CHAPTER 7

INSTRUMENTATION AND CONTROLS

7.1 Introduction

The instrumentation and control systems presented in this chapter provide protection against unsafe reactor operation during steady-state and transient power operations. They initiate selected protective functions to mitigate the consequences of design basis events. This chapter relates the functional performance requirements, design bases, system descriptions, and safety evaluations for those systems. The safety evaluations show that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

Because of the rapid changes that are taking place in the digital computer and graphic display technologies employed in a modern human system interface, design certification of the AP1000 focuses upon the process used to design and implement instrumentation and control systems for the AP1000, rather than on the specific implementation. The design specifics provided here are included as an example for illustration.

DCD Chapter 7 for the AP1000 has been written to describe the protection system hardware utilizing the Common Qualified Platform (Common Q) described in Reference 8 (which includes the NRC SER), and augmented by Reference 2. The I&C functional requirements of the AP600, which has received Design Certification, have been retained to the maximum extent compatible with the Common Q hardware and software.

The terminology used for Chapter 7 is intended to be independent of any product, but when this is not possible, Common Q terminology is used.

This chapter also discusses the instrumentation portions of the safety-related systems which function to achieve the system responses assumed in the accident analysis, and those needed to shutdown the plant. Section 7.1 describes the AP1000 instrumentation and control architecture, with specific emphasis on the protection and safety monitoring system. The plant control system is discussed briefly. Other systems are discussed in more detail in relevant sections or chapters. Section 7.2 discusses the reactor trip function, and Section 7.3 addresses the engineered safety features (ESF). Systems required for safe shutdown are discussed in Section 7.4 in support of other chapters. Safety-related display instrumentation is discussed in Section 7.5 and interlocks important to safety are presented in Section 7.6. Control systems and the diverse actuation system are discussed in Section 7.7.

Definitions

Terminology used in this chapter reflects an interdisciplinary approach to safety-related systems similar to that proposed in IEEE 603 (Reference 1).

Safety System – The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events.

Protection and Safety Monitoring System – The aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and ESF, and which provides the equipment necessary to monitor plant safety-related functions during and following designated events.

Protective Function – Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the protection and safety monitoring system logic and will be accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trip and engineered safety features (such as valve alignment and containment isolation).

Actuated Equipment – The assembly of prime movers and driven equipment used to accomplish a protective function (such as solenoids, shutdown rods, and valves).

Actuation Device – A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves).

Division – One of the four redundant segments of the safety system. A division includes its associated sensors, field wiring, cabinets, and electronics used to generate one of the redundant actuation signals for a protective function. It also includes the power source and actuation signals.

Channel – One of the several separate and redundant measurements of a single variable used by the protection and safety monitoring system in generating the signal to initiate a protective function. A channel can lose its identity when it is combined with other inputs in a division.

Degree of Redundancy – The number of redundant channels monitoring a single variable, or the number of redundant divisions which can initiate a given protective function or accomplish a given protective function. Redundancy is used to maintain protection capability when the safety-related system is degraded by a single random failure.

System-Level Actuation – Actuation of a sufficient number of actuation devices to effect a protective function.

Component-Level Actuation – Actuation of a single actuation device (component).

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network.

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the lower right-hand side is the protection and safety monitoring system. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual

channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The ESF coincidence logic performs system-level logic calculations, such as initiation of the passive residual heat removal system. It receives inputs from the plant protection subsystem bistables and the main control room.

The ESF actuation subsystems provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the ESF coincidence logic, remote shutdown workstation and the main control room.

The plant control system performs nonsafety-related instrumentation and control functions using both discrete (on/off) and modulating (analog) type actuation devices.

The nonsafety-related real-time data network, which horizontally divides Figure 7.1-1, is a high speed, redundant communications network that links systems of importance to the operator. Safety-related systems are connected to the network through gateways and qualified isolation devices so that the safety-related functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the data display and processing system.

The upper portion of the figure depicts the control rooms and data display and processing system. 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 data display and processing (plant computer) system is implemented in 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 its input from the real-time data network and delivers its output over the network to other users.

WCAP-15775 (Reference 7) describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture.

Protection and Safety Monitoring System

The protection and safety monitoring system provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The protection and safety monitoring system controls safety-related components in the plant that are operated from the main control room or remote shutdown workstation. Secure development and operational environments for the protection and safety monitoring system are used during design as described in Reference 22.

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

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system is the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system is composed of digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service. The metal impact monitoring system is described in subsection 4.4.6.4.

Plant Control System

The plant control system provides the functions necessary for normal operation of the plant from cold shutdown through full power. The plant control system controls nonsafety-related components in the plant that are operated from the main control room or remote shutdown workstation.

The plant control system contains nonsafety-related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation. The plant control system is described in subsections 7.1.3 and 7.7.1.

Diverse Actuation System

The diverse actuation system is a nonsafety-related, 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 diverse actuation system is described in subsection 7.7.1.11.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system).

The boundaries of the operation and control centers system for the main control room and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and the plant real-time data network, which provides plant parameters, plant component status, and alarms.

Data Display and Processing System

The data display and processing system provides the equipment used for processing data that result in nonsafety-related 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 data display and processing system also contains the real-time data network, which is a redundant data highway that links the elements of the AP1000 instrumentation and control architecture.

Incore Instrumentation System

The primary function of the incore instrumentation system is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the protection and safety monitoring system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The incore instrument assemblies house both fixed incore flux detectors and core exit thermocouples. The incore instrumentation system is described in subsection 4.4.6.1.

7.1.2 Protection and Safety Monitoring System

Reference 19, Section 2.1 provides an overview description of the protection and safety monitoring system.

7.1.2.1 Plant Protection Subsystems

Reference 19, Section 2.2 describes the plant protection subsystems.

7.1.2.1.1 Reactor Trip Functions

Reference 19, Section 1.1 describes the reactor trip functions.

7.1.2.1.2 Reactor Trip Switchgear Interface

Reference 19, subsection 2.2.3.1.1 describes the reactor trip switchgear interface.

7.1.2.1.3 Manual Reactor Trip

Reference 19, subsection 2.2.3.1.3 describes the manual reactor trip.

7.1.2.2 Engineered Safety Features Coincidence Logic

Reference 19, subsection 2.2.3.2.1 describes the Engineered Safety Features Coincidence Logic.

7.1.2.3 Engineered Safety Features Actuation Subsystems

Reference 19, subsection 2.2.3.2.2 describes the Engineered Safety Features Actuation Subsystems.

7.1.2.4 Reactor Trip Switchgear

Reference 19, subsection 2.2.3.1.1 describes the reactor trip switchgear.

7.1.2.5 Qualified Data Processing Subsystems

Reference 19, Section 4.2 describes the Qualified Data Processing Subsystems (QDPS).

7.1.2.6 Main Control Room Multiplexers

The protection and safety monitoring system does not use multiplexers to provide a signal path between the protection system equipment and the main control room. Each division's safety display communicates with the protection system equipment via that division's communications network as shown in Figure 2-2 of Reference 19.

7.1.2.7 Sensors

The protection and safety monitoring system monitors key variables related to equipment mechanical limitations, and variables directly affecting the heat transfer capability of the reactor. Some limits, such as the overtemperature ΔT setpoint, are calculated in the plant protection subsystem from other parameters because direct measurement of the variable is not possible. This subsection provides a description of the sensors which monitor the variables for the protection and safety monitoring system. For convenience the discussions are grouped into the following three categories:

- Process sensors
- Nuclear instrumentation detectors
- Status inputs from field equipment

The inputs described are those required to generate the initiation signals for the protective functions. The use of each parameter is discussed in the sections that deal with each protective function. For example, reactor trip is discussed in Section 7.2 and ESF actuation is described in Section 7.3.

7.1.2.7.1 Process Sensors

The process sensors are devices which measure temperature, pressure, fluid flow, and fluid level. Process instrumentation excludes nuclear and radiation measurements.

Additional information on these process variables is included as part of the description of each process system provided in other chapters. The process variables measured by the protection and safety monitoring system are listed in Sections 7.2, 7.3, and 7.5.

7.1.2.7.2 Nuclear Instrumentation Detectors

Three types of neutron detectors are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The intermediate range channels are capable of measuring overpower excursions up to 200 percent of full power.

The lowest range (source range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This generally is greater than two counts per second. The next range (intermediate range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps the higher portion of the intermediate range. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. Detector types for these three ranges are:

- Source range – proportional counter or pulse fission chamber
- Intermediate range – pulse fission chamber
- Power range – uncompensated ionization chamber

7.1.2.7.3 Equipment Status Inputs

Some inputs to the protection system are not measurements of process or nuclear variables, but are discrete indications of the status of certain equipment. Examples include manual switch positions, contact status inputs, and indications provided by valve limit switches.

7.1.2.8 Communication Functions

Reference 19, Section 3 describes the communication functions.

7.1.2.9 Fault Tolerance, Maintenance, Test, and Bypass

Reference 19, Section 7 describes the fault tolerance features, and Section 6 describes the maintenance, test, and bypass features of the protection and safety monitoring system.

7.1.2.10 Isolation Devices

Isolation devices are used to maintain the electrical independence of divisions, and to prevent interaction between nonsafety-related systems and the safety-related system.

Isolation devices are incorporated into selected interconnections to maintain division independence. Isolation devices serve to prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit.

7.1.2.11 Test Subsystem

Reference 19, Section 6 describes the test subsystem.

7.1.2.12 Safety-Related Display Instrumentation

Safety-related display instrumentation provides the operator with information to determine the effect of automatic and manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in Chapter 15. This instrumentation also provides for operator display of the information necessary to meet Regulatory Guide 1.97. A description of the equipment used to provide this function is provided in subsection 7.1.2.5. A description of the data provided to the operator by this instrumentation is provided in Section 7.5.

7.1.2.13 Auxiliary Supporting Systems

The safety-related system equipment is supported by the supply of uninterruptible electrical power. This electrical power is supplied by the Class 1E dc and UPS system discussed in Chapter 8.

7.1.2.14 Verification and Validation

[*Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program are provided in WCAP-16096-NP-A (Reference 9).*]* WCAP-16096-NP-A defines a software development process consistent with appropriate industry standards.

7.1.2.14.1 Design Process

[*WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:*

- *Conceptual phase (may also be referred to as design requirements phase)*
- *Requirements phase (may also be referred to as system definition phase)*
- *Design phase (may also be referred to as hardware and software development phase)*
- *Implementation phase (may also be referred to as hardware and software development phase)*
- *Test phase (may also be referred to as system integration and test phase)*
- *Installation and checkout phase (may also be referred to as installation phase)*

WCAP-16096-NP-A (Reference 9), WCAP-15927 (Reference 20), and NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

Reference 22 describes the process for ensuring that the design life cycle process for the protection and safety monitoring system meets the computer security requirements of IEEE 603 and Regulatory Guide 1.152.

The planning (or design requirements) phase documents are listed below. Figure 7.1-2 shows the relationship of the same documents.

Document 1: WNA-PN-00043-WAPP, NuStart/DOE Design Finalization Program"

Document 2: WNA-PQ-00201-WAPP, NuStart/DOE Design Finalization Program Project Quality Plan"

Document 3: WNA-PN-00045-WAPP, NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan"

Document 4: WNA-PD-00042-WAPP, NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan"

Document 5: WCAP-16096-NP-A, "Software Program Manual for Common Q Systems"

Document 6: NABU-DP-00014-GEN, "Design Process for Common Q Safety Systems"

Document 7: WNA-PV-00009-GEN, "Verification & Validation Process for the Common Q Safety Systems"

Document 8: WNA-PT-00058-GEN, "Testing Process for Common Q Safety Systems"

Document 9: NABU-DP-00015-GEN, "Common Q Software Configuration Management Guidelines"

Document 10: 00000-ICE-3889, "Coding Standards & Guidelines for Common Q Systems"

Document 11: APP-PMS-GER-020, "Protection and Safety Monitoring System Concept Phase V&V Summary Report"

Document 12: APP-PMS-T5-001, "AP1000 Protection and Safety Monitoring System Test Plan"

Document 13: WCAP-15927, "Design Process for AP1000 Common Q Safety Systems"

Document 14: APP-GW-J0R-012, "AP1000™ Protection and Safety Monitoring System Computer Security Plan"

Document 15: APP-GW-GLR-143, "AP1000™ Component Interface Module Technical Report"

7.1.2.14.2 Commercial Dedication

[*WCAP-16097-P-A (Reference 8) provides 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 as described in subsection 13.5.1.

7.1.3 Plant Control System

The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The plant control system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The plant control system also provides control of the nonsafety-related decay heat removal systems during shutdown. The plant control system accomplishes these functions through use of the following:

- Rod control
- Pressurizer pressure and level control
- Steam generator water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The plant control system provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The plant control system acts to maximize margins to plant safety limits and maximize the plant transient performance. The plant control system also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance.

The plant control system includes the equipment from the process sensor input circuitry through to the modulating and nonmodulating control outputs as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Nonmodulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The plant control system cabinets contain the process sensor inputs and the modulating and nonmodulating outputs. The plant control system also includes equipment to monitor and control the control rods.

The functions of the plant control system are performed by system assemblies including:

- Distributed controllers
- Signal selector algorithms
- Operator controls and indication
- Real-time data network
- Rod control system

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

- Rod position indication
- Rod drive motor-generator sets

7.1.3.1 Distributed Controllers

Each distributed controller processes inputs, performs system-level and component-level control calculations, provides capability for an operator interface to the controlled components, transmits control signals to discrete, modulating, and networked interfaced control components, and provides plant status and plant parameter information to the real-time data network.

The distributed controllers receive process inputs and implement the system-level logic and control algorithms appropriate for the plant operating mode. The distributed controllers receive process inputs from, and transmit process control outputs to, the actuated components. The distributed controller also transmits and receives process signals via the real-time data network. The real-time data network also provides for two-way communication between the distributed controllers and between the distributed controllers and the main control room and remote shutdown workstation.

Control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers. The major control functions which are implemented in different distributed controllers include reactor power control, feedwater control, pressurizer control, and turbine control.

7.1.3.2 Signal Selector Algorithms

Signal selector algorithms provide the plant control system with the ability to obtain inputs from the protection and safety monitoring system. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if one of four redundant protection channels is degraded by random failure simultaneous with another of the four channels bypassed for test or maintenance.

Each signal selector algorithm receives data from each of the redundant divisions of the protection and safety monitoring system. The data is received from each division through an isolation device.

The signal selector algorithms provide validated process values to the plant control system. They also provide the validation status, the average of the valid process values, the number of valid process values, an alarm (if one process value has been rejected), and another alarm (if two process values have been rejected).

For the logic values received from the protection and safety monitoring system, such as permissives, two-out-of-four (2/4) voting is used to provide a valid logic value to the plant control system.

The signal selection algorithm is executed in the PLS, and the results are not available to PMS or DAS. Therefore, PMS and DAS performance, controls, and displays are independent of the signal selector algorithm.

7.1.3.3 Operator Controls and Indication

The plant control operator interface is a set of soft control devices that replace conventional switch/light or potentiometer/meter assemblies used for operator interface with control systems. These soft control devices provide consistent operator interfaces for the plant control system. The soft controls are located on each operator workstation and the remote shutdown workstation. Each soft control device can control safety-related and nonsafety-related equipment.

The implementation of the soft controls is consistent with the following functional requirements:

- The soft control function does not affect the electrical or functional isolation of the safety-related and nonsafety-related equipment. This isolation is maintained upon a single failure of any equipment performing or supporting the soft control function.

- Failure of the operator displays does not prevent an operator from being able to safely shutdown the plant.

When the operator desires to operate a component, the graphical operator display which is indicating the component status is presented on the operator control console. This results in a message being sent to the soft control device. The soft control device then displays the appropriate control template. The operator then selects the desired control action on the template. After the operator verifies that the desired control action is properly selected, the operator then actuates the control action, causing the selected control action to be transmitted to the control device.

7.1.3.4 Real-Time Data Network

The real-time data network is a redundant data highway that supports both periodic and aperiodic data transfers of nonsafety-related signals and data. Periodic transfers consist of process data that is broadcast over the network at fixed intervals and is available to all destinations. Aperiodic data transfer is generally used for messages or file transfers.

The real-time data network provides communications among the distributed controllers, the plant protection and safety monitoring system gateways, the incore instrumentation, and the special monitoring system.

7.1.3.5 Rod Control System

The primary means of regulating the reactor power and power distribution is to position clusters of control rods in the reactor core using the rod control system.

The control rods are moved into and out of the reactor core by means of electromagnetic jacking mechanisms, called control rod drive mechanisms, located on the reactor vessel head. Each control rod drive mechanism consists of two gripper mechanisms, one stationary and one movable, that hold a notched driveline attached to the upper end of the control rod. The grippers and the lift armature are controlled by coils mounted external to the mechanism, concentric with the rod driveline. By controlling the sequence of energizing these coils, the mechanism can be made to step into, or out of, the reactor in increments. The rod control equipment provides this sequence control.

The control rods are arranged into symmetrical groups. The groups of control rods are divided into two categories: shutdown rods that are normally held fully withdrawn from the reactor, and control rods that are positioned to some intermediate insertion. In addition, there is a subcategory of control rods (low worth gray rods). If a rapid shutdown is necessary, the control, shutdown, and gray rods are dropped into the reactor by de-energizing their drive mechanisms.

Interlocks are provided to prevent the motion of the control rods outside of planned sequences.

7.1.3.6 Rod Position Indication

The position of each control rod is continuously monitored by the rod position indication system. This information is detected by the rod position detector assemblies. The signals from the detectors are processed by the data cabinets and transmitted to the distributed controllers. The distributed controllers further process the rod position information and transmit this information to the real-time data network.

7.1.3.7 Rod Drive Motor-Generator Sets

The rod drive motor-generator sets provide the power to the control rod drive mechanisms through the reactor trip switchgear. The rod drive motor-generator sets are included in the plant control system. The safety-related reactor trip switchgear is included in the plant protection and safety monitoring system.

There are two motor-generator sets with flywheels and one control cabinet. Each motor-generator is a three-phase induction motor, direct-coupled to a flywheel, and a synchronous alternator.

During normal operating conditions, both motor generator sets are operating in parallel and equally sharing the total load demand. Each motor-generator set is capable of supplying the entire load requirements when the other set is out of service.

7.1.4 Identification of Safety Criteria

7.1.4.1 Conformance of the Safety System Instrumentation to Applicable Criteria

The safety-related system instrumentation described in subsection 7.1.1 is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. Applicable General Design Criteria are listed in Section 3.1, NRC Regulatory Guides in subsection 1.9.1, and Branch Technical Positions in subsection 1.9.2. Industry Standards are cited as references.

The instrumentation and control portion of the safety-related system meets the requirements of IEEE 603-1991 as discussed in WCAP-15776 (Reference 12). The topics are listed in the same order as they appear in Sections 4 through 8 of IEEE 603-1991. IEEE 603 provides the design bases of the instrumentation and control portion of the safety system. Other criteria related to the IEEE 603-1991 requirements are also identified.

7.1.4.2 Conformance With Industry Standards

The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the following standards. The portions of the standards which are considered to be applicable are the portions of the standards which apply to instrumentation and control systems performing protection and control functions in an industrial environment:

- IEEE 323-1974; "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations"
- IEEE 344-1987; "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- IEEE 379-2000; "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems"
- IEEE 383-1974; "IEEE Standard for Type Test of Class IE Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations"
- IEEE 384-1981; "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"
- IEEE 420-1982; "IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations"
- IEEE 603-1991; "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
- IEEE 627-1980; "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations"
- IEEE 1050-1996; "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations"
- IEEE 1074-1995; "IEEE Standard for Developing Software Life Cycle Processes"
- EPRI TR-102323, Revision 1, "Guidelines for Electromagnetic Interference Testing in Power Plants"

7.1.5 AP1000 Protective Functions

Protective functions are those necessary to achieve the system responses assumed in the safety analyses, and those needed to shut down the plant safely. The protective functions are grouped into two classes, reactor trip and ESF actuation. The software associated with these functions is considered a basic component as defined in 10 CFR 21 (Reference 6).

Reactor trip is discussed in Section 7.2. ESF actuation is discussed in Section 7.3.

7.1.6 Combined License Information

7.1.6.1 The Combined License information requested in this subsection is addressed in WCAP-16361-P (Reference 17), and the applicable changes are incorporated into the DCD. The Westinghouse Setpoint Control Program (SCP) will be incorporated into the AP1000 DCD Technical Specifications in accordance with COL/DC-ISG-8. This will facilitate combined license (COL) applicants' adoption of the AP1000 DCD Technical Specifications. Prior to initial fuel load, a reconciliation of the setpoints against the final design for each plant will be performed.

The following words represent the original Combined License Information Item commitment, which has been addressed as discussed above:

> Combined License applicants referencing the AP1000 certified design will provide a calculation of setpoints for protective functions consistent with the methodology presented in Reference 5. Reference 5 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans.

7.1.6.2 The Combined License information requested in this subsection has been completely addressed in APP-GW-GLR-017 (Reference 18), and the applicable changes are incorporated into the DCD. No additional work is required by the Combined License applicant.

The following words represent the original Combined License Information Item commitment, which has been addressed as discussed above:

> Combined License applicants referencing the AP1000 certified design will provide resolution for generic open items and plant-specific action items resulting from NRC review of the I&C platform. This will include definition of a methodology for overall response time testing.

7.1.7 References

1. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

2. [*WCAP-17201-P, Revision 0, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15," February 2010.*]*

3. Not used.

4. Not used.

5. [*WCAP-14605 (Proprietary) and WCAP-14606 (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996.*]*

6. 10 CFR 21, "Reporting of Defects and Noncompliance."

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

7. WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report."

8. [*WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Revision 0, "Common Qualified Platform," May 2003.*]*

9. [*WCAP-16096-NP-A, Revision 01A, "Software Program Manual for Common Q Systems," January 2004.*]*

10. Not used.

11. Not used.

12. WCAP-15776, "Safety Criteria for the AP1000 Instrument and Control Systems," April 2002.

13. Not used.

14. Not used.

15. IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

16. Not used.

17. WCAP-16361-P (Proprietary) and WCAP-16361-NP (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006.

18. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC Items," Westinghouse Electric Company LLC.

19. WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 5.

20. [*WCAP-15927, Revision 2 (Non-proprietary), "Design Process for AP1000 Common Q Safety Systems," November 2008.*]*

21. Westinghouse Electric Company Quality Management System (QMS), Revision 5 (Non-Proprietary), October 1, 2002.

22. APP-GW-J0R-012, "AP1000 Protection and Safety Monitoring System Computer Security Plan," Westinghouse Electric Company LLC.

23. WCAP-17184-P, "AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report."

24. WCAP-17179-P (Proprietary) and WCAP-17179-NP (Non-Proprietary), "AP1000 Component Interface Module Technical Report," Revision 1.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

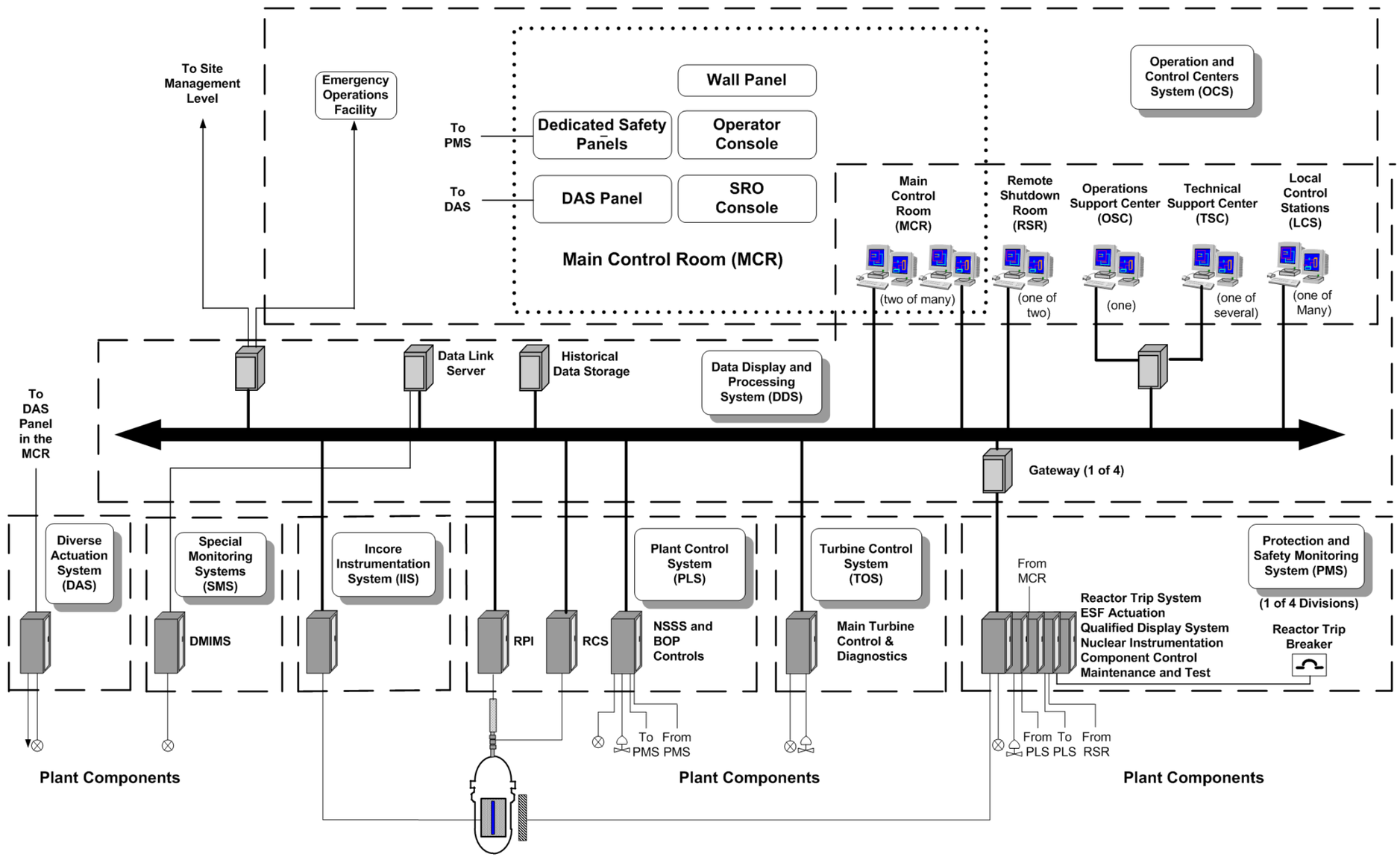

Figure 7.1-1

Instrumentation and Control Architecture

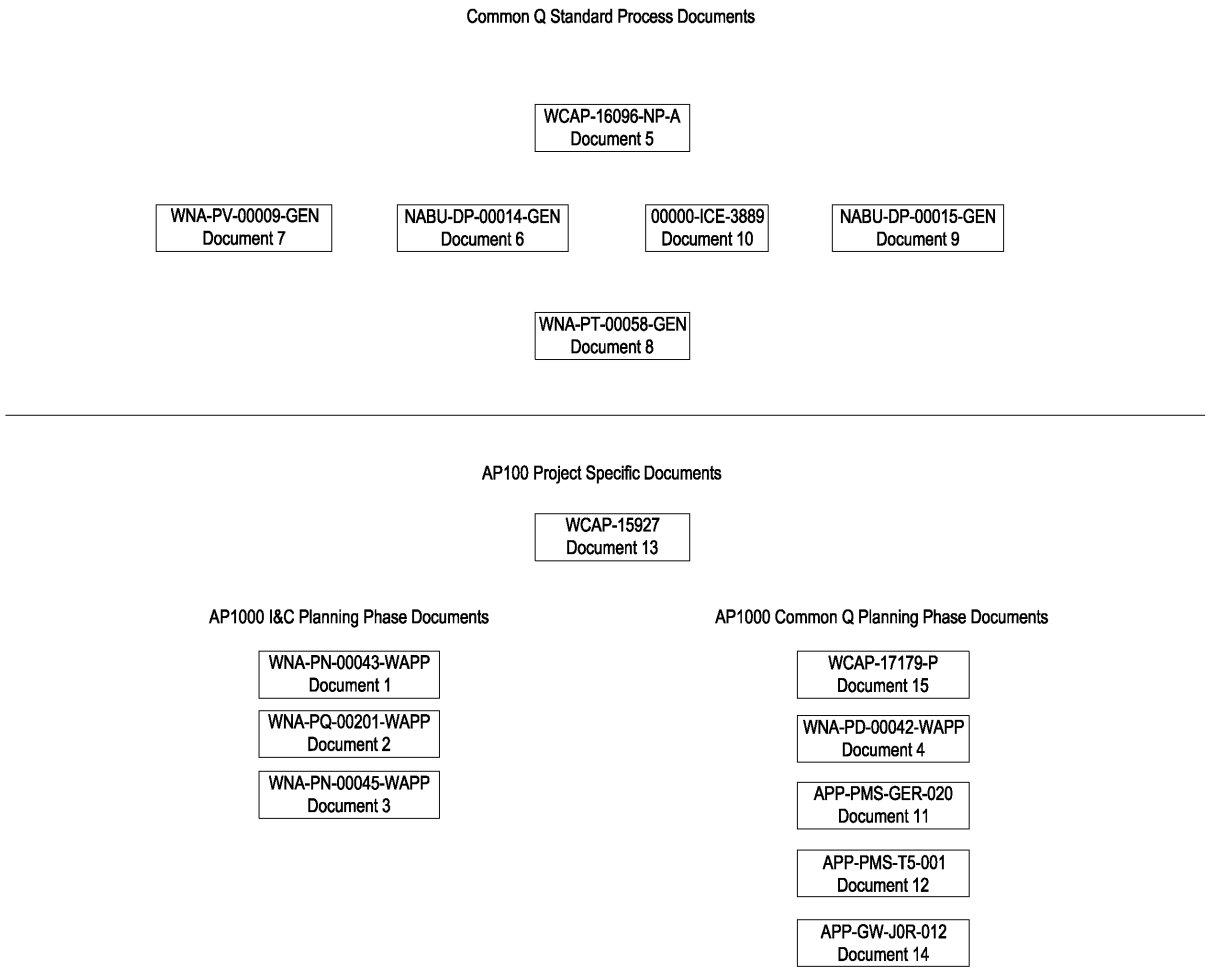

Figure 7.1-2

Common Q Standard Process and AP1000 Project-Specific Documents

Figures 7.1-3 through 7.1-11 not used.