18.12 Inventory

18.12.1 Inventory of Displays, Alarms, and Controls

[An inventory of instruments, alarms, and controls for the AP1000 systems is provided in the respective system piping and instrumentation diagrams and/or the respective system specification documents.

The AP1000 system design engineers determine the specific sensors, instrumentation, controls, and alarms that are needed to operate the various plant systems. The instruments, alarms, and controls for each system are documented in the piping and instrumentation diagram and/or the respective system specification documents. An instrument, alarm, and control is specified by the system design engineer if it is needed to control, verify, or monitor the operation of the system and its components. System functions and their respective functional requirements are considered by the system designer when determining the need for a specific instrument, alarm, or control.

The role of the Human System Interface design team in the determination of the total inventory list is one of verification. As described in Section 18.5, human system interface design team has functionally decomposed the plant. The top four levels of this model for the AP1000 are shown in Figure 18.5-1. Each Level 4 function has a function-based task analysis (FBTA) performed as described in the Task Analysis Implementation Plan. Considering the plant operating modes and emergency operations, the function-based task analysis:

- *Identifies the functions goals*
- *Identifies the processes used to achieve each goal*
- *Documents the performance of a cognitive task analysis of each process*

The cognitive task analysis of each process answers the monitoring/feedback, planning, and controlling questions. The answers to these questions identify the data for each functional process (instrumentation, indications, alarms, and controls) needed by the operator to make decisions. The results of the cognitive task analysis phase of each function-based task analysis are used to verify the inventory list of instruments, controls, and alarms developed by the AP1000 system designers and documented in the respective design documents.]*

18.12.2 Minimum Inventory of Main Control Room Fixed Displays, Alarms, and Controls

Background

[The human system interface design includes the appropriate plant displays, alarms, and controls needed to support a broad range of expected power generation, shutdown, and accident mitigation operations. Soft control displays and plant information displays are generated by a computer and can be changed 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 are used to direct operator attention. Soft controls are provided through devices such as a keyboard, touch screen, mouse, or other equivalent input devices. The majority of the operations for

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

both the AP1000 main control room and the remote shutdown workstation are expected to employ soft control displays and plant information displays.

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

Fixed-position alarms and displays are available at a fixed location and are continuously available, though not necessarily displayed, to the operator. Fixed-position displays can be accessed by the operator to monitor the plant status, based on indications from critical plant variables or parameters. Fixed-position alarms are designed to direct operator attention to the need to perform safety-related functions for which there is no automatic actuation function. 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-related system/component actuation. Fixed-position controls are available to the operator to perform tasks in the operation of safety-related 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 protection and safety monitoring system.]*

Design Basis and Minimum Inventory

[*A systematic process was implemented to identify the minimum inventory of AP1000 fixed-position controls, displays, and alarms, using established selection criteria directly related to the specific AP1000 accident mitigation operator actions and the critical safety functions identified in the emergency response guidelines.*

The AP1000 design basis for accident mitigation protects the following three fission product barriers:

- *Fuel matrix/fuel rod cladding*
- *Reactor coolant system pressure boundary*
- *Containment*

Therefore, the minimum inventory of fixed instrumentation includes those displays, controls, and alarms used to monitor the status of these fission product barriers and manually actuate the safety-related systems that achieve the critical safety functions protecting these barriers.

Six critical safety functions are identified in the Emergency Response Guidelines (ERGs). These critical safety functions are physical processes, conditions, or actions designed to maintain the plant conditions within the acceptable design basis.

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

The AP1000 critical safety functions are:

- *Reactivity control*
- *Reactor core cooling*
- *Heat sink maintenance*
- *Reactor coolant system integrity*
- *Containment environment*
- *Reactor coolant system inventory control*

The minimum inventory of AP1000 fixed instrumentation includes those displays, controls, and alarms that are used to monitor the status of these critical safety functions and to manually actuate the safety-related systems that achieve these critical safety functions.]*

Minimum Inventory Selection Criteria

[*The following selection criteria are used to develop the minimum inventory of instrumentation controls, displays, and alarms:*

- *Regulatory Guide 1.97 Types A, B, and C, Category 1 instrumentation*

- *Dedicated controls for manual safety-related system actuation (reactor trip, turbine trip, engineered safety feature actuation)*

- *Controls, displays, and alarms required to perform critical manual actions as identified from the PRA analysis*

- *Alarms provided for operator use in performing safety functions to respond to design basis events for which there is no automatically-actuated safety function*

- *Controls, displays, and alarms necessary to maintain the critical safety functions and safe shutdown conditions*

For the main control room, the minimum inventory of displays is provided by the safety-related displays of the qualified data processing system. For the remote shutdown workstation, the minimum inventory of displays is provided by the nonsafety-related displays of the plant information system.

An alarm is a device that provides warning by means of a signal or sound. The parameters and associated alarms, listed in DCD Table 18.12.2-1, identify challenges to the critical safety functions. This minimum inventory of alarms is embedded in displays as visual signals. For example, the visual signal may involve a change of color, brightness, flashing, or a combination of these. For clarity, these alarms are called visual alerts to distinguish them from other alarms which may include sound. For the main control, the visual alerts are embedded in the safety-related displays. For the remote shutdown workstation, the visual alerts are embedded in the nonsafety-related displays.

The minimum inventory resulting from the implementation of these selection criteria is provided in Table 18.12.2-1.]*

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

Regulatory Guide 1.97

[*The guidelines in Regulatory Guide 1.97 provide an effective basis for selection criteria to identify the minimum inventory of fixed displays, controls, and alarms, since these guidelines are consistent with monitoring the status of the fission product barriers and the associated critical safety functions in the AP1000 Emergency Response Guidelines.*

Regulatory Guide 1.97 provides a method to identify the post-accident monitoring (PAMS) instrumentation to monitor plant variables and systems during and following an accident. Selected post-accident monitoring instrumentation is required to remain functional over the range of the accident conditions and must be able to survive the accident environment for the length of time its function is required. The instrumentation helps the operator to identify the accident, to implement proper corrective actions, and to observe plant response to these actions in order to determine the need for additional actions. Five types of accident monitoring instrumentation and associated performance criteria are provided in the regulatory guide.

Within each type of post-accident monitoring instrumentation, there are three categories (Categories 1, 2, and 3) that are related to the qualification (seismic and environmental conditions) and reliability (safety-related power supply and single failures) of the specific instrumentation.

The Category 1 variables are considered as primary variables and meet appropriate qualification, design, and interface requirements discussed in subsection 7.5.2.2.1 and listed in Tables 7.5-2 and 7.5-3. These variables provide the appropriate capabilities and reliability that are required for the parameters. Only the Category 1 (primary) variables are included in the minimum inventory selection criteria. Category 2 and Category 3 instrumentation are not included in the selection criteria for the minimum inventory.

Type A, Type B, and Type C are considered in developing the selection criteria for identification of the minimum inventory, since these three types are related to monitoring the three fission product barriers. The details of instrumentation designed to meet the guidelines in Regulatory Guide 1.97 are presented in Section 7.5.

Type A variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.1, Type A variables provide primary information to permit the main control room operating staff to:

- *Perform the diagnosis in the AP1000 emergency operating procedures*
- *Take specified preplanned, manually-controlled actions, for which automatic controls are not provided, and that are required for safety-related systems to accomplish their safety-related function to recover from a design basis accident*

There are no specific, preplanned, manually-controlled actions for safety-related systems to recover from design basis events in the AP1000 design. Therefore, as reflected in Table 7.5-4, there are no Type A variables.

Type B variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.2, Type B variables provide information to the main control room operating staff to assess the process of accomplishing critical safety functions in the emergency response guidelines. The Type B variables are identified in Table 7.5-5.

Type C variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.3, Type C variables provide the control room operating staff with information to monitor the potential for breach or the actual gross breach of:

- *Incore fuel cladding*
- *Reactor coolant system boundary*
- *Containment boundary*

The Type C variables are identified in Table 7.5-6.]*

Dedicated Controls

[*The selection criteria of AP1000 minimum inventory include dedicated, fixed-position controls that provide the capability to manually initiate system-level actuation signals for the safety-related systems and components that are used to achieve the critical safety functions. These dedicated controls provide the capability to initiate manual reactor and turbine trip, safeguards actuation, individual actuation of various safety-related, passive components and containment isolation.*]*

Probabilistic Risk Assessment Critical Human Actions

[*As described in Section 18.7 and Reference 1, the human factors engineering design process includes integration of PRA and the associated human reliability analysis insights into the AP1000 design. The human reliability analysis integration includes the identification of critical human actions through the consideration of specific deterministic and PRA criteria. These selection criteria for minimum inventory identify dedicated, fixed-position displays, alarms, and controls required to support critical human actions identified from the integration of human reliability analysis into the human factors engineering design process.*]*

Dedicated Alarms

[*As specified by Criterion 1, the minimum inventory of instrumentation requires dedicated instrumentation displays of the Regulatory Guide 1.97 Type A variables so that the operator can identify the need to take preplanned manually-controlled actions to mitigate the consequences of a design basis event, where a safety-related system needed to support a critical safety function is not automatically actuated.*

The fourth criterion for minimum inventory is included to identify alarms needed to automatically alert the operator to the need to take these preplanned manually controlled actions.

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

One of the design goals of the AP1000 is to minimize the need for operator actions to mitigate the consequences of design basis events. As part of the implementation of this design goal, the safety-related systems required to mitigate the consequences of design basis events are automatically actuated. There are no specific preplanned, manually-controlled actions required for the safety-related systems to mitigate design basis events in the AP1000 design.

Another design goal for the AP1000 is to enhance defense in depth, which includes the use of automatically actuated safety-related systems as a backup to other automatically actuated safety-related systems. For example, if beyond-design-basis failures occurred such that the safety-related passive residual heat removal heat exchanger failed to actuate, other safety-related systems would automatically actuate to provide core cooling, without the need for operator action for either group of safety-related components. This design approach enhances overall plant safety.

The AP1000 minimum inventory includes a criterion for evaluating the need for dedicated alarms for preplanned operator actions. However, as a result of these two design approaches, the level of protection available to mitigate the consequences of an accident and to achieve the critical safety functions is provided without the need for preplanned operator actions for either the primary safety-related systems or the backup safety-related systems. Since there are no specific preplanned, manually-controlled actions for safety-related systems required to respond to design basis events in the AP1000 design, there are also no dedicated, fixed-position alarms identified in the minimum inventory list.]*

Critical Safety Functions and Safe Shutdown

[*The design basis for the AP1000 requires protecting the three fission product barriers in the plant (the fuel matrix and cladding, the reactor coolant system pressure boundary, and containment) following design basis events. The AP600 system/event matrix (Reference 2) identifies four safety-related, post-accident mitigation functions that are required as part of the design basis for the AP600 to protect the integrity of these fission product barriers. This document is directly applicable to AP1000. The design basis of the AP1000 requires safety-related systems that can perform these four safety-related functions for design basis events.*

The AP1000 Emergency Response Guidelines were developed by using the system/event matrix document as the plant response design basis and following the standardized process for Emergency Response Guideline development for Westinghouse PWRs. The design approach described in the system/event matrix document organizes the identified safety-related and nonsafety-related Systems, structures and components into the appropriate groups that perform the four safety-related design basis functions. In developing the AP1000 Emergency Response Guidelines, the same groups of safety-related and nonsafety-related systems in the system/event matrix are used to perform their basic design functions, but they are organized somewhat differently from the system/event matrix to support development of symptom-based functional guidelines that can be more effectively used by the operators. These four design basis safety functions identified in Reference 2 are expanded into the six critical safety functions in writing the symptom-based AP1000 Emergency Response Guidelines.

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

The six Emergency Response Guidelines critical safety functions (and the four design basis safety functions that the critical safety functions must satisfy) are physical processes, conditions, or actions taken using the safety-related and nonsafety-related systems to maintain the plant conditions within the acceptable design basis. These systems provide the physical equipment used to initiate and control the processes that achieve the critical safety functions.

By accomplishing the emergency response guideline critical safety functions following a design basis event, the plant is able to mitigate the consequences of the event and to establish and maintain safe shutdown conditions. The minimum inventory list identifies sufficient controls, displays, and alarms to monitor and control operation of the safety-related systems to achieve the six critical safety functions identified in the Emergency Response Guidelines and to establish and maintain safe shutdown conditions following an accident.

Tables 7.5-4, 7.5-5, and 7.5-6 identify the instrumentation and the associated Emergency Response Guidelines critical safety functions that each instrument supports for each of the Type A, B, and C post-accident instrumentation, respectively.]*

Minimum Inventory Selection Criteria Implementation Process

[*Section 7.5 provides a discussion of the development of the requirements of Regulatory Guide 1.97 and the implementation process for the AP1000 (Criteria 1, 2, and 4).*

Section 18.7 and Reference 1 provide a discussion of the implementation process for identification of critical PRA operator actions (Criteria 3). Chapter 30 of the AP1000 PRA describes the process for the human reliability analysis.]*

18.12.3 Remote Shutdown Workstation Displays, Alarms, and Controls

[*Subsection 7.4.3 discusses safe shutdown using the remote shutdown workstation following an evacuation of the main control room.*

The main control room provides the capability to perform accident mitigation and safe shutdown tasks for design basis events. The only types of events that would require evacuation of the main control room and control from the remote shutdown workstation are localized emergencies where the main control room environment is unsuitable for the operators or where the main control room workstations and equipment become damaged.

Evacuation of the main control room is not expected to occur coincident with any other design basis events. Subsection 9.5.1 of the Standard Review Plan (NUREG-0800) specifically excludes consideration of other design basis events coincident with a fire.

The design capability for the remote shutdown workstation is to provide the capability to establish and maintain safe shutdown conditions following a main control room evacuation, as described in subsection 7.4.3.1.1. The controls, displays, and alarms listed in Table 18.12.2-1 are retrievable from the remote shutdown workstation.]*

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

18.12.4 Combined License Information

This section has no requirement for additional information to be provided in support of the Combined License application.

18.12.5 References

[*1. WCAP-14651, "Integration of Human Reliability Analysis With Human Factors Engineering Design Implementation Plan," Revision 2, May 1997.*]*

2. WCAP-13793, "The AP600 System/Event Matrix," June 1994.

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

Table 18.12.2-1 (Sheet 1 of 2)

MINIMUM INVENTORY OF FIXED POSITION CONTROLS, DISPLAYS, AND ALERTS

Description	Control	Display	Alert[2]
Neutron flux		x	x
Neutron flux doubling[3]			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[3]		x	x
Remotely operated containment isolation valve status[3]		x	
Containment area high range radiation level		x	x
Containment pressure (extended range)		x	
CMT level[1]		x	

Table 18.12.2-1 (Sheet 2 of 2)

MINIMUM INVENTORY OF FIXED POSITION CONTROLS, DISPLAYS, AND ALERTS

Description	Control	Display	Alert(2)
Manual reactor trip (Also initiates turbine trip Figure 7.2-1, sheet 19.)	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-related)	x		

Notes:

1. Although this parameter does not satisfy any of the selection criteria of subsection 18.12.2, its importance to manual actuation of ADS justifies its placement 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-related displays as visual signals. For the remote shutdown workstation, the visual alerts are embedded in the nonsafety-related displays as visual signals.
3. These instruments are not required after 24 hours. (Subsection 7.5.4 includes more information on the class 1E valve position indication signals, specified as part of the post-accident monitoring instrumentation.)
4. This manual actuation capability is not needed at the remote shutdown workstation.