

December 29, 2010

Public/Redacted Version of the non-concurrence package – (a) Dissenting View on the AP1000 Instrumentation and Controls Designs Certification Amendment Advanced Final Safety Evaluation Report With Respect to Evaluation and Acceptance Methods Used for Demonstrating Conformance to Commission Regulations and (b) Staff Response to Dissenting View.

Redactions are based upon staff acceptance of Westinghouse request for withholding of proprietary information, submitted in a December 28, 2010 letter to NRC.

NON-CONCURRENCE PROCESS

SECTION A - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL

TITLE OF DOCUMENT

Advanced Final Safety Evaluation Report for AP1000 Design Cert Amendment - Digital I&C

DOCUMENT SPONSOR

Terry Jackson

NAME OF NON-CONCURRING INDIVIDUAL

Kenneth D. Mott

ADAMS ACCESSION NO.

SPONSOR PHONE NO.

301-415-7313

PHONE NO.

301-415-3242

☒ DOCUMENT AUTHOR

☒ DOCUMENT CONTRIBUTOR

DOCUMENT REVIEWER

☐ ON CONCURRENCE

TITLE

Electrical Engineer / Reactor Technical Reviewer

ORGANIZATION

NRO/DE/ICE/Branch 1

REASONS FOR NON-CONCURRENCE

The staff's advanced final safety evaluation report (AFSER) safety findings and conclusions for several of the the digital instrumentation and control (DI&C) design changes for the Revision 18, AP1000, design certification amendments (DCAs), do not provide reasonable assurance that the Revision 18, AP1000 DCA DI&C design changes, conform with the Commission's regulations.

The AP1000 DI&C Revision 18 design changes include changes made to the Anticipated Transient Without Scram mitigation initiations and the diverse actuation system (DAS) functionality and reliability. The protective functions associated with these systems are very important to the successful mitigation of postulated plant accident conditions.

NRC regulations, such as 10CFR50.62, require, among other things, that ATWS equipment must be designed to perform its function in a reliable manner to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS and that information sufficient to demonstrate the the adequacy of the ATWS equipment must be submitted to the Commission. NRC regulations, such as GDC 22, require, among other things, that diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

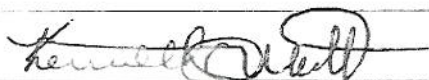
The NRC staff's AFSEr review did not consider appropriate analysis methods when making a reasoable assurance finding. Therefore, NRC staff's review and acceptance of the AP1000 DCA DI&C design chan ges does not demonstrate compliance with the applicable requirements.

Details of the basis for this position are described in the attached position papers:

Enclosure 1 (ADAMS Accession# ML_____)

☐ CONTINUED IN SECTION D

SIGNATURE




DATE

12-17-10

SUBMIT FORM TO DOCUMENT SPONSOR AND COPY TO YOUR IMMEDIATE SUPERVISOR AND
DIFFERING VIEWS PROGRAM MANAGER

**Dissenting View on the AP1000 Instrumentation
and Controls Design Certification Amendment
Advanced Final Safety Evaluation Report With
Respect to Evaluation and Acceptance Methods
used for Demonstrating Conformance to
Commission Regulations**

Signature: 

Kenneth D. Mott
Instrumentation and Controls Branch 1
Division of Engineering
Office of New Reactors

Date: 12-17-10

Dissenting View on the AP1000 Instrumentation and Controls Design Certification Amendment
Advanced Final Safety Evaluation Report With Respect to Evaluation and Acceptance Methods
used for Demonstrating Conformance to Commission Regulations

By

Kenneth D. Mott

NRC/NRO/DE/ICE1

December 16, 2010

Executive Summary

The author will describe and demonstrate that several of the staff's safety findings made for the Revision 18 AP1000 design certification amendment (DCA) diverse instrumentation and controls (I&C) design changes may not meet the applicable regulations and are inconsistent with United States Nuclear Regulatory Commission (NRC) policy and guidance that govern the review process to demonstrate conformance to Commission requirements for the adequacy and sufficiency of the AP1000 DCA diverse design protection mitigation features and the reliable actuation of these features.

If a proper review is not performed to ensure that proposed design changes to the certified AP1000 Revision 15 Design Certification Document (DCD) leave in place a design that continues to meet all applicable regulations, then possible design vulnerabilities may exist that may prevent the successful mitigation of postulated events which could result in radiation release exceeding applicable Commission regulatory limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The NRC staff review should be sufficient, thorough, and complete such that proposed design changes do not:

- Result in a design basis limit for a fission product barrier as described in the Certified AP1000 DCD final safety analysis report (FSAR) being exceeded or altered

The author will describe and explain how several of the AP1000 DCA DI&C design changes, combined with the staff not performing a complete and adequate review, may have introduced

- New event scenarios that have not been evaluated to ensure successful accident mitigation and adequate protection for the public

I. Background

A complete nuclear software related digital instrumentation and control (DI&C) overall mitigation design scheme helps to ensure that the plant operates safely and reliably by monitoring, controlling, and protecting critical plant equipment and processes. The digital I&C systems for advanced light water reactors (ALWRs) differ significantly from the analog systems used in operating nuclear power plants. Specifically, digital I&C systems share more data transmission functions and shares more process equipment than their analog counterparts.

Advanced reactors use a significant amount of identical digital software and hardware that are replicated across redundant trains of the primary, safety-related, digital I&C protective system. Therefore, a hardware design error, software design error, or software programming error may result in a common-mode failure (CMF) or common-cause failure (CCF) of redundant safety-related equipment. The concern is that the use of digital computer technology in I&C systems could result in safety significant CMFs and/or CCFs that defeat the redundancy achieved for the primary safety-related protection system and could result in the complete loss of the protective function or loss of more than one echelon of defense-in-depth performed by the primary safety-related digital I&C system. One of the principal factors for defense against CMF and CCF is diversity.

The regulatory requirements, for purposes of this paper, that govern the adequacy, sufficiency, and reliability of a DI&C design to prevent the loss of the protective function, or to demonstrate adequate diversity and defense-in-depth (D3) within the design to defend against postulated failure modes are:

- 10 CFR 50.62, "Requirements for reduction of risk from Anticipated Transient Without Scram events for light-water-cooled nuclear power plants"
- 10 CFR Part 50, Appendix A, General Design Criterion 22, "Protection System Independence"

The applicable design elements, for purposes of this paper, of 10CFR50.62 requirements, are:

- Each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the reactor trip system...
- This equipment must be designed to perform its function in a reliable manner....

The applicable design elements, for purposes of this paper, of General Design Criterion (GDC) 22, are:

- The protection system shall be designed to assure that the effects of ... normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function...
- 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.

Therefore, the AP1000 overall design basis for the DI&C design changes should demonstrate that the credited DI&C D3 design features and components conform to the applicable requirements such that postulated accident conditions on redundant channels do not result in loss of the protection function(s). The author will demonstrate how the staff's review may not have considered the correct review standards and methods such that staff would not have been able to make a reasonable assurance finding that the AP1000 DCA design changes meet the stated regulatory requirements.

II AP1000 DCA Design Diversity and Defense-In-Depth Design Basis

Section 15.8.3 of the AP1000 DCD, Tier 2, Final Safety Analysis Report (FSAR), Revision 18, states that diverse actuation system (DAS) provides the functions required by the requirements of 10CFR50.62, the Anticipated Transient Without Scram (ATWS) rule. Therefore, to conform to the requirement, the DAS has to be designed reliably to initiate turbine trip and auxiliary or emergency feedwater upon conditions indicative of ATWS events.

In Section 3.1.3 of the AP1000 DCD, Tier 2, FSAR, Revision 18, WEC describes compliance to GDC 22. As part of the design basis for compliance to GDC 22, WEC partially relied on the functionality of the DAS as stated below:

The AP1000 includes a non-safety related diverse actuation system. The diverse actuation system provides specific automatic functions including control rod insertion, turbine trip, passive residual heat removal heat exchanger actuation, core makeup tank actuation, isolation of critical containment lines, and passive containment cooling system actuation. This system is diverse and independent from the reactor protection system from sensors up to the actuation devices.

Therefore, the AP1000 design basis partially credits the operation and functionality of the DAS for addressing GDC 22 requirements to prevent the loss of the protective functions.

In addition, the design basis for the DAS, as stated in Revision 18, DCD, Tier 2, Section 7.7.1.11, states that the DAS "...provides a diverse backup to the protection system." It also states in the same section that "...where a common mode failure does occur, the diverse actuation system provides diverse protection." Therefore, the design basis credits the DAS to provide a diverse backup to the PMS for postulated CMFs of the PMS as a means to defend against the loss of protective function(s).

Information sufficient to demonstrate the adequacy and sufficiency of the DAS to address ATWS requirements shall be submitted to the Commission (10CFR50.62(c) (6)).

III Safety Concern

There are several AP1000 DCA DI&C design changes that have been made where the proper analysis was not provided by the applicant nor utilized by the staff to make a reasonable assurance finding that (1) the possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the certified Revision 15 AP1000 FSAR has been considered and that (2) analysis results of the design basis limits for a fission product barrier as described in the certified Revision 15 AP1000 FSAR, will not be exceeded due to the design changes. The applicable Revision 18 AP1000 DCA DI&C design changes are:

- A. Addition of a new DAS high hot leg trip to help mitigate against Anticipated Transient Without Scram (ATWS) events
- B. Modification of the DAS to field programmable gate array (FPGA) based technology where proposed surveillance testing will disable credited automatically actuated functions
- C. Addition of Tier 1 ITAAC to evaluate the reliability of only three DAS system's manual actuations

Case A

Section A4.2, "ATWS Analysis," of Revision 5, Volume 5, of the AP1000 PRA [ML033500078] states that the AP600 ATWS analysis ("AP600 ATWS Analysis," SAE-APS-98-11, dated January 22, 1998) concluded that the most limiting initiating event for an ATWS is a complete loss of normal feedwater (LONF). Appendix A, "Thermal Hydraulic Analysis to Support Success Criteria," of Revision 5, Volume 5, of the AP1000 PRA [ML033500078] only modeled the LONF to demonstrate adequate design diversity and that ATWS overpressure protection criterion were addressed with a S/G low level ATWS protective functions actuation only. In Appendix A, Section A4.1, "ATWS Background," the applicant states:

ATWS analysis was performed for the AP600 plant (Reference A-20). This analysis demonstrated that the AP600 plant could successfully ride out an ATWS event without inserting the control rods, considering that:

- Loss main feedwater is the most limiting initiating event
- PRHR HX provides an adequate heat sink
- The core reactivity feedback is sufficient to limit the peak RCS pressure to less than 3200 psig for more than 95 percent of full power core life

The applicant notes that LONF is the most limiting event. This analysis also proved that the AP600 response to ATWS is comparable to existing Westinghouse PWRs. It also states in Appendix A, Section A4.2, "ATWS Analysis," that:

Analysis has been performed for the AP1000 plant to verify that the peak RCS pressure is less than the ASME emergency stress limits, which occurs at greater than 3200 psia. In these analyses, the control rods are not inserted, even though DAS automatically de-energizes the motor generator set power. All of the mitigating system actions are modeled as being actuated by the DAS. DAS uses a low wide range S/G level signal to actuate the following:

- Automatic trip of the turbine
- Automatic trip of the reactor coolant pumps
- Automatic trip of the CMTs
- Automatic start of PRHR HX

Staff conducted an audit of the PRA model upgrade and updates for the Revision 18 AP1000 DCA PRA I&C model design changes. Staff concluded in the AFSER, Section 19.1.3.1, that:

Based on these results and the audit that provided confidence in the model upgrade and update process, the staff finds that the amended Level 1 internal events PRA at power did not change significantly. The staff finds that a plant-specific PRA report that is identical to the PRA for the certified design continues to provide an acceptable basis for risk insights and assumptions related to internal events.

By contrast, the applicant submitted, for the Revision 18 AP1000 DCA I&C design changes, Design Change No. 63 (DCN63), which changed the certified AP1000 design by adding an automatic high hot leg temperature trip to the DAS for ATWS mitigation. The applicant stated within DCN63 that the reason for this design change is:

In accordance with the original DAS design, which is modeled in the PRA, a reactor trip and turbine trip should occur for ATWS sequences with main feedwater available. Because feedwater is still available, the DAS Low Steam Generator water Level signal will not initiate the reactor or turbine trip. The DAS High Hot Leg temperature signal is needed to perform this function. This change adds a reactor trip and turbine trip from the DAS High Hot Leg Temperature.

Therefore, the applicant is clearly indicating that a LONF event for ATWS may not bind all other postulated ATWS events. The safety issue for this design change is now two-fold:

- Is the sole addition of the DAS High Hot leg temperature sufficient for mitigating ATWS concerns and addressing ATWS requirements? Why or Why not?
- Are there other plant parameters that would be more efficient for addressing ATWS concerns, versus the High Hot Leg Temperature Trip addition (i.e., addition of DAS High PRZ Level trip to prevent opening PRZ relief valves)

Case B

In WCAP-17184, Revision 2, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report" [ML102170263], July 2010, Section 6.1.2.2.4, states that the DAS ATWS mitigation functions should be available during MODE 1 when ATWS is a limiting event. It also states that the DAS ATWS mitigation function of reactor trip, turbine trip, and PRHR HX actuation should be available to provide ATWS mitigation capability. Therefore, if these credited automatic DAS ATWS functions are disabled at power, the AP1000 overall DI&C D3 ATWS mitigation scheme no longer conforms to the ATWS requirements of 10CFR50.62.

The DAS consist of two channels. The DAS uses two-out-of-two (2oo2) automatic actuation logic scheme to actuate automatic functions. When a required DAS channel is unavailable, the automatic DAS functions are unavailable. The Revision 18, AP1000 DCA technical specifications do not place any limiting conditions of operations (LCOs) on the plant for out of service or disabled DAS automatic functions. The Chapter 7 staff did not find that the Certified AP1000 DAS design for 2oo2 automatic actuation logic conformed to the requirements of 10CFR 50.62 in the FSER for the certified AP1000 DCD (NUREG-1793). However, staff found

in Chapter 19 of the FSER, Section 19.1.3.1.2.5, "Anticipated Transient Without Scram Sequences," to the certified AP1000 DCD that:

The following are the most important features of the AP1000 design that contributes to the reduction in the estimated CDF associated with ATWS sequences (CDF reduced to 5E-9/yr from the 4E-5/yr to 1E-8/yr range corresponding to CDFs associated with ATWS at operating PWR reactors):

The AP1000 design has two redundant and diverse reactor trip systems. The non-safety related DAS *is a reliable system capable* of initiating automatic and manual reactor trip using the motor-generator (M-G) sets when the reactor fails to trip via the PMS. *At operating reactors, the DAS is less reliable and cannot automatically initiate a reactor trip.*

Therefore, the staff in Chapter 19 has stated that it considers the DAS a reliable design and that it considers the DAS (ATWS) design at operating reactors to be "*less reliable.*" However, staff did not provide discussion on how it came to this safety conclusion (NOTE: Chapter 7 FSER staff did not make the safety finding that DAS met 10CFR50.62 reliability requirements for the I&C design). The standard for comparing existing plants with advanced reactors is stated by the Commission in its "Policy Statement on the Regulation of Advanced reactors [73 FR 60612]. In response to comment, the Commission states:

The policy statement does not state that advanced reactor designs must be safer than current generations, but rather that they must provide the same degree of protection of the environment and public health and safety and the common defense and security that is required for current-generation light water reactors.

The author performed a random review of current generation plant's ATWS automatic actuation logic. Table 1 below list the results of my review:

Table 1

Plant	Type of ATWS System	Parameter	Initiation Logic	Source of Data
Arkansas Nuclear One	Diverse Scram System (DSS)	4 channels sense pressurizer pressure	Any 2oo4 channels indicating loss of pressure	FSAR Section 7.7.1.6, Amendment No. 20
Beaver Valley	AMSAC (ATWS Mitigation System Actuation Circuitry)	3 channels monitor feedwater flow in 3 loops	Any 2oo3 loops indicating loss of flow	FSAR Sections 7.2.1.1.10 and 7.2.2.3.6, Revision 23
Byron/ Braidwood*	AMSAC	S/G level instruments	Any 2oo3 coincidence of S/G low level logic subsystems	FSAR Section 7.7.1.21.1, Revision 9
Callaway*	AMSAC	S/G level instruments	Any 3oo4 narrow range S/G levels below setpoint	Callaway-SP report, Section 7.7.1.11.1, Revision OL-14
Calvert Cliffs	Diverse Auxiliary Feedwater Actuation System	S/G level instruments	Any 2oo4 low S/G levels sensed on any S/G wide range level instruments	FSAR Section 7.10, Revision 34
Comanche Peak*	AMSAC	S/G levels instruments	Any 3oo4 S/G levels drops below setpoint	FSAR Section 7.8.1.1, Amendment No. 101
Crystal River	DSS and AMSAC	RCS pressure and feedwater flow	2oo2 actuation logic	FSAR, Section 7.5.2, Revision 32
Diablo Canyon	AMSAC	S/G water level	3oo4 S/G water levels below setpoint	FSAR, Section 7.6.1.4, Revision 15

Indian Point 3*	AMSAC	feedwater flow	Any 3004 feedwater flow indicating low flow	FSAR, Section 7.2.2, Revision 3
McGuire*	AMSAC	feedwater pump operation	Loss of 2003 pressure switches on a pump	FSAR Section 7.7.1.16, Revision 14
McGuire*	AMSAC	loss of feedwater flow	Any 3004 feedwater flow paths are blocked	FSAR Section 7.7.1.16, Revision 14
North Anna*	AMSAC	low S/G water level	Any 2003 S/G levels below AMSAC setpoint	FSAR Section 7.7.1.14, Revision 45
Vogtle*	AMSAC	low feedwater flow	Any 3004 main feedwater flow lines drop below setpoint	FSAR, Section 7.7.1.11.1, Revision 14
Wolf Creek*	AMSAC	low S/G Water level	Any 3004 S/G narrow range level signals fall below setpoint	FSAR Section 7.7.1.11, Revision 4

*Westinghouse PWR Plants

Therefore, based on the results from Table 1, it would appear that advanced reactors would need to demonstrate a design that can withstand an OOS channel and still be able to automatically actuate DAS credited automatic protective functions. However, the changes made in the AP1000 DCA show that for an OOS DAS channel, the DAS automatically actuated functions (i.e. ATWS mitigation) will be disabled until the channel is brought back to an operable status. Staff states in the AFSER that this design, based on the DI&C-ISG-02 standard of demonstrating defense against a "failure to actuate," meets this standard, and thus, conforms to 10CFR 50.62 requirements (10CFR50.62 reliability requirement states that "This equipment must be designed to perform its function *in a reliable manner*....")

Staff concluded in the AFSER for the AP1000 DCA that the applicant's response to DI&C-ISG-02 guidance safety concern that the DAS two out of two (2002) actuation design logic places greater concern on postulated system "failures to actuate" than on preventing spurious actuations (Staff states that Revision 17 meets requirements of 10CFR50.62). However, the applicant has never stated or made a design basis case to demonstrate that the DAS 2002 actuation logic is a design that demonstrates adequate protection against failures to actuate reliably. Yet, the staff concluded, incorrectly, in the AFSER that "no further evaluation is needed" and that "Revision 17 meets the requirements of 10CFR50.62."

Staff noted in Section 19.1.3.1.3 of the FSER for the certified AP1000 design (NUREG-1793), commenting on the risk importance of the DAS, that:

If the DAS becomes unavailable and the plant continues operating at power, the plant CDF would increase about 20 times.

Technical Specifications for the DAS automatically actuated protective functions would allow the DAS automatic functions to be disabled indefinitely. The applicant has not assigned limiting conditions of operation (LCOs) for disabled DAS automatic functions. It is the author's opinion that a design where one OOS channel would disable all automatic functions, and thus, the entire digital I&C could not demonstrate conformance to 10CFR50.62 and GDC 22 design requirements, is not design that cannot be found to be reliable.

Case C

In WCAP-17184, Revision 2, AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report [ML102170263], July 2010, Section 6.1.2.2.3, it states that the DAS manual controls provide non-Class 1E backup controls in case of common-mode failure of the PMS automatic and manual actuations. However, the new ITAAC will only perform an evaluation on three of the manual actuations to ensure reliability.

The manual functions, as listed in Table 2.5.1-2, "Diverse Actuation System," of Revision 18, Tier 1, AP1000 FSAR, Section 2.5-1, are:

- 1) Reactor and Turbine Trip
- 2) PRHR Actuation and IRWST Gutter Isolation
- 3) CMT Actuation and Trip All Reactor Coolant Pumps
- 4) **First-stage ADS Valve Actuation**
- 5) **Second-stage ADS Valve Actuation**
- 6) **Third-stage ADS Valve Actuation**
- 7) **Fourth-stage ADS Valve Actuation**
- 8) Passive Containment Cooling System (PCS) Actuation
- 9) Actuation
- 10) Isolation of Selected Containment Penetrations
- 11) Containment Hydrogen Igniter Actuation
- 12) **IRWST Injection Actuation**
- 13) **Containment Recirculation Actuation**
- 14) Actuate IRWST Drain to Containment

[**Bold**=Manual Actuators that will be Evaluated for reliability per Tier 1, Section 2.5-1, ITAAC 5].

ITAAC #5, in Tier 1, Section 2.5-1, of the Revision 18, AP1000 FSAR only proposes to evaluate three systems manual actuators controls on the DAS. These actuators selected are actuators that are not backed up by DAS automatic functions.

Section 7 of WCAP-17184 states that the PRA model assumes that the DAS functionality is tested once every six months and that during this testing the channel is bypassed so that an actuation signal is not generated and the likelihood of a spurious actuation is minimized. It also states that the PRA model assumes that the DAS will be returned to service within fourteen days if it is out of service. Therefore, the DAS automatic functions can be disabled for up to fourteen days. It must be noted that during this fourteen day period the plant would not meet its ATWS licensing basis or the Commission's ATWS requirements of 10CFR50.62.

IV Analysis to Demonstrate Conformance to Applicable Requirements

Digital I&C systems are vulnerable to CMF and CCF caused by software errors, which defeats the redundancy achieved by hardware architecture. In SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the NRC staff discussed concerns about CCF in digital systems in nuclear power plants. In Item II.Q of SECY-93-087, the staff submitted to the Commission a four-point defense-in-depth and diversity (D3) position to defend against CMFs and CCFs in digital systems. The Commission issued an SRM to SECY-93-087 modifying the four-point D3 position. Point 2 of the Commission's SRM to SECY-93-087, Item II.Q, states:

In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) *using best estimate methods*. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

The Commission's modified four-point position was captured in Revision 4 of the Branch Technical Position (BTP) HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," dated June 1997, of the

Standard Review Plan. BTP HICB-19 instructs the reviewer that in order to reach a conclusion of acceptability, several conclusions should be reached and supported by summation of the results of the analysis. BTP HICB-19, Paragraph B, Section 3, "Acceptance Criteria," list the conclusions that staff should reach in order to determine acceptability. Items #1 and #2 of that section state:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated *using best-estimate (realistic assumptions) analyses* should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated *using best-estimate (realistic assumptions) analyses* should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

Two of BTP HICB-19 objectives, as stated in the BTP, are:

- To verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.
- To verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.

Two of the regulatory requirements (or regulatory basis) listed for BTP HICB-19 are:

- 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram," requires in part various diverse methods of responding to anticipated transients without scram (ATWS).
- 10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the effects of natural phenomena, postulated accident conditions, normal operating, maintenance, and testing not result in the loss of protective function. "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."

It is clear that Commission policy, as well as staff D3 positions, direct the reviewer to base the acceptability of adequate and sufficient DI&C design diversity conformance to applicable

regulatory requirements within an overall digital I&C scheme, on an applicant's best estimate analysis.

The Revision 18, Tier 1, PMS automatically actuated engineered safety features that are credited to bring the plant to a safe sub-critically condition during postulated events, as listed in Revision 18 of the AP1000 DCD, Tier 1, Table 2.5.2-3, are:

PMS Automatically Actuated Protective Functions

1. Safeguards Actuation
1. Containment Isolation
2. Automatic Depressurization System (ADS) Actuation
3. Main Feedwater Isolation
4. Reactor Coolant Pump Trip
5. CMT Injection
6. Turbine Trip (Isolated signal to non-safety equipment)
7. Steam Line Isolation
8. Steam Generator Relief Isolation
9. Steam Generator Blowdown Isolation
10. Passive Containment Cooling Actuation
11. Startup Feedwater Isolation
12. Passive Residual Heat Removal (PRHR) Heat Exchanger Alignment
13. Block of Boron Dilution
14. Chemical and Volume Control System (CVS) Makeup Line Isolation
15. Steam Dump Block (Isolated signal to non-safety equipment)
16. MCR Isolation and Air Supply Initiation
17. Auxiliary Spray and Letdown Purification Line Isolation
18. Containment Air Filtration System Isolation
19. Normal Residual Heat Removal Isolation
20. Refueling Cavity Isolation
21. In-Containment Refueling Water Storage Tank (IRWST) Injection
22. IRWST Containment Recirculation
23. CVS Letdown Isolation
24. Pressurizer Heater Block (Isolated signal to non-safety equipment)
25. Containment Vacuum Relief

The Revision 18 AP1000 DCA design changed the certified AP1000 design by adding a High Hot Leg Temperature trip to the DAS for ATWS mitigation. Therefore, the automatically actuated protective functions that the DAS has to back-up the PMS and meet its design basis, as stated in Revision 18, Tier 1, Table 2.5.1-2 of the AP1000 DCD, are:

DAS Automatically Actuated Protective Functions

1. Reactor and Turbine Trip on Low Wide-range Steam Generator Water Level or Low Pressurizer Water Level or High Hot Leg Temperature
2. Passive Residual Heat Removal (PRHR) Actuation and In-containment Refueling Water Storage Tank (IRWST) Gutter Isolation on Low Wide-range Steam Generator Water Level or on High Hot Leg Temperature

3. Core Makeup Tank (CMT) Actuation and Trip All Reactor Coolant Pumps on Low Wide-Range Steam Generator Water Level or Low Pressurizer Water Level
4. Isolation of Selected Containment Penetrations and Initiation of Passive Containment Cooling System (PCS) on High Containment Temperature

Therefore, in order to meet its design basis and demonstrate conformance to the requirements of GDC 22 and 10CFR50.62, the applicant should submit a best estimate analysis to demonstrate that the small subset of DAS automatically actuated functions are in fact adequate and sufficient to (1) prevent the loss of the protective function, (2) demonstrate adequate D3 diversity within the design for postulated failure modes, and (3) to demonstrate that reliable ATWS mitigation requirements and concerns are met. Without a best estimate analysis, a basis does not exist to demonstrate conformance to applicable requirements.

However, staff found that the Revision 18 AP1000 DCA DI&C design changes were acceptable without utilizing a best estimate analysis.

V Summary of NRC Staff's Evaluation for the Revision 18, AP1000 DCA Design Changes

Table 2 below describes the design changes to the certified AP1000 design that staff accepted without a best estimate analysis:

Table 2

Staff made safety findings for	Rev 18 AP1000 DCA Change	Basis for Staff's Acceptance	Were Changes Demonstrated Adequate by best estimate Analysis?	Safety Finding Stated Where	Other Comments
DAS properly credited for providing diverse back-up to PMS; Changes between DCD Revisions 15 and 17 did not affect I&C design	Tier 1 addition of a new ATWS Trip; addition of time delay for opening PRHR discharge valves	PRA Assessment, Additional Technical Reports, Manual Actuations ITAAC,	No	AFSER Sections 7.8.2 and 7.8.3	Applicant has not demonstrated new trip is adequate or sufficient via best estimate analysis
10CFR50.62	Tier 1 addition of a new ATWS Trip	RAI Response stating original AP1000 PRA modeled the DAS	No	AFSER Section 7.8.3	Chapter 7 FSER staff did not conclude that design met 10CFR50.62 requirements for certified design
GDC 22	Tier 1 addition of a new ATWS Trip		No	AFSER Section 7.8.3	Old design certified w/o new trip. Is new trip adequate for GDC 22 criterion
10CFR50.62 (must be designed reliably)	New DAS Hot Leg trip and PRHR time delay adequate with 2oo2 automatic logic actuation	Staff states DI&C-ISG-02; "Failure to actuate" as basis	No	AFSER Section 7.8.2	Applicant has not provided design details to demonstrate design defenses against "failures to actuate"

Applicant provided sufficient information	New DAS Hot Leg trip and PRHR time delay adequate with 2oo2 automatic logic actuation	Applicant submitted new D3 report WCAP-15775, Revision 4, however, does not contain best estimate analysis	No	AFSER Section 7.8.3	DAS has 2oo2 automatic actuation logic. Therefore, for one channel OOS, all DAS automatic functions are disabled.
10CFR 52.47, (emphasis upon performance requirements and the technical justification therefor)	Tier 1 addition of a new ATWS Trip; addition of time delay for opening PRHR discharge valves	RAI response stating that time delay added to be consistent with the use of timers in the existing functional design	No	AFSER Chapter 23.C.3	A best estimate analysis would provide basis to demonstrate conformance to performance requirements (i.e., release does not exceed 10CFR100)

The passive residual heat removal (PRHR) system is credited with being a safety related means to allow the plant to ride out an ATWS event without rod insertion. This is stated in Revision 5, Volume 4, of the AP1000 Probabilistic Risk Assessment, Section 59 [ML033500078]. Therefore, any changes to ATWS trip modes and/or PRHR mitigation timing schemes should be analyzed with a proper analysis to ensure that all accident analysis assumptions and commitments are still accurate and staff safety conclusions made in the certified AP1000 design still hold true. Without a best estimate thermal hydraulic analysis, staff does not have a basis for acceptability.

VI The Author's reasons why he disagrees with staff utilizing risk results to make conclusions of safety

In 1995, the NRC issued Policy Statement 60 FR 42622, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register*, Volume 60, Number 42622, August 16, 1995, on the use of PRA, encouraging its use in all regulatory matters. Since that time, many uses have been implemented or undertaken. Consequently, confidence in the information derived from a PRA is an important issue, in that the accuracy of the technical content must be sufficient to justify the specific results and insights that are used to support the decision under consideration. Experience shows that one cannot eliminate all faults in complex digital I&C systems that can cause a system failure when the system is exposed to an operating environment or profile for which it was not designed, tested, or used. Exposure to such an operating environment or profile is possible for nuclear power plants because there are a large number of possible states and inputs for a DI&C system. When trying to estimate DI&C system reliability, it must be remembered that each digital I&C system, including software, is unique, and extrapolation of statistical data from one system to another may not necessarily be meaningful. Likewise, extrapolation of statistical data of the same system used in a different operating environment or profile is not necessarily meaningful. While digital I&C risk assessment methods have the potential to disclose design problems in digital I&C systems, the level of uncertainty associated with digital I&C risk assessment results and insights (in part due to a lack of consensus in the technical community over acceptable PRA models for digital I&C risk assessments and limited applicable data) is high.

On May 19, 2008, during the 552nd meeting of the Advisory Committee on Reactor Safeguards (ACRS), May 8-9, 2008, they reviewed the draft NUREG/CR-6962, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems" [ML081330429]. The ACRS committee made the following conclusions and recommendations in their letter:

1. Draft NUREG/CR-6962 provides convincing evidence that "traditional" probabilistic risk assessment (PRA) methods are not sufficient to adequately identify failure modes of DI&C systems.
2. Before publication of NUREG/CR-6962, it should be revised to state clearly that its methods do not address software failures and that it employs simulation in addition to traditional PRA methods. The revised NUREG/CR report should focus on failure mode identification only.
3. The distinction between traditional and non-traditional methods of modeling and analysis is artificial and should be abandoned. The staff should establish an integrated program that focuses on failure mode identification of DI&C systems and takes advantage of the insights gained from the investigations on traditional PRA methods and on advanced simulation methods.
4. The quantification of the reliability of DI&C systems should be given a low priority until a good understanding of the failure modes is developed.

During their discussions, as noted in the letter, the ACRS committee also reached the conclusion that:

The draft NUREG/CR report contains a discussion on the development of reliability models for DI&C systems and the collection of data for parameter estimation. It is premature to attempt to develop such models when our understanding of the failure modes of DI&C systems is still evolving. We also have serious concerns about the usefulness of the failure rate data sources cited. *The sections dealing with probabilities should be drastically reduced or deleted altogether.*

(emphasis added)

Staff's position on using quantitative reliability goals is stated in Appendix 7.1-C of the Standard Review Plan, Revision 4. It states:

Staff acceptance of system reliability is based on deterministic criteria described in IEEE Std. 603 and IEEE Std. 7-4.3.2, rather than on quantitative reliability goals. Therefore, the system design basis should discuss the methods to be used to confirm that these deterministic criteria have been met. The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for reliability of safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the I&C system.

In staff report NUREG-0460, Volume 3, "Anticipated Transients Without Scram For Light Water Reactors" [ML083590317], dated December 1978, staff noted the conclusions made from the Lewis Committee that:

In its recently published report to the NRC (NUREG/CR-0400), the Lewis Committee found, among other things,

"We are unable to determine whether the absolute probabilities of accident sequences in WASH-1400 are high or low, but we believe that the error bounds on those estimates are, in general, greatly understated. This is true in part because there is in many cases an inadequate data base, in part because of an inability to quantify common cause failures, and in part because of some questionable methodological and statistical procedures."

Staff stated in Volume 3 of NUREG-0460 that:

We had not proposed to require probabilistic calculations to demonstrate compliance with our safety objective, in part because of uncertainties in the present probabilistic studies.

and

We now believe that the resolution of ATWS concern should rest on engineering evaluation and judgment of the appropriateness of alternative plant modifications, rather than directly rest on quantitative risk analysis.

Staff finally concluded in Volume 3 of NUREG-0460 that:

For the reasons stated in Section 2.1 above, and in view of the still developing nature of probabilistic licensing criteria, we continue to believe that deterministic licensing requirements for ATWS are preferable to probabilistic requirements.

The NRC staff continues to hold that position today as documented in Digital I&C Interim Staff Guidance 03, "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments," Revision 0, August 2008 [ML080570048]. The NRC staff states that it is premature to risk-inform digital I&C regulatory matters. The uncertainties associated with digital I&C system risk assessments currently are large enough to reinforce the need for diversity, defense-in-depth, and adequate safety margins, and the retention of deterministic requirements designed to assure their continued existence. An advance in the state-of-the-art may be needed to permit a comprehensive risk-informed decision-making framework in licensing reviews of digital I&C systems for future and current reactors.

VII. Applicant's Technical Report Submission Shows that Increasing PRA Margin Does Not Necessarily Demonstrate Adequate Accident Mitigation

In Chapter 19 of the Final Safety Evaluation Report (NUREG-1793) of the Certified AP1000 Design Control Document (DCD), staff reviewed the technical information contained in WCAP-15985, Revision 1, "AP1000 Implementation of the Regulatory Treatment of Non-Safety Related Systems Process," issued April 2003 [ML0325408430]. This report provides the resolution of the regulatory treatment of non-safety systems (RTNSS) policy issue for the AP1000. The NRC policy, as stated in SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs" [ML003708005], deals with identifying and providing proper regulatory oversight to those systems in passive light water reactors that are designated non-safety related, but may have a significant role in accident and consequence mitigation.

In WCAP-15985, the applicant demonstrates how margin can be added to an overall PRA

study even though it would not help demonstrate adequate accident mitigation for postulated accident conditions. The applicant states in Section 2.3, "Uncertainty," of the report:

The objective of this PRA uncertainty evaluation is to determine which non-safety related SSCs should be identified to compensate for the PRA uncertainties. The approach is to identify SSCs that directly compensate for the uncertainty. It is recognized that for some of these uncertainties, there are no non-safety related SSCs that can directly compensate for these uncertainties. In such situations, margin is provided in the PRA by adding regulatory oversight on non-safety related SSCs that improve the PRA sensitivity study results for other sequences. For example, there are no non-safety related SSCs that can improve the PRA sensitivity study results associated with DVI [Direct Vessel Injection] line breaks. During a DVI line break, the Normal Residual Heat Removal System (RNS) injection flow spills out the break and does not inject water into the RCS. Providing short-term availability controls on a system such as the DAS for ATWS events is a way to add margin to the PRA sensitivity study by improving the overall PRA sensitivity study results, *even though it does not add margin to DVI line break events.*

Therefore, the applicant has demonstrated that by using a PRA analysis, they are able to add margin to improve an overall PRA sensitivity study, however, the sensitivity study's margin increase does not necessarily demonstrate that the postulated accident scenario has adequate functionality, diversity, reliability, or time to demonstrate that postulated fission product release will not exceed applicable limits.

The transcript of the June 5, 2008. Meeting between the United States Nuclear Regulatory Commission and the Advisory Committee On Reactor Safeguards [ML081610788], documented comments by the ACRS members to the Commission. One of the topics was concerned with the guidance contained in the Interim Staff Guidance (ISG) on DI&C PRA and the sensitivity analysis based on past activities and then start performing sensitivity analysis. The ACRS member concluded that:

We felt that this was inappropriate, that it would not lead to any meaningful conclusions and we recommended that the ISG be revised to emphasize the importance of the identification of failure modes and deemphasize all the sensitivity studies. *In fact, maybe eliminate them completely from the ISG anything that involves probabilities.*

[emphasis added]

VIII Accident scenario that has not been analyzed by thermal-hydraulic best estimate analysis to demonstrate conformance to applicable regulations

Postulated Accident #1:

ATWS Concern: For an anticipated operational occurrence (AOO) consisting of an inadvertent withdrawal of an individual rod or a bank of rods, combined with the failure of the controls rods to insert (ATWS event), with normal feedwater operating, will the high hot leg trip actuate before coolant flows out of a pressurizer (PRZ) pressure relief valve or exceed ATWS limitations?

IX Conclusion

Since a best estimate thermal hydraulic analysis has not been utilized to verify adequacy and sufficiency of conformance to applicable safety requirements, the changes made to the overall I&C design in the AP1000 DCA may contain design mitigation vulnerabilities which may result in exceeding design basis limits for a fission product barrier, radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.

Without having the proper analysis, the AP1000 DCA changes may contain unanalyzed failure modes and unanalyzed accident modes where the design basis does not demonstrate a sufficiently reliable or adequately diverse design for certain postulated failures. Therefore, the design does not demonstrate adequate protection to prevent the release of radioactive fission product less than applicable regulatory limits nor demonstrate adequate protection for the public. Therefore, the author does not concur with the safety conclusions stated in the AFSE to the AP1000 DI&C DCA and is following the non-concurrence process as a way to bring the AP1000 design into compliance with the Commission regulations by using a Commission approved best estimate analysis to demonstrate adequacy and sufficiency of I&C design diversity.

The author made the applicant aware of the need to submit a best estimate analysis at a public meeting in December 2008 [ML090090187], as a way to demonstrate design conformance to applicable regulations and requirements. The author has also tried to pursue a 10CFR52.63 backfit as a way to have the applicant submit the proper analysis for design conformance demonstration. The author has been unsuccessful with obtaining a best estimate analysis from the applicant.

Therefore, it is the author's opinion that the design has not been demonstrated to conform to applicable regulations.

X Recommendations

The author recommends that either (1) before issuing the rule for the AP1000 DCA changes, either a best estimate analysis should be submitted for staff review or (2) a 10CFR52.63 "backfit" should be issued against the amended certified design requesting the applicant to perform a best estimate analysis in accordance with the Commission's SRM to SECY-93-087 to demonstrate compliance to the requirements of 10CFR50.62 and GDC 22.

NON-CONCURRENCE PROCESS

TITLE OF DOCUMENT

See Below

ADAMS ACCESSION NO.

ML103420563

SECTION B - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL'S SUPERVISOR

(THIS SECTION SHOULD ONLY BE COMPLETED IF SUPERVISOR IS DIFFERENT THAN DOCUMENT SPONSOR.)

NAME

Terry W. Jackson

TITLE

Branch Chief

PHONE NO.

301-415-7313

ORGANIZATION

NRO/DE/ICE1

COMMENTS FOR THE DOCUMENT SPONSOR TO CONSIDER

☐

I HAVE NO COMMENTS

☒

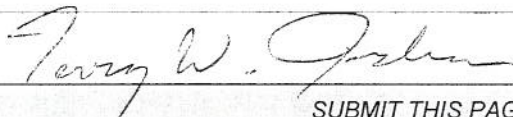
I HAVE THE FOLLOWING COMMENTS

The response to the non-concurrence is provided in the attachment, "Staff Response to Dissenting View on the AP1000 Instrumentation and Controls Design Certification Amendment Advanced Final Safety Evaluation Report With Respect to Evaluation and Acceptance Methods Used for Demonstrating Conformance to Commission Regulations."

☐

CONTINUED IN SECTION D

SIGNATURE



DATE

12/27/2010

SUBMIT THIS PAGE TO DOCUMENT SPONSOR

**Redacted Staff Response to Dissenting View on the AP1000
Instrumentation and Controls Design Certification Amendment
Advanced Final Safety Evaluation Report With Respect to Evaluation
and Acceptance Methods Used for Demonstrating Conformance to
Commission Regulations**

**Staff Response to Dissenting View on the AP1000 Instrumentation and Controls Design
Certification Amendment Advanced Final Safety Evaluation Report With Respect to
Evaluation and Acceptance Methods Used for Demonstrating Conformance to
Commission Regulations**

December 22, 2010

I. INTRODUCTION

On December 17, 2010, a non-concurrence was submitted by Kenneth Mott associated with the Advanced Final Safety Evaluation Report (AFSER) input for Chapter 7 of the AP1000 Standard Design Certification Amendment. In accordance with the non-concurrence process (draft Management Directive 10.158, "NRC Non-Concurrence Process"), the staff is providing (1) its summary of the dissenting view, (2) a summary of the staff's response to the dissenting view, and (3) a detailed response to the specific conclusions and statements provided in the non-concurrence.

During the staff's review of the AP1000 design certification amendment, Mr. Mott was assigned the review of Diverse Instrumentation and Control Systems as described in Standard Review Plan, Section 7.8. I am both Mr. Mott's supervisor and the document sponsor for the memo titled, "Advanced Final Safety Evaluation Report for the AP1000 Standard Design Certification Amendment – Chapter 7, "Instrumentation and Control (ADAMS Accession No. 103420563)."

II. SUMMARY OF DISSENTING VIEW

The non-concurrence states that AFSER does not provide reasonable assurance that the AP1000 Design Control Document (DCD), Revision 18, conforms with NRC regulations that apply to digital instrumentation and control (I&C) systems. Specifically, in the "Executive Summary" of the non-concurrence, the author states:

Several of the staff's findings made for the Revision 18 AP1000 design certification amendment (DCA) diverse instrumentation and controls (I&C) design changes may not meet the applicable regulations and are inconsistent with United States Nuclear Regulatory Commission (NRC) policy and guidance that govern the review process to demonstrate conformance to Commission requirements for the adequacy and sufficiency of the AP1000 DCA diverse design protection mitigation features and the reliable actuation of these features."

The specific regulations in question are discussed in Section I, "Background," of the non-concurrence. These regulations and their applicable requirements are:

- 10 CFR 50.62, "Requirements for reduction of risk from Anticipated Transient Without Scram [ATWS] events for light-water-cooled nuclear power plants," which requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuating device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.
- 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22, "Protection system independence," requires, in part, that 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 protective 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 protective function.

The AP1000 design utilizes the Diverse Actuation System (DAS) to meet 10 CFR 50.62 and, in part, to meet GDC 22. It is appropriate for the AP1000 design to address both of these requirements as they are listed as applicable requirements in Branch Technical Position (BTP) 7-19 of the Standard Review Plan (SRP). With regards to GDC 22, the DAS provides defense-in-depth and diversity in response to a software common-cause failure of the primary protection system in order to ensure the protective functions are not lost.

The non-concurrence identified a number of concerns that can be classified as the following in regards to the DAS:

1. Inadequate demonstration of reliability and availability for the AP1000 Diverse Actuation System (DAS) as required by 10 CFR 50.62
 - a. DAS uses a 2oo2 voting logic such that the automatic functions will not operate when subjected to a single failure or channel removed for maintenance/testing
 - b. DAS Technical Specification allowed outage times are not adequate
 - c. Staff did not explicitly state that DAS met 10 CFR 50.62 in the original design
2. Inadequate demonstration of DAS performance, as required by 10 CFR 50.62 and GDC 22, as it used a focused Probabilistic Risk Assessment (PRA) study instead of a deterministic, best-estimate, thermo-hydraulics analysis to establish the back-up functions of DAS
 - a. Use of the focused PRA study is inconsistent with NRC guidance

- b. Insufficient basis to determine the focused PRA study is an appropriate alternate method.

In order to address the concerns listed in the non-concurrence, the author recommends that the following actions be taken:

- Before issuing the rule for the AP1000 DCA changes, either a best-estimate analysis should be submitted for staff review, or
- A 10CFR 52.63 backfit should be issued against the amended certified design requesting the applicant to perform a best estimate analysis in accordance with the Commission's SRM to SECY-93-087 to demonstrate compliance to the requirements of 10 CFR 50.62 and GDC 22.

III. BACKGROUND

In the AP1000 I&C design, the Diverse Actuation System (DAS) provides back-up functions to the primary reactor protection system, or Protection and Safety Monitoring System (PMS). The PMS is a safety-related, digital protection system that is designed with high quality and incorporates design principles such as redundancy, independence, and high reliability. Despite the high quality and design principles incorporated into PMS, there is a potential for a software common-cause failure (CCF) to defeat the four redundant divisions. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 22, "Protection System Independence," requires that protection systems 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 a loss of the safety function. 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 safety function. As described in Section 3.1.1 of AP1000 DCD, Tier 2, Revision 18, Westinghouse Electric Company (WEC) included the DAS to provide a diverse means to perform the safety functions through a limited set of automatic or manual functions as part of the basis for meeting GDC 22.

The AP1000 design also incorporates automatic functions to address anticipated transients without scram (ATWS) in DAS. 10 CFR 50.62 requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system. Since an ATWS and CCF of the PMS are considered common-mode failures, and thus, beyond design basis events, DAS is classified as a non-safety system.¹

¹ The SRM to SECY-93-087 recognizes common-mode failures as beyond design basis events.

III.A Safety Significance

DAS mitigates the beyond design basis event of a software CCF of PMS and ATWS. To reach a radiological release for events involving DAS, the following events would need to occur:

1. An accident or transient occurs that requires PMS response
2. PMS fails to complete its intended functions due to a CCF²
3. Any automatic DAS function that may address the event fails
4. Operators fail to mitigate the event through manual actions

As described in Section 2.3.1 of WCAP-17184-P, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report," Revision 2, the DAS functions were developed using a focused PRA study. In conducting the study, non-safety systems such as chemical volume and control system, normal residual heat removal system, start-up feedwater system, and diverse actuation system were assumed failed. With those systems assumed failed, the core damage frequency (CDF) was determined to be $8.6\text{e-}6$ events per year and the large release frequency (LRF) was determined to be $5.9\text{e-}6$ events per year. Since the LRF did not meet the safety goal of $1\text{e-}6$ events per year, manual DAS functions, as described in Section 2.3.1 of WCAP-17184-P, were added. Addition of the manual DAS functions reduced the CDF to $3.1\text{e-}6$ events per year and LRF to $7.7\text{e-}7$ events per year in the focused PRA study. While DAS functions were identified using a focused PRA study, deterministic analyses were used to confirm or dictate DAS performance. Examples include the thermo-hydraulics analysis for the loss-of-normal feedwater ATWS event described in Section 15.2.9 of NUREG-1793 and the establishment of the DAS automatic setpoints from the safety analytical limits derived from the AP1000 Chapter 15 accident analysis.

III.B AP1000 Certified Design Review

As part of the AP1000 certified design, the staff approved the use of the AP1000 PRA to determine DAS functions in Section 7.1.6 of NUREG-1793. The staff acknowledged the use of the PRA and also discussed WCAP-13793, "AP600 System/Event Matrix," issued in 1994. In NUREG-1793, the staff stated:

Based on its review, the staff finds that the applicant has assessed the defense-in-depth and diversity of the AP1000 I&C system and has demonstrated that vulnerabilities to common-mode failures have been adequately addressed. The applicant has analyzed each postulated common-mode failure for each event that is evaluated in the accident analysis section of the DCD, and has addressed the diversity requirements within the design for each of these events. The DAS, as proposed, performs the same functions as the PMS when a postulated common-mode failure disables the PMS protection

² ATWS events assume an anticipated operational occurrence, as defined in 10 CFR Part 50, Appendix A, and the failure to insert the control rods due to an I&C or mechanical common-mode failure.

functions. In addition, the DAS, as proposed, includes displays, independent and diverse from the PMS that can support any necessary manual actions in the event that a postulated common-mode failure disables the PMS. Therefore, the staff concludes that the proposed design satisfies the Commission's position on I&C system diversity. Section 7.7.2 of this report further discusses the evaluation of the DAS.

The staff also acknowledged in Section 7.7.2 of NUREG-1793 that DAS used a 2oo2 voting logic arrangement and found it acceptable.

Use of the PRA was a deviation from staff guidance as described in NRC guidance at the time of the original AP1000 review, including BTP HICB-19 and the SRM to SECY-93-087. BTP HICB-19 and SECY-93-087 state that a deterministic, best-estimate, thermo-hydraulics analysis should demonstrate the acceptable performance of diverse I&C systems to address a transient or accident condition coincident with a common-cause failure of the reactor protection system. As evidenced by the quote from NUREG-1793 above, the staff found the use of the PRA-based method acceptable since it analyzed each common-cause failure event and provided for diversity for those events.

IV INADEQUATE DEMONSTRATION OF DAS RELIABILITY AND AVAILABILITY

IV.A DAS Voting Logic and Staff Approval

The non-concurrence discusses three concerns with regards to DAS reliability and availability: (1) 2-out-of-2 (2oo2) voting logic, (2) indefinite allowed outage times by Technical Specifications and Investment Protection Program, and (3) failure of the staff to state that the AP1000 met 10 CFR 50.62 in NUREG-1793. The concern with 2oo2 voting logic is that a single failure, or maintenance on a division of DAS, would prevent DAS from performing its automatic functions. As noted above, the NRC staff acknowledged and approved the DAS 2oo2 voting in Revision 15 of the AP1000 DCD.

As discussed in Section III of this document, the PMS is the primary protection system and is expected to be developed with high reliability. As such, PMS is expected to respond to transients and accidents to protect the public from radiological release. Although a common-cause failure of the PMS cannot be ruled out, such events should be of low probability given the quality and reliable design of the system. Therefore, back-up systems such as DAS, should be of sufficient quality and reliability, but do not require the same level of quality and reliability as the primary protection system.

While the staff's basis for accepting the 2oo2 voting logic in NUREG-1793 was not clear, the DAS meets the requirement in 10 CFR 50.62 for equipment design to perform its function in a reliable manner for the following reasons. As described in Section 15.8.3 of the AP1000 DCD, Tier 2, Revision 18, the AP1000 is equipped with a DAS, which provides the functions required by the ATWS rule (10 CFR 50.62). The ATWS core damage frequency for the AP1000 is below

the SECY-83-293 goal of 10^{-5} per reactor year. In NUREG-1793, the staff reviewed and approved the AP1000's basis for meeting the ATWS core damage frequency goal.

Reliability of digital systems can be achieved through various means including redundancy, fault detection and management, quality of design, and use of reliable components. Reliability can be defined as the likelihood that a given component or system will be properly functioning when needed, as measured over a given period of time. Reliability, in itself, does not account for any repair actions that may take place. Availability can be defined as the percentage of time that a given system will be functioning as required. In other words, availability is the probability that a system is not failed or undergoing a repair action when it needs to be used.

The AP1000 DAS design addresses reliability from a design/component approach and by fault detection and management. From a design/component reliability approach, Section 8.1 of WCAP-17184-P states that a failure modes and effects analysis, mean-time-between-failure analysis, and a reliability block diagram analysis will be performed on the DAS at the component level. Since the DAS detailed design is not complete at the design certification stage, nor required to be complete per 10 CFR 52.47, those analyses were not part of the staff's review. However, sufficient criteria in the AP1000 DCD are available to guide the detailed design analysis, such as the use of MIL-HDBK-217F for component failures and hardware reliability analysis. From a fault detection/management approach, Section 6.1.2.2.1 of WCAP-17184-P states that the DAS will include self-diagnostic features to identify failures such as: [

- -
 -
 -
 -
-]

The self-diagnostic features provide real-time indication to operators of a DAS failure, limiting the fault exposure time and improving DAS availability.

As part of the determination for meeting the ATWS core damage frequency goal, the AP1000 PRA assumed an availability goal of [] for DAS, as described in Section 8.2 of WCAP-17184-P. [] As committed in WCAP-17184-P, the detailed reliability analysis performed on the DAS would be consistent with the availability goal. Specifically, the reliability analysis will determine an expected failure rate based on hardware failures. Both the failure rate and expected repair time will be calculated and compared to the availability goal for consistency. By utilizing self-diagnostic features, the operators are given real-time indication of a DAS failure, which will allow maintenance to be performed in a timely manner. By using the self-diagnostic features, the fault exposure time is reduced on the DAS, thus improving DAS availability as it relates to latent, undetected faults.

Given the commitments in WCAP-17814-P regarding the reliability analysis and self-diagnostics, the staff finds that the DAS will operate reliably. DAS may be taken out of service for maintenance, or be subjected to a failure, but would meet the committed availability target, which is part of the overall basis for meeting the ATWS core damage frequency goal. NRC regulations such as 10 CFR 50.65, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants," would provide verification that the availability goal is being achieved. To address the deficiency of NUREG-1793 to provide a clear basis for the 2002 voting logic, the basis described in this section will be added to Section 7.8.2 of the AFSER for the AP1000 design certification amendment.

The non-concurrence notes that the staff's final safety evaluation report in NUREG-1793 did not state that WEC met 10 CFR 50.62. While the staff did not make an explicit statement in Chapter 7 of NUREG-1793 that the AP1000 design met 10 CFR 50.62, it did not make any statements to the contrary. However, the staff acknowledged the acceptability of the 2002 voting logic. Compliance to 10 CFR 50.62 was identified in Section 15.2.9 of NUREG-1793, which documented the reactor systems review of ATWS protection.

In the AP1000 design certification amendment, WEC proposed the following changes related to the DAS:

- Change in technology for the DAS from a microprocessor-based system to a field-programmable gate array (FPGA) based system
- Removal of Inspection, Tests, Analyses, and Acceptance Criteria (ITAAC) associated with Items 4(a) and (b) in AP1000 DCD, Tier 1, Table 2.5.1-4 related to the completion of the DAS design requirements (software and hardware plans) and system definition phase (DAS requirements specifications)
- Addition of a DAS instrument cabinet, relocation of some DAS equipment within the plant, and the addition of an electrical containment penetration
- Addition of an ITAAC to verify the performance of DAS manual actions
- Addition of a new DAS reactor/turbine trip based on high hot leg temperature and a time delay to Passive Residual Heat Removal actuation

As described in Section 7.8 of the AFSER under concurrence, the staff evaluated the changes in the DAS design in order to determine the scope of the AP1000 amendment review. According to 10 CFR 52.63, the Commission may not modify, rescind, or impose new requirements on the certification information unless the provisions in 10 CFR 52.63 are met. In other words, if design aspects of the AP1000 were not modified, then finality would apply to those portions of the design. None of the changes identified above were determined to affect the finality of the DAS 2002 voting logic. For instance, the change in DAS technology would not have changed the concern if DAS had remained a microprocessor-based system or been

altered to other technologies such as analog. Removal of the ITAAC was associated with design work accomplished on the DAS such as software/hardware development plans and requirements specifications. However, the new design work did not alter the DAS architecture from 2oo2 voting logic. The other DAS modifications involved addition of functions, addition of ITAAC, and movement of physical location of equipment which did not alter the 2oo2 voting logic.

Since finality of the DAS 2oo2 voting logic was recognized, the staff did investigate a potential backfit of the AP1000 design through 10 CFR 52.63. Specifically, the staff investigated a modification of the AP1000 design to require at least 2oo3 voting logic in the DAS. In the staff's pursuit of a backfit, the following criteria in 10 CFR 52.63 were considered: (1) compliance, (2) adequate protection, and (3) substantial improvement in safety. The staff developed the findings listed below during the pursuit of the backfit:

- Compliance – 10 CFR 50.62 requires the ATWS mitigation system to perform its function in a reliable manner. However, it is not specific enough to require single failure tolerance provided by 2oo3 or better voting logic. In addition, staff guidance in Section 7.8 of the Standard Review Plan and Branch Technical Position 7-19 for diverse I&C systems did not identify the necessary level of redundancy and reliability.
- Adequate Protection – As the DAS system and software common-cause failure is not considered within the design basis, it is difficult to conclude that it is an adequate protection issue.
- Substantial Improvement in Safety – The staff would need to show that there is substantial safety improvement if a 2oo3 voting logic was used instead of a 2oo2 arrangement. Appendix 1B of the AP1000 DCD, Tier 2, Revision 15, describes a Severe Accident Mitigation Design Alternatives evaluation that considered 2oo3 voting logic for DAS. The evaluation determined that the addition of a third division of DAS equipment and conversion to a 2oo3 voting logic was not cost effective as compared to the safety benefit. In discussions with NRC PRA review staff, although moving from a 2oo2 voting logic improves DAS reliability by approximately two orders of magnitude, the reliability improvement does not translate to an appreciable improvement in plant CDF or LRF due to the relative importance of DAS in the overall AP1000 plant design.

IV.B Limiting Conditions of Operation (LCO) for DAS Automatic Functions

The non-concurrence discussed the absence of Technical Specification LCOs for DAS automatic functions. Section 3.3.5 of the AP1000 Technical Specification identifies LCOs for DAS manual actions. If one or more manual DAS controls are inoperable, the licensee has 30 days to restore the controls to operable status. If that LCO is not met, the licensee is to perform Surveillance SR 3.3.1.6 (PMS Trip Actuating Device Operational Test) or Surveillance SR

3.3.2.2 (PMS Actuation Logic Test) once per 31 days on a staggered basis. The DAS manual functions could be inoperable until the next Mode 2 entry following a Mode 5 entry so long as the surveillance provisions are accomplished. The DAS automatic functions are controlled by the Investment Protection Short-Term Availability Controls as identified in Section 16.3 of the AP1000 DCD, Tier 2. Within those controls, a DAS automatic function is to be restored to operable status within 14 days. If that condition is not met, a report is to be submitted to the chief nuclear officer, or on-call alternate, outlining compensatory measures, cause for inoperability, and schedule for restoration. The DAS manual actions are included in Technical Specification since it meets the criteria of 10 CFR 50.36(c)(2)(ii)(D) in that it is a structure, system, or component which PRA shows to be significant to public health and safety. Specifically, the DAS manual actions were added to meet the PRA LRF goal. The allowed outage times for manual actions are based on the overall safety importance of DAS, and in the original staff review, it was determined that 30 day LCO was acceptable as compared to other allowed outage times imposed on equipment in the AP1000 and other reactors. Automatic ATWS mitigation functions are typically not included in Technical Specifications as demonstrated by many operating reactors that have transitioned to improved Technical Specifications. Automatic ATWS mitigation functions are typically addressed by administrative controls such as the Investment Protection Short-Term Availability Controls.

While the AP1000 is in operation, other regulatory requirements will require availability of the DAS. For example, 10 CFR 50.65(a)(1) states, in part, that licensees shall monitor the performance or condition of structures, systems, or components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that these structures, systems, and components, as defined in paragraph (b) of this section, are capable of fulfilling their intended functions. Paragraph (b) states that the scope of the rule includes non-safety systems that whose failure could cause a reactor scram or actuation of a safety system or those that are used in plant emergency operating procedures. Although DAS uses 2oo2 voting logic and reduces the likelihood of a spurious reactor scram or actuation of a safety system, its failure could cause a scram or actuation. Also, DAS would be relied upon in the emergency operating procedures for ATWS events and CCF of PMS. Therefore, DAS would be in the scope of the 10 CFR 50.65. In Section 8.2 of WCAP-17184-P, Revision 2, [

.] The unavailability value for DAS would be used to ensure compliance with 10 CFR 50.65 when the plant is in operation. Therefore, DAS would not be allowed to remain out of service for large periods of time.

V INADEQUATE DEMONSTRATION OF DAS PERFORMANCE

The non-concurrence identifies a concern with the failure of the staff to require WEC to submit a best-estimate analysis to verify adequate DAS functions and performance. As identified in Section IV.A of this response, a number of design changes were made to the DAS as part of the AP1000 design certification amendment. Only one design change potentially impacts the staff's approval for using a focused PRA to determine DAS functions. On May 20, 2010, WEC issued

a design change to add a new DAS reactor/turbine trip function based on high hot leg temperature. The basis for the change is the original DAS design depended, in part, on a low steam generator level trip to mitigate Anticipated Transient Without Scram (ATWS) events. The original DAS design, as modeled in the PRA, assumed that main feedwater would be available for the ATWS sequences where loss of normal feedwater was not part of the event. However, if main feedwater were available, the DAS Low Steam Generator Water Level signal would not trip the reactor or turbine.

The staff's review of the design change is described in Section 23.O of the staff's AFSER for AP1000 design changes meeting Interim Staff Guidance 11. As guided by Section 7.8 of the Standard Review Plan, review of ATWS functions is performed by reactor systems reviewers. Specifically, under "Review Interfaces," in Section 7.8, the organization responsible for the review of reactor systems evaluates consistency of the ATWS mitigation protective functions with the requirements of 10 CFR 50.62 and the ATWS analysis referenced in the safety analysis report (SAR), Chapter 15, for anticipated operational occurrences and to verify the adequacy of the design of mechanical systems used to mitigate ATWS. In addition, the reactor systems reviewers are guided by Section 15.8, "Anticipated Transients Without Scram." I&C reviewers are to ensure adequate reliability, diversity, quality, and qualification of systems used to mitigate ATWS events.

In reviewing the staff's technical evaluation of DAS High Hot Leg Temperature Trip design change, the staff noted the addition of a time delay for opening the Passive Residual Heat Removal and requested additional information in RAI-DCP-CN63-ICE-01. The applicant responded and noted that the time delay was provided to support sequencing of the output field devices associated with a system level-control function. Use of the time delay was consistent with the use of timers in the existing functional design (e.g., low steam generator water level logic). The staff found the additional information to be acceptable. Specifically, time delays are commonly used in system-level actuation systems, including primary protection systems, to sequence equipment operation. Determination of the time delay would be part of the detailed design of DAS since selection of actual equipment would impact the time delay. Section 6.1.5.2 of WCAP-17184-P states that the [

].

In reviewing the staff's safety evaluation report, one area for improvement was identified. Specifically, the staff should include a discussion regarding that the addition of the new DAS High Hot Leg Temperature Reactor and Turbine Trip and its impact on DAS reliability, quality, and qualification and the basis for the staff's determination. The addition of a new DAS trip is would be implemented with the existing planned hardware (through FPGA logic) and should require minimal hardware additions. Addition of the trip function would not impact DAS architecture or detailed development process so far as DAS reliability, quality, qualification, and independence would not be affected by the change. Therefore, the staff's original conclusion that DAS can perform its functions in a reliable manner is not changed.

The staff's evaluation in Section 23.O of the staff's AFSER also does not address the acceptability of the new DAS reactor and turbine trip from an ATWS performance perspective. While this aspect of the staff's review is outside the scope of the Chapter 7 AFSER under concurrence, additional text will be included into the Chapter 7 AFSER to discuss the staff's acceptability of the new DAS trip with regards to ATWS performance. Specifically, the staff evaluated ATWS for the AP1000 as documented in NUREG-1793. For that evaluation, the applicant analyzed a number of cases that included scenarios with and without normal feedwater operating. The most limiting case was confirmed to be the loss-of-normal-feedwater event with turbine bypass operable, resulting in the highest RCS pressure. Addition of the hot leg temperature DAS trip would not alter that conclusion. The additional trip provides additional margin for the limiting case, and hence, is a conservative change that is acceptable for ATWS response.

V.A Requiring a Best-Estimate Analysis

The non-concurrence identifies questions about DAS functionality, but does not point to specific concerns about the analysis that was approved in the AP1000 certified design. The basis for the staff's conclusion in the certified design was reviewed to determine if the scope of the staff's review should have been expanded to require and review a deterministic, best-estimate analysis of DAS performance.

In Chapter 7 of NUREG-1793, the staff identified WCAP-13793, "AP600 System/Event Matrix," Revision 0, as supplemental information to confirm the adequacy of the focused PRA study determining DAS functions. As discussed in NUREG-1793, although the document was developed for AP600, it was found to be applicable to AP1000 as the two designs utilize the same systems and possess similar plant response. Section 3 of WCAP-13793 states that 11 full power events and 6 shutdown events are considered, and although it is not a comprehensive list of events, the events discussed in the document are expected to envelope other events. Events that are covered include those such as loss of main feedwater, loss of offsite power, steam line breaks, and loss-of-coolant accidents. WCAP-13793 describes the levels of defense provided by the normal control systems, primary protection and engineered safety feature systems, and back-up systems such as DAS. In reviewing the events, there are three to five lines of defense described for the events. These lines of defense include automatic actions by the control, protection, and back-up systems, as well as manual actions by operators. In comparing the DAS manual and automatic functions against the events and their lines of defense in WCAP-13793, there was no specific deficiency in DAS automatic or manual functions that would require an expansion in the scope of the staff's review to require a deterministic, best-estimate analysis in addition to the focus PRA study that was approved in the certified AP1000 design.

Appendix A of WCAP-17184 describes the DAS setpoint methodology. For the DAS automatic functions, the DAS setpoints are based on the same safety analytical limit used by PMS. The safety analytical limit for PMS is described in the Chapter 15 accident analysis, which is more conservative than a best-estimate, thermo-hydraulics analysis. The DAS setpoints are based on a 75 percent probability/75 percent confidence level for random and independent terms for instrument errors. Since the PMS uses 95/95 percent criteria for random and independent terms, the DAS setpoints are offset from the PMS setpoints, but still capable to protect the safety analytical limit. Only the DAS containment temperature input did not have an equivalent PMS input. However, WEC provided an equivalent temperature to containment pressure which is a PMS input. Section 7.8.2 of the Chapter 7 AFSEER describes the staff's acceptability of the DAS setpoint methodology. Since the DAS setpoint methodology is linked to the Chapter 15 accident analysis through the safety analytical limit, it provides supplemental confidence that DAS automatic performance is acceptable.

Based on the review of information provided by WEC to date on the DAS design, there was no basis identified to require the staff's scope of review to expand and include a deterministic, best-estimate analysis for DAS performance.

VI RESPONSE TO SPECIFIC CONCLUSIONS AND STATEMENTS IN THE NON-CONCURRENCE

The following is a response to specific conclusions and concerns that were identified in the non-concurrence.

1. Applicable Criteria for Diverse Instrumentation and Control Systems (Executive Summary)

“The NRC Staff review should be sufficient, thorough and complete such that proposed designs changes do not:

- Result in a design limit for a fission product barrier as described in the Certified AP1000 DCD final safety analysis report (FSAR) being exceeded or altered”

Response: The non-concurrence notes that the NRC staff’s review should ensure the design changes do not result in exceeding a design basis limit for a fission product barrier. The subject of the non-concurrence is the DAS, which addresses beyond design basis events such as ATWS and common-cause failure of the PMS. The AP1000 Chapter 15 analysis addresses the design of the plant to ensure design basis limits for fission product barriers are not exceeded. In the Chapter 15 analysis, PMS is the credited I&C system. DAS is not credited in the Chapter 15 analysis.

2. Introduction of New Event Scenarios That Have Not Been Adequately Evaluated (Executive Summary)

“The author will describe and explain how several of the AP1000 DCD DI&C designs changes combined with the staff not performing a complete and adequate review, may have introduced

- New event scenarios that have not been evaluated to ensure successful accident mitigation and adequate protection for the public.”

Response: The non-concurrence states the design changes may have introduced new event scenarios that have not been evaluated to ensure successful accident mitigation. Section VIII of the non-concurrence poses a question regarding an existing ATWS scenario and the capability of the new DAS reactor and turbine trip to mitigate the event, but a description of new event scenarios could not be found upon review of the non-concurrence. Also, an evaluation of the available AP1000 documentation did not reveal any new event scenario. Therefore, the staff’s original conclusion in Section 15.2.9 of NUREG-1793 is still valid since DAS functions would adequately address ATWS events in order to meet 10 CFR 50.62.

3. Failure to Consider Appropriate Review Standards and Methods (Section I)

“The author will demonstrate how the staffs review may not have considered the correct review standards and methods such that staff would not have been able to make a reasonable assurance finding that the AP1000 DCA design changes meet the stated regulatory requirements.”

Response: In the staff's original safety evaluation documented in NUREG-1793, the staff approved the use of an alternate method for determining DAS functionality using a focused PRA study versus a deterministic, best-estimate analysis. Specifically, in NUREG-1793, the staff acknowledged the existing guidance for defense-in-depth and diversity, including Branch Technical Position HICB-19 which discusses the deterministic, best-estimate analysis. Use of alternate methods to meet NRC regulations is acceptable so long as they can be demonstrated to provide a level of safety commensurate with the staff's guidance. As described in Section III.B of this document, the staff documented their basis for accepting the defense-in-depth and diversity analysis.

4. Failure to Utilize Proper Analysis for Several AP1000 DAS Design Changes (Section III)

“There are several AP1000 DCA DI&C design changes that have been made where the proper analysis was not provided by the applicant nor utilized by the staff to make a reasonable assurance finding that (1) the possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the certified Revision 15 AP1000 FSAR has been considered and that (2) analysis results of the design basis limits for a fission product barrier as described in the certified Revision 15 AP1000 FSAR will not be exceeded due to the design changes. The applicable Revision 18 AP1000 DCA DI&C design changes are:

- A. Addition of a new DAS high hot leg trip to help mitigate against Anticipated Transients Without Scram (ATWS) events
- B. Modification of the DAS to field programmable gate array (FPGA) based technology where proposed surveillance testing will disable credited automatically actuated functions
- C. Addition of Tier 1 ITAAC to evaluate the reliability of only three DAS system's manual actuations”

Response: As discussed in the previous sections of this response, an evaluation was performed on the scope of review for the AP1000 I&C amendments and it was determined that the scope of the review was appropriate. The author proposes that a deterministic, best-estimate analysis is the proper analysis that should be used. However, neither the non-concurrence or an evaluation of the AP1000 documentation

points to any specific deficiency in the focused PRA study method that was submitted by the applicant in the original design review and approved by the staff. Therefore, sufficient basis has not been provided to conclude that the deterministic, best-estimate analysis is the only proper method.

The non-concurrence addresses three design changes that specifically may not provide reasonable assurance of safety. The new DAS reactor and turbine trip is discussed in the non-concurrence and a response is provided in Section V of this document. However, the only discussion of FPGA in the non-concurrence is in the comment identified above. As such, there was no identified issue with the use of FPGAs for DAS vs. the original design that used microprocessor-based technology. Also, the non-concurrence discusses the new ITAAC to evaluate the three DAS manual action times. However, the non-concurrence did not discuss any specific concern or recommendations regarding the new ITAAC. As indicated in Section 7.8.2 of the staff's AFSER, those manual actions addressed by the ITAAC are the manual actions that do not have a corresponding DAS automatic actions. Since an event, coincident with a CCF of PMS, and a failure of any corresponding DAS automatic actions would need to occur before operator action is needed for the excluded manual actions, the staff determined that a specific ITAAC to verify the other manual actions was not necessary.

5. Change in Limiting ATWS Event (Section III – Case A)

“Therefore, the applicant is clearly indicating that a LONF [Loss of Normal Feedwater] event for ATWS may not bind all other postulated ATWS events. The safety issue for this design change is now two-fold:

- Is the sole addition of the DAS High Hot leg temperature sufficient for mitigating ATWS concerns and addressing ATWS requirements? Why or Why not?
- Are there other plant parameters that would be more efficient for addressing ATWS concerns, versus the High Hot Leg Temperature Trip addition (i.e., addition of DAS High PRZ Level trip to prevent opening PRZ relief valves)”

Response: The non-concurrence makes a conclusion that since a new DAS trip was introduced, that the most limiting ATWS event is no longer loss of normal feedwater. Addition of the new DAS trip does not mean that the loss of normal feedwater is not the limiting event since the original design would have addressed this particular scenario with the low steam generator level trip. Addition of the new DAS trip addresses other ATWS events that are not as severe in consequences as the loss of normal feedwater event. Section 4.27.1 of the AP1000 Probabilistic Risk Assessment, Revision 1, states that ATWS precursor transients, with main feedwater available, are not as severe as the ATWS precursor transients without main feedwater for the following two reasons. First, it is expected that the operators will have longer response times to terminate the event. Thus, the success of various manual trips increases. Second, if the ATWS continues,

the pressure spike in the reactor coolant system is not as severe as in the case of loss of main feedwater. This allows the possibility of riding out the ATWS and to perform boration.

The non-concurrence also poses questions regarding the performance capabilities of the new DAS High Hot Leg Temperature trip. To address the concerns raised on the new DAS High Hot Leg Temperature trip performance, the Chapter 7 AFSER will be modified as discussed in Section V of this response.

6. Failure to Ensure Continuous Operation of DAS (Section III – Case B)

“In WCAP-17184, Revision 2, “AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report” [ML102170263], July 2010, Section 6.1.2.2.4, states that the DAS ATWS mitigation functions should be available during Mode 1 when ATWS is a limiting event. It also states that the DAS ATWS mitigation function of reactor trip, turbine trip, and PRHR HX actuation should be available to provide ATWS mitigation capability. Therefore, if these credited automatic DAS ATWS functions are disabled at power, the AP1000 overall DI&C D3 ATWS mitigation scheme no longer conforms to the ATWS requirements of 10 CFR 50.62.”

Response: The non-concurrence interprets 10 CFR 50.62 to require DAS to be operable at all times during power operation. However, 10 CFR 50.62 requires the ATWS mitigation functions to be able to perform its functions in a reliable manner. There are no specific requirements or guidance that ATWS mitigation functions should be able to perform their functions in the presence of a single failure and/or a portion of the system out for maintenance. In comparison, primary protection systems are required by GDC 21, “Protection system reliability and testability,” to perform their functions in the presence of a single failure and with one channel out for maintenance. GDC 21 requires protection systems to possess high functional reliability and explains what is required of high reliability in that protection systems should function in the presence of a single failure and channel out for maintenance. Therefore, protection systems are generally a 2oo4 or similar voting logic to meet GDC 21. DAS testability and reliability is consistent with ATWS mitigation systems in operating reactors in that the systems may be taken out for maintenance or testing for a short duration and would not be able to perform their functions during that time period. As described in Section IV.B, other NRC requirements such as 10 CFR 50.65 limit the amount of time that DAS could be out of service.

7. Inadequate Demonstration of How AP1000 DAS is More Reliable Than Operating Reactors (Section III – Case B)

“Therefore, the staff in Chapter 19 has stated that it considers the DAS a reliable design and that it considers the DAS (ATWS) design at operating reactors to be “less reliable.” However, staff did not provide discussion on how it came to this

safety conclusion (NOTE: Chapter 7 FSER staff did not make the safety finding that DAS met 10 CFR 50.62 reliability requirements for the I&C design)."

Response: As described in Section 8.2 of WCAP-17184-P, the AP1000 design provides an availability goal of [

]. This goal was also described in the PRA for the original AP1000 design certification review. The ability of DAS to meet the reliable criteria of 10 CFR 50.62 is based on the AP1000's ability to meet the ATWS core damage frequency goal of less than 1e-5 per reactor year, as described in Section 15.8.3 of the AP1000 DCD, Tier 2. The 1e-5 ATWS core damage frequency goal is also discussed in SECY-83-293. Therefore, whether DAS reliability is better or worse than ATWS mitigation systems in operating reactors is immaterial to the reasonable assurance of safety finding for the AP1000. Specifically, the AP1000 is a drastically different design (passive) as compared to current pressurized water reactors. The overall plant design would affect the necessary reliability of an ATWS mitigation system. As such, a higher reliability may be necessary on some operating reactors requiring them to incorporate voting logic that is single failure tolerant. As noted in Section IV.A of this response, the staff did not explicitly state that the AP1000 met 10 CFR 50.62 in Chapter 7 of NUREG-1793, but it was stated in Chapter 15 of NUREG-1793.

8. Failure to Require a DAS Design That Withstands a Channel Out of Service (Section III – Case B)

"It would appear that advance reactors would need to demonstrate a design that can withstand an OOS channel and still be able to automatically actuate DAS credited automatic protective functions."

Response: See the response to Item 6 of this section.

9. Failure to Require a Basis for the DAS 2oo2 Voting Logic (Section III – Case B)

"Staff concluded in the AFSEER for the AP1000 DCA that the applicant's response to DI&C-ISG-02 guidance safety concern that the DAS two out of two (2oo2) actuation design logic places greater concern on postulated system "failures to actuate" than on preventing spurious actuations (Staff states that Revision 17 meets requirements of 10 CFR 50.62). However, the applicant has never stated or made a design basis case to demonstrate that the DAS 2oo2 actuation logic is a design that demonstrates adequate protection against failures to actuate reliably. Yet, the staff concluded, incorrectly, in the AFSEER that "no further evaluation is needed" and that Revision 17 meets the requirements of 10CFR50.62."

Response: The non-concurrence notes that Digital I&C (DI&C) Interim Staff Guidance (ISG) 02, "Task Working Group #2: Diversity and Defense in Depth Issues," Revision 2, is referenced in the Chapter 7 AFSER, and the guidance states that failures to actuate are of more concern than spurious actuations. The specific reference in DI&C-ISG-02, is found in Section 4, "Effects of Common-Cause Failure." The nuclear industry requested clarification regarding the effects of CCFs that should be considered (e.g., fails to actuate and/or spurious actuation). Industry also requested that the staff determine whether spurious actuations should be considered when evaluating software CCF []. As described in the industry's request and the staff's position and rationale, the focus of the failure to actuate and spurious actuation is on the safety-related, primary protection system and not the diverse actuation system. Specifically, within the Rationale portion of Section 4, the guidance states:

There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip or actuation is not required by plant conditions.

The guidance in DI&C-ISG-02 does not imply that diverse actuation systems should be designed to prevent a "failure to actuate," but rather the failure of primary protection systems to actuate are generally of higher concern than their spurious actuation. Section 7.8.2 of the Chapter 7 AFSER, states:

The guidance in DI&C-ISG-02, Revision 2, "Diversity and Defense-in-Depth Issues," Section 4, states that spurious trips and actuations are of a lesser safety concern than failures to trip or actuate.

This statement should be removed from the Chapter 7 AFSER to avoid the perception that the guidance directs diverse actuation systems to be designed to prevent failures to actuate (i.e., single failure protection of DAS).

As stated in Section IV.A of this document, a basis was provided by the applicant for use of 2oo2 voting logic. Clarification will be provided in the Chapter 7 AFSER regarding the staff's original approval.

10. Inadequate Technical Specification Allowed Outage Times For DAS

“Technical Specifications for the DAS automatically actuated protective functions would allow the DAS automatic functions to be disabled indefinitely. The applicant has not assigned limiting conditions of operations (LCOs) for disabled DAS automatic functions. It is the author’s opinion that design where one OOS channel would disable all automatic functions, and thus, the entire digital I&C could not demonstrated conformance to 10CFR50.62 and GDC 22 design requirements, is not design that cannot be found to be reliable.”

Response: The technical reasons for the acceptability of the DAS Technical Specification limiting conditions of operation are described in Section IV.B of this response.

11. ITAAC Verification For Only Three DAS Manual Actions

“ITAAC #5, in Tier 1, Section 2.5-1, of the Revision 18 AP1000 FSAR only proposes to evaluate three systems manual actuations controls on the DAS. These actuations selected are actuations that are not backed up by DAS automatic functions.”

Response: See the response to Item 4 of this section with regards to the DAS manual action ITAAC.

12. Failure of DAS to Meet 10 CFR 50.62 if Out-of-Service For 14 Days (Section III)

“Therefore, the DAS automatic functions can be disabled for up to fourteen days. It must be noted that during this fourteen day period that plant would not meet its ATWS licensing basis or the Commission’s ATWS requirements of 10CFR50.62.”

Response: The non-concurrence states that the fact that the DAS will not be able to perform its ATWS functions when it is out of service. As discussed in the response to Item 7 above, 10 CFR 50.62 requires ATWS functions to be performed reliably, but does not provide specific requirements that it remain functional when a portion of the system is out of service for maintenance or a single failure. In contrast, primary protection systems are required to remain functional in the presence of a single failure and one channel in maintenance per GDC 21. Allowance for ATWS mitigation systems to be out of service and not able to perform their functions for a limited period of time is consistent with current practice at operating reactors. In addition, DAS out-of-service for limited periods of time would be acceptable for the AP1000 so long as the DAS availability goal is met.

13. Use of the Focused-PRA study is Inconsistent With Staff Position on Use of PRA for I&C Systems (Section IV)

“Therefore, in order to meet its design basis and demonstrated conformance to the requirements of GDC 22 and 10CFR50.62, the applicant should submit a best estimate analysis to demonstrate that the small subset of DAS automatically actuated functions, (2) demonstrate adequate D3 diversity within the design for postulated failure modes, and (3) to demonstrate that reliable ATWS mitigation requirements and concerns are met. Without a best estimate analysis, a basis does not exist to demonstrate conformance to applicable requirements. However, staff found that the Revision 18 AP1000 DCS DI&C design changes were acceptable without utilizing a best estimate analysis.”

Response: As discussed in Section V of this document, the use of the focused-PRA study to determine DAS functions is an alternative method to the staff guidance (BTP 7-19). Use of an alternative method is acceptable, and the applicant did provide a basis in their original submittal, which were the results of the focused PRA study, as well as other confirmatory analyses including thermo-hydraulic analyses.

14. Disagreement With Staff Utilizing Risk Results to Make Conclusions on Safety (Section VI)

Response: Section VI of the non-concurrence addresses various staff guidance regarding the use of PRA to make safety conclusions on digital I&C systems. However, applicants may propose alternate methods to staff guidance, which is the case with the AP1000. As discussed in this response, the use of the focused PRA study was reviewed and approved by the staff in the original design review. Upon review of this non-concurrence and available AP1000 documents, no specific concern could be identified where the use of the focused-PRA study would be invalid. The DAS design does possess elements of a deterministic evaluation. For example, Section 15.2.9 of NUREG-1793 discusses the thermo-hydraulics analysis that was performed in the original design for ATWS functions involving loss of normal feedwater. In addition, DAS automatic action setpoints are based on the safety analytical limits from the Chapter 15 analysis, which is more conservative than a best-estimate analysis. Therefore, DAS functionality is not entirely based on the focused PRA study.

15. Failure of the Focused PRA Study to Address Adequate Functionality, Diversity, Reliability, or Time to Demonstrate Applicable Limits Are Not Exceeded (Section VII)

“Therefore, the applicant has demonstrated that by using a PRA analysis, they are able to add margin to improve an overall PRA sensitivity study; however, the sensitivity study’s margin increase does not necessarily demonstrate that the postulated accident scenario has adequate functionality, diversity, reliability, or

time to demonstrate that postulated fission product release will not exceed applicable limits.”

Response: The non-concurrence concludes that since the PRA sensitivity study cannot add PRA margin to the Direct Vessel Injection (DVI) line break events, then the PRA sensitivity studies cannot be used to demonstrate that postulated accident scenarios have been adequately addressed. However, consideration must be given to the AP1000 plant design. Injection of coolant to the core during design basis events is through two DVI lines. Chapter 15 assumes and models the break of a single DVI line. If PMS fails to address the event, DAS contains automatic and manual functions to address such an event, which is similar to a loss-of-coolant event. However, if both DVI lines break, there is no mechanical mechanism to inject coolant into the core. Using a deterministic, best-estimate for determining DAS functions would not improve upon the situation since the limitation is the mechanical construction of the AP1000.

16. Failure to Analyze ATWS Scenario

“ATWS Concern: For an anticipated operational occurrence (AOO) consisting of an inadvertent withdrawal of an individual rod or a bank of rods, combined with the failure of the controls rods to insert (ATWS event), with normal feedwater operating, will the high hot leg trip actuate before coolant flows out of a pressurizer (PRZ) pressure relief valve or exceed ATWS limitations?”

Response: The non-concurrence poses a question regarding an ATWS event that involves inadvertent rod withdrawal and normal feedwater available. In Section 15.2.9 of NUREG-1793, the staff discussed its basis for acceptance of the ATWS mitigation functions for the AP1000. In particular, events with loss of normal feedwater were determined to be the most limiting and to encompass the other events.

The question asks if the new DAS High Hot Leg Temperature reactor trip will perform for the specific scenario. The major issue with an ATWS event is an over-pressure condition that could exceed the pressure limits of the reactor coolant system. In order to arrive at an over-pressure condition, the reactor coolant must continue to heat-up, causing an expansion in the coolant that exceeds the letdown capability of the plant. According to Appendix A of WCAP-17184-P, the DAS High Hot Leg Temperature setpoint is [] as compared to the PMS High Hot Leg Temperature setpoint of []. Both setpoints are based on the safety analytical limit in the Chapter 15 analysis. With a difference of only [], it is expected that the DAS setpoint and function would be sufficient to address a reactor coolant heat-up in sufficient time.

As discussed in Item 6 above, when main feedwater is available, the ATWS transient is less severe since there is a means to remove the primary heat. This would either allow the reactor to ride out the transient or provide sufficient time for operators to manually actuate the trip or boration.

VII. CONCLUSIONS AND RECOMMENDATIONS

The staff's review and documented conclusions were evaluated to ensure the review was of adequate scope and provided a reasonable assurance of safety. Most concerns in the non-concurrence involved the staff's original review in NUREG-1793 or other sections of the AFSER for the AP1000 DCD, Revision 18. The staff coordinated this response with individuals responsible for the reactor systems and PRA reviews, who concur on the response.

For the concern associated with inadequate demonstration of DAS reliability and availability, there were no design changes that affected the DAS 2002 voting logic. As described in the response, 10 CFR 50.62 requires ATWS mitigation systems (DAS) to perform its functions reliably. The AP1000 design provides criteria for DAS availability to meet the ATWS core damage frequency goal. Requirements such as 10 CFR 50.65 will ensure the availability goal is met during plant operation. Furthermore, the LCOs for the DAS manual and automatic functions are consistent with operating reactors and other new plant designs.

For the concern regarding inadequate demonstration of DAS performance via the focused PRA study, there was one change that potentially impacted the design as approved in NUREG-1793. In the certified AP1000 design, if main feedwater was available, then the low steam generator trip may not function for some ATWS events. Therefore, a new ATWS reactor and turbine trip based on high hot leg temperature was introduced as a design change. In reviewing the basis for the design change, the original error appears to involve the implementation of the DAS functional analysis and not the analysis method itself. Such implementation errors could occur with other analysis methods, including deterministic, best-estimate analyses. While the non-concurrence raises questions, it does not identify specific design issues that require a best-estimate, thermo-hydraulics analysis to be submitted and reviewed by the staff. Based on the review of available AP1000 documents, no specific issues were identified that would require submittal of a best-estimate, thermo-hydraulics analysis and staff review. Therefore, the staff's scope of review related to DAS functionality was appropriate in Chapter 7 of the AP1000 AFSER.

The review of the staff's AFSER did identify improvements. Specifically, the following improvements are recommended for addition to the Chapter 7 AFSER.

- The staff's technical evaluation in Section 23.O did not discuss the staff's basis that addition of the new DAS High Hot Leg Temperature trip did not impact DAS reliability, quality, and qualification. Such discussion should be added to Chapter 7 of the staff's AFSER.
- Section 23.O did not provide a discussion on the performance of the new DAS trip. While this aspect is normally addressed by reactor systems reviewers under Chapter 15 of the AFSER, a basis for why the addition of the new DAS trip is acceptable should be provided in Chapter 7 of the AFSER.

- Although staff's approval of the 2oo2 voting logic is discussed in Chapter 7 of NUREG-1793, the Chapter 7 AFSER should provide clarification to the technical basis for the staff's acceptance of the 2oo2 voting logic.

In conclusion, the staff's technical evaluation and conclusions, as discussed in the AFSER for Chapter 7 of the AP1000 DCD, Tier 2, Revision 18, was appropriate in scope and technical basis to ensure reasonable assurance of safety. In particular, the staff's conclusion that the AP1000 meets 10 CFR 50.62 and GDC 22 are still valid.

NON-CONCURRENCE PROCESS

TITLE OF DOCUMENT

ADAMS ACCESSION NO.

SECTION C - TO BE COMPLETED BY DOCUMENT SPONSOR

NAME

Terry Jackson

TITLE

Advanced Final Safety Evaluation Report for AP1000 Design Cert Amendment - Digital I&C

PHONE NO.

301-415-7313

ORGANIZATION

NRO/DE/ICE/Branch 1

ACTIONS TAKEN TO ADDRESS NON-CONCURRENCE (This section should be revised, as necessary, to reflect the final outcome of the non-concurrence process, including a complete discussion of how individual concerns were addressed.)

Division Response to non-concurrence

The commitment to raising potential safety issues and expressing different technical opinions is welcomed and valued. We appreciate staff's willingness to identify areas where applicants have deviated from written guidance and pursue information to enhance their safety findings.

The concerns raised by the non-concurrence do not require revision to the AP1000 Design Control Document Revision 18 Safety Evaluation Report for Standard Review Plan Chapter 7 Instrumentation and Controls" (SER). As described in the attachment to Section B of this Non-Concurrence Process Form (Section VII., conclusions and recommendations), certain sections of the staff's SER will be revised to clarify the bases for the staff's conclusions. These changes to the SER do not affect the design or analyses submitted by the applicant, nor address issues raised in the non-concurrence. Therefore, there is no need to seek re-concurrence by the non-concurring individual in the revised SER as his concerns remain unresolved.

In summary, I agree with the staff's determination that the AP1000 Digital I&C system meets regulatory requirements in Title 10 of the Code of Federal Regulations (CFR). I concur with Mr. Jackson's response to the non-concurrence specifically, Section B, Item VI. While the non-concurrence raises several interesting questions, it does not identify any basis or evidence of safety issues associated with the methods used or the resulting functions and actuations of the I&C system. Overall, the questions and concerns documented in the non-concurrence and the request for the "best estimate analysis" may provide additional assurance for the conclusions in the safety evaluation, however the existing technical documents submitted by the applicant and reviewed by the staff meet the regulatory requirements and demonstrate the safety of the digital I&C system. As some of the issues raised in the non-concurrence are outside the scope of Chapter 7, the Division of Engineering has collaborated with the Division of Safety and Risk Analysis (DSRA) on this response, and DSRA concurs in this response.

Final Status of the non-concurrence: The non-concurrence remains in place.

With concurrence from:

Laura A. Dudes, Deputy Director
Division of Engineering

Laura A. Dudes
12/27/10

Mark D. Lombard, Deputy Director
Division of Safety Systems and Risk Assessment

Mark D. Lombard 12/27/10

☐ CONTINUED IN SECTION D

SIGNATURE - DOCUMENT SPONSOR

DATE

12/27/10

SIGNATURE - DOCUMENT SIGNER

DATE

12-23-10

NON-CONCURRING INDIVIDUAL (To be completed by document sponsor when process is complete, i.e., after document is signed):

☐ CONCURS

☒ NON-CONCURS

☐ WITHDRAWS NON-CONCURRENCE (i.e., discontinues process)

☒ WANTS NCP FORM PUBLIC

☐ WANTS NCP FORM NON-PUBLIC