughout the entire modification process

The CPC/CEAC modification does not result in any changes to risk-important or credited human actions nor compromise defense-in-depth in accordance with RG 1.174:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- There is no over-reliance on programmatic activities to compensate for weaknesses in plant design.
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.

During design of the equipment, Westinghouse used Human Factors requirements as referenced in 00000-ICE-30158 Section 3.5.1 (Attachment 7). For software changes made from the reference design screens, WNA-IG-00871-GEN (Reference 9) was used to ensure NUREG-0700 (Reference 11) requirements were met. When revisions are made to Westinghouse documents, Entergy reviews and comments on these changes in accordance with fleet procedure EN-DC-149 (Reference 10). These reviews include human factors requirements.

The Engineering Change Package (ECP), developed in accordance with Entergy procedure EN-DC-115 (Reference 6), is also considering the human factors aspects of implementation. The ECP has completed the conceptual design phase, and the detailed design phase is currently in progress. The final design package currently has a scheduled completion date of early 2021. Additionally, Entergy procedure EN-DC-163 (Reference 7) ensures that all human factors aspects of the modification are understood and meet requirements and guidelines of NUREG-0700. The HFE analysis is reviewed and accepted by a Human Factors engineer and Operations.

3. Operating Experience Review

Waterford performed an extensive OE review as part of this modification. The review was accomplished using the INPO OE database, discussions/benchmarks with other utilities, and information from the system vendor. The following criteria were considered during this review:

1. Predecessor/Related Plants and Systems

The review focused on Palo Verde Nuclear Generating Station (PVNGS) with a similar Westinghouse Common Q CPC/CEAC systems:

As described in the LTR (Attachment 4), PVNGS is the reference design for the CPC/CEAC modification. The LTR describes the similarities and differences between the two designs. The Waterford project team visited PVNGS twice during the system requirements and design phase. Design, modification, installation, and operation-related OE were solicited from the PVNGS project team. This OE is documented in formal benchmarking reports tracked by LO-WLO-2018-00081 (initial Maintenance benchmark) and LO-HQNLO-2019-00086 (Engineering benchmark held in March 2020) (References 12 and 13). This OE will be incorporated into the Engineering Change.

2. Recognized Industry HFE Issues

All recognized industry HFE issues related to the Common Q flat panel display system have been documented in the Westinghouse corrective action program. There are no open issue reports for the Common Q flat panel display system. As referenced in NUREG-0711, NUREG/CR-6400, *Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience* (NUREG/CR-6400) (Reference 14), was reviewed. While there were no issues specific to the CPC/CEAC, the NUREG-6400 Section 7.1.3 issues related to Controls and Displays are applicable. For the CPC/CEAC modification:

- Operations staff provided extensive review and comments during design and development of the displays to ensure information was clear, relevant, and accessible.
- OM and MTP will both indicate when a data point value is invalid.

3. Related HSI Technology

Waterford chose the Common Q platform because it is the same platform as the CPCS reference design at PVNGS. The CPCS Common Q HSI is not required for the system to perform its automatic safety function. For these reasons, and also because of the extensive OE for the Common Q platform HSI, Waterford does not need to consider or compare other HSI technology.

4. Issues Identified by Plant Personnel

The Waterford project team includes representatives from Engineering, Operations, Maintenance, Operations Training, and Maintenance Training. Feedback is provided on the proposed system by team members using existing plant preferences and OE gathered on a PVNGS benchmarking trip.

The new Operator Module (OM) screens were designed based on the PVNGS design with input from Waterford operations personnel. The OM forms the primary graphical user interface (GUI) for the operator during normal system operation. Interviews with Operations team member highlighted difficulty assessing system status with the existing system OM, which provides the ability to only display a single point ID at one time. With the proposed OM, the Operator can choose from a number of different displays designed to support the specific operating condition or evolution in progress. Again, feedback was provided by Waterford team members to ensure the displays met Waterford requirements. Specifically, Waterford personnel provided specific point IDs to be included on the various group displays. This is an especially powerful tool for the diagnosis of core conditions during transients. The OMs also provide spatial dedication to channel specific alarms, providing quick diagnosis of system problems. These include Channel Trouble, Channel Test, CPC fail, CPC sensor failure, CEAC 1/2 fail, CEAC 1/2 sensor failure, CEAC 1/2 inoperable and CEAC 1/2 CEA Deviation.

Additionally, each channel also contains a Maintenance and Test Panel (MTP) display. This display performs all functions of the OM plus surveillance related functions. Similar to the discussion related to the OM, the proposed MTP provides different displays for the technician or operator to evaluate conditions or perform surveillance tasks. Both the OM and MTP are configured around the Common Q flat panel display system to ensure a consistent human machine interface.

5. Important Human Actions

The CPC/CEAC performs automatic safety functions. There are no important human actions performed by plant operators on the system identified in Waterford UFSAR Chapters 7 or 15.

6. Plant Modifications

An OE search using Waterford internal Paperless Condition Reporting System (PCRS) was done with a focus on human factors and digital modifications. Of note, CR-WF3-1996-1307 documented an event that identifies that audible alarms for metal and explosive detectors provided identical tones, which could be a Human Factors issue in identifying which alarm was present. While this does not translate directly to the CPC modification, the displays for OM and MTP provide distinct display changes when an alarm is present. For example, the dedicated alarms on the OM screen turn red (similar to a physical alarm bulb on the main control panel). This allows the operator to quickly diagnose the issue and perform the required actions. Additionally, the plant annunciator system lights the window for the annunciated alarm. The plant annunciator functionality and response remain unchanged from the existing process. Additionally, CR-WF3-2009-

4167 identifies color banding discrepancies between plant documentation and installed plant indicators. While this isn't directly applicable to the displays under the proposed system, the displays provide color-coded information and trends, which allow the operator to easily diagnose the current plant conditions. Any changes from the approved referenced design, made to software for the Waterford displays, was designed using WNA-IG-00871-GEN. This document ensures that any changes to the Common Q Display Software complies with the applicable human factor design principles of NUREG-0700.

4. Functional Requirements Analysis and Function Allocation

The CPCS is an automatic trip system credited for events summarized in LTR Section 3.3 (Attachment 4). These design functions are unchanged as a result of this license amendment. The CPCS will continue to generate an automatic Low DNBR and High LPD trip signals to the PPS for the credited events without required operator action. The function of coincidence logic for these trip signals and initiating reactor trip breakers opening is still allocated to the PPS. The CPC/CEAC modification is not adding or modifying CPCS design basis functions except for adding new pre-trip alarms for the auxiliary trips. Therefore, there is no change to the allocation between personnel and plant systems of functions important to safety. There is no increase in operations personnel task demands.

The Waterford Probabilistic Risk Assessment Human Reliability Analysis (PRA/HRA) was reviewed. The CPC/CEAC has no impacts to important risk significant human actions. The only impact is to the operator action to manually trip the reactor if the automatic trip signal does not work. Given the reliability of the automatic function, the manual action is not significant in the PRA results.

There are no CPCS-related operator functions credited in the Waterford UFSAR to prevent or mitigate an accident. No important human actions performed on the CPC/CEAC system are identified in Waterford UFSAR Chapters 7 or 15. Because no important human actions are added, changed, or deleted, there are no changes to the plant's functional requirements analysis or function allocation.

5. Task Analysis

As discussed above, no important human actions are performed on the CPC/CEAC system. Indications from the CPC/CEAC system provide input to important human actions identified in the Waterford PRA/HRA, namely, the manual action to scram the reactor. The input for this action is based on input from EPRI report TR-100259 which uses industry standard data for PWRs. This modification will not impact the use of this input and therefore will not impact the HRA.

Additional human actions selected for analysis include those from standard operating procedures that have existing task analyses in the Waterford Operations training program. The following additional human actions are selected for task analysis:

- Place a CPC Channel in Bypass
- Change addressable constants
- Display point IDs
- Remove a CEAC from service
- Respond to main control room annunciator

The CPCS is an automatic system; so, no new important human actions are being added by this proposed modification. Each task identified will be performed in a similar manner to the existing system with the primary changes being to the interface of the OM, MTP and CEAPD. Of note, the proposed Common Q system can display to the operator multiple points or trends at one time whereas the current system can only present one point at a time. Any other changes will be handled using formal training and procedure updates. The specific training actions are identified in the Training Program Development section. Procedure updates have direct input from Maintenance and Operations representatives, and all changes will be reviewed by those representatives as a part of the Engineering Change process. More details of the first four tasks are provided in 00000-ICE-30158 (Attachment 7) and WNA-DS-04517-CWTR3 (Attachment 8), and response to main control room annunciators will occur in accordance with site annunciator response procedures. In summary, there are no new tasks or changes to tasks that will impose high demands on personnel, no changes to existing tasks that result in a task significantly different from existing tasks, and no new tasks or changes to existing tasks that would inhibit personnel from safely performing maintenance, tests, inspections and surveillances.

6. Staffing and Qualifications

Because there are minimal changes to the task analysis, there is no change to required staffing levels or personnel qualifications. There is no change to the Emergency Preparedness program and no 10CFR50.54q evaluation is required. This change does not impact staffing or qualification with the assumption that operator training on the new digital platform is completed prior to installation.

7. Treatment of Important Human Actions

The CPCS will generate an automatic Low DNBR and High LPD trip signal to the PPS for UFSAR Chapter 15 credited events, and no operator action is required to accomplish the safety functions. No risk-important human actions associated with the CPC/CEAC system are modeled in the PRA/HRA and the impact due to modified HSI is considered negligible. Indications from the CPC/CEAC system provide input to important human actions identified in the Waterford PRA/HRA, namely, the manual action to scram the reactor. The input for this action is based on input from EPRI report TR-100259 (Reference 15) which uses industry standard data for PWRs. This modification will not impact the use of this input and therefore will not impact the HRA.

8. Human-System Interface Design

The HSI for the CPC/CEAC system consists of a mixture of display screens and traditional lights, indicators, recorders, and annunciators. The HSI does not perform any automatic safety functions. The CPC/CEACS system provides an automatic safety function, and operator actions are primarily limited to bypassing channels, acknowledging alarms, and selecting displays. There are no new functions performed by the operators.

The human machine interface with the CPC channel is primarily implemented by one of three means:

- Operator's Module (OM) located on the main control board (one per channel)
 - The OM is the primary means by which the operator communicates with the CPC and associated CEACs during normal operation.
 - The OM allows the following functions to be performed:
 - Monitor operator-selectable CPC and CEAC point IDs
 - Change Addressable Constants under key-switch control
 - Perform an Operating Bypass of the CPC channel when power level is below the bypass permissive setpoint under key-switch control
 - Monitor channel alarm conditions and perform limited diagnosis
 - Print OM display pages via a "Printscreen" icon
- Maintenance and Test Panel (MTP) located on at the CPC cabinet (one per channel)
 - The MTP is used in the equipment cabinet for maintenance and test functions.
 - The MTP has the same displays and function as the OM in the normal mode of operation.
 - Additional MTP functions include:
 - Provides fiber optically isolated data link to Plant Monitoring Computer
 - Provides for periodic surveillance testing
 - Provides CEA position-related information and cross channel comparison data to CEA Position Display via fiber optically isolated data link
 - Performs online monitoring of its associated CPC/CEAC/CEA Position Processors
 - Provides Maintenance PC functions, including downloading revised CPC channel software (subject to Software Load Enable interlock) and interrogating the CPC channel error buffers
 - In addition, the MTP supports an Inter-range Instrumentation Group (IRIG) B time synchronization input, which is used to provide a time of day stamp to the OM and MTP Printscreen function, System Event List and other displays.
- CEA Position Display (CEAPD) located on the main control board (one total)
 - CEAPD displays CEA position and perform cross channel comparisons of data received from the four CPC channels
 - CEAPD is non-1E and is not directly addressed in the LAR. This device will be evaluated under the Engineering Change through the 50.59 process.

In addition, the OM, MTP and CEAPD are supplemented by the plant annunciator system. All changes to the plant annunciator system will be captured in the engineering change package. All changes will be evaluated under EN-DC-115 and EN-DC-163 as described in previous sections. One particular change of note is that reflash capability is being added for certain annunciators. In the existing system, there are only two total CEACs. In the Common Q system, there are two CEACs per channel. Therefore, reflash capability will be added to the CEAC associated annunciators to ensure the operator can easily distinguish between one CEAC issue and multiple issues. The OMs will also aid in this diagnosis with the previously discussed spatially dedicated alarms.

9. Procedure Development

Changes to procedures are developed in accordance with Entergy's existing procedure development program, which is required by the Entergy Quality Assurance Program Manual (QAPM), described in the Waterford UFSAR, Section 13.3, "Written Procedures," and implemented by Nuclear Management Model (NMM) procedure EN-AD-101, NMM Procedure Process (Reference 19). This program meets the criteria of NUREG-0711, including procedure bases, the procedure writer's guide, procedure elements, procedure maintenance, and personnel access and use of procedures.

Integrated Operating procedures will be updated to incorporate startup testing activities associated with the CPC/CEAC system.

The CPC/CEAC operating and abnormal operating procedures will be updated to reflect changes to the design of the CPC/CEAC system (increasing CEACs from 2 to 8, etc.) and changes to operator interfaces.

Maintenance procedures will be updated with maintenance requirements and procedures for the CPC/CEAC equipment.

Surveillance procedures will be updated to perform TS required testing.

Alarm Response procedures are impacted by nomenclature changes to the overhead annunciator windows and by addition of more detailed plant computer alarm points. The annunciator changes also affect other procedures which reference the annunciators. There are no new Operator actions required to support alarm responses. Operations team members participating on the modification team will ensure appropriate Operations procedures are updated.

No Emergency Operating Procedures are affected by this modification.

Modified procedures for the CPC/CEAC system will be validated during testing prior to installation of the system. Impacted procedures that involve interfaces to other plant systems will receive tabletop reviews prior to installation of the CPC/CEAC system.

10. Training Program Development

Training will be conducted in accordance with the requirements of the Entergy QAPM and Waterford's INPO-accredited training program, as described in UFSAR Section 13.2, "Training," and implemented by NMM Policy EN-PL-101, Entergy Nuclear Organization and Functional Structure (Reference 17), and NMM Procedure EN-TQ-212, Conduct of Training and Qualification (Reference 18). The training program is formulated to provide an organization qualified to operate, maintain and support the facilities in a safe and reliable manner. The training program has been developed from a systematic analysis of job requirements using job and task analysis where available. This approach is consistent with Nuclear Regulatory Commission (NRC) regulations and the Institute of Nuclear Power Operations (INPO) recommendations for accreditation of training programs.

Waterford will utilize a systematic approach to training in accordance with EN-TQ-201, Systematic Approach to Training Process (Reference 20), to develop Operations and Maintenance training plans specific to the CPC/CEAC upgrade. These plans will address the changes required to training documentation, identify which personnel will be trained, identify what training is required and the objectives of that training, and include a schedule for both pre- and post-installation training.

11. Human Factors Verification and Validation

NUREG-0711 evaluations are used to confirm that a final design conforms to HFE design principles and that it enables personnel to successfully and safely perform their tasks to achieve operational goals. The three evaluation types spelled out in NUREG-0711 include:

- HSI Task Support Verification - an evaluation to verify that the HSI supports personnel task requirements as defined by task analyses.
- HFE Design Verification - an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines such as those provided in NUREG-0700.
- Integrated System Validation - an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant.

1. HSI Task Support Verification

This verification ensures that the HSI provides all alarms, information, and control capabilities required for personnel tasks. The upgrade to the CPC/CEAC does not impact reactor operating parameters or the functional requirements of the system. The replacement equipment continues to provide information and trip outputs to the Plant Protection System (PPS) channel under specified conditions. As such, the operator actions remain unchanged when upgrading to the Westinghouse Common Q platform, in that the same actions/responses occur with data received from the new digital system as with the existing digital system that is being replaced. Note that changing the number of CEACS from two to eight eliminated a time-critical operator action when both CEACS are inoperable. Because there are no significant changes to operator actions or

functions, no new task analyses were performed. Hence, with no operator actions changing, or new task analyses performed, HSI Task Support Verification is not required for the upgrade to the Westinghouse Common Q platform.

2. HFE Design Verification

This verification ensures that the characteristics of the HSI and the environment in which it is used conform to HFE guidelines. The OM and MTP of the reference CPCS design (PVNGS) was developed in conjunction with the plant operators to ensure the design supported their current tasks in the control room. The reference design has been in operation at PVNGS for over 15 years. The changes, from the Palo Verde reference design, to the OM and MTP for Waterford also involve plant operations personnel in support of their control room tasks. Any software changes for the Waterford OM and MTP will follow the Westinghouse human factors engineering guideline, WNA-IG-00871-GEN, which is based on NUREG-0700.

The HFE review included in the LTR as well as the HFE review of operator panel changes above ensures that the requirements of NUREG-0700 are met.

3. Integrated System Validation

Integrated system validation is the process by which an integrated system design (i.e., hardware, software, and personnel elements) is evaluated using performance-based tests to determine whether it acceptably supports safe operation of the plant.

Waterford will confirm the LTR's analysis of minimal operator impact during the Factory Acceptance Test (FAT) using the new CPC/CEAC hardware. In addition, a simulated implementation of the plant design will be installed to the Waterford control room training simulator. Testing of the simulator implementation will be conducted prior to its use in operator training. Testing for the replacement simulated systems will be conducted in accordance with ANSI Standard ANS-3.5-2009, Nuclear Power Plant Simulators for Use in Operator Training and Examination, endorsed by NRC Regulatory Guide 1.149, Revision 4, Nuclear Power Plant Simulation Facilities for Use in Operator Training and Title 10, Code of Federal Regulations, Part 55.46 (10CFR55), Simulation Facilities.

Operations will conduct a Training Needs Analysis to determine differences in critical tasks when comparing the retired and replacement CPC/CEAC systems. Training will be conducted to address results of this analysis within the six month period leading to the outage installing the replacement system. Operations Training segments may also be continued during the outage cycle as well as Just In Time (JIT) training just prior to plant startup operations. A variety of Operations procedures will be utilized during this training to identify potential impacts using the simulator prior to reference plant installation. The installation, testing, and use of the simulator for operator training will be performed prior to installation of the modification to the reference plant under provisions of Training Needs Assessment (TNA) described within ANSI Standard ANS-3.5-2009, Nuclear Power Plant Simulators for Use in Operator Training and Examination.

NUREG-0711, Section 11.4.3, "Integrated System Validation," states the following:

For the case of plant modifications, the applicability and scope of integrated system validation may vary. An integrated system validation should be reviewed for all modifications that may (1) change personnel tasks; (2) change tasks demands, such as changing task dynamics, complexity, or workload; or (3) interact with or affect HSIs and procedures in ways that may degrade performance. Integrated system validation may not be needed when a modification results in minor changes to personnel tasks such that they may reasonably be expected to have little or no overall effect on workload and the likelihood of error.

For the upgrade to the Westinghouse Common Q platform, an Integrated System Validation is not warranted as there is no change in important human actions for the replacement hardware. This modification will not change task dynamics, complexity or workload. Procedural and HSI changes will be handled by training programs developed by the previously mentioned training actions. Additionally, team reviewers will provide comments and ensure procedural impacts are adequately captured. Specifically, the HSI is designed such that the replacement CPC/CEAC provides the same information as the legacy system such that it is a reasonable expectation that there will be little or no overall effect on the operations staff with regards to workload or the likelihood of an error.

12. Design Implementation

Installation activities will occur during a refueling outage. The Engineering Change will be approved and planned with equipment received onsite months prior to the refueling outage in accordance with site milestones. The equipment will be stored outside the plant in a cyber and security controlled environment for storage and testing. There will be no temporary or interim configuration over multiple cycles. In addition, procedures will not require temporary revisions.

Prior to reactor shutdown for the applicable refueling outage, a CPC single channel with an I/O Simulator will be available for Simulator personnel to allow Operators the ability to train on the new interface. Once shutdown, the Simulator will begin implementation to directly reflect the main control room design. In parallel, implementation will begin in the main control room. Return to service of the plant equipment will not occur until Simulator installation is complete in accordance with the approved design of the Engineering Change to ensure Operators can obtain all required hands-on training before startup. This ensures that personnel will be familiar with the new system interfaces and not impact the way the plant is operated.

Since detailed implementation instructions are not yet developed, a high-level overview of implementation is provided herein. Legacy equipment will be removed from CPC cabinets using the applicable procedures and Engineering Change instructions. In addition, the legacy displays will be removed from the main control room cabinets, including Operator Modules and CEA Position Display System. Applicable modifications will be made to the auxiliary protection cabinets as identified in the Engineering Change, and new conduit/cable routing will occur where necessary. In addition, equipment will be added to the computer room as specified in the Engineering Change. Installation of new Common Q equipment will be installed in the auxiliary protection cabinets and control panels. The new Operator Modules will also be installed, including the specified peripherals. Final terminations and verifications and validations will

occur in accordance with Engineering Change instructions. Any identified annunciator changes in the Engineering Change will also be implemented. After all implementation is complete, the post-modification test will verify proper function of the system. The CPCS will be declared operable when all testing tasks have been completed satisfactorily in accordance with the test plan, governed by a qualified test engineer. All procedure updates and training must be complete for return to service.

13. Human Performance Monitoring

NUREG-0711 identifies that, *"A human performance monitoring strategy will help to provide reasonable assurance that the confidence developed by the completion of the integrated system validation is maintained over time."*

As identified in a previous section, with no changes being made to any important human actions with the installation of this replacement system, no Integrated System Validation is warranted. Since the system provides automatic functions (e.g., low DNBR trip, high LPD trip), the same as the existing CPC/CEAC systems, there are no changes to required operator actions. Therefore, there is no impact to Waterford's existing Human Performance Monitoring Program.

14. References

1. U.S. NRC Digital Instrumentation and Control Interim Staff Guidance-(ISG)-06, *Licensing Process*, Revision 2
2. IEEE Standard 603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*
3. NUREG-1764, *Guidance for the Review of Changes to Human Actions*, Revision 1
4. NUREG-0800 Chapter 18, *Standard Review Plan Human Factors Engineering*, Revision 3
5. NUREG-0711, *Human Factors Engineering Program Review Model*, Revision 3
6. NMM Procedure EN-DC-115, *Engineering Change Process*
7. NMM Procedure EN-DC-163, *Human Factors Evaluation*
8. Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*
9. *Human Factors Engineering Guideline for the Common Q Display System*, WNA-IG-00871-GEN, Westinghouse Electric Company LLC
10. EN-DC-149, *Acceptance of Vendor Documents*
11. NUREG-0700, *Human-System Interface Design Review Guidelines*, Revision 2
12. LO-HQNLO-2018-00081, CPCS Benchmarking Report
13. LO-HQNLO-2019-00086, CPCS Benchmarking Report
14. NUREG/CR-6400, *Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience*

15. EPRI report TR-100259, An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, June 1992
16. Entergy Quality Assurance Program Manual (QAPM)
17. NMM Policy EN-PL-101, *Entergy Nuclear Organization and Functional Structure*
18. NMM Procedure EN-TQ-212, *Conduct of Training and Qualification*
19. NMM Procedure EN-AD-101, *NMM Procedure Process*
20. NMM Procedure EN-TQ-201, *Systematic Approach to Training Process*

Enclosure, Attachment 14

W3F1-2020-0040

DRAFT

CPC Replacement Project Vendor Oversight Plan (VOP) Summary

1. Background

DI&C-ISG-06 Section C.2.2 provides Licensee Prerequisites for use of the Alternate Review Process (ARP) (Reference 7). In Section C.2.2.1, DI&C-ISG-06 describes that to use the ARP, the LAR should provide a description of the licensee's Vendor Oversight Plan (VOP). Section C.2.2.1 says that the LAR should include:

A description of the licensee's Vendor Oversight Plan. The plan, when executed, can be used to ensure that the vendor: (1) executes the project consistent with the LAR, and (2) uses an adequate software QA program. The Vendor Oversight Plan, when executed, helps ensure that the vendor will meet both the process and the technical regulatory requirements. Vendor oversight is a series of licensee interactions with the vendor and progresses throughout the entire system development life cycle. The plan should address the intended interactions among the vendor's design, test, verification and validation (V&V), and QA organizations.

The VOP is an important element of the ARP. Since the LAR approval is requested earlier in the project lifecycle than for the other DI&C-ISG-06 review processes (i.e. Tier 1, 2 or 3), the Staff needs to understand how the licensee intends to ensure that the vendor produces high quality software and system.

The Waterford Core Protection Calculator (CPC) System (CPCS) modification developed a VOP to ensure that Westinghouse executes the project consistent with:

- Entergy procurement documents (Reference 1)
- Westinghouse Electric Company (Westinghouse) Software Program Manual (SPM) and Westinghouse platform-related documentation, which have been NRC-approved as described in LTR Section 6.1 (LAR Attachment 4)
- Project description consistent with the LAR

2. Vendor Oversight Plan (VOP) Scope

This scope of the VOP is for the Westinghouse scope of the CPCS Replacement Project. The Westinghouse scope includes the hardware, software, design documentation, and licensing documentation. The VOP does not cover vendor oversight of the Architect Engineer (A/E) performing the modification process activities. For Waterford, the A/E is typically referred to as the Engineer of Choice (EOC) in the project documents. Waterford vendor oversight of the A/E is performed by Entergy engineering procedures and owner's acceptance review separate from this VOP (Reference 19).

Stakeholders identified in Section 5 will participate in vendor oversight activities to the extent that vendor activities can affect their needs. The level of vendor oversight follows a graded approach, based on project and technical risk factors, which are described in Section 6. All levels of the graded approach will include specifically defined performance measures and acceptance criteria which are described in Section 7. The various levels of graded oversight are described in Section 8. The site Corrective Action Process (CAP) will be used to document and ensure resolution of issues/problems. This is described in Section 9. Finally, oversight results will be documented as described in Section 10.

Vendor oversight activities include:

- Conducting Vendor oversight audits
- Conducting Quality Surveillances of vendor activities under Waterford Quality Assurance (QA) program including activities for the CPCS Replacement Project Critical Procurement Plan (CPP)
- Providing input to and review/confirmation of specific vendor activities and related information items
- Observing or witnessing specific vendor activities
- Participating directly in specific vendor activities
- Coordinating multi-disciplined interactions between various stakeholders
- Communicating status, schedule, and results of oversight activities through daily or weekly Waterford/Westinghouse Project Management team teleconferences, Waterford/Westinghouse Engineering team teleconferences, Waterford/Westinghouse Licensing team teleconferences
- Capturing issues in Waterford/Westinghouse corrective action programs
- Elevating emerging risks and issues (if necessary) to decision makers with higher authority
- Updating the VOP (if necessary) based on emerging results
- Conducting monthly Risk Review Meetings

The VOP is an umbrella document covering the range of activities in which Entergy is engaged to perform effective vendor oversight. Input for the VOP is drawn from:

- Procurement specification and other Westinghouse contract documentation,
- Project-specific specifications,
- NRC DI&C-ISG-06 Rev. 2 Licensing Process,
- WCAP-16096 Common Qualified Platform Software Program Manual (Reference 9),
- Entergy design engineering (Reference 18), project management (Reference 12), supply chain (Reference 13) and Quality Assurance (Reference 4) processes,
- EPRI Digital Engineering Guide (DEG) (Reference 3) and
- EPRI Handbook for Evaluating Critical Digital Equipment and Systems (Reference 8)

3. Project Organization and Roles (Stakeholders)

The following stakeholder roles and responsibilities are described in the VOP.

Entergy Project Team

- Project Manager
- Assistant Project Manager
- Quality Assurance (QA) Representative
- Lead Responsible Engineer
- Digital or I&C Engineers
- Cyber Security Engineer
- System Engineer
- Lead Licensing Engineer
- Human Factors Engineer
- Maintenance Representative
- Operations Representative
- Simulator Representative
- Various Test Coordinator/Engineers

Westinghouse Project Team

- Project Manager
- Quality Manager
- Design Engineers
- Cyber Security Engineer
- Simulator Project Representative
- Test Engineers and Software V&V Engineers
- CPCS Product Manager
- CPCS Technical Advisor
- CPCS Technical Lead
- CPCS Licensing lead

4. Development and Assessment of Potential Project and Technical Risk Factors

Potential Project and Technical Risk Factors were considered in accordance with EPRI DEG, Table 5-1 (Reference 3). The following topics were used to assess risk. Note that this list is not all-inclusive.

- Schedule
- Technical Staff
- Conceptual Design
- Hazards
- Procurement
- Human Factors Engineering
- Data Communications
- Cyber Security
- Plant Integration Design
- Testing
- Configuration Management
- Training

Risks were categorized as Low, Moderate, and High. Based on the risk categorization, vendor oversight activities have been prioritized.

Per Entergy procedure EN-PM-100 (Reference 13), a Project Risk Register has been developed. The Project Risk Register is reviewed and archived monthly to continuously assess risk throughout the course of the project, update as necessary, and work to resolve risks.

5. Determine Performance Measures and Acceptance Criteria

Performance measures and their acceptance criteria are included in the VOP. The scope of vendor oversight is expected to evolve during the project. Project-specific performance measures that warrant vendor oversight are updated as this list changes.

The performance measures are divided into three categories with acceptance criteria provided for each:

- Critical Characteristics,
- Design Artifacts, and
- Programmatic Elements.

1. Critical Characteristics

The Critical Characteristics are those important design, material, and performance characteristics of a system that, once verified, will provide reasonable assurance that the system will perform its intended critical functions. Note that the critical characteristics are drawn, in part, from the project's Critical Procurement Plan (Reference 6) and EPRI Topical Report 1011710 (Reference 8).

The critical characteristics are divided into the following categories:

- Physical,
- Performance,
- Environmental, and
- Cyber

2. Design Artifacts

The Design Artifacts are the set of design output documents described in the Westinghouse procurement documentation. These documents are generated in accordance with the Westinghouse SPM, which is NRC-approved. Examples of design artifacts include: System Requirements Specification (SyRS), Software Requirements Specification (SRS), Availability Analysis, Licensing Technical Report (LTR).

Waterford engineering procedures and processes provide the review framework for these design documents. Entergy procedure EN-DC-149, *Acceptance of Vendor Documents*, provides the process to be used to control the receipt, distribution, review, and revision of technical vendor documents. This process:

- Ensures review by appropriate departments and disciplines,
- Ensures that affected documents, programs, and data bases are updated,
- Ensures that the vendor is in compliance with the design specification and purchase order,
- Ensures the document is consistent with plant licensing and design basis, and
- Ensures technical review is performed based on the risk ranking of the project documents.

In addition, Waterford is utilizing the independent third-party review (ITPR) review process for critical design artifacts (e.g., SyRS, SRS, LTR, etc.). This independent review, by industry subject matter experts, allows:

- Entergy to provide additional, independent oversight of the Westinghouse products
- Entergy to receive independent feedback on the quality of their vendor oversight of Westinghouse design artifacts

3. Programmatic Elements

The Programmatic Elements include the vendor's programs and processes relevant to the project. The elements of the system lifecycle are described in the Westinghouse SPM (Reference 9). The SPM describes the requirements for the software design and development process including the software/hardware interface. The SPM also describes the requirements for the use of software in Common Q systems.

The following SPM plans are developed:

- *Software Safety Plan*, which identifies the processes that, will reasonably assure that safety-critical software does not have hazards that could jeopardize the health and safety of the public.
- *Software Quality Assurance Plan (SQAP)*, which describes the process and practice of developing and using software. The SQAP addresses standards, conventions, reviews, exception reporting and other software quality issues.
- *Software Verification and Validation Plan (SVVP)*, which describes the method of assuring correctness of the software.
- *Software Configuration Management Plan (SCMP)*, which describes the method of maintaining the software in an identifiable state at all times.
- *Software Test Plan*, which describes the method for testing software.

Some of these SPM plans will have project-specific instances (i.e., SVVP, SCMP, and Software Test Plan). These project-specific plans will be evaluated to ensure they are developed in accordance with the SPM.

The SPM describes the software lifecycle phases as:

- Concept
- Requirements Analysis
- Design
- Implementation or Coding
- Test
- Installation and Checkout
- Operation and Maintenance
- Retirement

Reviews will be performed of verification and validation (V&V) for each applicable lifecycle phase for each plan through Test. The Installation and Checkout, Operations and Maintenance, and Retirement phases are Entergy responsibility and not included in scope of VOP. However, per SPM PSAI #4, Entergy will review the Westinghouse Technical Manual, provided in accordance with Reference 1, to verify it satisfies the requirements for the Software Operations Plan per the Common Q SPM.

The VOP provides acceptance criteria related to the following important system development topics. Example Acceptance criteria are provided in sub-bullets below:

- Quality Assurance
 - Ensure that Westinghouse complies with the requirements of Appendix B to 10 CFR Part 50 and 10 CFR Part 21 to control the quality of safety-related materials, equipment, and services,
 - Ensure the Software Quality Assurance (SQA) program in accordance with the SPM is effective in controlling the software development process to assure quality, and meets the commitments described in the LAR for SQA.

- Configuration Management
 - Ensure that the Westinghouse Configuration Management Release Reports identifies, names, and describes the documented physical and functional characteristics of the code, specifications, design, and data elements to be controlled for the project. Verify that Westinghouse follows the configuration management process in the NRC-approved Common Q SPM.
- Software Verification and Validation (V&V)
 - Verify that Westinghouse follows the V&V requirements in the NRC-approved Common Q SPM. The description of the software V&V processes will address the following:
 - V&V organization responsibilities,
 - V&V processes, activities, and tasks,
 - V&V reporting,
 - V&V administrative controls for anomaly resolution and reporting, task iteration policy, and deviation policy, and
 - V&V test documentation.
- Software Safety
 - Verify that documentation exists to show that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation will show that:
 - System safety requirements have been adequately addressed for each activity group,
 - No new hazards have been introduced; that the software or logic requirements, design elements, and code elements that can affect safety have been identified, and
 - All other software or logic requirements, design, and code elements will not adversely affect safety.
- Secure Development Environment
 - Verify that the Westinghouse has a development environment that complies with the requirements the NRC-approved Common Q SPM, Section 12. SDE documentation exists for key attributes including:
 - Having a method for identifying the origin of critical components and ensuring that all critical asset components are compliant with the supplier's security requirements and free of counterfeits.
- Cyber Security
 - Verify that all known cyber security vulnerabilities of the operating system, vendor's software, firmware, or hardware is remediated or a description of why the vulnerability is not a concern for the system as installed is supplied.
- Software Lifecycle Processes
 - Verify that Westinghouse plans and performs application software lifecycle activities in a traceable and orderly manner in accordance with the SPM. The VOP evaluates the following lifecycle areas:

- Software Requirements – Ensure that project requirements are examined, understandable, and unambiguous. Reference is made to applicable drawings, specifications, codes, standards, regulations, procedures or instructions. Verify that security requirements are specified commensurate with the risk from unauthorized access or use. The requirements traceability shows where in the software or application logic design, the required action is being performed as well as providing traceability back to the system requirements that generated these software requirements.
- Software Design – Verify that the architecture is sufficiently detailed to allow for understanding the operation, flow of data, and the deterministic nature of the software or logic. Verify the technical adequacy of the design and ensure internal completeness, consistency, clarity, and correctness of the software design. In addition, the software or logic design specification will be reviewed to determine that it is understandable and traceable to the software requirements. While the software design will consider the operating environment, measures to mitigate the consequences of problems will also be an integral part of the design.
- Hardware Requirements
 - Verify the hardware is designed and manufactured to meet the physical and functional requirements described in the procurement specification, SyRS(s), and design documents and drawings.
- Plant Specific Action Items (PSAIs)
 - Ensure that PSAIs identified in the Topical Reports and further discussed in the Licensing Technical Report (LTR), are addressed as described in the LAR.

Entergy engineering procedures and processes provide the review framework for these design documents. Entergy procedure EN-DC-149, Acceptance of Vendor Documents, provides the process to be used to control the receipt, distribution, review, and revision of technical vendor documents (Reference 18). This process:

- Ensures review by appropriate departments and disciplines
- Ensures that affected documents, programs, and data bases are updated
- Ensures that the vendor is in compliance with the design specification and purchase order
- Ensures the document is consistent with plant licensing and design basis
- Ensures technical review is performed based on the risk ranking of the project documents

6. Implement Appropriate Oversight Methods

Vendor oversight is based on risk factors, of which performance measures are an attribute. Therefore, the amount and specific focus of the oversight activities vary as the project evolves. Oversight of Westinghouse occurs based on the various Risk Factors (Section 5) and

Performance Measures (Section 6). Waterford may adjust the risk factors as the project progresses.

LOW RISK factors indicate continued use of routine oversight methods, such as:

- Periodic Audits
- Periodic Surveillances
- Routine Design Reviews
- Routine Project Meetings

MEDIUM RISK factors indicate a need for supplemental oversight methods, such as:

- Increased surveillance frequency
- Interim design reviews
- Challenge boards
- Increased frequency of project meetings

HIGH RISK factors indicate a need for extraordinary oversight methods, such as:

- Placement of oversight staff inside the vendor's organization
- Management intervention
- Stop work order and implement recovery plan

7. Perform Corrective Actions

Condition reports for entry into the corrective action program document vendor performance or quality that is in question. The following conditions, as a minimum, trigger a condition report:

- Westinghouse noncompliance with the Westinghouse's own quality program, software processes, or hardware processes
- Nuclear safety may be adversely impacted if the digital item is installed and operated
- Unit generation may be adversely impacted if the digital item is installed and operated
- Digital item quality simply cannot be assured
- Digital item quality cannot be assured without a significant project delay
- Digital item quality is not assured, and identical or similar digital items are already installed in the facility, in other applications, and are considered operable or available
- Westinghouse has been awarded other Entergy POs or contracts to deliver other digital items, and performance measures indicate that the quality of the other items may not be assured

If the Waterford project team identifies performance issues, oversight would be enhanced to include:

- Periodic meetings to discuss and resolve issues
- Additional technical reviews or surveillances
- Management Intervention
- Stop work and implement recovery plan

8. Documentation

Per the EPRI DEG, for high consequence and high technology configurability, vendor oversight must be documented. Through DI&C-ISG-06 and public interactions, the NRC has expressed an interest in vendor oversight. Documentation would help provide assurance to the NRC, during an inspection, that Waterford has been conducting oversight of Westinghouse through the system development lifecycle.

Vendor oversight can be documented through multiple methods:

- Formal audit plans/reports
- Comments/feedback on design artifacts through the owner acceptance engineering process
- Teleconference notes
- Emails
- Written correspondence between Waterford and Westinghouse

Note that documentation format may vary but the content will provide the vendor oversight level of detail and corrective actions (if any).

9. Attachments

The VOP includes attachments for:

- CPCS Replacement Project Division of Responsibility
- CPCS Replacement Project Organization Chart
 - Entergy CPCS Project Organization Chart
 - Westinghouse CPCS Project Organization Chart

10. References

1. Entergy procurement documents
2. American Society of Mechanical Engineers (ASME), NQA-1:2015, Quality Assurance Requirements for Nuclear Facility Applications
3. EPRI Technical Report 3002011816, Digital Engineering Guide (DEG)
4. EN-QV-108, QA Surveillance Process
5. SPEC-18-00005-W, Rev 0
6. CPCS Replacement Project Critical Procurement Project (CPP), CPP-WF3-2019-002 (WTWF3-2019-00236)
7. NRC DI&C-ISG-06, Licensing Process, Revision 2
8. EPRI Topical Report 1011710, Handbook for Evaluating Critical Digital Equipment and Systems
9. WCAP-16096, Westinghouse Software Program Manual (SPM) for Common Q™ Systems
10. WCAP-16097, Westinghouse Common Qualified Platform Topical Report
11. CWTR3-19-21 R2, Attachment 1, Compliance Matrix
12. NMM procedure EN-PM-100, Conduct of Project Management

13. NMM procedure EN-MP-100, Critical Procurements
14. IEEE Std. 1028, Standard for Software Requirements and Audits
15. IEEE Std. 344-1975, Seismic Qualification of Equipment for Nuclear Power Generating Stations
16. RG 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Revision 3
17. CWTR3-19-23, Westinghouse Cyber Security Compliance Matrix
18. NMM procedure EN-DC-149, Acceptance of Vendor Documents
19. NMM procedure EN-DC-115, Engineering Change Process
20. NMM procedure EN-DC-163, Human Factors Evaluation

Enclosure, Attachment 15

W3F1-2020-0040

DRAFT
List of Regulatory Commitments

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

Commitment	Type (check one)		Scheduled Completion Date
	One-Time Action	Continuing Compliance	
Entergy will evaluate Waterford CPCS Replacement Project Site Acceptance Test (SAT) and Installation Test Plans using the software process testing characteristics described in BTP 7-14 Section B.3.2.4. This is Plant-specific Action Item #5 per WCAP-16097, <i>Common Qualified Platform Topical Report</i> .	<input checked="" type="checkbox"/>	<input type="checkbox"/>	