Westinghouse Electric Corporation
Energy Systems
Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-96-4747
DCP/NRC0532
Docket No.: STN-52-003

June 14, 1996

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

ATTENTION: T. R. QUAY

SUBJECT: REVISED DRAFTS OF CHAPTER 18 TABLE OF CONTENTS, 18.12 INVENTORY AND 18.2.4 HUMAN FACTORS ENGINEERING ISSUES TRACKING

Dear Mr. Quay:

Enclosed are revised drafts of the SSAR Chapter 18 Table of Contents, Section 18.12 Inventory and Subsection 18.2.4 Human Factors Engineering Issues Tracking. Section 18.12 resolves DSER open item 18.12.3-1. Subsection 18.2.4 provides a revised resolution to DSER open items 18.2.3.4-1, 18.2.3.4-2, 18.2.3.4-3, 18.2.3.4-4 and 18.3.3.2-3. The items will be closed when the draft sections are incorporated into the SSAR.

Please contact Susan V. Fanto on (412) 374-4028 if you have any questions concerning this transmittal.

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

/nja

Attachment

cc: J. Bongarra, NRC
J. Higgins, BNL
W. Huffman, NRC
H. Li, NRC
N. Liparulo, Westinghouse (w/o Enclosure)
J. O'Hara, BNL

2801A

100074



E004
1/1

Table of Contents (Draft)

### 18.2.4 Human Factors Engineering Issues Tracking

Tracking of human factors engineering issues is accomplished within the framework of the overall plant design process. In this manner, human factors engineering issues are addressed in the same way as those for other disciplines. The AP600 design issues tracking system consists of (1) a design configuration change control process and (2) a design issues tracking system database.

The design configuration change control process is used to control and implement a change to the design. It is used when the design to be changed has been previously released in a document for project use and placed under configuration control. A design change proposal is the vehicle used to initiate and document review of proposed design changes. Design change proposals include identification of impacts of the proposed design change from affected functional groups. In some instances, human factors engineering issues are addressed by the initiation of design change proposals whereas in other instances, they are addressed as a consequence of human factor engineering review of design change proposals originating from other disciplines. Design change proposals are maintained in a database that is used to track the status of each design change proposal from initiation through implementation and closure.

The design issues tracking system database is used to track AP600 design issues to resolution, including human factors engineering issues. This database receives input from the following three sources:

- Operating experience review
- Design reviews
- Design issues associated with the design of the man-machine interface / human system interface and the operations and control centers system

For each design issue entered into the database, the actions taken to eliminate or reduce the issue and the final resolution of the issue are documented.

The human factors issues in the operating experience review report (Reference 1, WCAP-14645) that are identified as requiring further consideration by the AP600 design are entered into the design issues tracking system database.

The design review process also provides input to the design issues tacking system database. Original designs, as well as major design changes, are subject to the design review process. For each design review, a design review data package is prepared. It includes checklists, including one specifically addressing human factor engineering questions, which are used by design review committee members to aid their review. For each design issue identified through the use of checklists or otherwise, an action item is initiated. Action items are entered into the design issues tracking system database. Human factors action items from design reviews are included in the database. For preliminary and intermediate design reviews, some action items may be deferred to a more appropriate, subsequent design review. The responsibility of entering design review action items into the design issues tracking system database is assigned to the responsible design manager (i.e., the manager responsible for the system reviewed) and program control and administration.

Human factors engineering design issues directly associated with the AP600 human system interfaces and the operations and control centers system (such as the main control room,

remote shutdown facility, and technical support center) are entered into the design issues tracking system database. These are design issues that are identified by the human system interface and operations and control centers system designers as issues that need to be addressed by the human system interface design.

The AP600 project manager, as shown on figure 18.4-2, is responsible for the maintenance and documentation of the design issues tracking system (the design change proposal process and the design issues tracking system database). For each issue entered into the design issues tracking system database, a "responsible engineer" field is used to assign an engineer the responsibility for resolution of the issue. This engineer is normally the responsible systems engineer.

### 18.2.5 Combined License Information

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

### 18.2.6 References

1. WCAP 14645, "Human Factors Engineering Operating Experience Review Report For The AP600 Nuclear Power Plant".

SSAR Section

## 18.12 Displays, Alarms, and Controls

### 18.12.1 Inventory of Displays, Alarms, and Controls

An inventory of instruments, alarms, and controls for the AP600 systems is provided in the respective system piping and instrumentation diagrams listed in subsection 1.7.2. Table 1.7-2 provides a list of piping and instrumentation diagrams and the corresponding SSAR figure number.

The AP600 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. 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 any of 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 Factors Engineering (HFE) design team in the determination of the total inventory list is one of verification. As described in Section 18.5, the HFE design team has functionally decomposed the plant. The top four levels of this model for a Westinghouse PWR, including the AP600, are shown in Figure 18.5-9. Each level four function has a Function-Based Task Analysis (FBTA) performed as described in the Task Analysis Implementation Plan. Considering all plant operating modes and emergency operations, the FBTA:

- 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 identifies 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 FBTA are used to verify the inventory list of instruments, controls, and alarms developed by the AP600 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 man-machine interface system 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, to allow control of different devices, or to display different information. These displays appear on display devices such as CRTs, 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 both the AP600 main control room and the remote shutdown workstation are expected

to employ soft controls, soft control displays, and plant information displays.

The AP600 man-machine interface system design also includes a minimum inventory of dedicated or fixed-position displays and controls. The minimum inventory of AP600 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 controls, alarms, and displays are available at a fixed location and are continuously available, 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. Fixed-position controls provide a means for manual reactor and turbine trip, and safety-related system/component actuation. They are available to the operator to perform tasks in the operation of safety-related systems and components that are 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 AP600 fixed-position displays, alarms, and controls, using established selection criteria that are directly related to the specific AP600 design basis for accident mitigation and the critical safety functions identified in the emergency response guidelines (and incorporated in the AP600 PRA evaluation).

The AP600 design basis for accident mitigation is to protect 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 that are used to monitor the status of these fission product barriers and to manually actuate the safety-related systems that achieve the critical safety functions to protect these barriers.

Six critical safety functions are identified in the Emergency Response Guidelines (ERGs). The recovery actions identified in the standardized ERGs for Westinghouse PWRs are based on satisfying the critical safety functions. These critical safety functions are physical processes, conditions, or actions taken using the safety-related and nonsafety-related systems and components to maintain the plant conditions within the acceptable design basis.

The AP600 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 AP600 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 displays, alarms, and displays:

1. Regulatory Guide 1.97 Type A / B / C, Category 1 instrumentation

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

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

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

The minimum inventory resulting from the implementation of these selection criteria is provided in Table 18.12.2-1, Minimum Inventory.

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 AP600 ERGs.

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. The 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 PAMS 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 design to meet the guidelines in Regulatory Guide 1.97 are presented in subsection 7.5. The basis for the use of each type of variable selected is described below.

Type A variables are defined in subsection 7.5.2-1.1. 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 AP600 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
- Attain and maintain a safe shutdown condition

There are no specific preplanned, manually-controlled actions for safety-related systems to recover from design basis events in the AP600 design. Therefore, as reflected in Table 7.5-4, there are no Type A variables.

Type B variables are defined in subsection 7.5.2-1.2. 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 7.5.2-1.3. 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:

- In-core fuel cladding
- Reactor coolant system boundary
- Containment boundary

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

Dedicated Controls

In addition to providing instrumentation displays to monitor the status of the fission product barriers (Type C, Category 1 variables) and the critical safety functions (Type B, Category 1 variables), the selection criteria of AP600 minimum inventory include dedicated, fixed position controls that provide the capability to manually initiate system-level actuation signals for the critical safety-related systems and components that are used to achieve these critical safety functions. For example, these dedicated controls provide the capability to initiate manual reactor and turbine trip, safeguards actuation, individual actuation of various safety-related, passive components and other important manual actuation signals such as containment isolation.

Probabilistic Risk Assessment Critical Human Actions

As described in section 18.7 and WCAP-14651, the HFE design process includes integration of PRA and the associated human reliability analysis in-sights into the AP600 design. The human reliability analysis integration includes the identification of critical human actions through the consideration of specific deterministic and PRA criteria. The minimum inventory also includes a selection criteria that identifies dedicated, fixed position displays, alarms, and controls required to support critical human actions identified from the integration of human reliability analysis into the HFE design process.

Dedicated Alarms

The selection criteria for AP600 minimum inventory also considered dedicated alarms for operator use in performing safety functions to respond to design basis events for which there is no automatically actuated safety function. Since there are no specific preplanned, manually-controlled actions for safety-related systems to recover from design basis events in the AP600 design, there are also no dedicated, fixed position alarms.

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 AP600 (Criteria 1, 2, and 4).

Section 18.7 and WCAP-14651 provide a discussion of the implementation process for identification of critical PRA operator actions (Criteria 3). Chapter 30 of the AP600 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 evacuation to the remote shutdown workstation are localized emergencies where the environment is unsuitable for the operators or where the actual 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 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 design basis for the remote shutdown workstation does not require the installation of dedicated, fixed position displays, alarms, and controls and the AP600 minimum inventory requirements are not applicable for the remote shutdown workstation.

## TABLE 18.12.2-1, MINIMUM INVENTORY

| Fixed Position Instrumentation | Control | Display | Alarm | SSAR Source |
|---|---|---|---|---|
| Neutron flux | | B1 | | Table 7.5-5 |
| RCS pressure | | B1, B2, C1 | | Table 7.5-5, 6 |
| WR $T_{hot}$ | | B1, B2 | | Table 7.5-5 |
| WR $T_{cold}$ | | B1, B2 | | Table 7.5-5 |
| Containment water level | | B1, C1 | | Table 7.5-5, 6 |
| Containment pressure | | B1, C2 | | Table 7.5-5, 6 |
| Pressurizer water level | | B1 | | Table 7.5-5 |
| Pressurizer reference leg temperature | | B1 | | Table 7.5-5 |
| Pressurizer pressure | | B1 | | Table 7.5-5 |
| Core exit temperature | | B1, C1 | | Table 7.5-5, 6 |
| RCS subcooling | | B1 | | Table 7.5-5 |
| IRWST water level | | B1 | | Table 7.5-5 |
| PRHR flow | | B1 | | Table 7.5-5 |
| PRHR outlet temperature | | B1 | | Table 7.5-5 |
| PCS storage tank water level | | B1 | | Table 7.5-5 |
| PCS cooling flow | | B1 | | Table 7.5-5 |
| IRWST to RNS suction valve status | | B1 | | Table 7.5-5 |
| Containment isolation valve position | | B1 | | Table 7.5-5 |
| Containment area high range radiation level | | C1 | | Table 7.5-6 |
| Containment pressure (extended range) | | C1 | | Table 7.5-6 |
| Containment hydrogen concentration | | C1 | | Table 7.5-6 |

| Fixed Position Instrumentation | Control | Display | Alarm | SSAR Source |
|---|---|---|---|---|
| Manual reactor trip | x | | | Table 7.2-4, PMS<br>Also initiates turbine trip<br>Figure 7.2-1 (Sheet 19), DAS<br>MG set trip |
| Manual safeguards actuation | x | | | Table 7.2-4, PMS<br>Also initiates reactor trip<br>Table 7.3-3, PMS |
| Manual CMT actuation | x | | | Table 7.2-4, PMS<br>Also initiates reactor trip<br>Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 19), DAS |
| Manual ADS actuation<br><br>(1-3 and 4)<br><br>1 / 2 / 3 / 4 | x | | | Table 7.2-4, PMS<br>Also initiates reactor trip<br>Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 20), DAS |
| Manual PRHR actuation | x | | | Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 19), DAS |
| Manual containment cooling actuation | x | | | Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 20), DAS |
| Manual IRWST injection actuation | x | | | Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 20), DAS |
| Manual containment recirculation actuation<br><br>CV line / MOV line | x | | | Table 7.3-3, PMS<br><br>Figure 7.2-1 (Sheet 20), DAS |
| Manual containment isolation | x | | | Table 7.3-3, PMS<br>Figure 7.2-1 (Sheet 20), DAS |

| Fixed Position Instrumentation | Control | Display | Alarm | SSAR Source |
|---|---|---|---|---|
| Manual main steam line isolation | x | | | Table 7.3-3, PMS |
| Manual feedwater isolation | x | | | Table 7.3-3, PMS |
| Manual containment hydrogen igniter | x | | | Figure 7.2-1 (Sheet 20), DAS |