Westinghouse

Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-6206
Direct fax: 412-374-5005
e-mail: sisk1rb@westinghouse.com

Your ref: Docket Number 52-006
Our ref: DCP_NRC_002683

October 30, 2009

Subject: AP1000 Instrumentation and Control Defense-in –Depth and Diversity Report

In support of Combined License application pre-application activities, Westinghouse is submitting document APP-GW-J1R-004 (WCAP-15775), Rev 3 "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report. This report describes the type of diversity that exists among the four echelons of defense for the AP1000 and identifies dependencies among the echelons.

This document was discussed during the December 2008 DAS Meeting and referenced in Action Item #1 from that meeting (Reference: ML090090187). It is provided to your office to assist the NRC staff in the ongoing review of the AP1000 Design Certification Amendment Application, Docket Number 52-006.

Questions or requests for additional information related to the content and preparation of these documents should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Very truly yours,

D. A. Lindgren /FOR

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Enclosure

1. APP-GW-J1R-004, Revision 3, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report"

0335ljb.doc

D063
NRO

cc:	D. Jaffe	-	U.S. NRC	1E
	E. McKenna	-	U.S. NRC	1E
	S. K. Mitra	-	U.S. NRC	1E
	T. Spink	-	TVA	1E
	P. Hastings	-	Duke Power	1E
	R. Kitchen	-	Progress Energy	1E
	A. Monroe	-	SCANA	1E
	P. Jacobs	-	Florida Power & Light	1E
	C. Pierce	-	Southern Company	1E
	E. Schmiech	-	Westinghouse	1E
	G. Zinke	-	NuStart/Entergy	1E
	R. Grumbir	-	NuStart	1E
	J. Ewald	-	Westinghouse	1E

ENCLOSURE 1

APP-GW-J1R-004

Revision 3

"AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report"

WCAP-15775
Revision 3

October 2009

AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report

WCAP-15775
Revision 3

AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report

John G. Ewald - I&C Lead

C. Daniel Stiffler - DAS Design Engineer

Seth Peasley – I&C Engineer

October 2009

AP1000 Document: APP-GW-J1R-004

Westinghouse Electric Company LLC
1000 Westinghouse Dr
Cranberry TWP, PA 16066

©2009 Westinghouse Electric Company LLC
All Rights Reserved

TABLE OF CONTENTS

TABLE OF CONTENTS ii
LIST OF TABLES iv
LIST OF FIGURES iv
LIST OF ACRONYMS AND ABBREVIATIONS v
GLOSSARY OF TERMS vi

1 INTRODUCTION 1-1
1.1 PREFACE 1-1
1.2 ARCHITECTURE OVERVIEW 1-1
1.3 SCOPE 1-2
1.4 SUMMARY AND CONCLUSIONS 1-2

2 AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE/ SYSTEMS DESCRIPTION 2-1
2.1 ARCHITECTURE DESCRIPTION 2-1
2.2 PROTECTION AND SAFETY MONITORING SYSTEM OVERVIEW 2-3
2.3 PLANT CONTROL SYSTEM OVERVIEW 2-3
2.4 DIVERSE ACTUATION SYSTEM OVERVIEW 2-3
2.5 DATA DISPLAY AND PROCESSING SYSTEM OVERVIEW 2-4
2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE 2-4

3 DEFENSE-IN-DEPTH FEATURES OF THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE 3-1
3.1 INTRODUCTION 3-1
3.2 DEFINITION OF COMMON-MODE FAILURES (CMFS) 3-1
3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES 3-2

4 EVALUATION OF NUREG/CR-6303 GUIDELINES 4-1
4.1 IDENTIFYING SYSTEM BLOCKS – GUIDELINES 1 AND 5 4-1
4.2 DETERMINING DIVERSITY – GUIDELINE 2 4-1
4.3 SYSTEM FAILURE TYPES – GUIDELINE 3 4-3
4.4 ECHELONS OF DEFENSE – GUIDELINE 4 4-4
4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6 4-4
4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7 4-4
4.7 EFFECT OF OTHER BLOCKS – GUIDELINE 8 4-5
4.8 OUTPUT SIGNALS – GUIDELINE 9 4-5
4.9 DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS – GUIDELINES 10 AND 11 4-5
4.10 DIVERSITY AMONG ECHELONS OF DEFENSE – GUIDELINE 12 4-5
4.11 PLANT MONITORING – GUIDELINE 13 4-6
4.12 MANUAL OPERATOR ACTION – GUIDELINE 14 4-7

TABLE OF CONTENTS (cont.)

5 EVALUATION OF DIVERSITY WITHIN THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE 5-1
5.1 INTRODUCTION 5-1
5.2 DIVERSITY OVERVIEW OF THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE 5-1
5.3 REACTOR SHUTDOWN 5-2
5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL 5-2
5.5 CORE DECAY HEAT REMOVAL 5-6
5.6 CONTAINMENT COOLING 5-7
5.7 CONTAINMENT ISOLATION 5-7
5.8 EVENT SCENARIOS 5-7

6 REFERENCES 6-1

LIST OF TABLES

Table 2.1 AP1000 Instrumentation and Control Echelons of Defense Echelons 2-5

Table 2.2 Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons 2-6

LIST OF FIGURES

Figure 2.1 AP1000 Instrumentation and Control Systems Interactions 2-2

Figure 5.1 AP1000 Instrumentation and Control Systems Diversity Architecture 5-3

Figure 5.2 AP1000 Diverse Instrumentation and Control Structure 5-4

LIST OF ACRONYMS AND ABBREVIATIONS

ADS	Automatic Depressurization System
ALWR	Advanced Light Water Reactor
AMSAC	Anticipated Transient Without Trip Mitigation System Actuation Cabinet
CMF	Common-Mode Failure
CMT	Core Makeup Tank
CRDM	Control Rod Drive Mechanism
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DCD	Design Control Document
DDS	Data Display and Processing System
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
HSI	Human-system interface
I&C	Instrumentation & Control
IRWST	In-containment Refueling Water Storage Tank
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PCS	Passive Containment Cooling System
PLC	Programmable Logic Controller
PLS	Plant Control System
PXS	Passive Core Cooling System
QDPS	Qualified Data Processing Subsystem
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System

GLOSSARY OF TERMS

This section contains clarifications of terms used in this report that are defined in NUREG/CR-6303 (Reference 2). These definitions are provided to aid in understanding of the report text, instrumentation and control architecture, and conformance to guidelines. The definitions and clarifications may vary from corresponding definitions in NUREG/CR-6303 because of development and evolution of the AP1000 instrumentation and control architecture. ***Definitions as stated in NUREG/CR-6303 are in Italics.***

Anticipated Operational Occurrences

> *"...those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser and loss of offsite power."* (10CRF50, Appendix A, Definition and Explanations)

Section 15.0.1 of the AP1000 DCD (Reference 6), "Classification of Plant Conditions," provides the definition and discussion of Anticipated Operational Occurrences.

Accidents

> *"Accidents are defined as those conditions of abnormal operation that result in limiting faults..."* (Standard Format, Section 15, "Accident Analysis," USNRC Reg. Guide 1.70)

Section 15.0.1 of the AP1000 DCD (Reference 6), "Classification of Plant Conditions," provides the definition and discussion of Accidents.

Block

> *"Generally, a system is described as an arrangement of components or black boxes interconnected by communication, electrical connections, pipes, or physical effects. This kind of description, often called a 'system architecture,' may be too complex or may not be partitioned conveniently for diversity and defense-in-depth analysis. A more convenient description may be obtained by restricting the portion of the system under consideration to instrumentation and control equipment and partitioning the restricted portion into 'blocks.' A 'block' is the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. The objective of choosing blocks is to eliminate the need for detailed examination of internal failure mechanisms while examining system behavior under reasonable assumptions of failure containment.*
>
> *"Examples of typical software-containing blocks are computers, local area networks or multiplexers, or programmable logic controllers (PLCs). A block can be solely hardware, but there are no solely software blocks; software-containing blocks suffer the distinction that both hardware or software faults (and sometimes both acting together) can cause block failure. Consequently, it is difficult to separate the effects of software from the machine that executes that software. For example, a software defect in one small routine can cause an entire computer to fail by corruption of other data or software..."*

Channel

"A channel is defined as a set of interconnected hardware and software components that processes an identifiable sensor signal to produce a single protective action signal in a single division when required by a generating station condition. A channel includes the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor protection system that can be unambiguously tested or analyzed from an input to an output."

Common-Mode (or -Cause) Failure

"Common-mode failures (CMFs) are causally related failures of redundant or separate equipment; for example, (1) CMF of identical subsystems across redundant divisions, defeating the purpose of redundancy, or (2) CMF of different subsystems or echelons of defense, defeating the use of diversity. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures..."

For this report, a distinction is made between CMFs and multiple failures. CMFs are further discussed in subsection 3.2. Multiple failures are addressed in the AP1000 Probabilistic Risk Assessment (PRA).

Defense-in-Depth

"Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. The classic three physical barriers to radiation release in a reactor – cladding, reactor pressure vessel, and containment – are an example of defense-in-depth."

Diversity

"Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. Diversity is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other. There are six important types of diversity to consider:

- *Human diversity*
- *Design diversity*
- *Software diversity*
- *Functional diversity*
- *Signal diversity*
- *Equipment diversity..."*

Echelons of Defense

NUREG/CR-6303 provides definitions of four echelons of defense. The definition of each level is reproduced in the following along with a brief description of the AP1000 instrumentation and control systems that accomplish the task.

1. Control system:

"The control echelon is that non-Class 1E manual or automatic equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is generally used to operate the reactor in the safe power production operating region. Indicators, annunciators, and alarms may be included in the control echelon. Reactor control systems typically contain some equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare common-mode failures of Class 1E reactor protection equipment."

The functions performed by the control system echelon of defense are included in the nonsafety Plant Control System (PLS). The PLS normally functions to maintain the plant within operating limits to avoid the need for a reactor trip or engineered safety features (ESF) actuation.

2. Reactor Trip or Scram System:

"The reactor trip echelon is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection)."

The automatic reactor trip functions performed by the reactor trip echelon of defense are included in the safety Protection and Safety Monitoring System (PMS). The nonsafety Diverse Actuation System (DAS) also provides automatic reactor trip capabilities.

3. ESF Actuation System (ESFAS):

"The ESFAS echelon is that safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). This echelon detects the need for and performs such functions as emergency cooling, pressure relief or depressurization, isolation, and control of various support systems (e.g., emergency generators) or devices (valves, motors, pumps) required for ESF equipment to operate."

The automatic ESF actuation functions performed by the ESFAS echelon of defense are included in the safety PMS. The nonsafety DAS also provides automatic actuation capability for a subset of ESF component actuations. AP1000 is a passive plant and does not require emergency generators, motors, or pumps to perform the ESF functions.

4. Monitoring and Indication System:

> *"The monitoring and indication echelon is the slowest and also the most flexible echelon of defense. Like the other three echelons, operators are dependent upon accurate sensor information to perform their tasks, but, given information, time, and means, can perform previously unspecified logical computations to react to unexpected events. The monitoring and indication echelon includes both Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate nominally assigned to the other three echelons."*

Monitoring and indication functions are provided by the nonsafety data display and processing system (DDS) and by the safety PMS. The safety manual reactor trip and manual ESF actuation functions performed by the monitoring and indication echelon of defense are included in the PMS. The nonsafety DAS also provides manual reactor trip and manual ESF actuation capabilities.

Instrumentation System

> *"A reactor instrumentation system is that set of equipment that senses various reactor parameters and transmits appropriate signals to control systems, to the reactor trip system, to the engineered safety features actuation system, and to the monitoring and indicator system for use in determining the actions these systems or reactor operators will take. Independence is required between control systems, safety-related monitoring and display systems, the two safety systems, and between redundant divisions of the safety systems."*

In this report, the instrumentation system includes the following systems in the instrumentation and control architecture:

- Protection and Safety Monitoring System (PMS)
- Plant Control System (PLS)
- Data Display and Processing System (DDS)
- Diverse Actuation System (DAS)

1 INTRODUCTION

1.1 PREFACE

Since January 1979 when NUREG-0493 (Reference 1) was issued, the instrumentation and control architecture for Westinghouse Pressurized Water Reactors has undergone refinement in both the systems architecture aspects of the overall design, and the detailed design of the instrumentation and control cabinets. Experience gained from the AP600 design, upgrading the instrumentation and control of domestic plants, providing instrumentation and control systems for international plants, and providing instrumentation and control for non-nuclear applications has been incorporated into the AP1000 instrumentation and control design. The ALWR Utility Requirements Document has provided valuable industry guidance that has also been incorporated into the design. Also, modern statistical tools have been applied to analyze the instrumentation and control design within the context of overall plant risk assessment, and these results have provided insight into design performance considerations. Because of these factors, the AP1000 instrumentation and control design has evolved beyond the RESAR-414 design that was evaluated in NUREG-0493.

Changes beyond the RESAR-414 design have been incorporated into the AP600 and AP1000 instrumentation and control architectures that must be considered in the diversity assessment:

1. Probabilistic risk assessment (PRA) methods were used to consider the role of both safety and nonsafety equipment in the prevention and mitigation of transients and faults. For the AP1000, this consideration has been reflected in the overall design of the AP1000's plant systems.

2. The nonsafety diverse actuation system (DAS) provides a reactor trip and engineered safety features (ESF) actuations diverse from the protection and safety monitoring system (PMS). The DAS is included to support the aggressive AP1000 risk goals by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated common-mode failures (CMFs).

In October 1994, the Nuclear Regulatory Commission published NUREG/CR-6303 (Reference 2) which described a deterministic method of analyzing computer-based nuclear reactor protection systems that identifies and evaluates design vulnerabilities to CMF. The AP1000 instrumentation and control systems follow closely the AP600 instrumentation and control systems, which were designed and analyzed before NUREG/CR-6303 was published. As with the AP600 design, PRA methods were used for the analysis of diversity and defense-in-depth analysis for AP1000, rather than the deterministic methods described in NUREG/CR-6303. These PRA methods are consistent with NUREG/CR-6303 and allow the designers to concentrate on situations that are the largest contributors to the predicted core melt frequency.

1.2 ARCHITECTURE OVERVIEW

The PMS is a Class 1E instrumentation and control system that is included in the AP1000 instrumentation and control architecture to address the anticipated operational occurrences and accidents outlined and described in Chapter 15 of the AP1000 Design Control Document (DCD) (Reference 6). The PMS is designed to meet plant licensing requirements by including design features such as: redundancy, functional diversity, failsafe design, continuous self-diagnostics, periodic surveillance test capability,

circuit isolation, and a design, verification, and validation process. Subsection 3.3 describes the fault tolerant features of the PMS.

The DAS is a nonsafety instrumentation and control system that is an enhanced version of the Anticipated Transient Without Trip Mitigation System Actuation Cabinet (AMSAC) in operating Westinghouse nuclear power plants. The DAS is included to enable the AP1000 instrumentation and control architecture to meet reliability goals in the AP1000 PRA, where the PMS is assumed to fail as a result of postulated failures beyond design basis, such as CMF.

1.3 SCOPE

Diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide different ways of responding to postulated plant conditions. NUREG/CR-6303 segregates the types of diversity into six different areas: human, design, software, functional, signal, and equipment. NUREG/CR-6303 defines echelons of defense as:

> *"...specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the engineered safety features (ESF) actuation system, and the monitoring and indicator system."*

This AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report describes the type of diversity that exists among the four echelons of defense for AP1000 and identifies dependencies among the echelons.

1.4 SUMMARY AND CONCLUSIONS

1.4.1 The AP1000 Instrumentation and Control Architecture complies with NUREG-0493. The Architecture pays special attention to Section 2, "Technical Discussion," and Section 3.3 "Guidelines," which contain guidelines, requirements, and recommendations for mitigating or preventing potential Common Mode Failures.

1.4.2 The AP1000 Instrumentation and Control Architecture complies with NUREG/CR-6303, in particular, Section 3 "Guidelines," which contains guidelines, requirements, and recommendations for mitigating or preventing potential Common Mode Failures.

1.4.3 The analysis to protect against CMF in the AP1000 instrumentation and control architecture was done as part of the PRA. In the PRA, failures of the instrumentation and control architecture, including common cause failures, were analyzed. The PRA report (Reference 7) describes this analysis of the AP1000 instrumentation and control systems. Chapter 26 of the PRA report describes the PMS model; Chapter 27 describes the DAS model; and Chapter 28 describes the Plant Control System (PLS) model. The conclusion is that the AP1000 instrumentation and control architecture is, as calculated by PRA analysis, sufficient to meet probabilistic safety goals.

2 AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE/ SYSTEMS DESCRIPTION

2.1 ARCHITECTURE DESCRIPTION

The instrumentation and control systems and functions have been structured into the architecture shown in Figure 2.1 and in DCD Figure 7.1-1 (Reference 6). Figure 2.1 is a simplified representation of the AP1000 instrumentation and control architecture that illustrates the interactions between the instrumentation and control systems. DCD Figure 7.1-1 shows the same instrumentation and control systems and their interfaces in detail. In this architecture, related functions are grouped into cabinets and then these cabinets are connected into systems by means of hardwired conductors, data links, and data highways. The cabinets communicate plant data between systems through a real-time data network.

The instrumentation and control architecture is arranged in a hierarchical manner. Above the real-time data network are the systems whose purpose is to facilitate the interaction between the plant operators and the instrumentation and control systems. These are the operations and control centers system and the data display and processing system (DDS). Below the real-time data network are the systems and functions that perform the protective, control, and data monitoring functions. These are the PMS, the PLS, the InCore instrument system, the special monitoring system, and the DAS.

The special monitoring and InCore instrumentation systems do not provide any functions directly related to the control or protection of the plant and are therefore not discussed in this document.

The operations and control centers system defines the arrangement of the main control room, the layout of the main control room workstations, the remote shutdown workstation, and contains the design process for the layout, and content of operating and safety displays, alarms, controls, and procedures for the preceding human-system interface (HSI). The HSI functions, developed under the operations and control centers system, are covered in the appropriate instrumentation and control systems such as the PMS, PLS, DAS, and DDS.

The main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided.

The DDS (plant computer) is implemented using a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains input from the real-time data network and delivers output over the network to other users.

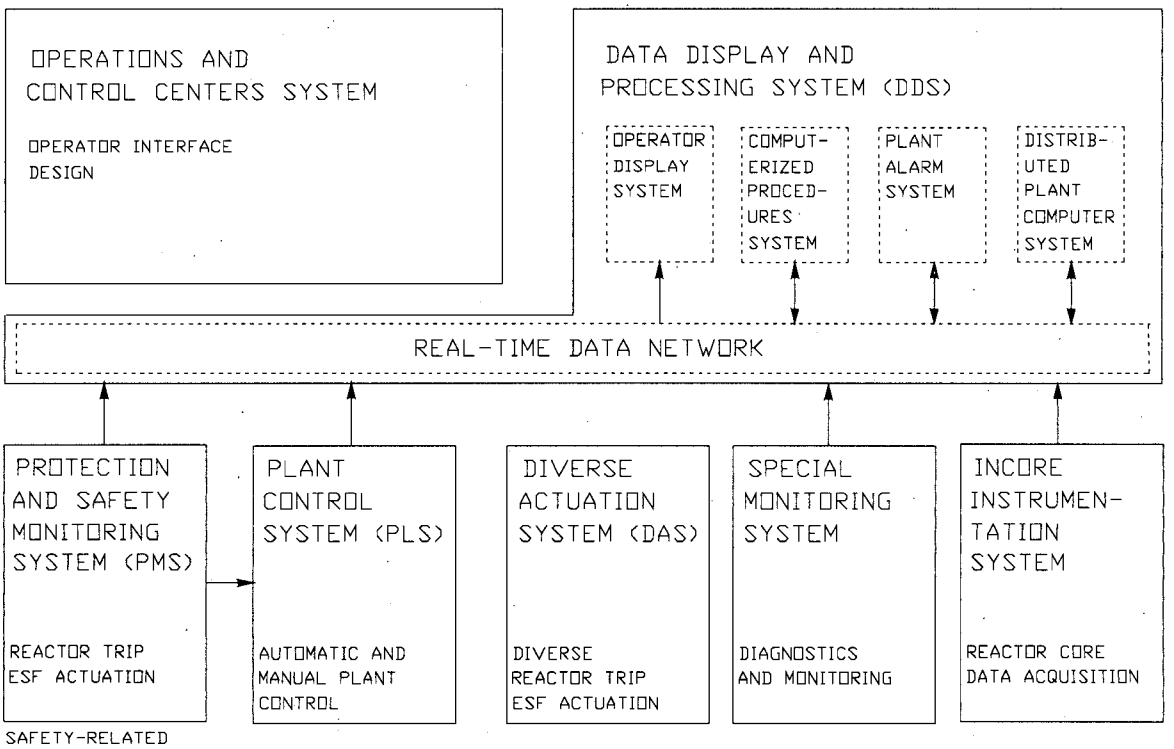

Figure 2.1 AP1000 Instrumentation and Control Systems Interactions

2.2 PROTECTION AND SAFETY MONITORING SYSTEM OVERVIEW

Located in the lower left of Figure 2.1 is the safety PMS. The PMS performs the reactor trip functions, the ESF actuation functions, and the Qualified Data Processing Subsystem (QDPS) functions. The instrumentation and control (I&C) equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are four-way redundant.

The PMS provides the safety functions necessary to monitor the plant during normal operation, to shutdown the plant, and to maintain the plant in a safe shutdown condition. The PMS controls safety components in the plant that are operated from the main control room or remote shutdown workstation.

In addition, the PMS provides the equipment necessary to monitor the plant safety functions during and following an accident as required by Regulatory Guide 1.97.

Further description of the PMS is contained in Chapter 7 of the AP1000 DCD.

2.3 PLANT CONTROL SYSTEM OVERVIEW

The nonsafety PLS is located to the right of the PMS in Figure 2.1. The PLS provides the functions necessary for normal operation of the plant from cold shutdown through full power. The PLS controls nonsafety components in the plant that are operated from the main control room or remote shutdown workstation.

The PLS contains nonsafety control and instrumentation equipment to control reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation.

The PLS provides margins to plant safety limits and the plant's transient performance. The PLS maintains the plant conditions within operating limits. The PLS provides the instrumentation and control to support defense-in-depth automatic and manual functions. The PLS also provides sensors for nonsafety plant monitoring functions.

The PLS is described further in Chapter 7 of the AP1000 DCD.

2.4 DIVERSE ACTUATION SYSTEM OVERVIEW

The DAS is located to the right of the PLS in Figure 2.1. The DAS is a nonsafety, diverse system that provides an alternate means of initiating reactor trip and actuating selected engineered safety features, and providing plant information to the operator. The DAS receives signals directly from dedicated sensors. The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware and software used in the PMS.

The DAS is described further in Chapter 7 of the AP1000 DCD.

2.5 DATA DISPLAY AND PROCESSING SYSTEM OVERVIEW

The nonsafety DDS is in the upper right of Figure 2.1. The DDS provides the equipment used for processing data that will result in nonsafety alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logging and historical storage and retrieval, and providing operational support for plant personnel.

The DDS also contains the real-time data network, which is a redundant data network that links the elements of the AP1000 instrumentation and control architecture.

2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE

The AP1000 instrumentation and control architecture conforms to the echelon of defense structure defined in Section 2.2 of NUREG/CR-6303 and the block structure described in Section 2.5 of NUREG/CR-6303. The four echelons are divided into three levels containing the nonsafety systems, safety systems, and nonsafety diverse systems that provide automatically and manually actuated functions to support these echelons.

The functions assigned to the instrumentation and control systems are implemented by processor-based subsystems, which are placed within a structure of cabinets. Table 2.1 maps the echelons of defense to the instrumentation and control architecture. The echelons are divided into a nonsafety layer, a safety layer, and a diverse layer to reflect the means provided by the systems to implement the functions of each echelon. Table 2.2 illustrates the relationships between these subsystems and cabinets and the block structure described in NUREG/CR-6303. This table shows the assignment of equipment to the blocks for each level within the echelons of defense.

Due to the nature of the processor implementation, the demarcation between measured variable blocks and derived variable blocks lies within the software structure of a channel or function. These blocks are combined into a single column for purposes of defining hardware assignments.

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, operator indications which are diverse from PMS. Figure 5.2 shows the integration of indication functions into the instrumentation and control architecture.

Table 2.1 AP1000 Instrumentation and Control Echelons of Defense Echelons

	LAYER 1 NONSAFETY SYSTEMS	LAYER 2 SAFETY SYSTEMS	LAYER 3 DIVERSE NONSAFETY SYSTEMS
CONTROL ECHELON	PLANT CONTROL SYSTEM (PLS) NOTES 1 & 2		
REACTOR TRIP ECHELON		PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
ESF ACTUATION ECHELON		PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
MONITORING AND INDICATION ECHELON	DATA DISPLAY AND PROCESSING SYSTEM (DDS)	PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
		CLASS 1E SYSTEMS	

Notes:

1. The PLS enables the plant to maintain conditions within operating limits and also provides automatic and manual actuations of the nonsafety defense-in-depth systems.
2. Automatic and manual actions are provided in the PLS, PMS, and DAS.

Table 2.2	Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons			
Echelon	**AP1000 Function**	**Measured and Derived Variable Blocks**	**Command Block**	**Manual Actions**
Plant Control	nonsafety	sensors, signal conditioning, (communication functions in PMS)[1]	real-time data network, output signal conditioning, output driver	system level soft control as determined by HSI design; component level soft control
	safety	NONE	NONE	NONE
	diverse	NONE	NONE	NONE
Reactor Trip	nonsafety	not applicable	not applicable	not applicable
	safety	sensors, signal conditioning, plant protection subsystem	voting logic, reactor trip switchgear	hardwired manual reactor trip to reactor trip breakers
	diverse	sensors, signal conditioning, diverse control logic	output driver, rod drive M/G set field breaker	hardwired manual reactor trip to rod drive M/G set field breaker
Engineered Safety Features Actuation	nonsafety	not applicable	not applicable	component level soft control
	safety	sensors, signal conditioning, plant protection subsystem	ESF coincidence logic, logic bus, ESF actuation subsystem	system level to ESF coincidence logic
	diverse	sensors, signal conditioning, diverse control logic	output driver	hardwired component level
Monitoring and Indication	nonsafety	sensors, signal conditioning, (communication functions in PMS)	real-time data network, alarm processors, operator workstations	see other three echelons
	safety	sensors, signal conditioning, QDPS	qualified operator displays	see other three echelons
	diverse	sensors, signal conditioning	diverse display devices	see other three echelons

[1] Used for safety sensors that provide isolated information to nonsafety systems.

3 DEFENSE-IN-DEPTH FEATURES OF THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE

3.1 INTRODUCTION

This section describes features of the instrumentation and control architecture that provide redundant design, fail-safe design, and failure detection and repair. Section 5 of this document discusses design diversity.

3.2 DEFINITION OF COMMON-MODE FAILURES (CMFS)

For the purpose of this report, CMFs are considered to be sets of causally related failures that occur within a limited time, and fall outside of system design capabilities for detection or mitigation of failures. The failures that meet this definition exhibit the following characteristics:

- The failures occur in a sufficient number of places in the instrumentation and control architecture such that redundant design is ineffective in enabling the system to tolerate the failure.
- The failures are such that fail-safe design is ineffective in enabling the system to tolerate the failure.
- The failures are undetectable, or they occur within a sufficiently short time that neither automatic nor manual responses are possible to enable the system to tolerate the failures.

An instrumentation and control system, or portion of a system, can be capable of tolerating some combinations of CMFs because:

1. Diverse design exists within the system.
2. Redundant design exists within the system.
3. Fail-safe design exists within the system.
4. The failure is detectable and sufficient time exists between instances of failure that automatic or manual response to the failure occurs.

In this evaluation, CMFs are postulated to cause complete failure of similar or identical equipment. This failure mode is assumed to cause complete loss of function of the PMS, but not loss of function of the DAS.

3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES

The instrumentation and control architecture contains design features whose primary intent is to meet licensing requirements and to enhance plant reliability and availability. However, these features also provide a degree of protection against CMFs, and, as a result, decrease the probability that a CMF will render a portion of the AP1000 instrumentation and control architecture unable to respond to a transient or plant fault. Among these design features that protect against failures, including CMF, are:

- The Design, Verification, and Validation Process - The design of the instrumentation and control systems hardware and software elements are controlled by a design, verification, and validation process that is described in either WCAP-13383 (Reference 3) or CE-CES-195 (Reference 4). WCAP-13383 provides details on the AP600 verification and validation plan. CE-CES-195 provides details on the Common Q verification and validation plan. Depending on the PMS system hardware used for AP1000, one of these programs will apply. These processes are formal, rigorous means to detect and correct design errors before they can result in common-mode errors in the plant.

- Use of a Distributed Processing Architecture - Instrumentation and control functions are divided among multiple subsystems so that diverse functions are separated into different subsystems. This, in conjunction with other design features such as division independence, has the effect of localizing certain CMFs to a single subsystem. For instances where functional diversity exists in the instrumentation and control architecture, complete system failure may not occur as a result of CMF.

- Redundancy - While redundant design of itself does not prevent CMFs, use of redundant subsystems can enable the plant to detect and respond to failures, including CMFs in those instances where sufficient time exists between occurrences of the individual failures.

- Modular Design - Modular design enhances the rapid isolation and repair of failures. For instances where failures, including CMFs, occur, but sufficient time between failure instances exists for detection and repair, modular design enables the redundant subsystems to be available for response to events.

- Fail-Safe/Fault Tolerant Design - Fail-safe design features in the instrumentation and control architecture, such as de-energizing to trip or actuate, provide the capability to, automatically or manually, put the plant into a safe condition following single failures and certain types of multiple failures. Fault tolerant design features, such as functional diversity and redundancy, also provide the capability to, automatically or manually, put the plant into a safe condition following single failures and certain types of multiple failures.

- Alarm System - The AP1000 alarm system is capable of alerting the operator to failures, including multiple failures, in other parts of the instrumentation and control systems. The main AP1000 alarm system is part of the DDS, which uses different hardware and software from the PMS.

- Continuous Self-Diagnostics - In the AP1000 instrumentation and control architecture, the subsystems continuously execute self-diagnostic software routines. Other self-diagnostic features, such as read-backs and watchdog timers continuously monitor operation of critical subsystems. These self-diagnostic features are designed to detect and report hardware failures, enabling the operator to act.

- Test Subsystem – The test subsystem rapidly and consistently verifies system operation. The use of the test subsystem enhances the timely detection of all failures, including CMF. The test subsystem also enhances the ability of plant personnel to quickly diagnose and repair failures detected by the continuous self-diagnostic features.

- Circuit Isolation - Circuit isolation is used to electrically isolate segments of the instrumentation and control architecture and to prevent propagation of electrical faults. This feature helps to limit the propagation of faults caused by failures, including CMF.

- Control of Setpoint and Tuning Adjustments - The instrumentation and control architecture has physical and administrative controls and multiple levels of security for access to setpoint and tuning adjustments. This helps to prevent CMF due to incorrect constants entered as a result of a maintenance error.

- Use of Engineering Units for Setpoints and Tuning Constants - Setpoints and tuning constants in the instrumentation and control architecture are entered in engineering units rather than as scaled values. This eliminates a potential common-mode error by removing scaling calculations.

- Signal Selector Algorithm in the Plant Control System - The signal selector algorithm in the PLS protects against failure, including CMF, of sensor signals shared by the protection and control systems. The signal selector algorithm alerts the operator to differences in output signals from redundant sensors.

- Physical Separation - Physical separation is provided between the four redundant divisions of equipment for the safety PMS, which in turn, are separated from nonsafety systems such as the PLS. Equivalent physical separation is also provided for supporting systems, such as electrical power. Physical separation meets the requirements of IEEE-384 (Reference 8). This physical separation provides protection from CMF induced by physical phenomena.

- Equipment Qualification - Equipment in the instrumentation and control architecture is qualified to environmental requirements, including temperature, humidity, vibration/seismic, electromagnetic interference/radio frequency interference (EMI/RFI), and surge withstand criteria commensurate with its safety classification and intended usage. The environmental qualification program provides assurance that physical phenomena will not introduce CMF until design requirements are exceeded.

- Other Features - The instrumentation and control architecture also contains other design features, such as ac power line protection and filtering, EMI/RFI design, and surge withstand networks at signal conditioning board inputs, which will prevent failure from specific causes. Due to these features, the causes that would induce multiple failures must be in excess of design and qualification test limits.

4 EVALUATION OF NUREG/CR-6303 GUIDELINES

NUREG/CR-6303 (Reference 2) describes a method for analyzing computer-based reactor protection system vulnerability to postulated software CMFs. NUREG/CR-6303 provides fourteen guidelines for performing a diversity and defense-in-depth analysis. The following sections describe the results of applying these guidelines to AP1000.

Section	Title	NUREG Guideline
4.1	Identifying System Blocks	1, 5
4.2	Determining Diversity	2
4.3	System Failure Types	3
4.4	Echelons of Defense	4
4.5	Postulated Common-Mode Failure of Blocks	6
4.6	Use of Identical Hardware and Software Modules	7
4.7	Effect of Other Blocks	8
4.8	Output Signals	9
4.9	Diversity for Anticipated Operational Occurrences and Accidents	10, 11
4.10	Diversity among Echelons of Defense	12
4.11	Plant Monitoring	13
4.12	Manual Operator Action	14

4.1 IDENTIFYING SYSTEM BLOCKS – GUIDELINES 1 AND 5

The safety instrumentation that provides the protective functions is divided into four redundant divisions. Table 2.2 shows how the cabinets and subsystems within each division can be mapped into blocks.

The nonsafety PLS uses redundant sensors and redundant subsystems to provide defense-in-depth functions. The nonsafety DAS uses redundant sensors and redundant subsystems to provide diverse actuation functions.

In this evaluation, however, CMFs are postulated to cause complete failure of similar or identical equipment. This failure mode is assumed to cause the complete loss of function of the PMS, but not loss of function of the DAS due to the diversity of implementation.

4.2 DETERMINING DIVERSITY – GUIDELINE 2

NUREG/CR-6303 identifies six aspects of diversity to address the issue of common-mode effects:

1. Design Diversity

   In the nonsafety DAS, energize to trip or actuate logic is used. In the safety PMS, de-energize to trip or actuate logic is used, except where energize to trip is necessary to meet plant system design requirements.

2. Equipment Diversity

For the DAS, the hardware which is used to provide the signal input and conditioning and automatic actions will be diverse from the equipment used for related functions in the PMS. In addition, the DAS provides a reactor trip by tripping the nonsafety rod drive motor-generator set field breakers in the plant control system. This means is diverse from the reactor trip switchgear used in the PMS for reactor trip.

3. Functional Diversity

The AP1000 is designed with multiple levels of defense for each anticipated operational occurrence and accident. These multiple levels of defense are described in WCAP-13793 (Reference 5). WCAP-13793 is an AP600 document that is applicable to AP1000. The PMS is a Class 1E system with 4-way divisional separation. Two-out-of-four voting is used for the reactor trip function and most ESF actuation functions. Multiple reactor trip functions and ESF actuations are provided for each anticipated operational occurrence and accident, generally using diverse sensors, as described in DCD Chapter 15 (Reference 6). The DAS has two automatic logic racks that support two-out-of-two voting for reactor trip and ESF actuations. The functional logic for the automatic PMS functions is shown in DCD Figure 7.2-1, sheets 1-18. The functional logic for the automatic DAS functions is shown in DCD Figure 7.2-1, sheets 19 and 20.

4. Human Diversity

The design, verification, and validation programs for instrumentation and control systems, as described in described in WCAP-13383 (Reference 3) and CE-CES-195 (Reference 4), require and specify the use of independent review. It is a requirement of the DAS that different people will be responsible for its design and fabrication, including verification and validation.

5. Signal Diversity

Signal diversity for specific events is provided within the safety level of the reactor trip and ESF actuation echelons. The signals used to produce reactor trips and ESF actuations within the PMS originate from different types of sensors as shown in DCD Tables 7.2-1 and 7.3-1. The DAS receives signals directly from its own dedicated sensors.

6. Software Diversity

The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware and software used in the PMS. The DAS uses no software in its operations.

4.3 SYSTEM FAILURE TYPES – GUIDELINE 3

NUREG/CR-6303 describes three different instrumentation failure types that are applicable to AP1000.

4.3.1 Type 1 Failure

Type 1 failures are postulated failures in one echelon that result in a plant transient that require a protection function to mitigate the transient. Generally, the postulated failure is assumed to occur in the control system echelon such that a plant transient occurs that results in an automatic reactor trip or ESF actuation. However, there are also postulated failures in the ESF that necessitate protective action.

Examples of Type 1 failures that are analyzed in the DCD Chapter 15 (Reference 6) accident analyses are described in WCAP-13793, "AP600 System/Event Matrix" (Reference 5). WCAP-13793 is an AP600 document that is applicable to AP1000.

The primary defense against Type 1 failures is to ensure that a protection function exists to mitigate each postulated credible failure that can occur in plant control or protection systems and can result in a plant transient and requires protective action.

4.3.2 Type 2 Failure

Type 2 failures are undetected failures that are manifested only when a demand is received to actuate a component or system. Failure to respond is due to a postulated CMF of redundant divisions or trains. For example, a software CMF in all four divisions of the plant protection subsystem could potentially degrade the operation of all four process divisions. Another example would be a postulated software CMF in a software module in the train-related ESF coincidence logic that could degrade the capability of the protection system to actuate ESF components or systems.

The primary defense against a Type 2 failure is to provide diversity within and between the four echelons of defense. The goal is to design a system in which all functions associated with an echelon of defense and the four echelons of defense are not susceptible to a postulated CMF.

4.3.3 Type 3 Failure

Type 3 failures are failures that occur because either the plant process does not respond in a predictable manner or the sensors measuring the plant process respond in an anomalous manner. An example of the first type of anomalous behavior was experienced during the Three Mile Island Unit 2 (TMI-2) event in 1979. A pressurizer relief valve stuck open resulting in the loss of reactor coolant. However, the pressurizer level sensors indicated acceptable pressurizer levels. The anomalous level indication occurred because coolant was being lost at the top of the pressurizer, which resulted in a high level indication due to the design of the delta-P level measurement circuit. An example of the second type of anomalous behavior is the response of the steam generator level measurement system following a high-energy line rupture inside containment. The delta-P measurement level transmitter is calibrated assuming the ambient reference leg temperature is at the normal containment operating temperature. If a high-energy line rupture occurs inside containment, the reference leg heats up to the elevated containment temperature,

which results in an anomalous high, indicated level in the steam generator, since the transmitter was calibrated at a lower temperature.

The primary defense against a Type 3 failure is to provide diverse sensors for measuring the plant response to an initiating event, e.g., using turbine impulse pressure and neutron Excore detectors for measuring reactor power. Another example would be using reactor coolant system (RCS) subcooling and core-exit thermocouple temperature to measure core cooling.

4.4 ECHELONS OF DEFENSE – GUIDELINE 4

The instrumentation and control architecture is divided into four echelons of defense, as defined in NUREG/CR-6303. The control echelon is provided by the PLS, with certain inputs provided from the PMS by means of isolated data links.

The PMS and the DAS provide the reactor trip echelon. The reactor trip function in the safety PMS is provided by: the plant protection subsystems, the voting logic, the dedicated datalinks, the reactor trip switchgear interface and the reactor trip switchgear. The nonsafety DAS and rod drive motor-generator set field breakers provide a diverse reactor trip function. In addition, the PLS will enable the plant to avoid the need to trip for certain events by maintaining the plant within acceptable limits.

The PMS and the DAS provide the ESF echelon. The ESF subsystems within the plant protection subsystems, the ESF coincidence logic, the ESF actuation subsystems, dedicated datalinks, and data highways provide the ESF function in the PMS. The DAS provides diverse means to actuate some ESF functions. In addition, the PLS actuates defense-in-depth plant systems to enable the plant to avoid the need for actuating the passive safety systems.

4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6

The CMF of processor-based subsystems postulated for this document is a failure that occurs in all similar subsystems. This postulated failure could be caused by failure of a common hardware element, or failure of a common software element. This failure mode is assumed to cause the complete loss of function of the PMS, but not loss of function of the DAS due to the diversity of the implementations. The result of this failure is that the entire system or systems fail to produce any protective actions. The evaluation of the instrumentation and control architecture based on this failure is contained in Section 5 of this document.

4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7

The PRA postulated CMF within the instrumentation and control architecture, in conjunction with random failures. The PRA evaluated the contribution to core damage due to instrumentation and control CMF to be acceptably low. It is conservatively assumed in the PRA that all software modules or hardware modules of a type will fail simultaneously. The diversity between the PMS and DAS assures that the joint CMF probability is acceptably low.

4.7 EFFECT OF OTHER BLOCKS – GUIDELINE 8

In the AP1000 instrumentation and control architecture, input signals are not shared between DAS and other systems.

For CMF within the PMS, the system is conservatively assumed to actuate no protective actions needed during an event.

4.8 OUTPUT SIGNALS – GUIDELINE 9

Optical or resistive isolation is provided between subsystems to prevent propagation of electrical failures in either direction. The four divisions of the PMS are physically separated. Since sensors are considered to be contained in a measured variable block for the purposes of the analyses in this report, failure of signal conditioning equipment influencing sensor performance is not considered. (Note that the instrumentation and control hardware contains features to minimize the occurrence of this failure mode.)

4.9 DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS – GUIDELINES 10 AND 11

The frequency of a postulated accident occurring in conjunction with CMFs of the PMS and failures of the DAS is calculated in the AP1000 PRA (Reference 7). Chapter 26 of the PRA report discusses the PMS modeling, and Chapter 27 presents the modeling of the DAS. Section 5 of this document provides a strategic evaluation of the ability of the instrumentation and control architecture to produce the following required protective actions to support the safety goals:

- Reactor shutdown
- Maintain reactor coolant inventory
- Initiate and maintain core decay heat removal
- Initiate and maintain containment cooling
- Initiate containment isolation

Note that the primary coolant system can be depressurized in a controlled fashion to mitigate certain events.

4.10 DIVERSITY AMONG ECHELONS OF DEFENSE – GUIDELINE 12

4.10.1 Control/Reactor Trip

For the low probability circumstance where an event that requires a reactor trip occurs coincident with a postulated CMF in the PMS, the DAS initiates the reactor trip in a diverse fashion. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation CMF probabilities combined with the event probability.

Additionally, both the PMS and DAS provide manual means of tripping the reactor. To support manual reactor trip, both the PMS and the DAS provide plant information to the operator. The PMS provides the Class 1E QDPS indications, while the DAS provides nonsafety diverse indications.

4.10.2 Control/ESFAS

For the low probability circumstance where an event that requires one or more ESF actuations occurs coincident with a postulated CMF in the PMS, the DAS initiates selected ESF actuations in a diverse fashion. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation CMF probabilities combined with the event probability.

Additionally, the PMS provides both system-level and component-level manual means of actuating ESF functions, and DAS provides manual means of actuating selected FSF functions. To support manual ESF actuation, both the PMS and the DAS provide plant information to the operator. The PMS provides the Class 1E QDPS indications, while the DAS provides nonsafety diverse indications.

4.10.3 Reactor Trip/ESFAS

Isolated, independent interconnections exist between the reactor trip and ESF actuation functions. Failure of the reactor trip function will not prevent the ESF actuation function from responding to other inputs, nor will failure of the ESF actuation function prevent the reactor trip function from responding to other inputs.

4.11 PLANT MONITORING – GUIDELINE 13

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, diverse operator indications. No sensors are shared between the RTS/ESFAS and the DAS. Diverse and independent signal conditioning and data acquisition functions will be performed in the RTS/ESFAS and DAS such that a postulated software common mode failure in the PMS platform will not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the PMS to the PLS and the DDS. The connections between the PMS and the PLS and DDS contain isolation devices to prevent failures in the PLS or DDS from affecting operation of the PMS. Once signals leave the PMS through the isolation devices, they are no longer safety-related, and are not used to provide any safety functions.

The signals from PMS to PLS and DDS meet the independence requirements of GDC-24, IEEE-603, IEEE-379, and IEEE-384.

No credible failure of the PLS or DDS will prevent the safety system from performing its safety function. The Gateway provides the connections used for plant monitoring and for surveillance of the reactor trip

and ESF actuation subsystems. The DDS provides the software and hardware used for displaying plant parameters and monitoring system performance.

The automatic functions of the PMS are designed to protect the AP1000 from potential operator-induced transients which may result from failures in the DDS or PLS.

4.12 MANUAL OPERATOR ACTION – GUIDELINE 14

The manual reactor trip and ESF actuation functions performed by the monitoring and indication echelon of defense is included in the safety PMS. The nonsafety DAS also provides manual reactor trip and selected ESF actuation capabilities.

Both the PMS and DAS provide manual means of tripping the reactor. The PMS provides a hardwired reactor trip to the reactor trip breakers. This capability is provided for both from the MCR and the Remote Shutdown Workstation. The DAS provides a diverse hardwired reactor trip to the rod drive motor-generator set field breaker.

The PMS provides both system-level and component-level manual means of actuating ESF functions. The DAS provides manual means of actuating selected ESF functions.

5 EVALUATION OF DIVERSITY WITHIN THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE

5.1 INTRODUCTION

The AP1000 fluid systems are designed with multiple levels of defense for a wide range of events. The designs of both the safety and the nonsafety systems support this multiple level design philosophy. The AP1000 instrumentation and control systems architecture reflects this multiple level of defense approach by including safety and nonsafety instrumentation systems that provide safety and nonsafety means of initiating protective functions.

This section of the document discusses the functions provided to protect the core and limit the spread of radioactivity during an event by initiating:

- Reactor Shutdown
- RCS Inventory Control
- Core Decay Heat Removal
- Containment Cooling
- Containment Isolation

5.2 DIVERSITY OVERVIEW OF THE AP1000 INSTRUMENTATION AND CONTROL ARCHITECTURE

For the purposes of discussing instrumentation and control diversity, the AP1000 instrumentation and control systems can be organized into three layers. The first layer contains the nonsafety PLS and the DDS. The PLS provides the monitoring, and the automatic and manual control of nonsafety functions. The PLS contains sensors, rod control cabinets, control logic cabinets, the rod drive motor/generator set, the pressurizer heater controller, the rod position indication system, and operator controls. The DDS provides operator displays and alarms in the main control room and remote shutdown area. Dedicated functional processors perform display and alarm processing. The display and alarm processors acquire the information from the other plant instrumentation and control systems by means of the real-time data network, which is also part of the DDS.

The second layer contains the PMS. The PMS provides the safety reactor trip function, ESF actuation functions, and qualified plant monitoring function. In the PMS, both automatic and manual means are provided to trip the reactor and actuate the engineered safety features. The PMS contains sensors, plant protection subsystems, ESF coincidence logic, ESF actuation subsystems, logic buses, reactor trip switchgear, protection multiplexers, operator controls, QDPS, and qualified displays.

The third layer contains the DAS. The DAS provides nonsafety, reactor trip functions, actuation of engineered safety features, and operator displays. In the DAS, both automatic and manual means are provided to trip the reactor and actuate selected engineered safety features. The DAS also provides monitoring of plant parameters required to ascertain the state of the plant and provide guidance for manual actions by the operator. The DAS is implemented in hardware that is diverse from the PMS.

Figure 5.1 shows, on an overview basis, the relationships between components of the PLS, DAS, and PMS, and illustrates the means provided to accomplish the automatic and manual actions. This figure illustrates the sources of signals for automatic trips and actuations, and shows operator displays. It also shows the manual controls and operator displays that facilitate operator actions.

Figure 5.2 shows how diverse sensors, cabinets, and operator controls are integrated into the instrumentation and control architecture.

5.3 REACTOR SHUTDOWN

Reactor shutdown is the process of bringing the reactor to a subcritical state in a timely manner and maintaining an adequate shutdown margin. This function is normally provided by inserting the control rods into the core either in a controlled manner (stepping) or by dropping them.

5.3.1 The control rods can be automatically or manually stepped into the core. The PLS provides automatic insertion of the control rods using signals from various sensors in the PLS and PMS. The PLS also provides controls for manual insertion of the control rods. The final actuation devices for reactor shutdown via the PLS are the control rod drive mechanisms (CRDMs).

5.3.2 The PMS provides automatic reactor shutdown by dropping the rods using the reactor trip switchgear. When the reactor trip switchgear opens, the CRDMs are de-energized and the rods drop into the core by gravity. The PMS also provides a manual reactor shutdown by means of controls that directly interface with the reactor trip switchgear.

5.3.3 The DAS provides the capability for automatic reactor shutdown by de-energizing the rod drive motor/generator set that supplies power to the CRDMs. This is a diverse means of de-energizing the control rod drive mechanisms and has the same effect as opening the reactor trip switchgear. The DAS also provides the capability for manual reactor shutdown by de-energizing the rod drive motor/generator set.

5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL

RCS inventory control is the process of maintaining sufficient borated water in the RCS to maintain the heat removal capability.

5.4.1 During normal plant operation, the pressurizer level control function of the PLS automatically controls the operation of the nonsafety chemical and volume control system (CVS) to maintain RCS inventory. In the event of a small RCS leak, the CVS makeup pumps automatically start on a low pressurizer level signal. The makeup pumps also start automatically on a core makeup tank (CMT) actuation signal.

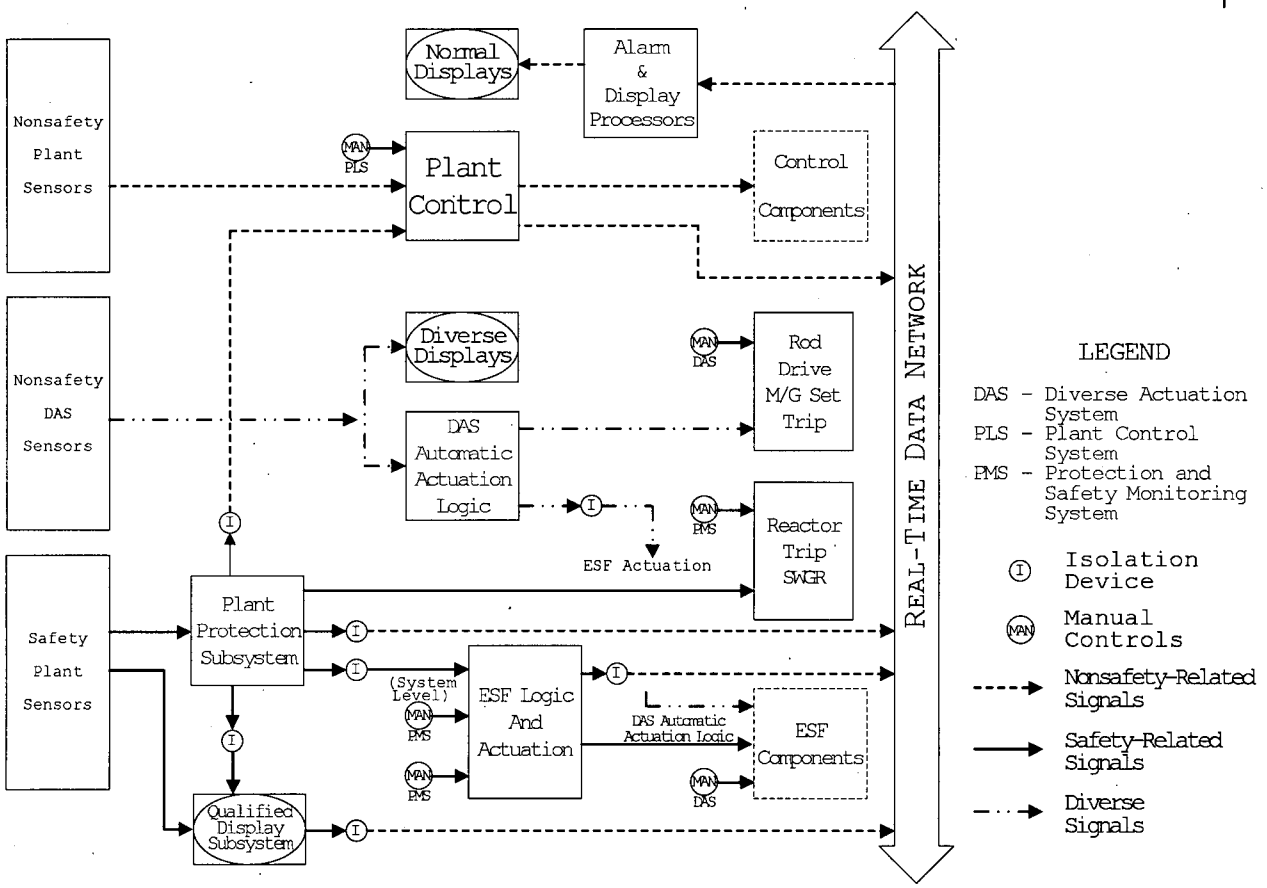

Figure 5.1 AP1000 Instrumentation and Control Systems Diversity Architecture

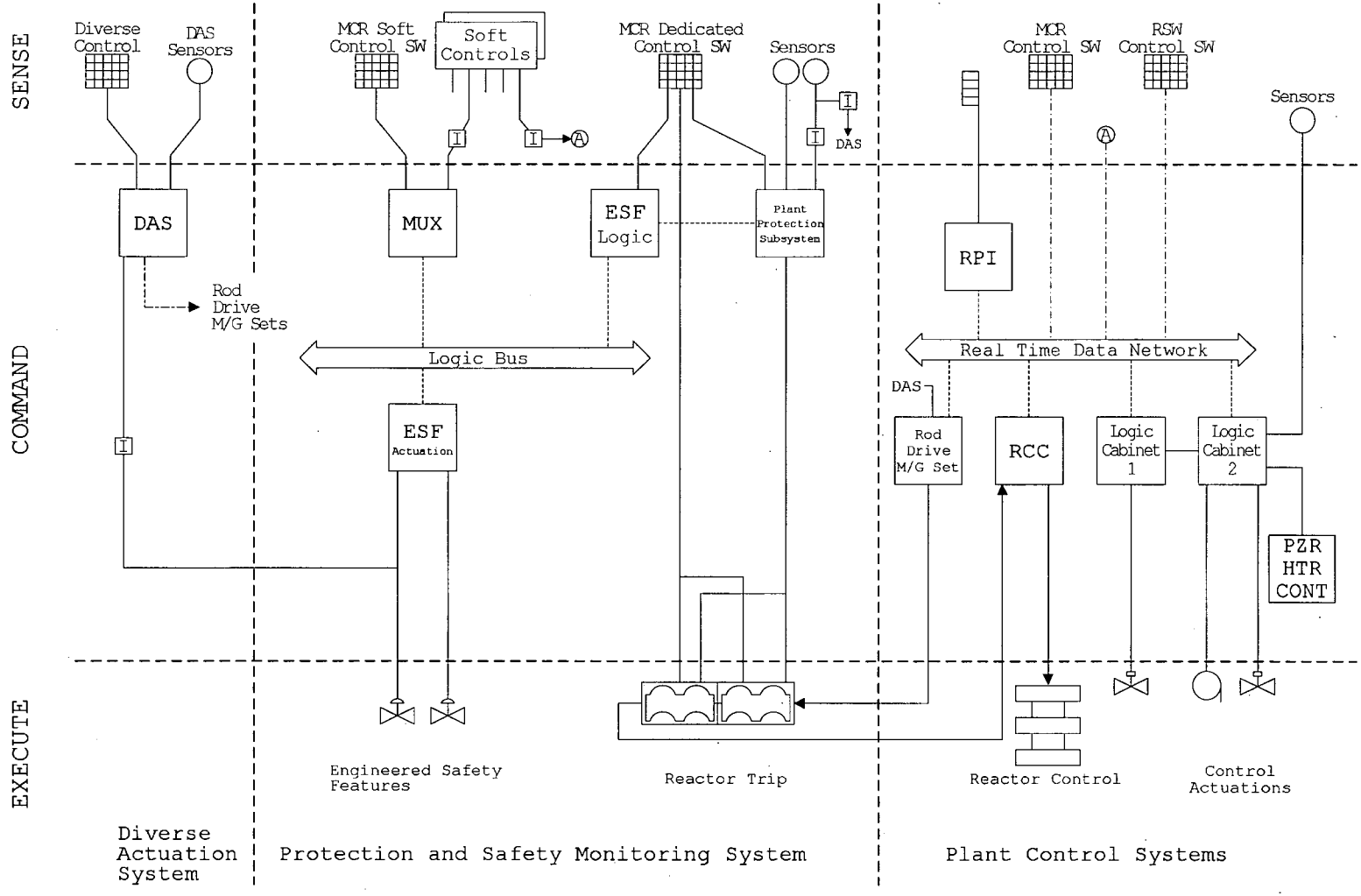

Figure 5.2 AP1000 Diverse Instrumentation and Control Structure

5.4.2 The safety passive core cooling system (PXS) provides emergency core decay heat removal, RCS emergency makeup, boration, and safety injection. The PXS includes four sources of passive injection for RCS inventory control. These injection sources provide injection in a sequenced manner, based upon RCS pressure. The CMTs are normally the first injection source, providing makeup at any RCS pressure. The PMS automatically initiates CMT injection. The PMS also provides the capability for manual actuation of the CMTs using control devices, the logic buses, and the ESF actuation subsystem.

5.4.3 The DAS provides the capability for nonsafety automatic actuation of the CMT injection. The DAS also provides the capability for nonsafety manual actuation of CMT injection using dedicated, hardwired controls.

5.4.4 The other three PXS injection sources provide makeup once the RCS is depressurized. The automatic depressurization system (ADS) uses four valve stages to provide a controlled depressurization of the RCS. The PMS automatically initiates each ADS stage. The PMS provides the capability for manual actuation of the ADS using control devices, the logic buses, and the ESF actuation subsystem.

5.4.5 The DAS also provides the capability for manual actuation of the ADS using dedicated, hardwired controls for the valves in each stage.

5.4.6 The second PXS injection source is the accumulator tanks. Injection from the accumulators is initiated once RCS pressure is below the static pressure in the accumulators. The PMS actuates the accumulator discharge isolation valves, which are normally open, with actuation power removed, during plant power operation.

5.4.7 The nonsafety normal residual heat removal system (RNS) can be manually actuated to provide RCS injection once RCS pressure is reduced to within the capability of the RNS.

5.4.8 The third PXS makeup source is the in-containment refueling water storage tank (IRWST). During plant power operation, the PMS automatically initiates IRWST injection once RCS pressure is within the injection head capability of the IRWST.

5.4.9 During shutdown operations, the IRWST discharge isolation valves are normally closed with actuation power available. The PMS automatically opens these valves to initiate IRWST injection on a low-low RCS hot leg level. These valves can also be manually opened using the PMS.

The DAS also provides the capability for nonsafety manual actuation of the IRWST injection.

5.4.10 The fourth PXS makeup source is the containment recirculation volume of reactor coolant and makeup water that collects in the recirculation screen areas in containment following an event. The PMS automatically opens the containment recirculation valves. The PMS also provides the capability for manual actuation of the containment recirculation valves.

5.5 CORE DECAY HEAT REMOVAL

Core decay heat removal is the process of maintaining a heat sink that is capable of cooling the reactor core after a reactor shutdown. A number of different systems can provide core decay heat removal. The system and components to be used for core heat removal will depend upon the plant operating mode. During some plant conditions, the same systems and components that maintain the RCS inventory provide core decay heat removal.

5.5.1 The nonsafety startup feedwater system supplies feedwater to the steam generators during non-power operation to provide core decay heat removal. The PLS automatically actuates the two nonsafety startup feedwater pumps and automatically controls feedwater flow to the steam generators. The startup feedwater pumps automatically start on either a low steam generator water level or low main feedwater flow signal. Startup feedwater flow control is based on the steam generator water level.

5.5.2 The PXS provides a safety core cooling process using the passive residual heat removal (PRHR) heat exchanger. The PMS automatically actuates the PRHR heat exchanger. The PMS also provides the capability for manual actuation of the PRHR heat exchanger using control devices, the logic buses, and the ESF actuation subsystem.

5.5.3 The DAS provides the capability for nonsafety automatic actuation of the PRHR heat exchanger. The DAS also provides the capability for manual actuation of the PRHR heat exchangers using dedicated, hardwired controls.

5.5.4 In addition to the startup feedwater system and the PRHR heat exchangers, core decay heat removal can also be automatically provided by the CMTs, accumulators, and IRWST, and manually provided by the nonsafety RNS, once RCS pressure has been reduced to within the capability of the RNS. Subsection 5.4 discusses the actuation of the components in these two systems.

5.5.5 During plant shutdown conditions before opening the RCS, core cooling is provided as discussed previously. During plant shutdown, some PXS components may not automatically actuate, but can be manually actuated, depending upon specific plant conditions. During these conditions, the RNS is normally operating and will automatically restart when power is restored following a loss of power to the RNS pumps.

5.5.6 During plant conditions when the RCS is not intact or with reduced RCS inventory (such as mid-loop operation), the RNS is normally operating and will automatically restart when power is restored following a loss of power to the RNS pumps. Various PXS components including the CMTs, accumulators, and PRHR heat exchangers are not available. The IRWST will automatically actuate on low-low RCS hot leg level. The IRWST can also be manually actuated.

5.6 CONTAINMENT COOLING

Containment cooling is the process of removing heat from the containment.

5.6.1 Nonsafety fan coolers normally provide containment cooling during power operation. The PLS is used to control the operation of the fan coolers.

5.6.2 If the fan coolers are unavailable or have insufficient capacity for the containment heat loads, the PMS automatically actuates the safety passive containment cooling system (PCS) to provide containment cooling. The PMS also provides the capability for manual control of the PCS using control devices, the logic buses, and the ESF actuation subsystem.

5.6.3 The DAS provides the capability for nonsafety automatic actuation of the PCS. The DAS also provides the capability for manual actuation of the PCS using dedicated, hardwired controls.

5.7 CONTAINMENT ISOLATION

Containment isolation is the process of closing safety valves in fluid lines that penetrate the containment to minimize the release of radioactivity from containment, following an event.

5.7.1 PMS provides automatic containment isolation by actuating the containment isolation valves on a safeguards actuation signal. The PMS also provides the capability for manual actuation of containment isolation valves using control devices, the logic buses, and the ESF actuation subsystem.

5.7.2 The DAS provides the capability for nonsafety automatic actuation of the containment isolation valves on high containment temperature. The DAS also provides the capability for manual containment isolation capability using dedicated, hardwired controls.

5.8 EVENT SCENARIOS

WCAP-13793, "AP600 System/Event Matrix" (Reference 5) contains a series of flowcharts and tables that illustrate these levels of defense, from an operational point of view, for a selected number of full power and shutdown events. WCAP-13793 is an AP600 document that is applicable to AP1000.

6 REFERENCES

1. NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.

2. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection systems," October 21, 1994.

3. WCAP-13383, Revision 1, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," June 1996.

4. CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems," May 26, 2000.

5. WCAP-13793, Rev. 2, "AP600 System/Event Matrix," April 2001.

6. APP-GW-GL-700, "AP1000 Design Control Document."

7. APP-GW-GL-022, "AP1000 Probabilistic Risk Assessment."

8. IEEE 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."