

ENCLOSURE 4

WCAP-17184 -NP

Revision 0

“AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report”

(Non-Proprietary)

Westinghouse Non-Proprietary Class 3

WCAP-17184-NP
APP-GW-GLR-146
Revision 0

December 2009

AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report



WCAP-17184-NP
APP-GW-GLR-146
Revision 0

AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report

C. Daniel Stiffler*, Principal Engineer
Repair, Replacement and Automation Services

December 2009

Reviewer: John G. Ewald*, Lead I&C Engineer
Nuclear Power Plants

Stephen Seaman*, Technical Consultant
Repair, Replacement and Automation Services

Kyra A. Durinsky*, Project Manager
Diverse Actuation System

Approved: John S. Strong*, Program Manager
NuStart/DOE Design Finalization

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

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2009 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
0	C. Daniel Stiffler	Initial Issue

FOREWORD

The AP1000™ Diverse Actuation System (DAS) described in this document is a non-safety Instrumentation and Control (I&C) System that provides a diverse backup to the Protection and Safety Monitoring System (PMS). This backup is included to support the AP1000 risk goals by reducing the probability of a severe accident, which could potentially result from the unlikely coincidence of postulated transients and postulated common-mode failure in the PMS and the Plant Control System (PLS).

The purpose of the DAS is to lessen the probability of plant damage if the PMS fails to function when required and to reduce the frequency of the fuel core melting or containment failure in the probabilistic risk assessment (PRA).

[

]^{a,c} The DAS supports both automatic and manual actuations.

[

]^{a,c}

The scope of the technical report is to identify the DAS architecture and associated licensing basis at the functional design level. The overall DAS detailed design is not identified in the report. However, select design details are identified only for the purpose of architectural completeness or licensing compliance.

Section 1 provides a discussion of the AP1000 DAS design process. Section 2 of this document summarizes the AP1000 DAS functional requirements which received Design Certification and are compatible with the ALS hardware and software. Section 3 provides an overview of the AP1000 DAS. Section 4 addresses the interfaces between the safety system and non-safety systems. Section 5 addresses security and access control implementation. Section 6 discusses the applicability of digital I&C Branch Technical Positions. Section 7 describes the maintenance, test, and calibration features of the DAS implementation. Section 8 describes DAS reliability and availability goals. Section 9 addresses the diversity implementation of the DAS. Section 10 discusses US Nuclear Regulatory Commission (NRC) Digital I&C Interim Staff Guidance (ISG) applicability. Section 11 is the summary and conclusion.

TABLE OF CONTENTS

LIST OF TABLES v

LIST OF FIGURES vi

LIST OF ACRONYMS AND ABBREVIATIONS vii

LIST OF TRADEMARKS ix

DEFINITIONS x

REFERENCES xi

1 AP1000™ DAS DESIGN PROCESS 1-1

 1.1 PROJECT DEFINITION PHASE 1-3

 1.2 SYSTEM DEFINITION PHASE 1-3

 1.2.1 System Requirements Analysis 1-3

 1.2.2 []^{a,c} 1-3

 1.3 DEVELOPMENT PHASE 1-3

 1.3.1 System Architectural Design 1-3

 1.3.2 Hardware Development Phase 1-3

 1.3.3 Implementation Phase 1-4

 1.4 SYSTEM TEST PHASE 1-4

 1.5 INSTALLATION PHASE 1-4

2 AP1000 DAS FUNCTIONAL REQUIREMENTS 2-1

 2.1 SAFETY & QUALITY CLASSIFICATION 2-1

 2.1.1 Generic Letter 85-06 “Quality Assurance Guidance for ATWS Equipment
 that is not Safety-Related” 2-1

 2.1.2 10 CFR 50.55a(a)(1), “Quality Standards” 2-1

 2.1.3 Environmental Characteristics 2-2

 2.2 REACTOR TRIP (RT) FUNCTIONS 2-2

 2.2.1 10 CFR 50.62 Compliance 2-3

 2.3 ENGINEERED SAFETY FEATURES (ESF) ACTUATION SYSTEM FUNCTIONS 2-3

 2.3.1 Probabilistic Risk Assessment (PRA) Functional Basis 2-3

 2.4 SYSTEM STATUS FUNCTIONS 2-5

 2.5 GENERAL DESIGN BASIS 2-5

 2.5.1 SECY-93-087 Compliance 2-5

 2.5.2 10 CFR 50.55a(h), “Protection and Safety Systems” 2-8

 2.5.3 GDC 1, “Quality Standards and Records” 2-8

 2.5.4 GDC 13, “Instrumentation and Control” 2-9

 2.5.5 GDC 19, “Control Room” 2-9

 2.5.6 GDC 22, “Protection System Independence” 2-10

 2.5.7 GDC 24, “Separation of Protection and Control Systems” 2-11

 2.6 PREVENTION OF SPURIOUS & ACCIDENTAL ACTUATIONS 2-11

 2.6.1 []^{a,c} 2-12

 2.7 MANUAL INITIATION CAPABILITY 2-12

 2.8 COMPLETION OF PROTECTIVE ACTIONS 2-12

 2.9 DIVERSITY AND DEFENSE-IN-DEPTH ANALYSIS 2-12

TABLE OF CONTENTS (cont.)

	2.9.1	PRA Function Selection Justification.....	2-13
3		DAS OVERVIEW	3-1
	3.1	SYSTEM DESCRIPTION.....	3-1
	3.1.1	Cabinet Location Justification	3-6
	3.1.2	Independence from Protection System Justification.....	3-6
	3.1.3	Manual and Automatic Control Separation	3-6
4		SYSTEM INTERFACES.....	4-1
	4.1	INTERFACE BETWEEN NON-SAFETY AND SAFETY EQUIPMENT	4-1
	4.1.1	BTP 7-11, “Guidance on Application and Qualification of Isolation Devices”	4-1
5		SECURITY AND ACCESS CONTROL	5-1
	5.1	10 CFR 73.54 AND REG GUIDE 1.152 COMPLIANCE	5-1
	5.2	ACCESS CONTROLS	5-1
6		USE OF DIGITAL SYSTEMS	6-1
	6.1	BRANCH TECHNICAL POSITION (BTP) APPLICABILITY	6-1
	6.1.1	BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control System”	6-1
	6.1.2	BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions”	6-1
	6.1.3	BTP 7-18, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems”.....	6-5
	6.1.4	BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems”.....	6-6
	6.1.5	BTP 7-21, “Guidance on Digital Computer Real-Time Performance”.....	6-7
7		MAINTENANCE, TESTING, AND CALIBRATION	7-1
	7.1	SUMMARY OF COMPLIANCE TO GENERIC LETTER 85-06 ENCLOSURE	7-1
	7.1.1	Generic Letter 85-06 Enclosure Summary	7-1
	7.1.2	DAS Compliance.....	7-2
8		RELIABILITY AND AVAILABILITY	8-1
9		NUREG/CR 6303 COMPLIANCE AND DIVERSITY IMPLEMENTATION	9-1
	9.1	[] ^{a,c}	9-1
	9.2	[] ^{a,c}	9-1
	9.3	[] ^{a,c}	9-1
	9.4	[] ^{a,c}	9-2
	9.5	[] ^{a,c}	9-2
	9.6	[] ^{a,c}	9-2
10		DIGITAL I&C INTERIM STAFF GUIDANCE (ISG)	10-1
	10.1	ISG-1, “CYBER SECURITY”	10-1
	10.1.1	ISG-1 Overview.....	10-1
	10.1.2	DAS Applicability	10-1
	10.2	ISG-2, “DIVERSITY AND DEFENSE-IN-DEPTH (D3)”	10-1
	10.2.1	ISG-2 Overview.....	10-1
	10.2.2	DAS Applicability	10-5
11		SUMMARY AND CONCLUSION	11-1

LIST OF TABLES

Table 6-1 DAS ATWS Channel Availability6-3

Table 6-2 DAS ATWS Availability Requirements6-4

Table 6-3 DAS ESF Channel Availability.....6-4

Table 6-4 DAS ESF Availability Requirements.....6-5

LIST OF FIGURES

Figure 1-1 Correlation to Standard Life Cycle Phases 1-2
Figure 3-1 DAS Block Diagram 3-2
Figure 3-2 DAS Architecture 3-3

LIST OF ACRONYMS AND ABBREVIATIONS

Acronyms used in the document are defined in WNA-PS-00016-GEN, “Standard Acronyms and Definitions” (Reference 1), or included below to ensure unambiguous understanding of their use within this document.

2oo2	Two-out-of-two
AC	Alternating Current
ADS	Automatic Depressurization System
AFW	Auxiliary Feedwater
ALS	Advanced Logic System
ALWR	Advanced Light Water Reactor
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CCF	Common Cause Failure
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CMT	Coolant Makeup Tank
CSI	CS Innovations
D3	Diversity and Defense-In-Depth
DAS	Diverse Actuation System
DBE	Design Basis Event
DC	Direct Current
DCD	Design Control Document
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FAT	Factory Acceptance Testing
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
GDC	General Design Criteria
HFE	Human Factors Engineering
HX	Heat Exchanger
I&C	Instrumentation and Control
IRWST	In-service Refueling Water Storage Tank
ISG	Interim Staff Guidance
LCO	Limiting Condition for Operations
LRF	Large Release Frequency
M-G	Motor-Generator
MCR	Main Control Room
MTBF	Mean Time Between Failure
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PLC	Programmable Logic Controller

LIST OF ACRONYMS AND ABBREVIATIONS (cont.)

PLS	Plant Control System (AP1000)
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PWR	Pressurized Water Reactor
QA	Quality Assurance
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RFI	Radio Frequency Interference
RPS	Reactor Plant Scram
RT	Reactor Trip
SAR	Safety Analysis Report
SCA	Sneak Circuit Analysis
SG	Steam Generator
SRP	Standard Review Plan
SSC	Structures, Systems, and Components
TWG	Technical Working Group
USC	United States Code
V&V	Verification and Validation
WR	Wide Range

LIST OF TRADEMARKS

AP1000™ is a trademark of Westinghouse Electric Company LLC.

[]^{a,c}

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.

DEFINITIONS

Actuated Equipment:

The assembly of prime movers and driven equipment used to accomplish a protective function (such as hydraulic solenoids, shutdown rods, and valves) (Reference 9, Section 7.1).

Actuation Device:

A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves) (Reference 9, Section 7.1).

Channel:

An arrangement of components and modules required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined (Reference 10).

Component-Level Actuation:

Actuation of a single actuation device (component) (Reference 9, Section 7.1).

Protection and Safety Monitoring System:

The aggregate of electrical and mechanical equipment, which senses generating station conditions and generates the signals to actuate reactor trip (RT) and engineered safety features (ESFs), and which provides the equipment necessary to monitor plant safety-related functions during and following designated events (Reference 9, Section 7.1).

Protective Function:

Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the PMS logic and will be accomplished by the trip and actuation subsystems. Examples of protective functions are RT and ESFs (such as passive residual heat removal [PRHR] actuation and containment isolation) (Reference 9, Section 7.1).

Safety System:

The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events (Reference 9, Section 7.1).

System-Level Actuation:

Actuation of a sufficient number of actuation devices to affect a protective function (Reference 9, Section 7.1).

REFERENCES

1. WNA-PS-00016-GEN, Rev. 4 (Proprietary), "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.
2. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," U.S. Nuclear Regulatory Commission, April 16, 1985.
3. APP-GW-J4-001, Rev. 1 (Proprietary), "AP1000 I&C System Design Specification," Westinghouse Electric Company LLC.
4. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
5. NUREG-0800, Rev. 4, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, June 1997.
6. APP-GW-G1-010, Rev. 0 (Proprietary), "AP1000 Nuclear Safety Classification and Seismic Requirement Methodology," Westinghouse Electric Company LLC.
7. APP-GW-G1-002, Rev. 1 (Proprietary), "AP1000 Plant Equipment Qualification Methodology," Westinghouse Electric Company LLC.
8. APP-GW-GL-022, Rev. 0 (Proprietary), "AP1000 Probabilistic Risk Assessment," Westinghouse Electric Company LLC.
9. APP-GW-GL-700, Rev. 17 (Proprietary), "AP1000 Design Control Document," Westinghouse Electric Company LLC.
10. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1991.
11. Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission.
12. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection systems," U.S. Nuclear Regulatory Commission, October 21, 1994.
13. WCAP-13383, Rev. 1 (Proprietary), "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," Westinghouse Electric Company LLC.

REFERENCES (cont.)

14. WNA-PN-00056-WAPP, Rev. 1 (Proprietary), "NuStart/DOE Design Finalization Diverse Actuation System Project Plan," Westinghouse Electric Company LLC.
15. APP-DAS-GEH-001, Rev. 0 (Proprietary), "AP1000 Diverse Actuation System Design Process," Westinghouse Electric Company LLC.
16. APP-GW-J1R-004, Rev. 3 (Proprietary), "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Westinghouse Electric Company LLC.
17. 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," U.S. Nuclear Regulatory Commission.
18. Regulatory Guide 1.152, Rev. 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
19. APP-GW-E1-006, Rev. 0 (Proprietary), "AP1000 Cyber Security Design Criteria," Westinghouse Electric Company LLC.
20. Westinghouse Level II Policies and Procedures, Rev. 0 (Proprietary), Westinghouse Electric Company LLC, effective August 3, 2009.
21. APP-GW-GLR-143, Rev. 0 (Proprietary), "AP1000 Component Interface Module Technical Report," Westinghouse Electric Company LLC.

1 AP1000™ DAS DESIGN PROCESS

The development of the AP1000 Diverse Actuation System (DAS) is a joint effort between Westinghouse and CS Innovations (CSI). [

] ^{a,c} The DAS will utilize the Advanced Logic System (ALS) platform that is designed and manufactured by CSI. The ALS platform is based on field programmable gate array (FPGA) technology. [

] ^{a,c} The overall process maps into a standard Life Cycle Model. The descriptions of each phase explain the handoff points between the organizations. The following are the development phases:

- Design Requirements Phase
- System Definition
- Hardware and any Software Development Phase
- System Test Phase
- Installation Phase

Figure 1-1 shows both how these phases align with industry standard process and the organization that is responsible for the major effort.

a,c

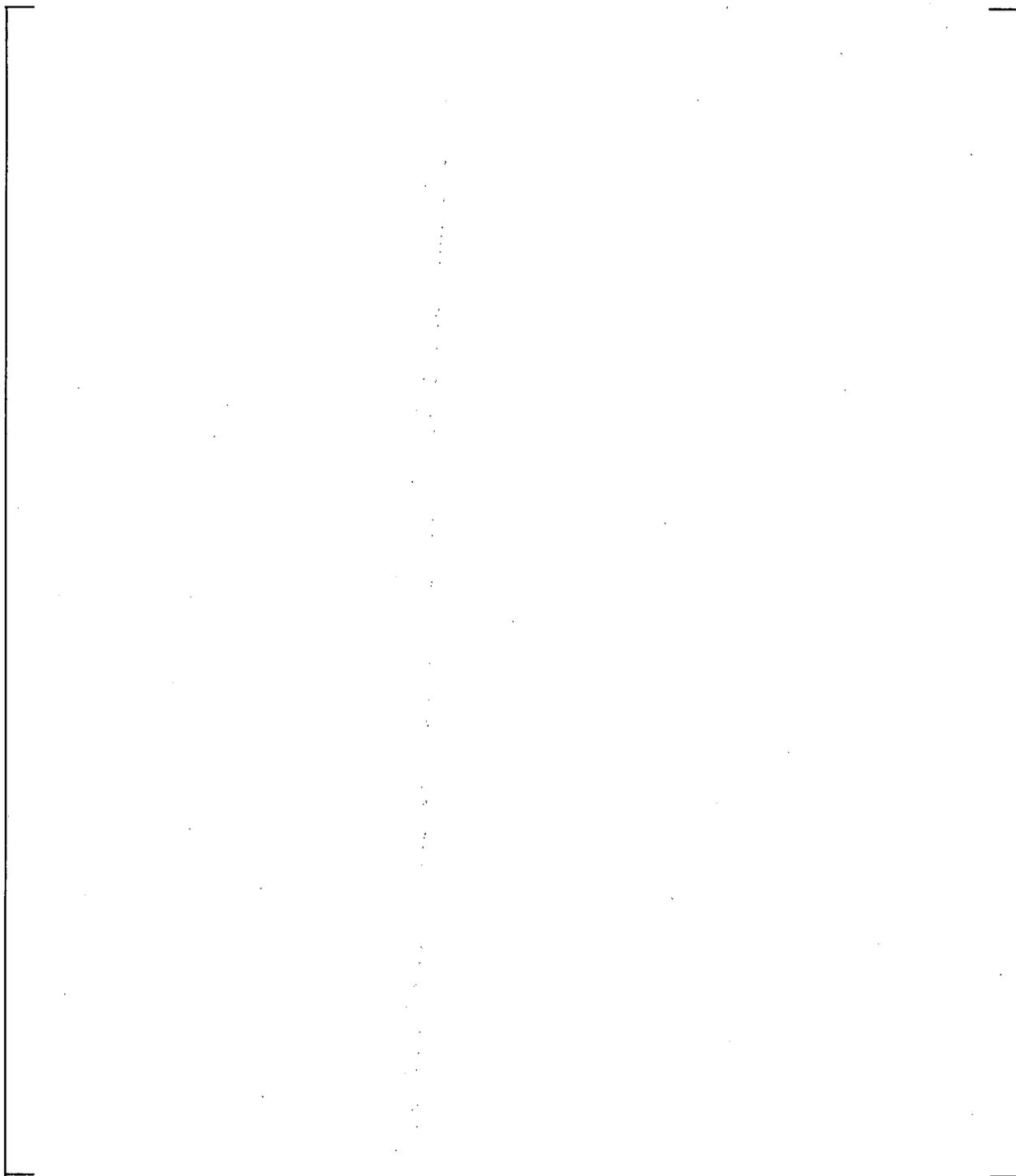


Figure 1-1 Correlation to Standard Life Cycle Phases

1.1 PROJECT DEFINITION PHASE

The project definition phase is a planning phase performed by Westinghouse prior to the design of the system. The major tasks in this phase are the project management planning and project baselining. As part of this planning, the project execution strategy is established, resources are identified, and organizational interfaces are defined.

1.2 SYSTEM DEFINITION PHASE

[
] ^{a,c} The output of this phase is the Functional Requirements Document, [
] ^{a,c}

1.2.1 System Requirements Analysis

In this task the project technical baseline is analyzed to specify the system requirements. These requirements comprise the overall requirements and constraints for the DAS. This task produces the Functional Requirements Document. [
] ^{a,c}

1.2.2 [] ^{a,c}

[
] ^{a,c}

1.3 DEVELOPMENT PHASE

[

] ^{a,c}

1.3.1 System Architectural Design

Westinghouse will identify the major hardware elements of the DAS and all of the interconnections as part of the development phase. The system requirements are allocated among these items. System hardware requirements are identified and external signals are allocated to individual elements within the DAS. [
] ^{a,c}

1.3.2 Hardware Development Phase

In this phase the final configuration of the production unit hardware is specified. The cabinet configuration drawings and cabinet interconnecting wiring diagrams are developed and issued during this

phase. [

] ^{a,c} The AP1000 plant-specific drawings will be formally issued by Westinghouse and contain all of the information necessary to produce the production unit hardware.

1.3.3 Implementation Phase

The implementation phase includes the development and production of a first article of the hardware.

[

] ^{a,c}

Once design verification is complete, Westinghouse is responsible for performing all qualification testing.

1.4 SYSTEM TEST PHASE

Individual hardware items are designed, implemented, and tested during the development phase. In the system test phase, completed cabinets containing the appropriate hardware are connected together as a system. System testing will be conducted on the completed system per the system test procedures. [

] ^{a,c}

The system test will be used as the factory acceptance testing (FAT).

1.5 INSTALLATION PHASE

The installation phase includes the installation and testing of the AP1000 DAS in the plant. [

] ^{a,c}

2 AP1000 DAS FUNCTIONAL REQUIREMENTS

2.1 SAFETY & QUALITY CLASSIFICATION

2.1.1 Generic Letter 85-06 “Quality Assurance Guidance for ATWS Equipment that is not Safety-Related”

2.1.1.1 Generic Letter 85-06 Overview

The NRC staff developed QA guidance for non-safety-related anticipated transient without scram (ATWS) equipment. The enclosure to Generic Letter 85-06 (Reference 2) provides the explicit QA guidance required by 10 CFR 50.62, “Requirements for Reduction of Risk from ATWS Events for Light-Water-Cooled Nuclear Power Plants” (Reference 4). The lesser safety significance of the equipment encompassed by 10 CFR 50.62 as compared to safety-related equipment, necessarily results in less stringent QA guidance.

2.1.1.2 DAS Compliance

Since the DAS performs many of the functions which are associated with reducing risks from ATWS events, it is designed to meet the quality guidelines established by Reference 1.

2.1.2 10 CFR 50.55a(a)(1), “Quality Standards”

2.1.2.1 10 CFR 50.55a(a)(1) Overview

Structures, systems, and components (SSCs) must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

2.1.2.2 DAS Compliance

The DAS functions are rated as safety Category B. [

] ^{a,c} The DAS functions may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated environmental conditions.

The DAS equipment is designed to comply with Equipment Class D requirements. [

] ^{a,c} Class D is of sufficient quality to perform the necessary function under the associated event conditions. The DAS function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Quality standards also applicable to the DAS are identified in 10 CFR 50.62 (c.1) (Reference 4); NUREG-0800, BTP 7-19 B.1 (3) (Reference 5); Generic Letter 85-06 (Reference 2); [] ^{a,c}

[]^{a,c}

2.1.3 Environmental Characteristics

[]^{a,c}

The DAS is located in a controlled environment, but is capable of functioning during and after normal and abnormal events and conditions that include:

- Temperature range of 40° to 120°F
- Non-condensing relative humidity up to 95 percent
- RFI/EMI

[]^{a,c}

2.2 REACTOR TRIP (RT) FUNCTIONS

The DAS automatically initiates a reactor and turbine trip upon the occurrence of low steam generator wide range (WR) water level or low pressurizer water level.

[]^{a,c}

The DAS provides the capability for manually initiating a reactor and turbine trip from a dedicated DAS control panel which is located in the MCR. []^{a,c}

[

] ^{a,c}

RT is initiated by energizing breaker trip coils on the field breakers of the control rod motor-generator sets. Opening these breakers causes the loss of power to the control rod drive mechanisms, resulting in the release of the control rods so that they fall into the core.

Turbine trip is initiated by energizing coils which actuate trip solenoids within the Turbine Control System.

2.2.1 10 CFR 50.62 Compliance

The DAS is designed to meet the requirements established by 10 CFR 50.62 (Reference 4). 10 CFR 50.62 requires that each PWR contain equipment from sensor output to final actuation device, that is diverse from the reactor protection system, to automatically initiate the auxiliary feedwater (AFW) system and turbine trip under conditions indicative of ATWS. The DAS is comprised of equipment from sensor output to final actuation device that is diverse from the RT system. The DAS performs an automatic reactor and turbine trip under conditions indicative of ATWS [

] ^{a,c}

2.3 ENGINEERED SAFETY FEATURES (ESF) ACTUATION SYSTEM FUNCTIONS

2.3.1 Probabilistic Risk Assessment (PRA) Functional Basis

The purpose of the DAS is to lessen the probability of plant damage if the Protection and Safety Monitoring System (PMS) fails to function when required and reduces the frequency of the fuel core melting or containment failure in the PRA [

] ^{a,c}

[

]a,c

[

] ^{a,c}

2.4 SYSTEM STATUS FUNCTIONS

[

] ^{a,c} The following sequence and alarm points are provided to the operators in the MCR.

- Manual DAS actuations have been enabled
- An automatic actuation signal has been generated from either of the DAS processor cabinets
- The DAS has manually initiated an output actuation command
- Any DAS channel has been bypassed (test/maintenance mode)
- DAS automatic logic has failed or malfunctioned

2.5 GENERAL DESIGN BASIS

2.5.1 SECY-93-087 Compliance

2.5.1.1 Section I-B, “Anticipated Transient Without Scram” Overview

As discussed in SECY-90-016, the ATWS Rule (10 CFR 50.62 [Reference 4]) was promulgated to reduce the probability of an ATWS and to enhance mitigation capability if such an event occurred. The NRC staff recommended that the commission approve its position that diverse scram systems should be provided for evolutionary advanced light water reactors (ALWRs).

2.5.1.2 DAS Compliance

The DAS provides a diverse method for RT. RT is initiated by energizing breaker trip coils on the field breakers of the control rod motor-generator sets. Opening these breakers causes the loss of power to the control rod drive mechanisms resulting in the release of the control rods so that they fall into the core.

[

] ^{a,c}

2.5.1.3 Section II-A, "Industry Codes and Standards" Overview

In SECY-91-273, "Review of Vendors' Test Program to Support the Design Certification of Passive Light-Water Reactors," dated August 27, 1991, the NRC staff raised the concern that a number of design codes and industry standards dealing with new plant construction had recently been developed or modified, and that the NRC has not yet determined their acceptability.

The NRC staff recommended that the commission approve the position consistent with past practice that it will review both evolutionary and passive plant design application using the newest codes and standards that have been endorsed by the NRC.

2.5.1.4 DAS Compliance

The DAS complies with applicable codes and standards for non-safety systems as [

] ^{a,c}

2.5.1.5 Section II- Q, "Defense Against Common-Mode Failures in Digital I&C Systems" Overview

I&C systems help ensure that the plant operates safely and reliably by monitoring, controlling, and protecting critical plant equipment and processes. The digital I&C systems for ALWRs differ significantly from the analog systems used in operating NPPs. Specifically, digital I&C systems share more data transmission functions and more process equipment than their analog counterparts.

Redundant trains of digital I&C systems may share databases (software) and process equipment (hardware). Therefore, a hardware design error, software design error, or software programming error may result in a common-mode or common-cause failure of redundant equipment. The NRC staff is concerned that the use of digital computer technology in I&C systems could result in safety significant common-mode failures. Quality and diversity are important defenses against common-mode failures.

The NRC staff has concluded that analyses that demonstrate adequate, rather than equivalent, defense against the postulated common-mode failures would be allowed in the diversity assessment required of the applicant. The critical safety functions that require backup manual controls and displays would be specified. The intent is to permit the use of diverse digital equipment that is not affected by the identified common-mode failures and to reduce complexity in the design.

As a result of these changes, the staff revised the initial position proposed in the draft commission paper. The staff recommends that the commission approve the following revised staff position:

1. The applicants shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed. The staff considers software design errors to be credible common-mode failures that must specifically be included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. Other methods proposed by an applicant will be reviewed individually.
2. 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). The vendor or applicant shall demonstrate adequate diversity within the design for each of these events. For events postulated in the plant SAR, an acceptable plant response should not result in a non-coolable geometry of the core, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.
3. If a postulated common-mode failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or non-digital systems are considered acceptable means. Manual actions from the control room are acceptable if adequate time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated individually.
4. A set of safety-grade displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above. The specific set of equipment shall be evaluated individually, but shall be sufficient to monitor the plant states and actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition. In addition, the specific equipment should be intended to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

2.5.1.6 DAS Compliance

The DAS provides defense-in-depth and is diverse from the PMS [

] ^{a,c} The DAS provides a diverse set of manual system-level controls and associated indications for critical safety functions as identified in BTP 7-19, Position 4 (Reference 11).

2.5.2 10 CFR 50.55a(h), “Protection and Safety Systems”

2.5.2.1 10 CFR 50.55a(h) Overview

(h) *Protection and safety systems.* (1) IEEE Standard 603-1991 (Reference 10), including the correction sheet dated January 30, 1995, which is referenced in paragraphs (h)(2) and (h)(3) of this section, is approved for incorporation by the Director of the Office of the Federal Register in accordance with 5 United States Code (USC) 552(a) and 1 CFR Part 51. IEEE Standard 279, which is referenced in paragraph (h)(2) of this section, was approved for incorporation by the Director of the Office of the Federal Register in accordance with 5 USC 552(a) and 1 CFR Part 51.

(2) *Protection systems.* For NPPs with construction permits issued after January 1, 1971, but before May 13, 1999, protection systems must meet the requirements stated in either IEEE Standard 279, “Criteria for Protection Systems for Nuclear Power Generating Stations,” or in IEEE Standard 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. For NPPs with construction permits issued before January 1, 1971, protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Standard 603-1991 and the correction sheet dated January 30, 1995.

(3) *Safety systems.* Applications filed on or after May 13, 1999 for construction permits and operating licenses under this part and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Standard 603-1991 and the correction sheet dated January 30, 1995.

2.5.2.2 DAS Applicability

The DAS is a non-safety system with no required redundancy requirements. IEEE Standard 603 (Reference 10) is not applicable for the DAS.

2.5.3 GDC 1, “Quality Standards and Records”

2.5.3.1 GDC 1 Overview

SSCs important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A QA program shall be established and implemented in order to provide adequate assurance that these SSCs will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of SSCs important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

2.5.3.2 DAS Compliance

The DAS quality standards are discussed in Section 2.1, “Safety and Quality Classification.”

2.5.4 GDC 13, “Instrumentation and Control”

2.5.4.1 GDC 13 Overview

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

2.5.4.2 DAS Compliance

The DAS design is driven by NRC 10 CFR 50.62 (Reference 4) and BTP 7-19, Position 4 (Reference 11).

CFR 50.62 identifies that each PWR must have equipment from the sensor output to the final actuation device that is diverse from the RT system to automatically initiate the AFW system and initiates a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and independently (from sensor output to the final actuation device) from the existing RT system.

BTP 7-19, Position 4 identifies that a set of displays and controls located in the MCR should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

The DAS provides a diverse (alternate) and independent method for []^{a,c} tripping the reactor, []^{a,c} Additionally, a set of dedicated, independent displays of select plant indications and manual controls is provided in the MCR to meet the criteria in BTP 7-19, Position 4.

The DAS lessens the probability of plant damage if the PMS fails to function when required and reduces the frequency of the fuel core melting or containment failure []^{a,c} The DAS is not needed if the PMS functions properly.

2.5.5 GDC 19, “Control Room”

2.5.5.1 GDC 19 Overview

A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a

safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Applicants for and holders of construction permits and operating licenses under this part who apply on or after January 10, 1997; applicants for design approvals or certifications under part 52 of this chapter who apply on or after January 10, 1997; applicants for and holders of combined licenses or manufacturing licenses under part 52 of this chapter who do not reference a standard design approval or certification; or holders of operating licenses using an alternative source term under 10 CFR 50.67, shall meet the requirements of this criterion, except that with regard to control room access and occupancy, adequate radiation protection shall be provided to ensure that radiation exposures shall not exceed 5 rem total effective dose equivalent as defined in 10 CFR 50.2 for the duration of the accident.

2.5.5.2 DAS Compliance

The PMS is designed with remote shutdown capabilities that meet GDC 19 criteria.

[

] ^{a,c}

2.5.6 GDC 22, “Protection System Independence”

2.5.6.1 GDC 22 Overview

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.

2.5.6.2 DAS Compliance

[

] ^{a,c}

[

]a,c

DAS diversity from the PMS is discussed in Section 9.

2.5.7 GDC 24, “Separation of Protection and Control Systems”

2.5.7.1 GDC 24 Overview

The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

2.5.7.2 DAS Compliance

The DAS is not interlocked with the plant control (PLS). As a best engineering practice, the DAS also uses an architecture that is diverse from the PLS to eliminate common mode failure concerns with plant control.

2.6 PREVENTION OF SPURIOUS & ACCIDENTAL ACTUATIONS

Specific design features are incorporated in the DAS to prevent spurious actuations. [

]a,c

Accidental actuations are primarily associated with DAS manual actuation functions. [

]a,c

[
] ^{a,c}

2.6.1 [] ^{a,c}

[

] ^{a,c}

2.7 MANUAL INITIATION CAPABILITY

DAS manual and automatic controls are not interlocked. [

] ^{a,c}

2.8 COMPLETION OF PROTECTIVE ACTIONS

[

] ^{a,c}

2.9 DIVERSITY AND DEFENSE-IN-DEPTH ANALYSIS

The DAS design is primarily PRA-based. [

] ^{a,c}

2.9.1 PRA Function Selection Justification

See subsection 2.3.1 for the discussion on the DAS PRA basis and associated function selection.

3 DAS OVERVIEW

3.1 SYSTEM DESCRIPTION

[

] ^{a,c} DAS automatic actuation is supported by redundant logic subsystems. The signal processing block utilizes the ALS designed and manufactured by CSI. The ALS utilizes FPGA technology to implement the hardware architecture platform for the DAS automatic actuation functionality. [

] ^{a,c}

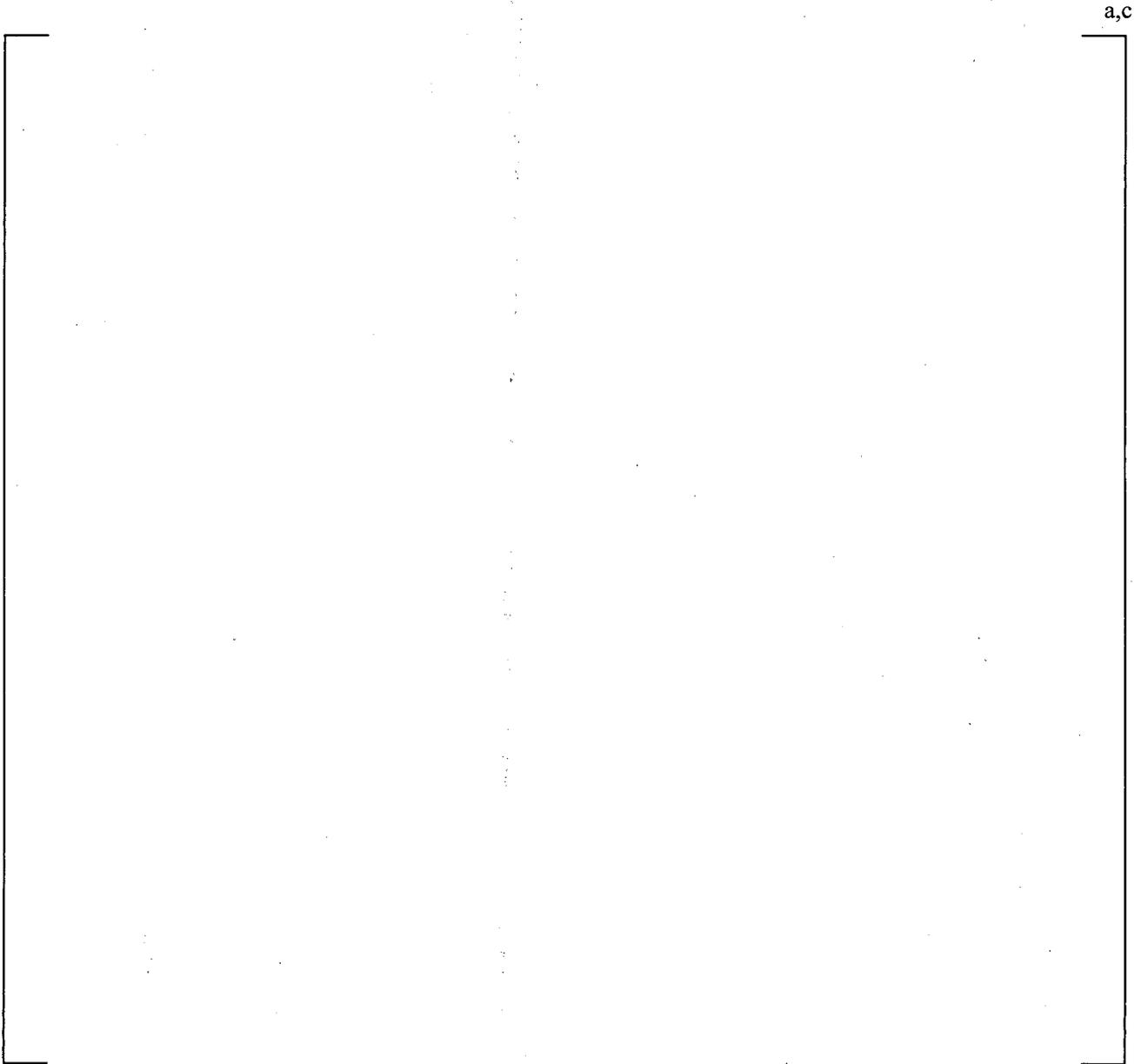


Figure 3-1 DAS Block Diagram

Figure 3-2 provides an overview of the DAS cabinetry layout.

a,c



Figure 3-2 DAS Architecture

The DAS consists of the following equipment:

- DAS Instrumentation Cabinet
- DAS Processor Cabinet 1
- DAS Processor Cabinet 2
- DAS Squib Valve Controller Cabinet
- DAS Manual Actuation Controls (located on the DAS Control Panel and the DAS Instrumentation Cabinet)
- DAS Process Instrumentation Displays (located on the DAS Control Panel and the DAS Instrumentation Cabinet)

DAS Instrumentation Cabinet

The DAS Instrumentation Cabinet contains plant process field terminations, power supplies, signal conditioning, dedicated plant process displays, and termination areas associated with the interconnection of this cabinet to other equipment.

The DAS Instrumentation Cabinet receives the plant process signals from the dedicated DAS sensors. The cabinet provide signal conditioning of process signals associated with dedicated DAS sensors. The DAS sensors are provided by other systems. The signals received from these DAS sensors are filtered, scaled, and provided to the DAS process indicating displays and are input to the DAS processor cabinets via serial data communication links. [

] ^{a,c}

DAS Processor Cabinets

The two DAS processor cabinets contain the DAS logic subsystem, power supplies, signal conditioning, output conditioning, and termination areas associated with the interconnection of these cabinets to other equipment.

The DAS logic subsystem evaluates select process signal inputs provided by Instrumentation Cabinet against fixed setpoints to determine the need for automatic DAS actuation. [

] ^{a,c}

DAS Squib Valve Controller Cabinet

The squib valve controller cabinet contains the individual squib valve controllers which interface with the igniters of the squib valves. [

] ^{a,c}

DAS Manual Actuation Controls

Manual actuation of DAS functions is provided by manual actuation controls. [

] ^{a,c}

[

] ^{a,c}

DAS Manual Actuation Switches

The DAS manual actuation switches are located on a dedicated panel which is located in the MCR. [

] ^{a,c}

DAS Process Indicating Displays

The DAS process indications are located on the DAS Control Panel and the DAS Instrumentation Cabinet. Each DAS process indicating display receives its associated plant process signal via serial data communication data links routed from the DAS Instrumentation Cabinet. The DAS process indicating displays are powered from the instrumentation cabinet DC power supplies.

3.1.1 Cabinet Location Justification

[

] ^{a,c}

The DAS cabinets are located in a different fire zone from the PMS cabinets.

[

] ^{a,c}

3.1.2 Independence from Protection System Justification

For most control and indication functions, the DAS is standalone system within the AP1000 I&C suite. DAS contains a few interfaces with other systems.

[

] ^{a,c}

3.1.3 Manual and Automatic Control Separation

The DAS manual and automatic controls are separated in the architecture. [

] ^{a,c}

4 SYSTEM INTERFACES

4.1 INTERFACE BETWEEN NON-SAFETY AND SAFETY EQUIPMENT

As previously identified, the DAS is standalone system within the AP1000 I&C suite for most control and indication functions. DAS contains a few interfaces with other systems.

4.1.1 BTP 7-11, “Guidance on Application and Qualification of Isolation Devices”

4.1.1.1 BTP 7-11 Overview

BTP 7-11 provides guidelines for reviewing the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. This BTP deals with the criteria and methods used to confirm that the design of isolation devices assures that credible failures in the connected non-safety or redundant channels will not prevent the safety systems from meeting their required functions.

Isolation devices should be classified as part of the safety system and powered in accordance with criteria of IEEE Standard 603-1991 (Reference 10) or IEEE Standard 279-1971 and the guidelines of Regulatory Guide 1.75. If non-safety power sources interface to the isolation device, the applicant/licensee should verify that the non-safety power is not required for the device to perform its isolation function.

4.1.1.2 DAS Compliance

The DAS utilizes a limited number of non-safety to safety interfaces: motor operated valve control at the associated motor control center. The isolation is accomplished by the safety system for these interfaces.

5 SECURITY AND ACCESS CONTROL

5.1 10 CFR 73.54 AND REG GUIDE 1.152 COMPLIANCE

The DAS functional and follow-on detailed design implementation is compliant with 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Reference 17).

As previously identified in Section 3.1.2, the DAS is standalone system within the AP1000 I&C suite for most control and indication functions. DAS contains only a few interfaces with other systems. In addition, the DAS uses the CSI ALS platform. []^{a,c}

The overall DAS design is subject to independent verification and validation (V&V) by Westinghouse security engineering personnel to meet the intent of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" (Reference 18), []^{a,c}

Cyber security assessments are performed throughout the design lifecycle to ensure cyber security controls are implemented per 10 CFR 73.54 (Reference 17).

[

] ^{a,c}

5.2 ACCESS CONTROLS

[

] ^{a,c}

6 USE OF DIGITAL SYSTEMS

6.1 BRANCH TECHNICAL POSITION (BTP) APPLICABILITY

6.1.1 BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control System"

6.1.1.1 BTP 7-14 Overview

An appropriate set of life cycle activities is provided in Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Standard 1074-1995, "Standard for Developing Life Cycle Processes."

Commercial-off-the-shelf software and software embedded in commercial-off-the-shelf components, such as meters, circuit breakers, or alarm modules should be appropriately evaluated to confirm that required characteristics are met. Electric Power Research Institute (EPRI) Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as approved by NRC's safety evaluation dated July 17, 1997, describes an acceptable method for performing this evaluation. NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," provides additional background information.

6.1.1.2 DAS Applicability

[

] ^{a,c}

6.1.2 BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions"

6.1.2.1 BTP 7-17 Overview

Surveillance test and self-test features for digital computer-based protection systems should conform to the guidance of Regulatory Guide 1.22 and Regulatory Guide 1.118. Bypasses necessary to enable testing should conform to the guidance of Regulatory Guide 1.47.

Failure Detection

Failures detected by hardware, software, and surveillance testing should be consistent with the failure detectability assumptions of the single-failure analysis and the failure modes and effects analysis (FMEA).

Self-Test Features

Digital computer-based I&C systems should include self-test features to confirm computer system operation on system initialization. Digital computer-based I&C systems should generally include continuous self-testing. Some small, standalone, embedded digital computers may not need self-testing.

Typical self-tests include monitoring memory and memory reference integrity, using watchdog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

Self-test functions should be verified during periodic functional tests.

Surveillance Testing

Systems should be able to conduct periodic surveillance testing consistent with the technical specifications and plant procedures. As delineated in Regulatory Guide 1.118, periodic testing consists of functional tests and checks, calibration verification, and time response measurements.

Actions on Failure Detection

The design should have either the automatic or manual capability to take compensatory action on detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other.

6.1.2.2 DAS Applicability

Failure Detection

[

] ^{a,c}

Self-Test Features

See the discussion under “Failure Detection.”

Surveillance Testing

The DAS manual controls provide non-Class 1E backup controls in case of common-mode failure of the PMS automatic and manual actuations [

] ^{a,c}

[

] ^{a,c}

Actions on Failure Detection

ATWS Mitigation Function of DAS

The DAS ATWS mitigation function of RT, turbine trip, and PRHR HX actuation should be available to provide ATWS mitigation capability. The PRHR HX is the passive functional equivalent of the conventional-plant AFW system. PRHR provides a safety-grade heat sink. This function is important based on 10 CFR 50.62 (Reference 4) (ATWS Rule) and because it provides margin in the PRA

[

] ^{a,c}

] ^{a,c}

[]^{a,c}

Table 6-2 DAS ATWS Availability Requirements		

[]^{a,c}

Table 6-3 DAS ESF Channel Availability				

[]^{a,c}

[

] ^{a,c}

6.1.3 BTP 7-18, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems”

6.1.3.1 BTP 7-18 Overview

Purchased programmable logic controller (PLC) hardware, embedded and operating systems software, programming tools, and peripheral components should be qualified to a level commensurate with the system they are designed to support. EPRI TR-106439 and EPRI TR-107330 describe an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides additional information on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors for purchased PLC software.

6.1.3.2 DAS Applicability

The DAS does not employ PLC technology. BTP 7-18 is not applicable to the DAS.

6.1.4 BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems”

6.1.4.1 BTP 7-19 Overview

The NRC staff has identified four echelons of defense against common-cause failures:

- Control System – Consists of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor.
- RT System – Consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- Engineered Safety Features Actuation System (ESFAS) – Consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).
- Monitoring and Indicators – Consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of ALWR design certification applications for designs that use digital protection systems, the NRC has established the following four-point position on Diversity and Defense-in-Depth (D3) for ALWRs and for digital system modifications to operating plants:

- Point 1: The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.
- Point 2: In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.
- Point 3: If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
- Point 4: A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The above four-point position is based on the NRC concern that software design errors are a credible source of common-cause failures. Software cannot typically be proven to be error-free and is therefore considered susceptible to common-cause failures because identical copies of the software are present in redundant channels of safety-related systems. For digital system modifications to operating plants, retention of existing displays and controls in the MCR may satisfy Point 4.

6.1.4.2 DAS Applicability

DAS defense-in-depth features are discussed in Reference 16.

The DAS is a non-safety-related I&C system, diverse and separate from the safety-related system. The DAS provides the functions necessary to reduce the risk associated with a postulated common mode failure of critical protection system I&C functions. [

] ^{a,c}

The DAS is in compliance with BTP 7-19, Position 4 (Reference 11); a set of displays and controls located in the MCR is provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

6.1.5 BTP 7-21, "Guidance on Digital Computer Real-Time Performance"

6.1.5.1 BTP 7-21 Overview

If the following criteria are met, the NRC staff may conclude that the design or completed system will meet timing requirements, can be verified as correct and timely, or that a prototype system accurately reflects the performance and correctness expected of the actual plant. Some of the criteria described

herein may be met by submissions describing a software development process or verification methods that include real-time concerns.

Limiting Response Times

Limiting response times should be shown to be consistent with safety requirements (e.g., suppress power oscillations, prevent fuel design limits from being exceeded, prevent a non-coolable core geometry). Setpoint analyses and limiting response times should also be shown to be consistent. The reviewer should verify that limiting response times are acceptable to the organizations responsible for reactor systems, electrical systems, and plant systems before accepting the limiting response times as a basis for timing requirements.

Digital Computer Timing Requirements

Digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems. Computer system timing requirements that should be addressed in a software requirements specification are described in Standard Review Plan (SRP) BTP 7-14.

Architecture

The level of detail in the architectural description should be sufficient that the NRC staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available. Subsequent detailed design and implementation should develop refined timing allocations down to unit levels in the software architecture.

Design Commitments

Design basis documents should describe system timing goals.

Performance Verification

The means proposed, or used, for verifying a system's timing should be consistent with the design.

Use of Cyclic Real-Time Executive

In systems that include a cyclic real-time executive (operating system), a typical cycle includes application modules, diagnostic modules, and other support modules. A watchdog timer is normally set at the beginning of each cycle and reset at the end. If the cycle is not completed before the watchdog timer period is complete, an error is generated.

Use of Part-Scale Prototypes

In systems that have not been implemented and tested on a full scale, expected system delays on scale-up should be calculated and shown to be less than limiting system response times (NUREG/CR-6083, Sections 2.1.3 and 2.1.4).

6.1.5.2 DAS Applicability

[

] ^{a,c}

7 MAINTENANCE, TESTING, AND CALIBRATION

[

] ^{a,c}

The DAS will contain the necessary equipment to maintain, test, and calibrate the system along with simple maintenance tools such as voltmeters.

Each automatic actuation channel is provided with manual block and unblock functions at the cabinet level. These functions provide the capability for testing the DAS channels while the plant is operating by simulating a process signal change for a channel plant parameter value. [

] ^{a,c}

7.1 SUMMARY OF COMPLIANCE TO GENERIC LETTER 85-06 ENCLOSURE

7.1.1 Generic Letter 85-06 Enclosure Summary

The enclosure to Generic Letter 85-06 provides the explicit QA guidance required by 10 CFR 50.62. The lesser safety significance of the equipment encompassed by 10 CFR 50.62, as compared to safety-related equipment, necessarily results in less stringent QA guidance. An enclosure summary is as follows:

10 CFR 50 Appendix B Requirement

XI. Testing

Measures are to be established to test, as appropriate, non-safety-related ATWS equipment prior to installation and operation and periodically. Results of the tests should be evaluated to ensure that the test requirements have been satisfied.

XIV. Inspection, Test, and Operating Status

Measures are to be established to indicate status of inspection, test, and operability of installed non-safety-related ATWS equipment.

7.1.2 DAS Compliance

Subsection 6.1.2 provides an overview of the testing and surveillance requirements required for the ATWS feature in the DAS.

8 RELIABILITY AND AVAILABILITY

[

] ^{a,c}

The following is a summary of the analyses that will occur for the DAS during the detailed design phase.

A FMEA is a systematic, inductive reasoning process that determines the role of each component of an I&C system in achieving the overall system dependability goals. The FMEA will establish the qualitative reliability of the DAS and the information gained will be used to develop an analysis report. The report will be used to provide licensing support to prove the DAS meets and/or exceeds the reliability goals set for the system.

The DAS also has quantitative reliability goals and availability goals that must be measured. Since the DAS uses simpler functions, a reliability block diagram analysis will be used to determine the overall system function availability. The FMEA will be used as a guide for the analysis to determine the important system functions that need to be illustrated in the analysis. The reliability block diagram analysis will be used to estimate the functional availability and failure rates for the DAS. The results of this analysis may also be used to support licensing.

In order to perform the reliability block diagram analysis, the predicted failure rates of the various elements that make up the system are needed. A Mean Time Between Failure (MTBF) analysis will be performed on all major components of the system and will be documented in a bill of materials which lists the elements applied in the DAS, along with the estimated failure rates. The failure rates can be determined from a combination of sources such as MIL-HDBK-217F component failure models per field data, manufacturer data sheets or engineering judgment.

Once the FMEA, MTBF, and reliability block diagram analysis have been performed, the data will be used to support a maintainability analysis. The maintainability analysis will divide the DAS system elements into a number of classes that share similar attributes. For each class, a checklist will be applied in each of the listed repair activities to assist in the characterization of typical durations for the activity. The durations will then be used to estimate an overall mean time to repair that will provide important input to determine the optimum number of spares to have on hand at the site. A DAS report will be prepared to support quantitative analysis as well as provide the utility valuable information for risk-informed decisions in the I&C maintenance area.

[

] ^{a,c}

9 NUREG/CR 6303 COMPLIANCE AND DIVERSITY IMPLEMENTATION

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection System" (Reference 12) provides a method for analyzing computer-based nuclear reactor protection systems that discovers and identifies vulnerabilities to common-mode failure. [

] ^{a,c}

9.1 [] ^{a,c}

[

] ^{a,c}

9.2 [] ^{a,c}

[

] ^{a,c}

9.3 [] ^{a,c}

[

] ^{a,c}

[

]a,c

9.4 [

]a,c

[

]a,c

9.5 [

]a,c

[

]a,c

9.6 [

]a,c

[

]a,c

10 DIGITAL I&C INTERIM STAFF GUIDANCE (ISG)

10.1 ISG-1, “CYBER SECURITY”

10.1.1 ISG-1 Overview

The original issue raised by the Nuclear Energy Institute (NEI) asserted that Regulatory Positions 2.1-2.9 provided within Regulatory Guide 1.152 (Reference 18) conflict with NEI 04-04, Rev. 1, with regard to the protection of safety-related digital I&C systems. However, through the Digital I&C Technical Working Group (TWG) effort, the NRC staff has illustrated that the programs are complementary.

The guidance provided within Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 describes an acceptable method that can be used by licensees and applicants to provide cyber security protection for digital I&C systems used in safety-related applications. The NRC staff recognizes that alternative methods may be employed to achieve an equivalent level of protection. The staff is also sensitive to the fact that the industry is interested in pursuing efficient implementation of cyber security enhancements through the use of existing programs whenever possible.

The NRC is planning to issue additional regulatory guidance on the subject of cyber security defensive measures for safety systems. This regulatory guidance will be based on requirements in 10 CFR 73.1 and the proposed security regulations (i.e., 10 CFR 73.55m), if the commission ultimately adopts this provision. Until this new regulatory guidance is issued, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-related digital I&C systems in NPPs may address applicable cyber security issues through the use of either Regulatory Guide 1.152; Regulatory Positions 2.1-2.9) or the version of draft NEI 04-04, Rev. 2, in conjunction with the correlation table.

10.1.2 DAS Applicability

[

] ^{a,c}

10.2 ISG-2, “DIVERSITY AND DEFENSE-IN-DEPTH (D3)”

10.2.1 ISG-2 Overview

10.2.1.1 1. Adequate Diversity and 2. Manual Operator Actions

There is no distinction in the D3 guidance for digital reactor plant scram (RPS) designs for new NPPs and current operating plants. In the context of this interim staff guidance, the RPS consists of the RTS and the ESFAS.

While the NRC considers common cause failures (CCFs) in digital systems to be beyond design basis, the digital RPS should be protected against CCFs. The licensee or applicant should perform a D3 analysis to demonstrate that vulnerabilities to CCFs are adequately addressed. NUREG/CR-6303, “Method for

Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” dated December 1994 and Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” of NUREG-0800, “Standard Review Plan,” describe an acceptable process for performing a D3 analysis.

When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room.

If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident. The automated backup function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The automated backup system should be similar in quality to systems required by the ATWS rule (10 CFR 50.62, “Requirements for Reduction of Risk from ATWS Events for Light-Water-Cooled Nuclear Power Plants”), as described in the enclosure to Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related”.

If manual operator actions are used as backup, a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions can be maintained within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident. The NRC staff will review the acceptability of such actions in accordance with DI&C-ISG-05, “Highly-Integrated Control Rooms – Human Factors Issues,” Revision 1. For actions with limited margin, such as less than 30 minutes between time available and time required for operators to perform the protective actions, a more focused staff review will be performed.

In addition to the above guidance, a set of displays and controls (safety or non-safety) should be provided in the MCR for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal, RCS integrity, and containment isolation and integrity. The displays and controls should be unaffected by the CCF in the RPS. However, these displays and controls could be those used for manual operator actions as described above. Implementation of these manual controls should be in accordance with existing regulations.

10.2.1.2 BTP 7-19 Position 4 Challenges

The NRC staff recommends that BTP 7-19, Position 4 be re-written to state:

“In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual system level actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to

function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hard-wired connections.”

Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division. This recommendation does not prohibit the use of manual controls for operating individual safety system components after the corresponding safety system functions have been actuated.

10.2.1.3 Effects of CCF

Many possible types of protection system failures may occur as a result of failure to actuate. Among these, a simple failure of the total system might not be the worst case failure, particularly when analyzing the time required for identifying and responding to the condition. For example, a failure to trip might not be as limiting as a partial actuation of an emergency core cooling system, with digital indications of a successful actuation. In cases such as this, it may take an operator longer to evaluate and correct the safety system failure than it would if there was a total failure to send any actuation signal. For this reason, the evaluation of failure modes as a result of software CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate.

The primary concern is that an undetected failure within the digital system could prevent proper system operation. A failure or fault that is detected can be addressed; however, failures that are non-detectable may prevent a system actuation when required. Consequently, non-detectable faults are of concern. Therefore, a diverse means to provide the required safety function, or some other safety function that will adequately address each licensing basis event should be provided.

In general, spurious trips and actuations are of a lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failures to respond to abnormal operating occurrences and design basis events.

For these reasons, spurious trips or actuations of safety-related digital protection systems resulting from CCFs do not need to be addressed beyond what is already set forth in plant design basis evaluations.

However, in accordance with the augmented quality guidance for the diverse backup system used to cope with a CCF, the design of a diverse automated or diverse manual backup actuation system should consider and address how to significantly reduce or eliminate the potential for a spurious actuation of the protective system.

10.2.1.4 CCF Applicability

There are two design attributes that are sufficient to eliminate consideration of CCF:

1. Diversity – In Example 1 of Staff Positions 1 and 2 in this ISG, sufficient diversity exists in the protection system such that CCFs within the channels can be considered to be fully addressed without further action.

Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 and BTP 7-19 determines that the two diverse digital systems are not subject to a CCF.

In this case, no additional diversity would be necessary in the safety system.

2. Testability – A system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses.

10.2.1.5 Echelons of Defense

The RTS and ESFAS functions may be combined into a single digital platform. The four echelons of defense described in BTP 7-19 are only conceptual and, with the exception of the subset of monitoring and indication noted in Point 4, BTP 7-19 does not imply that these echelons of defense must be independent or diverse. Rather, where a postulated CCF impairs a safety function, a plant response in accordance with the acceptance criteria of Section 3 of BTP 7-19 should be demonstrated, regardless of the echelons of defense that may be affected.

10.2.1.6 Single Failure

Based upon the definition of single failure in 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” and the guidance provided by IEEE Standard 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” as endorsed by Regulatory Guide 1.53, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems, Rev. 2,” a digital system CCF, which includes software CCFs, does not meet the criteria of a single failure in design basis evaluations (which assume a single failure coincident with a design basis event). IEEE Standard 379-2000 states, “Common cause failures not subject to single-failure analysis include those that can result from external environmental effects (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference), design deficiencies, manufacturing errors, maintenance errors, and operator errors.”

Since digital system CCFs are not classified as single failures, postulated digital system CCFs should not be assumed to be a single random failure in design basis evaluations. Consequently, best-estimate techniques can be employed in performing analyses to evaluate the effect of digital system CCFs coincident with design basis events.

As with ATWS mitigation systems, if a postulated digital system CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is not subject to the same CCF, should be included in the overall system design. This diverse means should perform either the same function or a different function that will mitigate accidents or events that require the safety function assumed failed by the postulated CCF. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform under the associated event conditions.

10.2.2 DAS Applicability

[

] ^{a,c}

11 SUMMARY AND CONCLUSION

The AP1000 DAS is a limited scope system and is simple in implementation by design. The DAS is a non-safety system and, therefore, redundancy is not required. The DAS provides a back-up to the PMS. []^{a,c} The DAS is not needed if the PMS functions properly.

The DAS is in compliance with NRC BTP 7-19, Position 4 (Reference 11); a set of displays and controls located in the MCR should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. In addition, the DAS meets the NRC 10 CFR 50.62 (Reference 4) criteria; [

] ^{a,c}