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

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

Attention: Mr. Larry Burkhart

Direct tel: 412-374-5355
Direct fax: 412-374-5456
e-mail: corletmm@westinghouse.com

Your ref: Project 711
Our ref: DCP/NRC1498

April 15, 2002

SUBJECT: Transmittal of Westinghouse Document, "Safety Criteria for the AP1000 Instrumentation and Control Systems," WCAP-15776, Rev. 0, Non-Proprietary, dated April 2002

Enclosed please find six (6) copies Westinghouse document "Safety Criteria for the AP1000 Instrumentation and Control Systems," WCAP-15776, Rev. 0, Non-Proprietary, dated April 2002. This document is referenced in Chapter 7 of the AP1000 Design Control Document, APP-GW-GL-700, Revision 1.

There is no information proprietary to Westinghouse included in this WCAP.

Please contact me at 412-374-5355 if you have any questions concerning this submittal.

Very truly yours,

M. M. Corletti
Passive Plant Projects & Development
AP600 & AP1000 Projects

/Attachment
1. WCAP-15776, Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems" (6 copies)

D063

DCP/NRC1498
Project 711

April 15, 2002

bcc: *C. B. Brinkman - Westinghouse, Rockville, MD
W. E. Cummins - Westinghouse, Pittsburgh, PA, EC E3
H. A. Sepp - Westinghouse, Pittsburgh, PA, EC E4-07A
R. P. Vijuk - Westinghouse, Pittsburgh, PA, EC E3-05
J. W. Winters - Westinghouse, Pittsburgh, PA, EC E3-08

*(w/attachments)

Westinghouse Non-Proprietary Class 3

WCAP - 15776

Safety Criteria for the AP1000 Instrumentation and Control Systems

Westinghouse Electric Company LLC

AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____ S _____

RFS#: _____ RFS ITEM #: _____

AP1000 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
APP-GW-J1R-008	0	Page 1 of 54	W-WINTERS

ALTERNATE DOCUMENT NUMBER: WCAP-15776 WORK BREAKDOWN #:

ORIGINATING ORGANIZATION: Westinghouse Electric Co., LLC

TITLE: **Safety Criteria for the AP1000 Instrumentation and Control Systems**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE: N/A	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
N/A	N/A	N/A

ORIGINATOR	SIGNATURE/DATE	
T. P. Hayes	T. P. Hayes	4/4/02
AP1000 RESPONSIBLE MANAGER	SIGNATURE*	APPROVAL DATE
J. W. Winters	J. W. Winters	4 APR 02

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

WCAP-15776

Safety Criteria for the AP1000 Instrumentation and Control Systems

T. P. Hayes
AP1000

April 2002

Reviewer: Carl A Vitalbo
C. A. Vitalbo
Protection Systems Design

Approved:
J. W. Winters
AP1000

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

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ac	Alternating Current
ADS	Automatic Depressurization System
DAS	Diverse Actuation System
dc	Direct Current
DDS	Data Display and Processing System
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
HVAC	Heating, Ventilation, and Air Conditioning
IDS	Class 1E dc and Uninterruptible Power Supply System
LCO	Limiting Condition for Operation
MCR	Main Control Room
MTTR	Mean Time to Repair
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment
RSW	Remote Shutdown Workstation
RTD	Resistance Temperature Detector
SSE	Safe Shutdown Earthquake
T_{cold}	Reactor Coolant Inlet Temperature
T_{hot}	Reactor Coolant Outlet Temperature
UPS	Uninterruptible Power Supply
V&V	Verification and Validation
VBS	Nuclear Island Nonradioactive Ventilation System
VES	Main Control Room Emergency Habitability System

1 INTRODUCTION

This report describes the design bases that apply to the power, instrumentation, and control portions of the safety systems for the AP1000. The design bases presented are those addressed by IEEE 603-1991 (Reference 1).

2 DESIGN BASES FOR SAFETY SYSTEMS

2.1 DESIGN BASIS: DESIGN BASIS EVENTS AND THE CORRESPONDING PROTECTIVE ACTION APPLICABLE TO EACH MODE OF OPERATION (PARAGRAPHS 4.1 AND 4.2 OF IEEE 603-1991)

The safety systems are designed to protect the health and safety of the public by limiting the release of radioactive material during Conditions II, III, and IV events to acceptable limits, as defined in AP1000 accident analyses.

To facilitate the design of the safety systems, a number of specific limits on certain process and design variables have been chosen which, if met, imply that the radioactive material release limits can be met with a high degree of confidence. These specific limits are defined on an accident-by-accident basis in the accident analyses.

The protection and safety monitoring system (PMS) automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level.

The safety analyses demonstrate that even under conservative critical conditions for design basis accidents, the safety systems provide confidence that the plant is put into and maintained in a safe state following a Condition II, III or IV accident. Therefore, the safety systems meet IEEE 603-1991 and are redundant and separate, including permissives and blocks.

2.2 DESIGN BASIS: PERMISSIVE CONDITIONS FOR EACH OPERATING BYPASS CAPABILITY (PARAGRAPH 4.3 OF IEEE 603-1991)

The PMS is designed so that protective functions are initiated and accomplished during various reactor operating modes. The following specific design bases apply:

- Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Hardware and software used to achieve automatic removal of the block of a protective function are part of the PMS and, as such, are designed in accordance with the criteria in this report.

- Blocks of a protective function are automatically cleared when the protective function is required to function.

2.3 DESIGN BASIS: VARIABLES REQUIRED TO BE MONITORED FOR PROTECTIVE ACTION AND THEIR RANGES AND RATES OF CHANGE (PARAGRAPH 4.4 OF IEEE 603-1991)

The variables monitored for reactor trips are:

- Neutron flux
- Reactor coolant pump bearing water temperature
- Pressurizer pressure

- Water level in the pressurizer
- Reactor coolant flow in each loop
- Speed of each reactor coolant pump
- Water level in each steam generator
- Reactor coolant inlet temperature (T_{cold}) in each loop
- Reactor coolant outlet temperature (T_{hot}) in each loop
- Position of each manual reactor trip switch

Table 2-1 lists the ranges, accuracies, and response times for each reactor trip variable.

The variables monitored for engineered safety features (ESFs) actuation are:

- Pressurizer pressure
- Pressurizer water level
- Reactor coolant temperature (T_{hot} and T_{cold}) in each loop
- Containment pressure
- Containment radioactivity level
- Steam line pressure in each steam line
- Water level in each steam generator (narrow and wide ranges)
- Source range neutron flux
- Core makeup tank level
- Reactor coolant level in each of the two hot legs
- Loss of ac power sources
- In-containment refueling water storage tank level
- Main control room (MCR) supply air radioactivity level
- Reactor coolant pump bearing water temperature
- Startup feedwater flow
- Spent fuel pool level
- Reactor coolant pressure in each of the two hot legs

Table 2-2 lists typical ranges, accuracies, and response times for the variables used in engineered safety features actuation. The time response is the maximum allowable time for an actuation signal to reach the necessary components. It is based on following a step change in the applicable process parameter from 5 percent below to 5 percent above (or vice versa) the actuation setpoint with externally adjustable time delays set to OFF.

The technical specifications specify the allowable values for the limiting conditions for operation (LCOs) and the trip setpoints for the reactor trip and ESF actuation.

Table 2-1 Reactor Trip Variables, Limits, Ranges, and Accuracies (Design Basis for Reactor Trip) (Nominal)

Protective Functions	Variables to be Monitored	Range of Variables	Typical Accuracy	Typical Response Time (sec)[1]
Source Range High Neutron Flux	Neutron flux	6 decades of neutron flux: 1 to 10^6 counts per second	±11.0% of span	0.2
Intermediate Range High Neutron Flux	Neutron flux	8 decades of neutron flux overlapping source range by 2 decades and including 100% power	±12.5% of span	0.2
Power Range High Neutron Flux (Low Setting)	Neutron flux	1 to 120% of full power	±7.0% of span	0.2
Power Range High Neutron Flux (Hi-Setting)	Neutron flux	1 to 120% of full power	±7.0% of span	0.2
Power Range High Positive Flux Rate	Neutron flux	1 to 120% of full power	±1.0% of span	0.2 (step input of 20% full power)
Overtemperature ΔT			±11.5% of ΔT span	7.0 (T_{avg} or ΔT)
	Reactor coolant inlet temp. (T_{cold})	490 to 610°F	±2.5% of span	6.0
	Reactor coolant outlet temp. (T_{hot})	530 to 650°F	±3.5% of span	6.0
	Pressurizer pressure	1700 to 2500 psig	±2.5% of span	1.5
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)		2.0
Overpower ΔT			±3.5% of ΔT span	7.0 (T_{avg} or ΔT)
	Reactor coolant inlet temp. (T_{cold})	490 to 610°F	±2.5% of span	6.0
	Reactor coolant outlet temp. (T_{hot})	530 to 650°F	±3.5% of span	6.0
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)	±7.0% of span	0.2

Table 2-1 (cont.) Reactor Trip Variables, Limits, Ranges, and Accuracies (Design Basis for Reactor Trip) (Nominal)

Protective Functions	Variables to be Monitored	Range of Variables	Typical Accuracy	Typical Response Time (sec)[1]
Pressurizer Low Pressure	Pressurizer pressure	1700 to 2500 psig	±2.5% of span	1.2
Pressurizer High Pressure	Pressurizer pressure	1700 to 2500 psig	±2.5% of span	1.2
Pressurizer High Water Level	Pressurizer water level	0-100% of entire cylindrical portion of pressurizer	±2.25% of span	1.6
Low Reactor Coolant Flow	Coolant flow	0 to 120% of rated flow	±3.0% of span	1.6
Low Reactor Coolant Pump Speed	Pump speed	0 to 120% of rated speed	±0.2% of span	0.42[2]
Low Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±2.0% of span	1.6
High Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±2.0% of span	1.6
Reactor Coolant Pump High Bearing Water Temperature	Reactor coolant pump bearing water temperature	70-450°F	±1.0% of span	2.0
Automatic or Manual Safeguards Actuation	See Table 2-2	See Table 2-2	See Table 2-2	See Table 2-2
Manual Reactor Trip	Switch position	N/A	N/A	N/A
Automatic or Manual Depressurization System Actuation	See Table 2-2	See Table 2-2	See Table 2-2	See Table 2-2
Automatic or Manual Core Makeup Tank Injection	See Table 2-2	See Table 2-2	See Table 2-2	See Table 2-2
Reference Leg Temperature Compensation[3]	Ref. leg temperature	100-700°F	±3.0% of span	1.5

Notes:

1. Time from step change of the variable being monitored from 5% below to 5% above the setpoint. Value defined until the signal reaches the reactor trip breakers.
2. The time delay is the time to generate a trip after the pump speed has reached the trip setpoint during a speed decrease that is linear with respect to time.
3. This temperature compensation is not a protective function per se; however, these signals provide density compensation used in the pressurizer high water level protective function.

Table 2-2 Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)

Variable to be Monitored	Range of Variable	Typical Accuracy	Typical Response Time (sec)
Pressurizer pressure	1700 to 2500 psig	±2.5% of span	1.2(1)
Steam line pressure	0 to 1200 psig	±3.0% of span	1.2(1)
Steam line negative pressure rate	0 to 250 psig/sec	±0.5% of span	1.6(2)
Reactor coolant inlet temperature (T_{cold})	490 to 610°F	±2.5% of span	6.0(1)
Reactor coolant outlet temperature (T_{hot})	530 to 650°F	±3.5% of span	6.0(1)
Containment pressure	-5 to 10 psig	±3.0% of span	1.2(1)
Reactor coolant system hot leg level	0 to 100% of span	±3.0% of span	1.6(1)
In-containment refueling water storage tank level	0 to 100% of span	±1.0% of span	1.6(1)
Undervoltage on ac buses	250 to 400 Vac	±6.5% of setpoint	1.5(1)
Steam generator narrow range water level	0 to 100% of span (narrow range taps)	±2% of span	1.6(1)
Steam generator wide range water level	0 to 100% of span (wide range taps)	±15.5% of span	1.6(1)
Core makeup tank narrow range upper water level	0 to 100% of span	±6% of span	1.6(1)
Core makeup tank narrow range lower water level	0 to 100% of span	±6% of span	1.6(1)
Reactor coolant pump bearing temperature	70 to 450°F	±1.0% of span	2.0(1)
Spent fuel pool level	0 to 28 feet	±3.0% of span	1.6(1)
Reactor coolant system wide range pressure	0 to 3300 psig	±3.0 of span	1.2(1)
Pressurizer water level	0 to 100% of cylindrical portion of pressurizer	±2.25% of span	1.2(1)
Startup feedwater flow	0 to 1000 gpm	±4.0% of span	1.6(1)
Neutron flux (flux doubling calculation)	1 to 10^6 c/sec	±11.0% of span	10.0(1)(3)

Table 2-2 (cont.) Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)

Variable to be Monitored	Range of Variable	Typical Accuracy	Typical Response Time (sec)
Control room supply air radiation level	10^{-7} to 10^{-2} μCi/cc	±5.0% of full scale	5.0(1)
Containment radioactivity	10^{0} to 10^{7} R/hr	±5.0% of full scale	5.0(1)

Notes:

1. Listed response time is the time for a step change of a variable, from 5% below to 5% above the setpoint, to reach the actuated device.
2. Listed response time is the time for a negative 20% step change of steam line pressure to reach the actuated device.
3. Response time depends on time constant settings.

2.4 DESIGN BASIS: MINIMUM CRITERIA FOR MANUAL ACTIONS (PARAGRAPH 4.5 OF IEEE 603-1991)

Means are provided in the MCR for manual initiation of protective functions at the system level. The manual controls are a backup to the automatic protection provided by the PMS. Manual actuation relies on minimum equipment and, once initiated, proceeds to completion unless the operator deliberately intervenes. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of that function.

Control Room Habitability

When a source of ac power is available, the non-safety nuclear island nonradioactive ventilation system (VBS) provides heating, ventilation, and air conditioning (HVAC) service to the MCR, the technical support center, and the remote shutdown workstation (RSW) for normal and abnormal conditions. The VBS and its support systems provide these functions in a reliable and failure tolerant fashion. If offsite power is not available, one of the two onsite nonsafety diesels automatically provides backup power. The VBS is designed to maintain the MCR area environment between 67°F and 75°F and within a relative humidity range of 25 percent to 60 percent, during plant normal operation and abnormal operation when VBS is operable and supporting systems are available.

The VBS system provides for cooling, heating, humidity control, filtration, and pressurization following design basis accidents except for a station blackout (loss of nonsafety ac power, including the nonsafety diesels) or when radioactivity is detected in the MCR air supply which could lead to exceeding GDC-19 operator lose limits. If nonsafety ac power is not available (including the diesels) or MCR radioactivity is detected, the main control room emergency habitability system (VES) is capable of providing emergency ventilation and pressurization for the MCR. The VES also provides emergency passive heat sinks for the MCR, instrumentation and control rooms, and dc equipment rooms.

The size of the VES air storage tanks is sufficient to deliver the required airflow to the MCR to meet the ventilation and pressurization requirements for 72 hours. The function of providing passive heat sinks for the MCR, instrumentation and control rooms, and dc equipment rooms is part of the VES. The heat sinks for each room limit the temperature rise inside each room during the 72-hour period following a loss of VBS.

In the unlikely event that the VBS is unavailable for more than 72 hours, MCR habitability is maintained by operating one of the two MCR ancillary fans to supply outside air to the MCR. For the post-72 hour period, the VBS is designed to maintain the MCR below a temperature approximately 4.5°F above the average outdoor air temperature.

Fixed Position Displays

The AP1000 human system interface design includes a minimum inventory of dedicated or fixed-position displays and controls. The minimum inventory of fixed-position instrumentation includes those displays, controls, and alarms used to monitor the status of critical safety functions and to manually actuate the safety systems that achieve these critical safety functions. Table 2-3 lists the minimum inventory of fixed-position displays, alarms, and controls. Although not continuously displayed, the fixed-position displays and alarms are quickly and easily retrievable.

Table 2-3 Minimum Inventory of Fixed Position Controls, Displays, and Alerts			
Description	**Control**	**Display**	**Alert[2]**
Neutron flux		x	x
Neutron flux doubling			x
Startup rate		x	x
RCS pressure		x	x
Wide range T_{hot}		x	
Wide range T_{cold}		x	x
RCS cooldown rate compared to the limit based on RCS pressure		x	x
Wide range T_{cold} compared to the limit based on RCS pressure		x	x
Change of RCS temperature by more than 5°F in the last 10 minutes			x
Containment water level		x	x
Containment pressure		x	x
Pressurizer water level		x	x
Pressurizer water level trend		x	
Pressurizer reference leg temperature		x	
Reactor vessel - Hot leg water level		x	x
Pressurizer pressure		x	
Core exit temperature		x	x
RCS subcooling		x	x
RCS cold overpressure limit		x	x
IRWST water level		x	x
PRHR flow		x	x
PRHR outlet temperature		x	x
PCS storage tank water level		x	
PCS cooling flow		x	
IRWST to RNS suction valve status		x	x
Remotely operated containment isolation valve status[3]		x	
Containment area high range radiation level		x	x
Containment pressure (extended range)		x	

Table 2-3 (cont.) Minimum Inventory of Fixed Position Controls, Displays, and Alerts

Description	Control	Display	Alert[2]
CMT level[1]		x	
Manual reactor trip (Also initiates turbine trip.)	x		
Manual safeguards actuation	x		
Manual CMT actuation	x		
Manual main control room emergency habitability system actuation[4]	x		
Manual ADS actuation (1-3 and 4)	x		
Manual PRHR actuation	x		
Manual containment cooling actuation	x		
Manual IRWST injection actuation	x		
Manual containment recirculation actuation	x		
Manual containment isolation	x		
Manual main steamline isolation	x		
Manual feedwater isolation	x		
Manual containment hydrogen igniter (nonsafety)	x		

Notes:

1. Although this parameter does not satisfy any of the selection criteria, the importance of this parameter to the manual actuation of the automatic depressurization system (ADS) justifies the placement of this parameter on this list.
2. These parameters are used to generate visual alerts that identify challenges to the critical safety functions. For the main control room, the visual alerts are embedded in the safety displays as visual signals. For the remote shutdown workstation, the visual alerts are embedded in the nonsafety displays as visual signals.
3. These instruments are not required after 24 hours.
4. This manual actuation capability is not needed at the remote shutdown workstation.

2.5 DESIGN BASIS: SPATIALLY DEPENDENT VARIABLES (PARAGRAPH 4.6 OF IEEE 603-1991)

Thermowell-mounted resistance temperature detectors (RTDs) installed in each reactor coolant loop provide the hot and cold leg temperature signals required for input to the protection and control functions. The hot leg temperature measurement in each loop is accomplished using three fast-response, dual-element, narrow-range RTDs. The three thermowells in each hot leg are mounted approximately 120 degrees apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. The PMS averages these signals using electronic weighting to generate a hot leg average temperature. The process electronics includes provisions to allow for operation with only two RTDs in service. The process electronics bias the two RTD measurements to compensate for the loss of the third RTD.

Radially varying cold leg temperature is not a concern because the resistance temperature detectors are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant so that radial temperature variations do not exist.

Radial neutron flux is not a spatially dependent concern because of core radial symmetry. Calculations involving overtemperature and overpower ΔT use axial variation in neutron flux. Excore detectors furnish this axially-dependent information to the overtemperature and overpower calculators.

2.6 DESIGN BASIS: RANGE OF CONDITIONS FOR SAFETY SYSTEM PERFORMANCE (PARAGRAPH 4.7 OF IEEE 603-1991)

Equipment is environmentally qualified to meet the accident conditions through which it operates to mitigate the consequences of the accident. Equipment is seismically qualified to meet safe shutdown earthquake (SSE) levels.

The Class 1E dc and Uninterruptible Power Supply system (IDS) supplies electrical power to the safety systems. The safety systems perform their safety functions within the range of voltage and frequency provided by IDS.

The digital equipment design has additional design margin to accommodate a loss of the normal HVAC. The passive HVAC protects the safety system digital equipment upon failure or degradation of the active HVAC. The passive HVAC limits the rate of temperature rise in the rooms containing the digital equipment. The cabinets containing the digital equipment have temperature sensors that provide an alarm if internal cabinet temperatures reach an excessive value. In addition, the equipment is qualified at a temperature which envelopes the worse case temperature for which the equipment must continue to function.

The digital equipment will be qualified in accordance with EPRI TR-102323. Susceptibility and emissions testing of the equipment will be performed for both conducted and radiated signals. The tests will be performed on each subsystem in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the equipment performs within its design specifications.

If the tests show that susceptibilities exist in the range of interest, then the following assessments will be performed:

1. Further evaluations of test data and analyses will be performed which determine that the susceptibilities pose no hazard to the safe operation of the equipment.

2. If necessary, a site survey will be required to verify that the actual environment at the equipment location does not exceed the susceptibility level.

2.7 DESIGN BASIS: PROTECTION AGAINST NATURAL PHENOMENA AND UNUSUAL EVENTS (PARAGRAPH 4.8 OF IEEE 603-1991)

The ability to initiate and accomplish protective functions is maintained during and following natural phenomena as credible to the plant, such as earthquakes, tornadoes, hurricanes, floods, and winds. Plant safety is provided despite degraded conditions caused by internal events such as fire, flooding, explosions, missiles, electrical faults, and pipe whip.

2.8 DESIGN BASIS: RELIABILITY METHODS (PARAGRAPH 4.9 OF IEEE 603-1991)

The PMS meets its unavailability allocation, i.e., the PMS together with the diverse actuation system (DAS) shall contribute less than 3.0 hours per year to the overall plant unavailability. The PMS is designed to contribute less than 2.5 hours per year to the plant unavailability calculations.

The primary design features provided by the PMS to meet this requirement are:

- The ability to withstand single failures, including loss of power sources.
- Provision made for the periodic in-situ testing of equipment.
- Modular design allowing on-line replacement.
- Extensive diagnostic facilities to identify the location of faulty modules and components.

WCAP-13383 (Reference 3), CE-CES-195 (Reference 4), and NABU-DP-00014-GEN (Reference 5) describe planned design processes for the PMS hardware and software. A verification and validation (V&V) program demonstrates the adequacy of the hardware and software. WCAP-13383 provides details on the AP600 verification and validation program. CE-CES-195 provides details on the Common Q verification and validation program. Depending on the protection and safety monitoring system hardware used for AP1000, one of these programs will apply to AP1000.

See Section 3.4 for a discussion of quality methods and procedures.

2.9 DESIGN BASIS: CRITICAL POINTS (PARAGRAPH 4.10 OF IEEE 603-1991)

The safety systems are designed to protect the health and safety of the public by limiting the release of radioactive material during Conditions II, III, and IV events to acceptable limits, as defined in AP1000 accident analyses.

To facilitate the design of the safety systems, a number of specific limits on certain process and design variables (plant conditions) have been chosen which, if met, imply that the radioactive material release limits can be met with a high degree of confidence. These specific limits are defined on an accident by accident basis in the accident analyses.

The PMS automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level. The critical points in time are determined by the PMS response time modeled in the accident analyses. The PMS is designed and tested to meet the response times assumed in the accident analyses.

The operator can reset the system level signal when the plant conditions no longer exceed the limits established by the safety analyses. There are no automatic resets of plant safety systems.

2.10 DESIGN BASIS: EQUIPMENT PROTECTIVE PROVISIONS (PARAGRAPH 4.11 OF IEEE 603-1991)

No credible single failure of an equipment protective device prevents the initiation or accomplishment of a safety function at the system level.

The equipment protective features are designed to place the safety systems in a safe state, or into a state that has been demonstrated to be acceptable, if the safety equipment fails or the equipment protective device operates. Each protection channel has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.

- Engineered safety features actuated components are designed to fail into a state that has been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.

- Sensor circuits are designed, where possible, so that a loss of power will produce a 'safe' signal or will produce an off-scale value or a signal that can be identified by the protection system as 'bad.' Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate or use redundant signal or equipment where available, etc.)

- Actuation signals from multiple protection system divisions are provided for selected actuated equipment to improve the reliability of the protection system and minimize the impact of equipment protective provisions.

2.11 DESIGN BASIS: SPECIAL DESIGN BASES (PARAGRAPH 4.12 OF IEEE 603-1991)

A nonsafety DAS, diverse and separate from the safety systems, is included in the AP1000 design to provide the functions necessary to reduce the risk associated with postulated common mode failures of critical protection system instrumentation and control functions.

3 SAFETY SYSTEM CRITERIA

3.1 CONFORMANCE TO GENERAL FUNCTIONAL REQUIREMENTS (PARAGRAPH 5.0 OF IEEE 603-1991)

The PMS automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset value. The preset values are verified by calculating total instrument channel errors and determining that the difference between the preset value and the safety analysis limit for that function equals or exceeds the calculated value.

Range selection for the instrumentation covers the expected range of the process variable monitored. The PMS is designed so that trip setpoints do not require process transmitters to operate within five percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the PMS stipulate the minimum allowable accuracy.

3.2 CONFORMANCE TO THE SINGLE FAILURE CRITERION (PARAGRAPH 5.1 OF IEEE 603-1991)

A credible single failure within the safety system does not prevent the initiation or accomplishment of a protective function at the system level, even when a channel is intentionally bypassed for test or maintenance.

The safety system includes sufficient redundancy to meet system performance requirements even if the system is degraded by a single failure. Redundancy begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics. Redundant actuations are also provided. Two or more diverse functions initiate most protective actions.

No single failure within the safety system causes a Condition II event to progress to a Condition III event, or a Condition III event to progress to a Condition IV event.

Connections between redundant divisions or connections that carry signals to nonsafety systems include isolation devices. The isolation devices are tested to verify that credible faults, such as physical damage, short circuits, open circuits, or the application of credible fault voltages on the devices output terminals, do not propagate back to the isolator's input terminals. The isolation devices provide confidence that, where nonsafety systems use protection signals, credible single failures in the nonsafety system do not degrade the performance of the safety system.

To prevent common mode failures, additional measures such as functional diversity, physical separation, and testing as well as administrative control during design, production, installation, and operation are employed.

One design goal of the PMS is to minimize inadvertent reactor trips and engineered safety features actuations. Redundancy is provided for critical circuits which could malfunction and give an erroneous trip or engineered safety features initiation signal. The reactor trip circuit breaker arrangement prevents a single failure from causing a reactor trip. The two-out-of-four actuation logic for reactor trip requires trip signals from two-out-of-four divisions.

For engineered safety features initiation, the actuation logic for each component is performed redundantly within the coincidence logic. This redundant logic minimizes the probability of a random single failure causing inadvertent actuation. It also enables the safeguards actuation logic to meet single failure criterion during periodic testing. Dedicated switches which are used to initiate engineered safety features at the system level are connected to the local coincidence logic cabinets using two-pole, energize-to-actuate, ungrounded dc circuits. These circuits minimize inadvertent actuations caused by fire induced failures.

The design to reduce the likelihood of inadvertent trips or engineered safety features actuations does not negate the ability of the safety system to meet the single failure criterion, even when channels are bypassed for test or maintenance.

WCAP-15775 (Reference 6) describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture.

3.3 CONFORMANCE TO THE REQUIREMENT FOR COMPLETION OF PROTECTIVE ACTION ONCE IT IS INITIATED (PARAGRAPH 5.2 OF IEEE 603-1991)

Once initiated, protective functions at the system-level proceed to completion. The operator can stop the action of engineered safety features on a component-by-component basis by deliberate intervention. Component-level manual reset controls permit the operator to take this action only after the system-level signal is reset. One of the reasons component reset is provided is to stop safeguard functions if they are inadvertently actuated.

3.4 CONFORMANCE TO THE REQUIREMENTS FOR QUALITY COMPONENTS AND MODULES (PARAGRAPH 5.3 OF IEEE 603-1991)

The quality of components and modules is consistent with use in a nuclear generating station safety system. The AP1000 quality assurance program conforms to GDC-1.

Verification and Validation

A V&V program demonstrates the adequacy of the hardware and software for the PMS. Either WCAP-13383 (Reference 3) or CE-CES-195 (Reference 4) provides details on the verification and validation program. WCAP-13383 is an AP600 reference. CE-CES-195 is a Common Q document. The software development process is consistent with the following standards:

- ANSI/IEEE ANS-7-4.3.2-1993; "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

- IEEE 828-1990; "IEEE Standard for Software Configuration Management Plans"

- IEEE 829-1983; "IEEE Standard for Software Test Documentation"
- IEEE 830-1993; "Recommended Practice for Software Requirements Specifications"
- IEEE 1012-1986; "IEEE Standard for Software Verification and Validation Plans"
- IEEE 1028-1988; "IEEE Standard for Software Reviews and Audits"
- IEEE 1042-1987; "IEEE Guide to Software Configuration Management"

Design Process

WCAP-13383 provides a planned design process for hardware and software development during the following life cycle stages:

- Design requirements phase
- System definition phase
- Hardware and software development phase
- System test phase
- Installation phase

NABU-DP-00014-GEN (Reference 5), a Common Q document, also provides a planned design process for hardware and software development during similar life cycle stages:

- Conceptual phase
- System definition phase
- Software design phase
- Hardware design phase
- Software implementation phase
- Hardware implementation phase
- System integration phase
- Installation phase

Depending on the protection and safety monitoring hardware used for AP1000, either WCAP-13383 or NABU-DP-00014-GEN describe design processes that will be used for AP1000.

Commercial Dedication

WCAP-13383 (Reference 3) and CENPD-396-P (Reference 7) provide for the use of commercial off-the-shelf hardware and software through a commercial dedication process. Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant.

3.5 CONFORMANCE TO THE REQUIREMENTS FOR EQUIPMENT QUALIFICATION (PARAGRAPH 5.4 OF IEEE 603-1991)

Electrical equipment within the safety system is environmentally and seismically qualified to meet the conditions through which it must operate to mitigate the consequences of the accident.

3.6 CONFORMANCE TO THE REQUIREMENTS TO MAINTAIN SYSTEM INTEGRITY (PARAGRAPH 5.5 OF IEEE 603-1991)

The safety system instrumentation is designed to maintain its capability to initiate its protective functions during and following natural phenomena as credible to the plant, such as earthquakes, tornadoes, hurricanes, floods and winds. Functional capability of the system is maintained during events such as fires, flooding, explosions, missiles, electrical faults, and pipe whip. The equipment is environmentally and seismically qualified.

Redundancy of equipment provides protective functions despite loss of one of the redundant divisions.

Potential causes of fire and missiles that might occur due to postulated faults within the safety system equipment are identified and addressed. Equipment is built to industry codes, standards, and practices aimed at providing reliability and safety. For example, wiring used within electrical equipment and devices used to protect wiring from overcurrent (such as breakers, fuses, and current limiters) are sized and coordinated according to National Electric Code. Insulation used is flame retardant and meets National Electric Code, IEEE, and Underwriter's Laboratory guidelines applicable to the environment where the wiring is located. Electronics are housed in cabinets of metal construction. Wiring leaving the protection cabinets to the other redundant protection divisions or nonsafety areas uses isolation devices. In addition, the low power level of the digital equipment limits the fire ignition potential.

The PMS is designed to place the safety systems in a safe state, or into a state that has been demonstrated to be acceptable, if the input instrument fails. Each protection channel has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a state that has been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.
- Sensor circuits are designed, where possible, so that a loss of power will produce a 'safe' signal or will produce an off-scale value or a signal that can be identified by the protection system as 'bad.' Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate, or use redundant signal or equipment where available, etc.).
- De-energize-to-actuate circuits are used for engineered safety feature actuation system (ESFAS) functions where spurious actuation is not a concern.

3.7 CONFORMANCE TO THE REQUIREMENTS TO MAINTAIN INDEPENDENCE BETWEEN REDUNDANT PORTIONS OF A SAFETY SYSTEM (PARAGRAPH 5.6.1 OF IEEE 603-1991)

The flexibility of the safety system enables physical separation of redundant divisions. Division independence is carried throughout the system, extending from the sensor to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Wiring for redundant divisions uses physical separation, analyses, isolation, tests, or barriers to provide independence of the circuits. Separation of wiring is achieved using separate wireways, cable trays, and containment penetrations for each division. Separate power feeds energize each redundant protection division. This design meets the requirements of GDC-21.

Eight reactor trip breakers, two breakers for each division, interrupt power to the control rod drive mechanisms. The breaker main contacts are arranged so that opening both breakers in any two divisions interrupts power to all control rod drive mechanisms, permitting the rods to free fall into the core.

The design philosophy is to make maximum use of a variety of measurements. The PMS system continuously monitors numerous diverse system variables. Generally, two or more diverse protection functions would end an event before intolerable consequences could occur. This design meets the requirements of GDC-22.

Where redundant equipment communicates, such as at the plant protection subsystems, isolation devices are employed to preserve electrical independence of the divisions. They also preserve the independence of safety equipment from nonsafety systems that may use protection signals.

The physical separation criteria for safety system cabinets includes the applicable recommendations contained in Paragraph 6.6 of IEEE 384-1981 (Reference 8). The application of these criteria to instrumentation cabinets is endorsed by Regulatory Guide 1.75 (Reference 9).

3.8 CONFORMANCE TO THE REQUIREMENTS TO MAINTAIN INDEPENDENCE BETWEEN SAFETY SYSTEMS AND EFFECTS OF A DESIGN BASIS EVENT (PARAGRAPH 5.6.2 OF IEEE 603-1991)

The design meets the requirements to maintain independence between safety systems and the effects of design basis events by conforming to Paragraph 5.4 of IEEE 603-1991.

3.9 CONFORMANCE TO THE REQUIREMENTS TO MAINTAIN INDEPENDENCE BETWEEN SAFETY SYSTEMS AND OTHER INTERCONNECTED EQUIPMENT (PARAGRAPH 5.6.3.1 OF IEEE 603-1991)

Signals from safety system equipment for control system use are transmitted through isolation devices. These devices are part of the safety system and are tested to confirm that credible failures at the output of the isolation device do not prevent the associated safety system channel from meeting the minimum performance requirements. Credible failure tests include: physical damage; short circuits; open circuits; grounds; and the application of the maximum ac or dc potentials that may be present in any cabinet where the isolation device is located or in any wireway where its electrical or optical lines run.

The safety system maintains its ability to initiate and accomplish protective functions despite credible equipment malfunctions within the non-safety system. The following design bases apply:

- Where the control system uses signals from protection channels, no credible single failure in the protection channel causes a control system action requiring protective action by the redundant channels monitoring the same variable.

- Where nonsafety systems use signals derived from protection channels, no credible failure in the nonsafety system prevents the safety system from meeting its performance requirements.

3.10 CONFORMANCE TO THE REQUIREMENTS TO MAINTAIN INDEPENDENCE BETWEEN SAFETY SYSTEMS AND OTHER EQUIPMENT IN PROXIMITY (PARAGRAPH 5.6.3.2 OF IEEE 603-1991)

Nonsafety wiring is separated from safety wiring. Analyses, tests, or physical barriers are used to verify the adequacy of wire routing where separation distances are less than those suggested by regulatory guides or industry standards.

3.11 CONFORMANCE TO THE REQUIREMENTS REGARDING THE EFFECTS OF A SINGLE RANDOM FAILURE (PARAGRAPH 5.6.3.3 OF IEEE 603-1991)

The plant control system keeps the reactor operating away from safety limits. Should a control system fail and cause a parameter to approach its limit, the protection system trips the reactor. The setpoints are chosen so that the design bases established for credible events are met. The accident analyses do not assume a control system action to reduce the severity of an accident. Assumptions made on control systems are worst case assumptions - that their failure drives the parameters involved toward their worst direction for safety. The safety system setpoints account for these malfunctions.

Isolation devices prevent credible faults in the control system from degrading the functional capability of the protection system.

3.12 CONFORMANCE TO THE REQUIREMENTS REGARDING INDEPENDENCE OF CLASS 1E EQUIPMENT AND CIRCUITS (PARAGRAPH 5.6.4 OF IEEE 603-1991, IEEE 384-1981, REGULATORY GUIDE 1.75)

There are five separation groups for the cable and raceway system: group A, B, C, D, and N. Separation group A contains safety circuits from division A. Similarly, separation group B contains safety circuits from division B; group C from division C; group D from division D; and group N contains nonsafety circuits.

Cables of one separation group are run in separate raceway and physically separated from cables of other separation groups. Group N raceways are separated from safety groups A, B, C and D. Raceways from group N are routed in the same areas as the safety groups according to spatial separation stipulated in Regulatory Guide 1.75 (Reference 9) and IEEE 384-1981 (Reference 8) with the following exceptions:

- Within the MCR and RSW (nonhazard areas), the minimum vertical separation for open top cable tray is 3 inches and the minimum horizontal separation is 1 inch.

- Within general plant areas (limited hazard areas), the minimum vertical separation is 12 inches, and the minimum horizontal separation is 6 inches for open top cable trays with low-voltage power circuits for cable sizes <2/0 AWG. For configurations that involve exclusively limited energy content cables (instrumentation and control), these minimum distances are reduced to 3 inches and 1 inch respectively.

- Within panels and control switchboards, the minimum horizontal separation between components or cables of different separation groups (both field-routed and vendor-supplied internal wiring) is 1 inch, and the minimum vertical separation distance is 6 inches.

- For configurations involving an enclosed raceway and an open raceway, the minimum vertical separation is 1 inch if the enclosed raceway is below the open raceway.

The exceptions to the guidance in Regulatory Guide 1.75 are based on test results used to support exceptions to the separation guidance for operating nuclear power plants. A summary of test results from ten electrical separation test programs is documented in Reference 10. These test programs support the AP1000 exceptions.

Non-Class 1E circuits are electrically isolated from Class 1E circuits, and Class 1E circuits from different separation groups are electrically isolated by isolation devices, shielding and wiring techniques, physical separation (in accordance with Regulatory Guide 1.75 for circuits in raceways), or an appropriate combination thereof.

When isolation devices are used to isolate Class 1E circuits from non-Class 1E circuits, the circuits within or from the Class 1E equipment or devices are identified as Class 1E and are treated as such. Beyond the isolation device(s) these circuits are identified as non-Class 1E and are separated from Class 1E circuits in accordance with the above separation criteria.

Power and control cables are installed in conduits, solid bottom trays, or ventilated bottom trays (ladder-type). Solid tray covers are used in outdoor locations and indoors where trays run in areas where falling debris is a problem. Instrumentation cables are routed in conduit or solid bottom cable tray with solid tray covers as required. The cables are derated for specific application in the location where they are installed.

Separate trays are provided for each voltage service level: 6.9 kV, low voltage power (480 Vac, 120 Vac, 125 Vdc), high-level signal and control (120 Vac, 125 Vdc), and low level signal (instrumentation). A tray designed for a single class of cables shall contain only cables of the same class except that low voltage power cables may be routed in raceways with high level signal and control cables if their respective sizes do not differ greatly and if they have compatible operating temperatures. When this is done in trays, the power cable ampacity is calculated as if all cables in the tray are power cables. Low voltage power cable and high level signal and control cable will not be routed in common raceways if the fault current, within the breaker or fuse clearing time, is sufficient to heat the insulation to the ignition point. In general, a minimum of 12 inches vertical spacing is maintained between trays of different service levels within the stack.

3.13 CONFORMANCE TO THE REQUIREMENTS TO PROVIDE CAPABILITY FOR TEST AND CALIBRATION (PARAGRAPH 5.7 OF IEEE 603-1991)

Capability for testing and calibrating channels and devices used to derive the final system output signal from the various channel signals is provided. Testing from the sensor inputs of the PMS through to the actuated equipment is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power would upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down.

Each division of the PMS includes a test subsystem. The test subsystem provides for verification of the setpoint values and other constants, and verification that proper signals appear at other locations in the system.

Verification of the signal processing algorithms is made by exercising the test signal sources (either by hardware or software signal injection) and observing the results up to, and including, the attainment of a channel partial trip or actuation signal at the power interface. When required for the test, the tester places the voting logic associated with the channel function under test in bypass.

The overlapping test sequence continues by inputting digital test signals at the output side of the threshold functions, in combinations necessary to verify the voting logic. Some of the input combinations to the coincidence logic cause outputs such as reactor trips and engineered safety feature (ESF) initiation. The reactor trip circuit breaker arrangement is a two-out-of-four logic configuration, such that the tripping of the two circuit breakers associated with one division does not cause a reactor trip. To reduce wear on the breakers through excessive tripping, and to avoid a potential plant trip resulting from a single failure while testing is in progress, the test sequence is designed so that actual opening of the trip breakers is only required when the breaker itself is being tested.

The test subsystem does not test the ESF actuators. This portion of the test may be accomplished by using component-level actuation signals. For those final devices that can be operated at power without upsetting the plant or damaging equipment, the test is performed by actuating the manual actuation control that causes the device to operate. Position switches on the device itself send a signal back to the ESF actuation subsystem, where it is transmitted to the MCR for display purposes. The display verifies that the manual command is successfully completed, thus verifying operability of the final device. For those devices that cannot be tested at power without damage or upsetting the plant, continuity of the wiring up to the actuation device is verified. Operability of the final equipment is demonstrated at reduced power or at shutdown, depending on the equipment.

Where actuated equipment is not tested during reactor operation, it is established that:

- There is no practicable system design that permits operation of the equipment without adversely affecting the safety or operability of the plant.

- The probability that the safety system fails to initiate the operation of the actuated equipment is maintained acceptably low without testing the equipment during reactor operation.

- The equipment is routinely tested when the reactor is shutdown

When channels are bypassed for the purposes of testing, the bypass is manually instated and removed by the test subsystem.

3.14 CONFORMANCE TO REQUIREMENTS TO PROVIDE DISPLAYS FOR MANUALLY CONTROLLED ACTIONS (PARAGRAPH 5.8.1 OF IEEE 603-1991)

No manually controlled actions are assumed in the DCD Chapter 15 analyses. AP1000 has no Regulatory Guide 1.97 Type A variables.

3.15 CONFORMANCE TO REQUIREMENTS TO PROVIDE SYSTEM STATUS INDICATION (PARAGRAPH 5.8.2 OF IEEE 603-1991)

The initiation of a protective action is identified and indicated down to the channel-level. Except for post-accident monitoring information, this status information is not safety related. As such, it is transmitted to the MCR for indication and recording from the PMS using the data display and monitoring system.

PMS status information is provided to the operator. Status information is of four types:

- Parameter values
- Logic status
- Equipment status
- Actuation device status

Alarms and annunciators also alert the operator of deviations from normal operating conditions, so that he may take appropriate action to avoid a challenge to the safety system.

3.16 CONFORMANCE TO REQUIREMENTS TO PROVIDE INDICATION OF BYPASSES (PARAGRAPH 5.8.3 OF IEEE 603-1991)

The PMS provides the operator, via the data display and processing system (DDS), with continuous indications of bypassed status. The display of the status information allows the operator to identify the specific bypassed functions, and to determine if the logic has reverted to two-out-of-three. In addition to the status indication, an alarm is sounded in the MCR if more than one bypass is attempted for a given protection function.

3.17 CONFORMANCE TO REQUIREMENTS FOR LOCATION OF DISPLAYS (PARAGRAPH 5.8.4 OF IEEE 603-1991)

The majority of the operations for both the MCR and the RSW employ soft controls, soft control displays, and plant information displays. A computer generates soft control displays and plant information displays. The operator can change these displays to perform different functions, allow control of different

devices, or display different information. These displays appear on display devices such as cathode ray tubes, flat panel screens, or visual display units. Alarms direct operator attention. Devices such as a keyboard, touch screen, mouse, or other equivalent input devices provide soft controls.

The AP1000 human system interface design includes a minimum inventory of dedicated or fixed-position displays and controls. The minimum inventory of fixed-position instrumentation includes those displays, controls, and alarms used to monitor the status of critical safety functions and to manually actuate the safety systems that achieve these critical safety functions. Table 2-3 lists the minimum inventory of fixed-position displays, alarms, and controls.

Fixed-position alarms and displays are available at a fixed location and are continuously available, though not necessarily displayed, to the operator. The operator can access fixed-position displays to monitor the plant status, based on indications from critical plant variables or parameters. Fixed-position alarms direct operator attention to the need to perform safety functions for which there is no automatic actuation. Although not continuously displayed, the fixed-position displays and alarms are quickly and easily retrievable. Fixed-position controls provide a means for manual reactor and turbine trip, and safety system/component actuation. Fixed-position controls are available to the operator to perform tasks in the operation of safety systems and components used to mitigate the consequences of an accident and to establish and maintain safe shutdown conditions following an accident. The fixed-position controls are a manual backup to the automatic protection signals provided by the PMS.

3.18 CONFORMANCE TO REQUIREMENTS CONTROLLING ACCESS TO SAFETY SYSTEM EQUIPMENT (PARAGRAPH 5.9 OF IEEE 603-1991)

The PMS provides for administrative control over access to the means for manually bypassing protection channels and for manually blocking protective functions. Administrative control of access is provided to setpoint adjustments, channel calibration adjustments, and test points. Cabinet doors are normally locked.

3.19 CONFORMANCE TO THE REQUIREMENT TO FACILITATE SYSTEM REPAIR (PARAGRAPH 5.10 OF IEEE 603-1991)

The PMS facilitates the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in diagnostics provide a mechanism for periodically verifying the operability of modules in the PMS, and of rapidly locating malfunctioning assemblies. Continuous on-line error checking also detects and locates failures. Channel bypass permits replacement of malfunctioning sensors or channel components, without jeopardizing plant availability, while still meeting the single-failure criterion.

3.20 CONFORMANCE TO THE REQUIREMENTS FOR IDENTIFICATION OF SAFETY SYSTEM EQUIPMENT (PARAGRAPH 5.11 OF IEEE 603-1991)

Redundant divisions of the safety system have distinctive markings.

The color-coded nameplates described below provide identification of equipment, associated with protective functions and their division associations.

Division	Color Coding
Division A	BROWN with WHITE lettering
Division B	GREEN with BLACK lettering
Division C	BLUE with WHITE lettering
Division D	YELLOW with BLACK lettering

Non-cabinet mounted protective equipment and components have an identification tag or nameplate. Small electrical components, such as relays, have nameplates on the enclosure that houses them.

3.21 CONFORMANCE TO THE REQUIREMENTS FOR AUXILIARY FEATURES (PARAGRAPH 5.12 OF IEEE 603-1991)

Electrical Power

The IDS provides reliable power for the safety equipment required for the plant instrumentation, control, monitoring and other vital functions needed for shutdown of the plant. In case of a total loss of off-site and on-site ac power sources, the dc batteries constitute the sources of electrical power for operation of the required dc and ac instrument Uninterruptible Power Supply (UPS) loads.

The IDS system provides power for the safety equipment required for safe shutdown of the plant, and for mitigation and control of accident conditions in the plant.

HVAC

When a source of ac power is available, the non-safety VBS provides HVAC service to the instrumentation and control rooms for normal and abnormal conditions. The VBS and its support systems provide these functions in a reliable and failure tolerant fashion. If offsite power is not available, one of the two onsite nonsafety diesels automatically provides backup power. The VBS is designed to maintain the instrumentation and control rooms between 67°F and 75°F and within a relative humidity range of 25 percent to 60 percent during plant normal operation and abnormal operation when VBS is operable and supporting systems are available.

If the VBS system is not available (including loss of ac power), the VES provides emergency passive heat sinks for the instrumentation and control rooms and dc equipment rooms. The heat sinks for each room limit the temperature rise inside each room during the 72-hour period following a loss of VBS.

In the unlikely event that power to the VBS is unavailable for more than 72 hours, the temperature of the instrumentation and control rooms is maintained by operating two ancillary fans to supply outside air to two divisions of instrumentation and control rooms.

Other Auxiliary Features

The test subsystem; alarm sensors such as cabinet temperature sensors, voltage sensors, and door switches; and isolators are designed to ensure that these components do not degrade the safety systems below an acceptable level.

3.22 CONFORMANCE TO THE REQUIREMENTS FOR MULTI-UNIT STATIONS (PARAGRAPH 5.13 OF IEEE 603-1991)

The AP1000 is a single-unit plant. If more than one unit were built on the same site, the units would not share any of the safety systems.

3.23 CONFORMANCE TO THE REQUIREMENTS FOR HUMAN FACTORS (PARAGRAPH 5.14 OF IEEE 603-1991)

The human factors engineering design process of the AP1000 has been developed to conform to NUREG-0711, "Human Factors Engineering Program Review Model" (Reference 2). The 10 elements of the design process provide a structured top-down system analysis using accepted human factors engineering principles. The design of the MCR and the other operation and control centers reflect state-of-the-art human factors principles.

The 10 human factors engineering program elements are:

1. Human Factors Engineering Program Management – The AP1000 human factors engineering program plan that is used to develop, execute, oversee, and document the human factors engineering program. This program plan includes the composition of the human factors engineering design team.

2. Operating Experience Review – This operating experience review has identified, analyzed, and addressed human factors engineering-related problems encountered in previous designs.

3. Functional Requirements Analysis and Functional Allocation – The functional requirements analysis has defined the plant's safety functions, decomposed each safety function, compared the safety functions and processes with currently operating Westinghouse pressurized water reactors, and provided the technical basis for those processes that have been modified. The objective of this allocation process was to define the AP1000 safety function requirements and allocate functions between the human and the machine appropriately.

4. Task Analysis – The task analysis provides one of the bases for the human system interface design; provides input to procedure development; provides input to staffing, training, and communications requirements of the plant; and ensures that human performance requirements do not exceed human capabilities.

5. Staffing – The staffing analysis provides input from the designer for the determination of the staffing level of the operating crew in the AP1000 MCR.

6. Integration of Human Reliability Analysis with Human Factors Engineering.

7. Human System Interface Design.

8. Procedure Development.

9. Training Program Development.

10. Human System Interface Design Test Program.

3.24 CONFORMANCE TO THE REQUIREMENTS FOR RELIABILITY (PARAGRAPH 5.15 OF IEEE 603-1991)

See Section 3.4 for a discussion of quality methods and procedures.

The I&C safety systems of the AP1000 are analyzed in the AP1000 Probabilistic Risk Assessment (PRA). See the AP1000 PRA report, Chapter 26, for details.

4 SENSE AND COMMAND FEATURES – FUNCTIONAL AND DESIGN REQUIREMENTS

4.1 CONFORMANCE TO THE REQUIREMENTS FOR AUTOMATIC INITIATION AND CONTROL OF PROTECTIVE FUNCTIONS (PARAGRAPH 6.1 OF IEEE 603-1991)

The PMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. The PMS automatically initiates appropriate safety functions whenever a variable measured by the PMS reaches a trip or actuation setpoint.

4.2 CONFORMANCE TO THE REQUIREMENTS FOR MANUAL INITIATION AND CONTROL OF PROTECTIVE FUNCTIONS (PARAGRAPH 6.2 OF IEEE 603-1991)

Manual initiation of protective functions at the system-level is available. Fixed-position controls are provided for use as a manual backup to the automatic protection signals provided by the PMS. Manual initiation of a protective function at the system level performs all actions performed by automatic initiation, such as providing the required action sequencing functions and interlocks.

The controls for manual initiation of protective functions at the system level are located in the MCR and are easily accessible to the operator.

Manual initiation depends on the operation of the minimum of equipment and, once initiated, proceeds to completion unless deliberate operator intervention is taken. No single failure in either the automatic portion, manual portion, or shared portion prevents manual or automatic initiation of a protective function at the system level. This capability is achieved through the redundant structure of the PMS.

The PMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. For events where the PRHR heat exchanger is actuated, the plant automatically cools down to the safe shutdown condition. When a stabilized condition is reached automatically following a reactor trip, it is expected that the operator may, following event recognition, take manual control and proceed with orderly shutdown of the reactor in accordance with the normal, abnormal, or emergency operating procedures. The exact actions taken and the time at which these actions occur depend on what systems are available and the plans for further plant operation. However, for these events, no operator actions are required to maintain the plant in a safe and stable condition.

4.3 CONFORMANCE TO THE REQUIREMENTS CONCERNING PROTECTION SYSTEM FAILURES INTERACTING WITH CONTROL SYSTEMS (PARAGRAPH 6.3 OF IEEE 603-1991)

Certain information derived from protection channels is used to control the plant. This reduces the number of penetrations into critical pressure boundaries, such as into the reactor coolant loops, pressurizer and steam generators. It also helps reduce congestion and enhance separation.

A control system channel selection algorithm is used so that malfunctioning protection channels do not send erroneous information to the control system. PMS malfunctions in a channel do not cause a control system action that results in a protection function actuation using the remaining redundant channels monitoring that variable. Therefore, where protection signals are used for control, functional isolation is provided between the control and protection systems.

The selection algorithm continuously monitors the redundant protection system channels, which send information to the control systems. The algorithm provides the control system with signals considered valid.

As long as at least three redundant channels of information are available, the selection algorithm rejects an invalid signal. This is done by comparing the redundant channels to one another. Any signal that deviates from the others by more than a reasonable amount is rejected, consistent with normal instrument channel drift and calibration tolerances. A discussion of the signal selection algorithm used is contained in WCAP-13382 (Reference 11). Reference 11 is an AP600 document that describes the signal selection algorithm used by both the AP600 and AP1000.

4.4 CONFORMANCE TO REQUIREMENTS CONCERNING THE DERIVATION OF SYSTEM INPUTS (PARAGRAPH 6.4 OF IEEE 603-1991)

To the extent feasible and practical, protection system inputs are derived from signals that are direct measures of the desired variables. Tables 2-1 and 2-2 list these variables for reactor trip and for engineered safety features actuation.

The PMS calculates two variables where direct measurement is not feasible. These are the thermal overtemperature ΔT reactor trip and the overpower ΔT reactor trip.

4.5 CONFORMANCE TO THE REQUIREMENTS TO PROVIDE CAPABILITY FOR TESTING AND CALIBRATION (PARAGRAPHS 6.5 OF IEEE 603-1991)

Means are provided for checking the operational availability of each PMS input sensor during reactor operation. These are accomplished by one of the following techniques:

- Perturbing the monitored variable

- Cross-checking between channels that have a known relationship to each other and that have read-outs available

- Introducing and varying a substitute input to the sensor of the same nature as the measured variable

The PMS facilitates the diagnosis, location, and repair or adjustment of malfunctioning components.

4.6 CONFORMANCE TO REQUIREMENTS ON OPERATING BYPASSES (PARAGRAPH 6.6 OF IEEE 603-1991)

In addition to the test and maintenance bypasses described in Section 4.7, several operating bypasses are provided. These bypasses automatically block certain protective actions that would otherwise prevent modes of operations such as start-up. The operating bypasses are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

4.7 CONFORMANCE TO REQUIREMENTS ON MAINTENANCE BYPASS (PARAGRAPH 6.7 OF IEEE 603-1991)

The safety system is designed to permit the bypass for maintenance, test, or repair of any one protection channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

With one channel bypassed, the PMS does not permit the bypass of a second channel in the group monitoring the same variable. An attempt to apply multiple bypasses is blocked, and trip/actuation is not triggered by the attempt.

Channel Level Bypass Capability

A protection division takes inputs from one or more process sensors, performs compensation or other calculation, and terminates in one or more bistable functions where the process variable is compared against setpoints. The logic portion of the PMS receives the partial trip outputs from these comparisons and combines them with the partial trip status of the other channels to initiate a protective function, such as reactor trip.

Generally, there are four protection channels for each actuation function. Accident analyses or reliability studies assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each actuation function, the technical specifications limit the period allowed for a channel to be bypassed or out of service. The time specified in the technical specifications is determined by considering the degree of redundancy provided for the function and the importance of the function.

Reactor Trip and ESF Logic

The technical specifications limit the period allowed for reactor trip logic and ESF logic to be bypassed or out of service.

Control of Access

The operator initiates maintenance bypasses. The operator has complete administrative control over bypass actuation. The bypass is manually initiated and the operator interface is located inside the PMS cabinets. The PMS cabinet doors are normally locked according to administrative procedures.

4.8 CONFORMANCE TO THE REQUIREMENTS FOR SETPOINT UNCERTAINTIES (PARAGRAPH 6.8.1 OF IEEE 603-1971)

Three values applicable to reactor trip and ESF actuations are specified:

1. Safety analysis limit
2. Allowable value
3. Nominal setpoint

The safety analysis limit is the value assumed in the accident analysis and is the least conservative value.

The allowable value is the technical specification value and is obtained by subtracting a safety margin from the safety analysis limit. The safety margin accounts for instrument error, process uncertainties such as flow stratification and transport factor effects, etc.

The nominal setpoint is the value set into the equipment and is obtained by adding or subtracting allowances for instrument drift from the allowable value. The nominal setpoint allows for the normal expected instrument setpoint drifts such that the technical specification limits are not exceeded under normal operation.

As described above, allowance is made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal setpoint value that is actually set into the equipment. The only requirement on the instrument's accuracy is that, over the instrument span, the error must always by less than or equal to the error value allowed in the accident analysis. The instrument does not need to be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

Combined License applicants referencing the AP1000 certified design will provide a calculation of setpoints for protective functions consistent with the methodology presented in Reference 12. Reference 12 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans.

4.9 CONFORMANCE TO THE REQUIREMENTS ON THE USE OF MULTIPLE SETPOINTS (PARAGRAPH 6.8.2 OF IEEE 603-1971)

For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the PMS hardware and software are designed to provide positive means or administrative control to ensure that the more restrictive trip setpoint is used. The hardware and software used to prevent improper use of less restrictive trip settings are considered part of the PMS.

5 EXECUTIVE FEATURES - FUNCTIONAL AND DESIGN REQUIREMENTS

5.1 CONFORMANCE TO THE REQUIREMENTS FOR AUTOMATIC CONTROL EXECUTION (PARAGRAPH 7.1 OF IEEE 603-1991)

The PMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. The PMS automatically initiates appropriate safety functions whenever a variable measured by the PMS reaches a trip or actuation setpoint.

5.2 CONFORMANCE TO THE REQUIREMENTS FOR MANUAL CONTROL EXECUTION (PARAGRAPH 7.2 OF IEEE 603-1991)

Fixed-position safety controls are provided which satisfy the following criteria:

1. Each remotely operated, safety valve has manual actuation capability. This manual actuation capability is capable of moving the valve to its safety position(s)[1].

2. System level dedicated switches provide this manual valve actuation capability, i.e., individual Class 1E switches are not used.

3. In cases where actuation of the manual controls is onerous[2], 2-out-of-2 logic is used, i.e., two switches must be actuated at the same time in order for the actuation to take place.

4. Redundant switches are used. Where 1-out-of-1 logic is required, two switches are used, each located on separate MCR panels. Where 2-out-of-2 logic is required, four switches are used, two located on each of two separate panels.

5.3 CONFORMANCE TO THE REQUIREMENTS FOR COMPLETION OF PROTECTIVE ACTION (PARAGRAPH 7.3 OF IEEE 603-1991)

Once initiated, protective functions at the system-level proceed to completion. The action of engineered safety features can be stopped on a component-by-component basis by deliberate operator intervention. Component-level manual reset controls permit the operator to take this action only after the system-level signal is reset. One of the reasons component reset is provided is to stop safeguard functions if they are inadvertently actuated.

---

[1] Note that all of the AP1000 valves have only one safety-related position except the reactor vessel head vent valves, which have two (open and closed).

[2] Onerous actuation is defined as that which causes a breach of the reactor coolant system pressure boundary or a need to shut down the plant to cold conditions to effect repairs.

5.4 CONFORMANCE TO THE REQUIREMENTS FOR OPERATING BYPASS EXECUTION (PARAGRAPH 7.4 OF IEEE 603-1991)

Operating bypasses automatically block certain protective actions that would otherwise prevent modes of operations such as start-up. The operating bypasses are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

5.5 CONFORMANCE TO THE REQUIREMENTS FOR MAINTENANCE BYPASS EXECUTION (PARAGRAPH 7.5 OF IEEE 603-1991)

The safety system permits the bypass for maintenance, test, or repair of any one protection channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

Reactor Trip Breaker Bypass Capability

Opening pairs of reactor trip breakers actuates a reactor trip; one pair is associated with each of four divisions of the PMS. The breaker arrangement provides 2-out-of-4 logic, such that opening any two pairs of breakers de-energizes the control rod drive mechanisms, thus causing the reactor trip. During maintenance and testing of the trip actuation logic, the trip signals to the undervoltage trip attachments of the reactor trip breakers are not actuated. The PMS will not allow more than one pair (one division) of breakers to be bypassed at any one time. In the event that an attempt to bypass the breakers from one division occurs while another division is in the bypass mode, the reactor does not trip and an alarm is actuated in the control room. If two of the three remaining divisions generate a trip signal (two-out-of-three), the reactor trips. The breaker bypass status is communicated between the PMS cabinets by the same system of isolated data links that carry the partial trip information.

Reactor Trip Breakers and ESF Actuation

The technical specifications limit the period allowed for reactor trip breakers and ESF actuation subsystems to be out of service.

Control of Access

The operator initiates maintenance bypasses. The operator has complete administrative control over bypass actuation. The bypass is manually initiated and the operator interface is located inside the PMS cabinets. The PMS cabinet doors are normally locked according to administrative procedures.

6 POWER SOURCE REQUIREMENTS

6.1 CONFORMANCE TO THE REQUIREMENTS FOR ELECTRICAL POWER SOURCES (PARAGRAPH 8.1 OF IEEE 603-1991)

The IDS provides reliable power for the safety equipment required for the plant instrumentation, control, monitoring and other vital functions needed for shutdown of the plant. In case of a total loss of off-site and on-site ac power sources, the dc batteries provide electrical power for operation of the required dc and ac instrument UPS loads.

The IDS system provides power for the safety equipment required for safe shutdown of the plant, and for mitigation and control of accident conditions in the plant.

The IDS system is designed with four independent, Class 1E 125 Vdc divisions (A, B, C and D). Each division has one 24-hour battery bank. In addition, divisions B and C each have one 72-hour battery bank. Each battery bank has its own battery charger. Each of the four divisions is electrically isolated and physically separated to prevent a single event from causing the loss of more than one division.

The IDS is designed to provide power to the critical plant loads required for plant safe shutdown and monitoring, when all the on-site and off-site ac power sources at the plant are lost and cannot be recovered for a period of up to 72 hours.

The normal source of power for the Class 1E dc system is the non-Class 1E ac power system. Battery chargers serve as isolation devices for the connection between the Class 1E system and the non-Class 1E system. If the normal source of ac power is not available, the Class 1E batteries have sufficient capacity for the critical plant loads required for plant safe shutdown for a period of up to 72 hours.

The Class 1E dc power supply system operates ungrounded in order to ensure that a single ground fault will not preclude system operation.

6.2 CONFORMANCE TO THE REQUIREMENTS FOR NON-ELECTRICAL POWER SOURCES (PARAGRAPH 8.2 OF IEEE 603-1991)

AP1000 non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, are not required for safety functions.

6.3 CONFORMANCE TO THE REQUIREMENTS FOR MAINTENANCE BYPASS (PARAGRAPH 8.3 OF IEEE 603-1991)

The Class 1E dc and UPS system includes a single spare battery bank with spare battery charger. The spare battery bank and battery charger can replace any one of the 24-hour or 72-hour battery banks and associated battery chargers while maintaining electrical isolation and physical separation. In the case of a failure, maintenance or unavailability of the normal battery bank and the battery charger, the spare can be connected to the affected bus using permanently installed cable connections. The configuration of the spare battery connections permits connection of only one battery bank and battery charger at a time. Apart from normal maintenance and testing, the spare battery charger remains continuously energized to

keep the spare battery fully charged and ready for replacing any battery on demand. The time required to connect the spare battery to a Class 1E division is much less than the time allowed for the Limiting Condition for Operation (LCO) associated with the loss of one Class 1E dc division.

Regulating transformers provide backup sources of power for the UPS system. If an inverter is inoperable or the Class 1E 125 Vdc input to the inverter is unavailable, the load is transferred automatically to the backup ac source by a static transfer switch featuring a make-before-break contact arrangement. The diesel generator backed non-Class 1E 480 Vac bus provides the backup power through the Class 1E regulating transformer.

A manual maintenance bypass switch with overlapping contacts provided at the inverter facilitates connection of the backup power source when the inverter is removed from service for maintenance. The automatic or manual transfer from one power source to another does not affect the ability of the PMS to perform its safety functions.

7 REFERENCES

1. IEEE 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generator Stations," December 31, 1991.

2. NUREG-0711, "Human Factors Engineering Program Review Model," July 1994.

3. WCAP-13383, Revision 1 (NP), "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. NABU-DP-00014-GEN, Rev. 0, "Design Process for Common Q Safety Systems," March 9, 2001.

6. WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," March 2002.

7. CENPD-396-P, Rev. 01, "Common Qualified Platform," May 2000.

8. IEEE Standard 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," September 18, 1980.

9. Regulatory Guide 1.75, Revision 2, "Physical Independence of Electric Systems," September 1978.

10. Young, G. L. et al., "Cable Separation - What Do Industry Programs Show?," IEEE Transactions of Energy Conversion, September 1990, Volume 5, Number 3, pp. 585-602.

11. WCAP-13382 (P), WCAP-13391 (NP), "AP600 Instrumentation and Control Hardware Description," May 1992.

12. WCAP-14605 (P), WCAP-14606 (NP), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996.