Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NTD-NRC-95-4532
DCP/NRC0383
Docket No.: STN-52-003

August 18, 1995

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

ATTENTION: T. R. QUAY

SUBJECT: PROPOSED DRAFT/MARKUP OF SSAR SECTION 18.9.8

Dear Mr. Quay:

Enclosure 1 is submitted as a proposed response to the following AP600 Draft Safety Evaluation Report:

| Open Item | Addressed By |
|---|---|
| 18.9.3-1 | Section 18.9.8, top of page 18.9-53 |
| 18.9.3-2 | Section 18.9.8.2, pages 18.9-53, 54, 56, 57 |
| 18.9.3-3 | Section 18.9.8.2, pages 18.9-56, 57 |
| 18.9.3-4 | Section 18.9.8.1, page 18.9-53<br>Section 18.9.8.3, pages 18.9-59, 60 |
| 18.9.3-6 | Section 18.9.8.3.4, page 18.9-80 |
| 18.9.3-7 | Section 18.9.8.3.4, page 18.9-80 |
| 18.9.3-8 | Section 18.9.8.4, page 18.9-81 |
| 18.9.3-9 | Section 18.9.8.1, page 18.9-53 |
| 18.9.3-10 | Section 18.9.8.3, page 18.9-59 |

2547A

220069



E004 1/1

If you have any questions, please contact Steve Kerch at (412) 374-5104 or Andrea Sterdis at (412) 374-5292.

Nicholas J. Liparulo, Manager
Nuclear Safety Regulatory and Licensing Activities

/nja

Enclosure 1: Proposed Draft/Markup of SSAR Section 18.9.8

cc: Jim Bongarra
John O'Hara
Brian A. McIntyre
NRC HHFB
Brookhaven National Laboratory
Westinghouse (w/o Enclosures)

NTD-NRC-95- 4532

**NUCLEAR SAFETY REGULATORY & LICENSING ACTIVITIES REVIEW VOUCHER**

SUBJECT: Proposed Draft/Markup of SSAR section 18.9.8

Document Type (WCAP, Letter, Presentation, etc.) _____

Document Generated within: (Div.) AIBA Author: Andrea Stridis Ext: 5292

This document has undergone:

(X) Normal Review

Cognizant Mgr./Tech Lead

( ) Proprietary Information Review

Mgr. NSRLA or Designee

---

□ YES ☒ NO APPLICATION FOR WITHHOLDING PROPRIETARY INFORMATION

AW-95-_____

Project/WCAP No. _____

Purpose: (Approval, Response to NRC, Supplemental Info.) _____

Valid Charge No: (for review of document package) _____

---

**IDS INFO - NOTE: [SEE EXAMPLE ON BACK]**

| | |
|---|---|
| Shop Order: | |
| Plant: | AP600 SSAR |
| System: | |
| Component: | |
| Topical Area: | |
| Access: | |

**NOTE:** bcc: P.A. CHAHOY/WECe 5-41, 1L, 1A (AND ALL AFFIDAVITS)

#### 18.9.7.7.3 Dedicated Controls for Safe Shutdown Interface Design Specification

The dedicated controls for safe shutdown interface design specification is written after the functional requirements and performance requirements for these controls are written.

### 18.9.7.8 Controls Integration

The controls integration testing follows the verification and validation methods outlined in Section 18.8.

### 18.9.7.9 Controls Software Specification

The controls software specification is written after the controls software requirements are defined.

### 18.9.7.10 Controls Hardware Specification

The controls hardware specification is written after the controls functional requirements and performance requirements are defined.

### 18.9.7.11 Controls Verification

The controls verification process is performed during the M-MIS design process as described in Section 18.8.

## 18.9.8 Design of Plant Procedures

Plant procedures are developed and used by the Combined License applicant's plant staff so that startup, routine, nonroutine, and emergency activities are conducted in a safe manner. Activities affecting safety-related structures, systems, and components are performed by following detailed and approved plant procedures. ~~The general methodology for developing plant procedures is provided in this section.~~

~~The major procedures that are to be developed for the AP600 include the following:~~

- ~~Normal Operating Procedures~~
- ~~Abnormal Operating Procedures~~
- ~~Emergency Operating Procedures~~
- ~~Alarm Response Procedures~~
- ~~Maintenance Procedures.~~

~~The operating and maintenance procedures for the AP600 design implement the recommendations of Regulatory Guide 1.33.~~

As stated in subsection 13.5.3, the development of plant procedures is the responsibility of the Combined License applicant. The Combined License applicant referencing the AP600 certified design is responsible for addressing plant procedures, including the following:

- Normal operation
- Abnormal operation
- Emergency operation
- Alarm response
- Maintenance
- Administrative

~~A general overview of the system of procedures that is developed is shown in Figure 18.9.8-1.~~

### 18.9.8.1 Computerized Plant Procedures

*The following activities, described or referenced below, are beyond the scope of design certification:*

- *Development of the AP600 emergency operating procedure writer's guide and the AP600 emergency operating procedures*
- *Complete functional and detailed design of the AP600 computerized procedure system*
- *Design review of the AP600 computerized procedure system*
- *Performance of the human factors engineering verification and validation, including emergency operating procedures*

The AP600 is designed to provide computer-based operating procedures for the presentation of plant procedures to the operating staff. There is no paper backup of the plant procedures in the AP600 control room. Design options are being explored to determine the operator's course of action in the unlikely event of a loss of the computer-based procedures system.

Lay-down areas are available in the control room and outside the control room for paper documents to be used efficiently and effectively.

The Combined License applicant is responsible for developing the administrative procedures to ensure that the computer-based procedure database is available only to authorized personnel.

### 18.9.8.~~1~~2 Development of the Emergency Operating Procedures

The emergency operating procedures (EOPs) for the AP600 design define the actions required of ~~by~~ the plant operating staff during emergency conditions. The main purpose of the ~~(EOPs)~~ emergency operating procedures is to provide ~~guidance~~ operator procedures ~~to the operators~~ for the prevention or mitigation of the consequences of emergency conditions. These

procedures include automatic actions that occur in the event of an emergency, operator actions to help prevent or mitigate the consequences of an emergency, and operator actions necessary to stabilize the plant condition. Emergency operating procedures ~~EOPs~~ provide a conservative course of action for the operator and are flexible enough to accommodate variations.

The use of a comprehensive set of human-factored, symptom-based emergency operating procedures ~~EOPs~~ that encompass both optimal recovery and function restoration guidance enhances human reliability and decreases adverse results for a broad range of initiating events and subsequent multiple failures or operator errors. These emergency operating procedures ~~EOPs use the Westinghouse Owners Group (WOG)~~ are developed from a set of emergency response guidelines (ERGs) ~~as their basis~~. The emergency operating procedure ~~EOP~~ development process for the AP600 ~~is also~~ is based on the same accepted and established process used extensively by utilities with Westinghouse pressurized water reactors (PWRs).

For the AP600, the Westinghouse Owners Group generic ERGs ~~areare~~ modified and adapted to the specific plant configuration of the AP600 (Reference 23). (AP600 Document No. GW-GJR-100, Rev. 0 provides the AP600-specific ERGs.) Plant-specific ~~EOPs~~ emergency operating procedures are written using the criteria described below.

Delete "red lining" and use "Strikeout."

~~The first step in developing the AP600-specific emergency response guidelines (ERGs) is to compare the low-pressure (LP) reference plant, design with the AP600 design. To identify the design differences with respect to emergency operations between the ERG low-pressure reference plant design and the AP600 design, a comparison of the systems of the two plants is made. This comparison is performed in a systematic and complete manner by reviewing all systems. The low-pressure reference plant is chosen as the initial starting point in the development of AP600-specific ERG's because the charging pumps are not part of the emergency core cooling system, thus making the AP600 more similar to the low-pressure reference plant. Because of the major functional similarities between the AP600 design and the low-pressure ERG reference plant, the ERG process can easily be applied to the AP600 design.~~

~~Subsection 18.9.8.1.1.2, provides the high-level operator action strategies initially developed for the AP600 design. The high-level operator action strategies are developed to identify possible operator actions used to assist in determining instrumentation and control needs. Supporting analysis to demonstrate the effectiveness of these operator actions is performed in a manner similar to that used for the Westinghouse Owners Group ERG supporting analyses. These actions are then subject to modification or rearrangement, in order to incorporate the results of the analyses. The AP600 specific ERGs correspond to the same type of guidelines provided in the low-pressure ERGs. Once the supporting analyses are completed and the operator action strategies finalized, additional detail is added, resulting in AP600 specific ERGs.~~

~~18.9.8.1.1.1 Differences Between the Two-Loop Low-Pressure Reference Plant and the AP600 Plant~~

~~This subsection establishes the high-level operator action strategies for emergency operations for the AP600 design. Since the Westinghouse Owners Group ERGs are the industry-approved reference for Westinghouse-designed pressurized water reactors, they are used for and adapted to the AP600.~~

~~The objective of this section is to compare the ERG reference plant system designs upon which the ERGs are based, to the AP600 system designs to determine design differences with respect to emergency operation high-level operator action strategies. The results of this comparison are used as the basis for determining the applicability of the transient and accident analyses basis of the ERGs to the AP600 and preparation of high-level operator action strategies for the AP600 based on the ERGs.~~

~~18.9.8.1.1.2 High-Level Operator Action Strategies~~

~~The high-level operator action strategies for emergency operations are found in this subsection in Tables 18.9.8-1 through 18.9.8-37. Tables 18.9.8-1 through 18.9.8-13 contain the optimal recovery strategies encompassing the following:~~

- ~~Diagnosis (E-0, ES-0.0)~~
- ~~Reactor trip response (ES-0.1, ES-0.2, ES-0.3)~~
- ~~Loss of reactor or secondary coolant (E-1)~~
- ~~Safety injection termination (ES-1.1)~~
- ~~Post-LOCA cooldown and depressurization (ES-1.2)~~
- ~~Faulted steam generator isolation (E-2)~~
- ~~Steam generator tube rupture (E-3)~~
- ~~Loss of all ac power sources (ECA-0.0)~~
- ~~LOCA outside containment (ECA-1.1)~~
- ~~Uncontrolled depressurization of all steam generators (ECA-2.1).~~

~~Tables 18.9.8-14 through 18.9.8-19 contain strategies encompassing the following six critical safety functions:~~

- ~~Subcriticality (F-0.1)~~
- ~~Core Cooling (F-0.2)~~
- ~~Heat Sink (F-0.3)~~
- ~~Integrity (F-0.4)~~
- ~~Containment (F-0.5)~~
- ~~Inventory (F-0.6).~~

~~Tables 18.9.8-20 through 18.9.8-37 contain function restoration strategies encompassing the following:~~

- ~~Loss of subcriticality (FR-S.1, FR-S.2)~~
- ~~Loss of core cooling (FR-C.1, FR-C.2, FR-C.3)~~

- ~~Loss of heat sink (FR-H.1, FR-H.2, FR-H.3, FR-H.4, FR-H.5)~~
- ~~Loss of vessel integrity (FR-P.1, FR-P.2)~~
- ~~Loss of containment integrity (FR-Z.1, FR-Z.2, FR-Z.3)~~
- ~~Loss of inventory (FR-I.1, FR-I.2, FR-I.3).~~

~~The critical safety functions and the corresponding function restoration strategies are provided for the prevention or mitigation of emergency conditions without the need for diagnosis of specific initiating events.~~

~~18.9.8.1.1.3 AP600 Specific Emergency Response Guidelines~~

~~The AP600 emergency response guidelines are developed as part of the M-MIS design process, described in Section 18.8.~~

The AP600 emergency operating procedures ~~EOPs follows~~ meet the guidelines of NUREGs 0899 (Reference 12), 0737 Supplement 1 (Reference 13), and 1358 (Reference 14).

The ~~of~~ AP600 emergency operating procedures ~~EOPs is~~ are based on two primary elements. The technical content, ~~is~~is developed from the AP600 ~~technical guidelines~~ ERGs, along with additional sources of information such as design characteristics, transient and accident analysis, engineering judgment, and operating experience.

~~The second, the presentation of information in the~~ The other element is that the emergency operating procedures ~~EOPs,~~ follow the principles defined in the AP600 ~~procedures~~ emergency operating procedure writer's guide. The ~~procedures~~ emergency operating procedure writer's guide ~~helps to~~ provides confidence in consistent production of high-quality emergency operating procedures~~EOPs~~. In addition, the use of a procedures writer's guide is necessary for the integration of human factors principles when converting technical guidelines into an acceptable emergency operating procedure ~~EOP~~ format.

~~Technical guidelines~~ The AP600 ERGs ~~represent the~~ are a translation of engineering data derived from operating experience and transient and accident analysis into information presented in such a way that it can be used to write emergency operating procedures~~EOPs~~. ~~The AP600 technical guidelines (the AP600 ERG's) will be developed using the criteria defined in Subsection 18.9.8.1.1.~~

The ~~procedures~~ emergency operating procedure writer's guide contains the necessary information and guidance for translating the AP600 ERGs into AP600 emergency operating procedures~~EOPs~~. The use of a procedures writer's guide in writing AP600 emergency operating procedures ~~EOPs~~ provides confidence that the emergency operating procedures ~~EOPs~~ are usable, accurate, complete, readable, convenient to use, and acceptable to main control room personnel.

Emergency operating circumstances invariably involve some degree of stress ~~(psychological, time or load)~~ and/or degraded environmental conditions unique to that situation. ~~or both that may not be present when other types of procedures are used.~~ The AP600 ~~procedures~~

emergency operating procedure writer's guide addresses the goals, requirements and recommendations identified in the writer's guide section of NUREG-0899 (Reference 12).

The emergency operating procedure writer's guide addresses the additional tools that computer-based procedures are able to provide the operator. The analysis of plant operating procedures is explicitly incorporated into the computer-based procedures system. For example, the writer's guide discusses:

- Parameters that need to be continuously monitored (for example, the steam generator level) which are not covered by notes, cautions, or foldout page items
- Actions that may be initiated, but need not be completed prior to leaving the step, or may be completed at a later time
- Prioritizing parallel information (for example, cautions, notes, foldout page items, and critical safety functions)
- Number of attempts and time between attempts for parallel information items

The process of translating the AP600 ERGs into action steps that make up the emergency operating procedures ~~EOPs~~ is the responsibility of the procedure writer. The AP600 ERGs identify the plant objectives to be met, the systems and subsystems required, the required level of performance, the situations requiring operator action and the order in which the actions must be carried out. It is the task of the procedure writer to extract the relevant information, and to carry out additional function, task, or technical analysis required in order to provide the emergency operating procedures~~EOPs~~.

Operating experience and information contained in the ~~procedures~~ emergency operating procedure writer's guide is used throughout this process so that the emergency operating procedures ~~EOPs~~ are written in a form that optimizes operator performance. As the sequence and relationships among action steps are developed, the technical guidelines are followed by the emergency operating procedure ~~EOP~~ writers. This AP600 emergency operating procedure ~~EOP~~ development process is iterative and usually begins at a system level and becomes more specific at the subsystem and the component levels. It is during this iterative process that the specific operator tasks are identified and written in the form of action steps.

The orientation of the AP600 emergency operating procedures ~~EOPs~~ parallels that of the AP600 ERGs and is function-oriented, with provisions for specific event-based actions (for example, loss of coolant accident, steam generator tube rupture, secondary break). Function oriented emergency operating procedures ~~EOPs~~ provide the operator with guidance on how to verify the adequacy of safety functions and on how to restore and maintain those functions when they are degraded.

The analysis of functions and tasks used in the development of AP600 emergency operating procedures ~~EOPs~~ is provided by the AP600 ERGs ~~and the Westinghouse Owners Group (WOG) low pressure ERGs~~. This information provides the initial cut at identifying functions,

their associated hardware systems, the actions that are taken (by man and machine) and the circumstances under which they are taken.

Once the necessary technical and operator task information is defined and the information contained in the writer's guide is used the emergency operating procedures are produced. This process selects approaches and sequences for presenting the operator actions while at the same time addresses such concerns as content, organization, format and style of expression and presentation.

The AP600 emergency operating procedures ~~EOPs are~~ are subjected to a verification and validation (V&V) on the AP600 simulator. This process ~~addresses~~ addresses the following objectives:

a. The emergency operating procedures ~~EOPs~~ are technically correct. (They accurately reflect the AP600 ERGs.)

b. The emergency operating procedures ~~EOPs~~ are written correctly. (They accurately reflect the AP600 writer's guide.)

c. The emergency operating procedures ~~EOPs~~ are usable. (They can be understood and followed without confusion, delays, errors.)

d. There is a correspondence between the emergency operating procedures ~~EOPs~~ and the main control room/plant hardware (controls, equipment, indications) that becomes a reference for use both inside and outside of the main control room. Emergency operating procedures ~~EOPs~~ use the same designation, use the same units of measurement, and operate consistent with the plant hardware.

e. The language and level of information presented in the emergency operating procedures ~~EOPs~~ are compatible with the number, qualifications, training and experience of the operating staff.

f. There is a high level of confidence that the emergency operating procedures ~~EOPs~~ work. (That is, the emergency operating procedures ~~EOPs~~ guide the operator in mitigating transients and accidents.)

Emergency operating procedure ~~EOP~~ discrepancies found during the verification/validation process ~~are~~ are corrected and factored into the emergency operating procedures ~~EOPs~~ prior to issuance.

Reference 24, WCAP-14401 provides a Programmatic Level Description of the HFE Verification and Validation, which includes emergency operating procedure V&V.

~~The final step in the AP600 EOP implementation process is operator training. During training, operators are encouraged to point out additional recommendations that further~~

~~improve the EOPs. Valid comments are resolved and incorporated into the EOPs. Once this final step is complete, the AP600 EOPs are reviewed and approved for implementation.~~

~~**18.9.8.1.3 Emergency Operating Procedures**~~

~~The AP600 plant-specific Emergency Operating Procedures are developed as part of the M-MIS design process, described in Section 18.8.~~

~~**18.9.8.2 Abnormal Operating Procedures**~~

~~Abnormal operating procedures (AOPs) specify the operator actions necessary to restore the plant to a normal operating condition following a plant perturbation. The abnormal operating procedures for the AP600 are developed as part of the M-MIS, described in Section 18.8.~~

~~**18.9.8.3 Alarm Response Procedures**~~

~~Alarm response procedures specify the operator actions necessary to respond to individual plant alarms. An alarm occurs as a result of some variable departing from its normal operating band. The alarm response procedures detail the actions that are taken to restore the affected variable to normal conditions. The alarm response procedures are developed as part of the M-MIS design process, described in Section 18.8.~~

~~**18.9.8.4 Normal Operating Procedures**~~

~~Procedures are written for the normal operation of the AP600. These normal operating procedures (NOPs) provide the actions to be taken by the operator to start up the plant, operate the plant at power, shut down the plant, operate individual plant systems, perform surveillance testing and remove equipment from service for maintenance activities. The normal operating procedures are developed as part of the M-MIS design process, described in Section 18.8.~~

~~**18.9.8.5 Maintenance Procedures**~~

~~Maintenance procedures (MPs) are written that define the practices to be followed and actions to be taken to maintain, repair, and modify plant equipment. The MPs are developed based on the specific vendor equipment supplied for the plant.~~

### 18.9.8.63 Functional Design of the Computerized Plant Procedures

The functional design of the computer-based procedures system is generated using a design process which is a systems engineering approach wherein high-level requirements for the system are first defined. This is followed by successively more detailed requirements. Engineering expertise in plant procedures and man-machine interface design is a major input to the design process. The design of the system is enhanced over time by a Design Review and by discussions with plant operating personnel.

The ERGs and the emergency operating procedure writer's guide identify the content and format of the emergency operating procedures. The content and format described therein is the basis for the type of information presented in the computer-based representation of the Emergency Operating Procedures.

The AP600 operating procedures are computer-based from the point of view of presentation to the operating staff. There is no paper backup of the plant procedures in the AP600 control room. Design options are being explored to determine the operator's course of action in the unlikely event of a loss of the computer-based procedures system.

The computer-based presentation of the procedures encompasses the format of the procedures identified in the writer's guide(s), and in relevant instances makes explicit items, such as, for example, direct monitoring of parameters which need to be continuously monitored during procedure execution.

### 18.9.8.63.1 Computerized Procedures Introduction/Background

Active human response in most complex situations is guided by a mix of an individual's experience, the training that the individual has received, and procedures, that is, formalized guidelines developed, usually by others, in anticipation of that or a similar situation. To the extent that the human's response is directed by applying knowledge obtained through formal training and derived from the individual's own experience, the individual's responses are knowledge based. To the extent that the individual's response consciously follows an established set of procedures, supported by training in applying and using those procedures, the individual's response is rule based.

The relative proportions of knowledge-based response and rule-based response that result in whatever action is taken varies from one situation to the next and from individual to individual.

Normal and emergency plant procedures are developed well in advance of their applications by experienced specialists. The procedures not only guide the user along a recommended course of action but also aid the detection of anomalous conditions and recommend changes in the normal course of action in dealing with these anomalies.

Steps frequently appear in an "IF-THEN-ELSE" format. If a given set of conditions exists (including, usually, completion of prior procedure steps) as indicated by evaluation of the appropriate plant sensor responses, the operator executes the next recommended action. If the required conditions do not exist or cannot be verified, the operator executes a specified alternative action. The functions involved in generating rule--based responses consist of the following:

- Collecting specified data
- Processing that data through a prespecified train of logic
- Recognizing the action recommended by the course taken
- Executing that action.

The functions involved in generating responses are as amenable to computer application as to human application. Indeed, rule-based responses (but not necessarily execution of the resultant recommended actions) generated by a programmed computer may actually be preferable to responses generated by a human operator for three reasons.

First, the likelihood of error in computer-generated responses is significantly smaller than that in human generated responses, provided the basic procedures are well formulated, especially in the "ELSE" aspects.

Second, the human confronted with the situation can be freed from the non-cognitive component of the response-generating activity. The individual can concentrate on applying his knowledge to comprehending the situation, detecting anomalous conditions and determining appropriate courses of action.

Third, the computer can provide a much-desired, independent verification of the course of action chosen by the human operator before executing action steps.

This symbiosis of man and machine by transferring to the computer the rule-based functions at which it excels is the goal of the computerized procedures system.

### 18.9.8.63.2 Mission of Computerized Procedures

The mission of the computerized procedures system is to assist power plant operators in monitoring and controlling the execution of plant procedures. The AP600 Computerized Procedures System Functional Requirements and Design Basis, provides high-level design requirements, performance requirements, and functional requirements for the computerized procedures system [WCAP-14388 (Reference 22)].

~~### 18.9.8.6.3 Computerized Procedures Design Basis~~

~~The design basis of the computerized procedures system is:~~

- ~~To guide the user step by step through the procedures by monitoring the appropriate plant data and by identifying the recommended course of action~~
- ~~To provide the necessary parallel information that allows the user to assess other plant conditions that may require attention, and that are embodied in notes, cautions, foldout page items (for emergency operating procedures - EOPs) and the critical safety functions (for EOPs).~~

~~### 18.9.8.6.4 Computerized Procedures Performance Requirements~~

~~The following requirements define the performance of the computerized procedures system:~~

~~1 The system guides the user in charge of implementing the operational strategy through the relevant procedures step by step.~~

2 The system monitors on-line the plant parameter values and component states available in the plant computer so as to provide the user with the status of each procedure step.

3 The system provides the user with the procedurally recommended action in the event that the expected response is not obtained in a given procedure step.

4 The system supports the user in understanding the status of the current procedure step by continuously displaying the high-level statement for that step.

5 The system supports the user in understanding why a given procedure step is in a certain condition by displaying the status of the relevant plant parameters or components or both.

6 The system provides feedback to the user on the results of his actions by periodically re-executing the logic of the current procedure step and subsequently updating the information displayed.

7 The system provides the capability for the user to transition to other operating procedures as required and to automatically select and display the new procedure when requested. This includes the capability for the user to randomly access any procedure.

8 The system provides the user with a continuously displayed, on-line summary of the status of the critical safety functions (for emergency operating procedures), when required.

9 The system provides feedback to the user if a Caution, Precaution, Limitation, Note, or Foldout Page item (for EOP's) requires attention by periodically monitoring the status of the relevant items and displaying such information.

10 The system provides the user with prompts that are easy to understand and straightforward to use, consistent with the plant man-machine interface design philosophy.

11 The system generates a chronological record of the execution of the operating procedures, including parameter and component states and actions taken.

12 The system includes the capability to produce a computer listing verifying that the procedure logic encoded accurately reproduces the paper procedures. This function is off-line.

13 The system includes the capability to access a (previously defined) graphics display that appears on a separate video display unit. This provides for the integration with main control room displays.

14 The system includes the capability to read an external data file to enhance the use of the system for training purposes. The structure of this external data file is specified.

15. The system includes the capability to modify or edit the procedures in a straightforward manner. This is accomplished by using a relational data base management system.

16. The system provides for the security of the procedural data base so that only authorized personnel make changes.

17. The system is redundant so as to provide for a backup if one of the user stations fails.

**18.9.8.6.5 Computerized Procedures Functional Requirements**

**18.9.8.6.5.1 General System Requirements**

**Accessing the Computerized Procedures System**

Overview: The user accesses the computerized procedures system manually. The computerized procedures system also has an automatic initiation capability. The manual access is used in cases where the user controls the initiation of the system when, for example, a reactor trip, safety injection or station blackout occurs or when a particular procedure is invoked. The automatic mode of access is used in cases where the computerized procedures system can itself track the occurrence of one (or more) of the those events.

Functional Requirements: The user accesses the computerized procedures system manually via an interface. The user opens the computerized procedures system icon, or equivalent, and either a default procedure is selected by the system or the user selects a procedure from a menu.

The computerized procedures system is capable of being triggered (initiated) automatically in response to, events such as a reactor trip, safety injection, or station blackout. Potential entry conditions into the operating procedures are monitored at intervals of no more than five seconds. The system is triggered within two seconds of any of these occurrences, independently of whether the computerized procedures display is activated.

Upon initiation, the computerized procedures system obtains the previous one hour of data from the historical retrieval system in the plant computer system. The computerized procedures system uses the historical retrieval system for trending or rate of change data.

**Data Availability**

Overview: Data is available on the CRT display to support progression through the procedures. In cases where plant data are not available to the computerized procedures system, the system identifies which data are not available. The user provides the answer to the relevant procedural question. (Data here is the state of the procedure substep or step, for example, pressure greater than 1000 psia, reactor trip verified or pump xxx running.)

Functional Requirements: The data for procedure steps, substeps, and subsubsteps are available on the computerized procedures display. This includes information contained in

curves, attachments, and tables, as appropriate. This also includes trending information. Data computed from steam tables and after references is also included. This data is updated at intervals of no more than two seconds.

The data for precautions, cautions, notes, limitations, and foldout page items (for EOP's) are available on the computerized procedures display. These items are checked at intervals of no more than five seconds. Once a violation has occurred, the data for the violation is updated at intervals of no more than two seconds.

The data for continuously controlled parameters and initiated actions is available on the computerized procedures display. These data, once active, are checked at intervals of no more than five seconds.

A special alert indicator, or equivalent, is available on the computerized procedures display. This indicator is a visual cue to the user that a precaution, caution, note, limitation or foldout page item is violated, that a critical safety function (for EOP's) state has changed and requires attention, or that a continuously controlled parameter has moved out of its allowable range.

The critical safety functions (for EOP's) summary status is available on the computerized procedures display. The critical safety functions are updated at intervals of no more than five seconds.

The computerized procedures system identifies which data are unavailable because of either "BAD" data quality or unavailability in the data base. The user provides the answer to the relevant procedural question.

The computerized procedures system display is updated with current plant data at intervals of no more than two seconds.

The data that the computerized procedures system uses are updated with current plant data at intervals of no more than two seconds.

An active version of the critical safety function status trees (for EOP's) is available for display as part of the computerized procedures system.

A display indicating the possible transitions from the current procedure is available as part of the computerized procedures system.

The computerized procedures system has the capability to display relevant procedure entry conditions.

The computerized procedures system has the capability to access a (previously defined) graphics display, which appears on a separate video display unit. This graphics information complements the textual procedural information presented by the computerized procedures system.

A display indicating which procedures are active during the current transient or operation is available as part of the computerized procedures system. (This is called the procedure road map.)

**User Control**

Overview: The user has control over the computerized procedures system. The system does not advance to the next substep or step, it does not respond to precaution, caution, note, limitation or foldout page violation, nor does it transition to a new step or procedure without the user's concurrence. User commands are of the form, "continue to step x," "transition to procedure y," "display RNO column," (RNO response not obtained) "forward," "backward," "execute step," and "go to step z."

Functional Requirements: The user has complete control over the operation of the computerized procedures system.

The computerized procedures system advances to the next substep or step, responds to a precaution, caution, note, limitation, or foldout page violation, or transition to a new step or procedure only with the concurrence of the user.

The user uses a "continue to next step x" command, or equivalent, to inform the computerized procedures system that the user wishes to continue to the next relevant part of the procedure.

The user uses a "transition to procedure y" command, or equivalent, to inform the computerized procedures system that the user wishes to transition to the next appropriate procedure, as indicated by the system.

The user uses a "display RNO column" command, or equivalent, to inform the computerized procedures system that he wishes to view the "response not obtained" column of the operating procedures. The user is informing the system at this point that he either does not believe that the expected action has truly been completed or, that he wishes to view the "response not obtained" column of the procedures for information purposes.

The user uses a "forward" command, or equivalent, to inform the computerized procedures system that he wishes to view upcoming procedure steps. The system, by a mechanism such as scrolling, allows the user to view those steps.

The user uses a "backward" command, or equivalent, to inform the computerized procedures system that the user wishes to review previous procedure steps. The system, by a mechanism such as scrolling, allows the user to review those steps. The computerized procedures system has the capability to return to the original procedure step, or to continue onward from the point to which the user returned, depending upon the wishes of the user.

The user uses an "execute step" command, or equivalent, to inform the computerized procedures system that the user wishes to execute a particular procedure step.

The user uses a "go to step z" command, or equivalent, to inform the computerized procedures system that the user wishes to go to the recommended procedure step.

The user uses a "yes" command, or equivalent, to inform the computerized procedures system that he agrees with the query presented by the system.

The user uses a "no" command, or equivalent, to inform the computerized procedures system that he does not agree with the query presented by the system.

User prompts are processed by the computerized procedures system in no more than two seconds. This is the time from initial user response to the appearance of a new display. Indication that his request is acknowledged, presentation of background information, and presentation of the complete display is generally consistent with the plant computer man-machine interface design. However, these requirements are examined on an individual basis in cases where the intended use of the computerized procedures system dominates specific timing goals.

**Navigation Through the Procedures**

Overview: The computerized procedures system aids the user in navigating through the procedures. The system keeps track of what procedures have been started and completed and is able to retrace the path back through the procedures as the need arises.

Functional Requirements: The computerized procedures system aids the user in navigating through the procedures.

The computerized procedures system keeps track of the step-by-step progression through the current procedure.

The computerized procedures system keeps track of the transitions to various procedures made during the course of the transient recovery.

The computerized procedures system has the capability to guide the user both forward through the procedures and backward through the procedures as dictated by the use of the operating procedures or by the user's choice.

Embedded in these rules are the priorities associated with the critical safety functions, notes, cautions, foldout page items, continuously controlled parameters, and initiated actions. These are handled (that is, displayed) in the order required by the particular procedures.

For example, for Emergency Operating Procedures, the order could be the following:

- RED critical safety function
- ORANGE critical safety function
- Foldout Page item
- Caution violation

- Continuously controlled parameter out of range
- Initiated action not completed
- YELLOW critical safety function
- Note violation.

Within groups, except for the critical safety functions, there is no inherent priority structure. The display related to one of the preceding items does not appear until the user completes a substep or step.

**Data Quality**

Overview: The computerized procedures system informs the user if the data used by the system is unreliable. The data quality conventions are exactly those that are used in other parts of the computer system. Upon the indication of the "BAD" data, the user provides the answer to the relevant procedural question.

Functional Requirements: The computerized procedures system identifies which data are unreliable for the relevant procedural issue.

The data quality conventions used in the computerized procedures system are identical to those used in other parts of the computer system.

The user provides the answer to the relevant procedural question upon indication of bad data. The user decides whether to continue to the next step or to initiate the action specified in the response not obtained part of the procedure.

**Testing the Computerized Procedures System**

Overview: The computerized procedures system has the capability to be tested to verify that the computerized version of the procedures accurately replicates the logic of the written version. This testing is as automated as practicable to minimize both time and personnel requirements. The result of the testing is a printed output that permits checking of the computerized procedures system.

Functional Requirements: The computerized procedures system has the capability to be tested periodically to verify that the computerized version of the procedures accurately replicates the logic of the original written version.

The output of the testing process is in an easy-to-read format so that a person familiar with the procedures may compare this output with the paper version of the procedures in order to verify the accuracy of the computerized procedures system.

**Documentation**

Overview: The computerized procedures system has the capability to record the user's progression through the procedures, including the information seen on the display and

responses to this information. This recording is available in both CRT display form and hard-copy form.

Functional Requirements: The computerized procedures system has the capability to record for later use the user's progression through the procedures. This recording is available in both CRT display form and hard copy form.

The long form of the recording, triggered upon the user's response, includes the current procedure title, the current high level statement of the step, the current substep, the data associated with the current substep, any procedurally recommended action, the previous two high level step statements, the upcoming two steps, the contents of the special alert indicator window, if any, the time at which the user responded to a prompt, the status of the critical safety functions, if applicable, the status of any precaution, caution, note, limitation, or foldout page violations, if any, and the user's response.

As a part of the long form of the recording, the critical safety function status trees (for EOP's) are printed upon their initial activation. Subsequent to this, if a change occurs in the terminus of any tree, then that tree is recorded as well.

Pop-up windows that are selected by the user from the computerized procedures system during the use of the system are included as a part of the long form of the recording. The long form of the recording is formatted to look like the CRT display from which it was derived.

The short form of the recording, triggered upon the user's response, includes only the current procedure title, the current high level statement of the step, the time at which the user responded to a prompt, the status of the critical safety functions, if applicable, the status of any precaution, caution, note, limitation, or foldout page violations, if any, and the user's response. The short version of the recording is formatted as a simple list, to facilitate quick review by members of the operating staff.

The procedure entry conditions display is printed each time a procedure is entered, and it is a part of the long version of the recording.

**System Redundancy**

Overview: The computerized procedures system has the capability for redundancy to provide a backup in the event of failure of one of the user stations.

Functional Requirements: The computerized procedures system has the capability for redundancy to provide a backup in the event of failure of one of the user stations.

If a primary workstation or CRT fails, the user moves to a backup station to execute the computerized procedures system. The user uses a menu option access procedures, or equivalent, to specify the procedure to be displayed and the starting step number. The user is encouraged to start at step 1 so that the precautions, notes, cautions, and limitations and other information are reinitiated as active data to be monitored by the system.

The user can use the print log, menu option to retrieve the log from the historical storage and retrieval system, and review the historical information contained therein. This helps to provide confidence that information lost in the failure of the primary workstation is recovered.

**18.9.8.6.5.2 Entry Conditions Requirements**

**Display and Annotation of Entry Conditions**

Overview: The computerized procedures system has the capability to display any entry conditions that it has used as the basis for selecting the current procedure. These entry conditions are clearly identified.

Functional Requirements: The computerized procedures system has the capability to display any entry conditions that it has used as the basis for selecting the current procedure.

The entry conditions that are displayed includes the procedure title, procedure purpose, and the symptoms and entry conditions in the format given in the interface design requirements (see Subsection 18.9.8.6.6).

If "BAD" data is encountered upon evaluation of entry conditions, the computerized procedures system evaluates the entry conditions, and the system icon, or equivalent, changes color or not according to the results of the evaluation. The entry conditions display is examined to determine what data is "BAD".

**18.9.8.6.5.3 Procedure Step Information Requirements**

**Display and Annotation of Sequential Procedure Information**

Overview: The computerized procedures system has the capability to display the currently active procedure title, the high-level statement of the current step, the states of the parameters or components relevant to the step, and the actions required, in response to the current status of the step.

In addition, the system has the capability to display past procedure steps, as well as upcoming procedure steps, to give the user the context of where the user is in the procedure. Information contained in curves, attachments and tables are also available to the user on the system display. If a procedure step requires trending information, the system also has the capability to provide such information.

The information related to the sequential progression through the procedure is available to the user.

Functional Requirements: The computerized procedures system has the capability to display the title of the currently active procedure. In situations where transitions to other procedures are required, the new procedure title is displayed upon selection.

The computerized procedures system has the capability to display a high-level statement of the currently active procedure step, indicating the status of the step.

The computerized procedures system has the capability to display the status of any parameters or components relevant to the currently active procedure step or substep.

The computerized procedures system has the capability to display the data contained in curves, attachments, or tables that is relevant to the currently active procedure step.

The computerized procedures system has the capability to display any actions that are required related to the currently active procedure step.

The computerized procedures system has the capability to display the status of the previously completed procedure steps.

The computerized procedures system has the capability to display the upcoming procedure steps within the currently active procedure.

**18.9.8.6.5.4 Parallel Information Requirements**

**Display and Annotation of Parallel Information**

Overview: The computerized procedures system has the capability to display the information that is monitored in parallel with the sequential execution of the procedure. This includes notes, precautions, cautions, limitations, and foldout page items and the critical safety function status trees (for EOP's). This also includes parameter and component state changes that have been initiated but not completed upon exiting the currently active procedure step, as well as continuously controlled parameters that are monitored for more than a single procedure step, such as steam generator level.

Functional Requirements: The computerized procedures system has the capability to display information related to notes, precautions, cautions, limitations, and foldout page items. This includes both the display of the currently active items and the display of violations of items.

The computerized procedures system has the capability to inform the user of the violation of any note, precaution, caution, limitation, or foldout page item through the special alert indicator.

The computerized procedures system has the capability to interrupt the flow through the sequence of the currently active procedure to display information related to note, precaution, caution, limitation, or foldout page violations, initiated actions, continuously controlled parameters and the critical safety functions (for EOP's). This interruption only occurs at a convenient point in the sequence, such as at the end of a substep or step, so as not to confuse the user. The interruption also is accomplished without erasing current procedure information.

The computerized procedures system has the capability to display the critical safety function status trees (for EOP's), both in summary form and in their complete form. The display of the critical safety function status trees in either form is completely consistent with the prioritizing rules associated with their use.

The computerized procedures system has the capability to inform the user of a change in state of the critical safety functions (for EOP's) that results in a more severe challenge to the plant. This is accomplished directly through the display of the critical safety function summary and also through the use of the special alert indicator.

If a completed procedure step (or substep) or a note, precaution, caution, limitation, or foldout page item involves a parameter that from that point onward should be continuously controlled, the computerized procedures system has the capability to monitor that parameter. The system alerts the user with an appropriate message or cue if the parameter exceeds its allowable range. This occurs through the use of the special alert indicator.

If an action is initiated in the currently active procedure step, or a note, precaution, caution, limitation, or foldout page item, but not completed, the computerized procedures system has the capability to monitor the parameter or component until such time that the action is complete. The system alerts the operator with an appropriate message or cue if the action is not completed after a predefined time or by a certain predefined step.

The computerized procedures system maintains a list of the incomplete steps, which are available to the user for his information.

**18.9.8.6.6 Computerized Procedures Interface Design Requirements**

**18.9.8.6.6.1 Requirements of the Computerized Procedures System Display**

Display Element: Presentation of the computerized procedures system display.

Functional Requirements: The computerized procedures system is displayed in a representative format, as indicated in Figure 18.9.8-2.

The computerized procedures system display is of a fixed window size, allowing room for icons. The default size is as close to full screen size as possible. It is not useful to resize the computerized procedures system display, and the users are trained not to do so.

The computerized procedures system displays pop-up windows, as they are required or requested by the user, on a second CRT screen. (In cases where a second CRT screen is not available, the pop-up windows are displayed on the computerized procedures system display.)

~~18.9.0.6.6.2 Requirements of Component and Parameter States~~

~~Display Element: Presentation of component and parameter states.~~

~~Functional Requirements: The computerized procedures system displays the component and parameter states consistently, except where other considerations apply, in the following manner:~~

~~Descriptors and States~~

~~Descriptors are essentially components and parameters, such as component cooling water pumps, feedwater pumps, pressurizer level, reactor coolant system pressure, and steam generator level. States represent the current status of these components and parameters, such as running, not running, greater than 50%, less than 2200 psia, and stable, respectively. A list of the descriptors and states is provided as the procedures are analyzed.~~

~~The display of descriptors and states is consistent for the display of procedure information and notes, cautions, and foldout page items.~~

~~The display of components and parameter states includes the appropriate step, substep, or subsubstep labels, as close as possible to the paper version of the procedures.~~

~~When a component or parameter is not in its correct state according to the procedure, the computerized procedures system displays this component or parameter in reverse video, or equivalent.~~

~~Display Element: Data Quality~~

~~Functional Requirements: The computerized procedures system displays component and parameter states, with no quality code attached, if these states are based on "GOOD" sensor data.~~

~~When "BAD" data is encountered, the state is evaluated and assigned a "BAD" quality code, so that the user knows what information is required in the procedure and also that the displayed information is "BAD". Color coding is used to increase the visibility of the "BAD" data.~~

~~Unavailable data is color coded by the computerized procedures system. In addition, the data is displayed in terms of a descriptor and a positive state.~~

~~The computerized procedures system displays component or parameter states as defined previously. A quality code is attached if these states are based on "FAIR" sensor data.~~

~~The user prompts for the computerized procedures system allows the user the opportunity either to continue to the next step or to see the procedurally recommended action if the component or parameter states are based on "BAD" or unavailable data.~~

The user prompts for the computerized procedures system are the same whether the component and parameter states are based on "GOOD" data or "FAIR" data. The system treats the data as "GOOD" data in each of the two cases. The difference is only that the system cues the user that the data is "FAIR".

The computerized procedures system informs the user if "BAD" or unavailable data is present in the critical safety function status trees, notes, cautions or foldout page items.

The quality code appears on the bar of the relevant critical safety function status tree summary.

#### 18.9.8.6.6.3 Requirements of the Display of Current Procedure Information

Display Element: Procedure Entry Conditions.

Functional Requirements: The computerized procedures system provides for the display of the purpose of the currently active procedure and the entry conditions for that procedure.

In the case of plant process parameters determining the entry into the procedure, the state(s) of the parameter(s) that caused entry into the procedure, along with time tags for this information, are clearly identified, in a manner consistent with the display of component and parameter states previously described.

The display containing the procedure entry conditions are accessed through the cursor control device, in a pop-up window, at the request of the user.

Display Element: High Level Statement of Procedure Step.

Functional Requirements: The computerized procedures system provides a concise, high level statement of the procedure step on the display. This appears on the display, as shown in item 1 in Figure 18.9.8-2. If the purpose of the procedure step is to verify turbine trip, the high level statement reads "VERIFY TURBINE TRIP", exactly as written in the paper procedures. Appropriate color coding is used to indicate whether the step is satisfied.

Display Element: Component and/or Process Parameter Status and Actions Required.

Functional Requirements: The computerized procedures system provides the component process parameter states relevant to the current procedure step, note, caution, or foldout page item on the display. This appears on the display, as shown in item 2 in Figure 18.9.8-2. In the case of turbine trip, the components of concern are the turbine stop valves. If the turbine stop valves are closed, the "TURBINE STOP VALVES CLOSED", appears on the display. This represents the supporting information that the operator requires in order to verify the high level statement that the turbine is indeed tripped. It is the information required by the procedure substeps.

If any of the supporting information is in the form of figures, tables, or attachments, the computerized procedures system provides this information in two ways: in the form of the results of the figure, table, or attachment, and in the form of the display of the figure or attachment itself.

The computerized procedures system provides the procedurally recommended actions relevant to the current step on the display, as shown in item 3 in Figure 18.9.8-2. For example, if the turbine is not tripped, then the action "MANUALLY TRIP TURBINE", exactly as in the "response not obtained" column of the procedures, appears on the display.

If the number of substeps exceeds the available display area, the computerized procedures system provides scrolling capability to enable the user to view the entire step.

The computerized procedures system provides for the display of figures required during the execution of the procedures. The figure is a reproduction of that which is in the paper procedures, consistent with other X-Y plots in the plant computer system. If an equation is available for the creation of the curve, then it is used in the computerized procedures system.

In addition to the figure, the current value of the parameters plotted in the figure are also shown. The figures are accessible through the cursor control device, when directed by the procedure and when required by the user.

The computerized procedures system provides for the display of attachments relevant to a particular procedure. The attachment is clearly identified. The attachments are accessible through the cursor control device, when directed by the procedure and when required by the user.

The computerized procedures system provides for the display of tables relevant to a particular procedure. The table is clearly identified. The tables are accessible through the cursor control device, when directed by the procedure and when required by the user.

Display Element: Current Procedure Title.

Functional Requirements: The computerized procedures system provides the current procedure title, procedure number, revision number and date, on the display, as shown in item 4 in Figure 18.9.8-2.

Display Element: Past and Future Procedure Steps.

Functional Requirements: The computerized procedures system provides for the display of two past procedure steps, as shown in item 5 in Figure 18.9.8-2. These are displayed in the form of high level statements of the steps. Included are an indication of whether the step involved is an initiated action or a continuously controlled parameter.

The computerized procedures system provides for the display of two future procedure steps, as shown in item 6 in Figure 18.9.8-2. These are displayed in a form identical to the paper version of the high-level statement of the procedure step.

The computerized procedures system provides scrolling capability to enable the user to view the previously executed steps. The past steps are displayed with the time associated with the completion of those steps.

The computerized procedures system provides scrolling capability to enable the user to view future steps.

Display Element: Procedure Transition Display.

Functional Requirements: The computerized procedures system provides for the display of a procedure transition map. This display indicates possible transitions out of or into the currently active procedure, as well as movements within the procedure.

The display shows the current procedure step and the path taken through the procedure up to the current time. This is accomplished by highlighting the current and past steps completed.

The display shows the entry point into the currently active procedure.

#### 18.9.8.6.6.4 Requirements of the Procedure Road Map Display

Display Element: Procedure Road Map Display.

Functional Requirements: The computerized procedures system provides for the display of a procedure road map display, which indicates the procedures that are active during the current transient or operation.

The procedure road map display shows the entry and exit points for the active procedures, including the cases where notes, cautions, foldout page items or the critical safety function status trees cause procedure transitions.

#### 18.9.8.6.6.5 Requirements of the Current Time and Date

Display Element: Time and Date Stamp.

Functional Requirements: The computerized procedure system (or the host computer system) provides a current clock time and date stamp on the display, as shown in item 7 in Figure 18.9.8-2. The time is in the form HOURS:MINUTES:SECONDS.

The date is in the form MONTH/DAY/YEAR.

~~18.9.8.6.6.6 Requirements of the Display of Parallel Processed Information~~

~~Display Element: Critical Safety Function Status Summary (for Emergency Operating Procedures).~~

~~Functional Requirements: The computerized procedures system provides a summary status of the critical safety function status trees, as shown on the display in item 8 in Figure 18.9.8-2. This summary is in the following form:~~

~~The critical safety function is in a horizontal bar graph form, arranged vertically from the highest priority function to the lowest priority function.~~

~~The letter designating the function is inside each bar.~~

~~The bars increase in width as the challenge to a function increases.~~

~~The bars change color as the challenge to a function increases, from GREEN to YELLOW to ORANGE to RED, with GREEN being satisfied, YELLOW not satisfied, ORANGE being a severe challenge, and RED being an extreme challenge.~~

~~Any time the status of the critical safety functions changes for the worse, a message indicating the state of the highest priority function displayed, such as RED BRANCH ON FUNCTION X, as in item 9 in Figure 18.9.8-2. Examples of such an occurrence are the following: the appearance of any YELLOW states, starting with the GREEN states; the appearance of any ORANGE state, starting with any combination of GREEN and YELLOW states; and the appearance of a higher priority RED state, starting with any combination of GREEN, YELLOW, and/or lower priority RED state. A full description of the priorities inherent in the critical safety functions are developed in the EOP development effort.~~

~~Any time the status of the critical safety functions changes for the worse, a message such as "CSF VIOLATION", (CSF Critical Safety Function) or equivalent, is displayed in the special alert indicator portion of the screen.~~

~~Display Element: Critical Safety Function Status Trees (for EOPs).~~

~~Functional Requirements: The computerized procedures system provides for the display of the critical safety function status trees. Curves that are part of the status trees are available for display, either integrated into the status tree display itself or as a separate display.~~

~~The displays of the critical safety function status trees are accessible by the user through the cursor control device.~~

~~The critical safety function status tree displays reflect actual plant conditions. The active branches of the trees are coded to indicate the current path through the trees.~~

The user is able to transition to the appropriate function restoration procedure by using the cursor control device to choose from a menu containing the procedures.

Display Element: Notes, Cautions, Precautions, Limitations, and Foldout Page Items.

Functional Requirements: The computerized procedures system provides for the display of relevant notes, cautions, precautions, limitations and foldout page items, as shown in item 9 in Figure 18.9.8-2. The displays function in the following manner:

On the first occurrence of a note or caution, the textual statement of the item appears in the area shown in item 9 in Figure 18.9.8-2, exactly as in the paper version of the procedures, along with component and parameter states. The statement disappears after the completion of the step associated with the note or caution.

Subsequent to the initial display of the note or caution (foldout page items are displayed only upon selection by the user), violations of notes, cautions, or foldout page items are displayed in the area shown in item 9 in Figure 18.9.8-2, in the format for components, parameters, states, and actions described earlier. In addition, an indication of the violation is displayed in the special alert indicator window of the screen, such as, "CAUTION VIOLATION".

In the event of more note, caution, or foldout page item violations than will physically fit in the allotted display space, the user is able to scroll to view the current violations. Also available for viewing are the currently active notes, cautions, and foldout page items, with the ones that are currently violated coded to be especially salient. The notes, cautions, and foldout page items that are not violated show their current states.

Display Element: Initiated Actions.

Functional Requirements: The computerized procedures system provides for the display of the indication of the noncompletion of actions that are initiated in a previous procedure step, in the area shown as item 9 in Figure 18.9.8-2.

The computerized procedures system provides for a display of the initiated actions. This list includes the current state of the initiated actions as well as the step associated with the action.

If an initiated action is not completed within a certain period of time or by a specified step, specified by the procedure builder, a message such as "INITIATED ACTION NOT COMPLETED", appears in the special alert indicator portion of the display.

Display Element: Continuously Controlled Parameters.

Functional Requirements: The computerized procedures system provides for the display of continuously controlled parameters moving out of their allowable range, in the area shown in item 9 of Figure 18.9.8-2. These are items that need to be monitored beyond the procedure step in which they appear, such as steam generator level.

The computerized procedures system provides for the display of a message such as "CONTINUOUSLY CONTROLLED PARAMETER OUTSIDE OF ALLOWABLE RANGE", in the special alert indicator portion (item 10) of Figure 18.9.8-2.

The computerized procedures system provides for a display of the current continuously controlled parameters used. This list includes the current state of the continuously controlled parameters as well as the step associated with the parameter. The list also includes the time at which the parameters are no longer in a continuously controlled mode or the time at which the parameters are outside their allowable range.

Display Element: Steps Not Completed.

Functional Requirements: The computerized procedures system provides for a display of steps not completed using a pop-up window. This list includes the procedure step number, the relevant component or parameter states, and the time at which the step was skipped.

**18.9.8.6.6.7 Requirements of the Display of Graphic Information**

Display Element: Existing Graphic Information.

Functional Requirements: The computerized procedures system provides for the access of previously defined graphic information, serving to complement the textual information provided by the system.

The access to the previously defined graphic information is through a pull-down menu, or equivalent, showing a list of the graphic displays relevant to a particular procedure step, note, caution, foldout page item, or critical safety function.

**18.9.8.6.6.8 Requirements of Accessing a Random Procedure**

Display Element: Menu of Procedures.

Functional Requirements: The computerized procedures system provides for the access of any procedure deemed appropriate by the user. The access to this "random" procedure is through a pull-down menu, or equivalent, showing a list of the procedures available to the user.

**18.9.8.6.6.9 Requirements of User Prompts**

Display Element: User Prompts.

Functional Requirements: When a procedure step is satisfied, the computerized procedures system prompts are:

CONTINUE TO STEP Y DISPLAY RNO COLUMN.

where Y is the next step to be completed. This is shown in the area indicated by item 11 in Figure 18.9.8-2.

The DISPLAY RNO COLUMN prompt gives the user the option to view the response not obtained (right-hand column) section of the procedures.

When there are multiple substeps to be completed, the prompts are:

CONTINUE WITH STEP X  DISPLAY RNO COLUMN.

where X is the current step.

When a step is not completed, the computerized procedures system prompts are:

CONTINUE WITH RNO  CONTINUE WITH STEP X.

CONTINUE WITH RNO enables the user to complete an RNO that has more than one layer. CONTINUE WITH STEP X allows the user to immediately go to the next substep. If the step has no remaining substeps, the prompt CONTINUE TO STEP Y replaces CONTINUE WITH STEP X.

Whenever the CONTINUE TO STEP Y prompt is used, the additional message THE STEP HAS NOT BEEN COMPLETED is be attached to the prompt if the step is not completed. This reminds the user that actions are necessary to satisfy the step. The user has the option of exiting the step.

The RETURN prompt is used to return to the procedure and step in effect.

When a procedure step or a Caution, Note, or Foldout Page item or a critical safety function requires a transition to another procedure, the computerized procedures system prompts are:

TRANSITION TO PROCEDURE X  "APPROPRIATE PROMPT"

where "APPROPRIATE PROMPT" is a continuation prompt that allows the user to bypass the transition.

When a procedure step or a caution, note, or foldout page item requires going to another step not immediately following the current step, the computerized procedures system prompts are:

GO TO STEP Y  "APPROPRIATE PROMPT"

where "APPROPRIATE PROMPT" is a continuation prompt that allows the user to bypass the go to.

When the user wishes to execute a previously executed past step or a future step, the computerized procedures system provides for the use of a pull-down menu, from which he may select whatever procedure step is selected.

When the user wishes to view a list of continuous, rolled parameters, initiated actions, overridden actions, notes, cautions, precautions, ons, foldout page items, or critical safety function violations, the computerized proced, s system provides a pull-down menu.

For parallel information, the prompts are:

CONTINUE TO NEXT PI CONTINUE WITH PROCEDURE STEP X

(PI Parallel Information) for cases where there are several violated items of parallel information. Note that PI is replaced by the actual item CAUTION, NOTE. CONTINUE WITH PROCEDURE STEP X allows the user to bypass the parallel information window and return to the procedure step execution. If there is only one violated piece of parallel information, only the CONTINUE WITH PROCEDURE STEP X prompt is present.

The RETURN, TRANSITION TO PROCEDURE X, and GO TO STEP Y prompts are used the same for the cases of parallel information as they are in the cases of procedure step execution.

### 18.9.8.63.73 Computerized Procedures Hardware Specification

The computerized procedures system is a software system. It runs on the hardware selected for the operations control centers. As long as memory, disk, and processing requirements are satisfactory, the system does not dictate specific hardware requirements.

### 18.9.8.63.834 Computerized Procedures Verification and Validation (V&V)

Verification is a process to demonstrate that the results of a given cycle phase fulfill the functional requirements. (Refer to the man machine interface system verification and validation plan described in Section 18.8.)

Validation is the process of evaluating software at the end of the software development process to demonstrate compliance with functional requirements.

An analysis of the requirements of the computer-based procedures system described in Reference 22 indicates that the system provides clear-cut advantages over a paper version of the procedures implementation. Explanatory material such as, for example, procedure purpose and entry conditions is available to the operator in a pop-up window. The use of the "road map" feature along with the "access procedures" option helps the operator execute multiple procedures, while keeping a record of where the operator left each procedure. The computer-based procedures system provides the capability for the operator to directly access a custom graphic display, thereby coordinating procedure use with plant graphical information.

Additional features and capabilities provide further help to the operator, as discussed in the computer-based procedures Reference [WCAP-14388 (Reference 22)].

Situation awareness is provided by the computer-based procedures system by, for example, the display of a summary status of the Critical Safety Functions, when applicable. Furthermore, displays of active Notes, Cautions and Foldout page items are available to the operator. These features provide high-level, supplementary information to the operator for the purpose of tracking the event or transient while following the sequential progression through the procedures.

The analysis of Reference 22 indicates that the computer-based procedures system effectively aids the operator in utilizing the guidance provided by the procedures. However, the verification and validation of the operating procedures within the AP600 scope on the AP600 simulator as a part of the validation of the integrated MMIS ensures that the computer-based procedures system meets its goals and that any unresolved human engineering issues are addressed. Reference 24, WCAP-14401, provides a programmatic level description of the AP600 human factors engineering V&V which includes computerized plant procedures.

### 18.9.8.4 Combined License Information Item

The Combined License applicant is responsible for developing administrative procedures to ensure that the computer-based procedures database is available only to authorized personnel.

~~18.9.8.6.9 Computerized Procedures Validation~~

~~Validation is the process of evaluating software at the end of the software development process to demonstrate compliance with functional requirements. (Refer to the man-machine interface system verification and validation plan described in Section 18.8.)~~

## 18.9.9 The AP600 Training Program

*The following activities, described or referenced below, are beyond the scope of design certification:*

- *Development and execution of the training program for the human factors engineering verification and validation test subjects*
- *The human factors engineering V&V*
- *Insights to the training program for operators, resulting from the human factors engineering V&V, for consideration by the Combined License applicant during their training program development.*

- ~~Cold shutdown~~
- ~~Refueling.~~

~~The staffing recommendations and operating philosophy are based on the human engineering design and implementation process described in Section 18.8 and the recommended operating staff qualifications described in Subsection 18.9.12.~~

### ~~18.9.14 Main Control Area Validation~~

~~The main control area validation is included as part of the validation of the integrated M-MIS discussed in Subsection 18.8.2.3.~~

### 18.9.~~15~~12 References

1. U.S. Nuclear Regulatory Commission 1979, "Human Factors Evaluation of Control Room Design and Operator Performance at TMI-2," NUREG/CR-1270 (Washington DC, United States Nuclear Regulatory Commission).

2. American Nuclear Standards Institute, 1980, "Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors," ANSI/ANS-4.5-1980, LaGrange Park, IL.

3. Rasmussen, J., 1986, "Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering" (New York, North-Holland).

4. U.S. Nuclear Regulatory Commission 1981B, "Guidelines for Control Room Design Reviews," NUREG-0700 (Washington, DC, United States Nuclear Regulatory Commission).

5. Smith, S. L. and Mosier, J. N., 1986, "Guidelines for Designing User Interface Software" (Bedford, MA, Mitre Corp.).

6. ISA 1979, "Annunciator Sequences and Specifications," ISA-S18.1 (Research Triangle Park, NC, Instrument Society of America).

7. EPRI Draft Report, "A Procedure for Reviewing and Improving Alarm Systems," MPR Associates, Apr. 1983, EPRI Project 2011, Interim Report.

8. U.S. Nuclear Regulatory Commission 1983, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Regulatory Guide 1.97, Revision 3 (Washington, DC, United States Nuclear Regulatory Commission).

9. Roth, E. M., Woods, D. D., and Pople, H. E., Jr., 1992 (in press), "Cognitive Simulation as a Tool for Cognitive Tasks Analysis" in Ergonomics, a special issue on Cognitive Engineering.

10. Lesgold, A. M., Lajoie, S., Eastman, R., Eggan, G., Gitomer, D., Glaser, R., Greenberg, L., Logan, D., Magone, M., Weiner, A., Wolf, R., and Yengo, L., 1986, "Cognitive Task Analysis to Enhance Technical Skills Training and Assessment," Technical Report (Pittsburgh, PA, Learning Research and Development Center).

11. Means, B., Mumaw, R., Roth, C., Schlager, M., McWilliams, E., Gagne, E., Rice, V., Rosenthal, D., and Heon, S., 1988, "ATC Training Analysis Study: Design of the Next-Generation ATC Training System," HII Technical Report (Alexandria, VA, HumRRO International, Inc.).

12. U.S. Nuclear Regulatory Commission 1982A, "Guidelines for the Preparation of Emergency Operating Procedures," NUREG-0899 (Washington, DC, United States Nuclear Regulatory Commission).

13. U.S. Nuclear Regulatory Commission 1980, "Clarification of TMI Action Plan Requirements," NUREG-0737 (Washington, DC, United States Nuclear Regulatory Commission).

14. U.S. Nuclear Regulatory Commission 1989B, "Lessons Learned from the Special Inspection Program for Emergency Operating Procedures," NUREG-1358 (Washington, DC, United States Nuclear Regulatory Commission).

15. Schneider, W. and Detweiler, M., 1988, "The Role of Practice in Dual-Task Performance: Toward Workload Modeling in a Connectionist/Control Architecture," in "Human Factors," 30, pages 539-566.

16. Gentner, D. and Stevens, A. L., CA, 1983, "Mental Models" (Hillsdale, NJ, Erlbaum).

17. Kieras, D. E. and Boviar, S., 1984, "The Role of a Mental Model in Learning to Operate a Device," in Cognitive Science, pages 255-273.

18. Collins, A., Brown, J. S., and Newman, S. E., 1989, "Cognitive Apprenticeship: Teaching the Crafts of Reading, Writing, and Mathematics," in "Knowing, Learning, and Instruction: Essays in Honor of Robert Glaser," L. Resnick (ed.), (Hillsdale, NJ, Erlbaum).

19. Schneider, W. and Shiffrin, R., 1977, "Controlled and Automatic Human Information Processing: I. Detection, Search, and Attention," in Psychological Review, 84, pages 1-66.

20. Mumaw, R. J. and Roth, E. M., 1992, "How to be More Devious with a Training Simulator: Redefining Scenarios to Emphasize Cognitively Difficult Situations, Simulation Multi-Conference: Nuclear Power Plant Simulation and Simulators," Orlando, FL, Apr. 6-9, 1992, STC Paper 92-1SJ4-VIRTU-P1 (Pittsburgh, PA, Westinghouse Electric Corp., Science and Technology Center).

21. Mumaw, R. J. Swaizler, D., Roth. E. M., & Thomas, W. A. (1994). "Cognitive Skill Training for Nuclear Power Plant Operational Decision Making," (NUREG/CR-6126). Washington, D. C.: Nuclear Regulatory Commission.

22. Functional Design of the AP600 Computerized Plant Procedures System, WCAP-14388 (Proprietary) [WCAP-14389 Nonproprietary], May 31, 1995.

23. AP600 Emergency Response Guidelines, GW-GJR-100, Rev. 0, May 31, 1995.

24. Programmatic Level Description of the AP600 Human Factors Engineering Verification and Validation Plan, WCAP-14401, April 13, 1995.

## LIST OF TABLES

Table 18.9.8-1 (Sheet 1 of 2)

**AP600 – E-0 REACTOR TRIP OR SAFETY INJECTION**

1. Verify Reactor Trip
   a. If Reactor Will Not Trip, Go To FR-S.1, Response to Nuclear Power Generation/ATWS
2. Verify Turbine Trip
3. Check If Safety Injection (SI) Is Actuated
   a. If SI not actuated, go to ES-0.1, Reactor Trip Response
4. Verify Feedwater (FW) Isolation
5. Verify Containment Isolation
6. Verify Core Make-up Tank (CMT) Actuated
7. Verify SI Valve Alignment
8. Check If Main Steam Lines Should Be Isolated
9. Check If PRHR Should Be Actuated
10. Check If ADS Should Be Actuated
11. Verify RCPs Tripped
12. Verify Passive Containment Cooling Not Required
13. Check RCS Average Temperature Stable Or Trending To No-Load
14. Check Power To AC Busses
15. Check SFW Pumps Running
16. Check Total SFW Flow – Greater Than Required Flow For Heat Sink
17. Check SFW Valve Alignment
18. Check CVS Makeup Pumps Running
19. Establish Charging Flow
20. Check CCS Pumps Running
21. Check CCS Valve Alignment
22. Check SW Pumps Running
23. Check SW Valve Alignment
24. Check Containment Fan Coolers
25. Check Chilled Water Pumps
26. Check Chilled Water Valve Alignment
27. Check If SGs Are Not Faulted
    a. If SGs Are Faulted, Go To E-2
28. Check If SG Tubes Are Not Ruptured
    a. If SG Tubes Are Ruptured, Go To E-3
29. Check If RCS Is Intact
    a. If RCS Is Not Intact, Go To E-1
30. Check If SI Flow Should Be Terminated
31. Go To ES-1.1, SI Termination, Step 1
32. Initiate Monitoring Of Critical Safety Function Status Trees

~~Table 18.9.8-1 (Sheet 2 of 2)~~

~~**AP600 E-0 REACTOR TRIP OR SAFETY INJECTION**~~

~~33. Check SG Levels~~
~~a. If Narrow Range Level Continues To Increase, Go To E-3~~
~~34. Check Secondary Radiation Normal~~
~~a. If Abnormal, Go To E-3~~
~~35. Check Auxiliary Building Radiation Normal~~
~~a. If Cause Of Radiation Is LOCA Outside Containment, Go To ECA-1.1~~
~~36. Check If DGs Should Be Stopped~~
~~37. Return To E-0, Step 25~~

~~Table 18.9.8-2~~

~~**AP600 - ES-0.0 REDIAGNOSIS**~~

~~1. Check If Any SG Is Not Faulted~~
~~2. Check If All SGs Are Not Faulted~~
~~3. Check If SG Tubes Are Ruptured~~
~~4. You Should Be In E-3 Or ECA-3 Series Guideline~~

~~Table 18.9.8-3~~

## ~~AP600 ES-0.1 REACTOR TRIP RESPONSE~~

~~1. Check RCS Temperature Stable At Or Trending To No-Load~~
~~2. Check FW Status~~
~~3. Check If PRHR Should Be Actuated~~
~~4. Verify All Control Rods Fully Inserted~~
~~5. Check PRZR Level Control~~
~~6. Check PRZR Pressure Control~~
~~7. Check SG Levels~~
~~8. Verify All AC Busses~~
~~9. Transfer Condenser Steam Dump To Pressure Control Mode~~
~~10. Check RCP Status~~
~~11. Check If Source Range Detectors Should Be Energized~~
~~12. Shut Down Unnecessary Plant Equipment~~
~~13. Maintain Stable Plant Conditions~~
~~14. Determine If Natural Circulation Cooldown Is Required~~

~~Table 18.9.8-4~~

## ~~AP600—ES-0.2 NATURAL CIRCULATION COOLDOWN~~

~~1. Try To Restart An RCP~~
~~2. Borate RCS To Cold Shutdown Boron Concentration~~
~~3. Verify Cold Shutdown RCS Boron Concentration By Sampling~~
~~4. Check RCS Makeup Control System~~
~~5. Verify All CRDM Fans Running~~
~~6. Initiate RCS Cooldown To Cold Shutdown~~
~~7. Check RCS Hot Leg Temperatures Less Than 550°F~~
~~8. Depressurize RCS To SI Block Permissive~~
~~9. Block SI Actuation~~
~~10. Maintain RCS Conditions~~
~~11. Monitor RCS Cooldown~~
~~12. Initiate RCS Depressurization~~
~~13. Continue RCS Cooldown And Depressurization~~
~~14. Check For Steam Void In Reactor Vessel~~
~~15. Check If Accumulators Should Be Locked Out~~
~~16. Maintain Letdown Flow~~
~~17. Check If RHR System Can Be Placed In Service~~
~~18. Continue RCS Cooldown To Cold Shutdown~~
~~19. Continue Cooldown Of Inactive Portion Of RCS~~
~~20. Determine If RCS Depressurization Is Permitted~~

~~Table 18.9.8-5~~

## ~~AP600 ES-0.3 NATURAL CIRCULATION COOLDOWN WITH VOID IN REACTOR VESSEL~~

1. ~~Try To Restart An RCP~~
2. ~~Establish PRZR Level To Accommodate Void Growth~~
3. ~~Decrease RCS Hot Leg Temperature To RHR Entry Temperature~~
4. ~~Depressurize RCS~~
   a. ~~Stop Depressurization On High PRZR Level OR RHR Entry Pressure~~
5. ~~Check PRZR Level Less Than High Value~~
   a. ~~If Level High, Reduce Level With Letdown~~
6. ~~Check If Accumulators Should Be Locked Out~~
7. ~~Check If RHR System Can Be Placed In Service~~
8. ~~Continue RCS Cooldown To Cold Shutdown~~
9. ~~Continue Cooldown Of Inactive Portion Of RCS~~
10. ~~Determine If RCS Depressurization Is Permitted~~

~~Table 18.9.8-6~~

## ~~AP600 – E-1 LOSS OF REACTOR OR SECONDARY COOLANT~~

~~1. Check If Any SGs Are Faulted~~
~~a. If Faulted Not Isolated, Go To E-2, Faulted Steam Generator Isolation~~
~~2. Control Intact SG Level~~
~~a. If Any Increasing In An Uncontrolled Manner, Go To E-3, Steam Generator Tube Rupture~~
~~3. Check Secondary Radiation~~
~~a. If Abnormal, Go To E-3, Steam Generator Tube Rupture~~
~~4. Control Charging Flow To Maintain CMT Level~~
~~5. Check If SI Mode Of Operation Can Be Terminated~~
~~a. Subcooling Exists~~
~~b. Heat Sink Exists~~
~~c. RCS Pressure Stable Or Increasing~~
~~d. CMT Level Stable Or Increasing~~
~~e. PRZR Level On Span~~
~~f. If Criteria Not Met, Go To Step 7~~
~~6. Transition To ES-1.1, SI Termination~~
~~7. Check If ADS Should Be Actuated~~
~~8. Check If Passive Containment Cooling Should Be Stopped~~
~~9. Check RCS And SG Pressures~~
~~a. All SGs Stable Or Increasing~~
~~b. RCS Stable Or Decreasing~~
~~c. If a And b Not Met, Return To Step 1~~
~~10. Begin Evaluating Plant Status~~
~~11. Should ES-1.2, Post-LOCA Cooldown And Depressurization Be Performed~~
~~a. If ADS Not Actuated, Go To ES-1.2, Post-LOCA Cooldown and Depressurization~~
~~12. Check If RHR Should Be Established~~
~~13. Check If Long-Term Cooling Established~~
~~14. Should Accumulators Be Isolated~~
~~15. Should Intact SGs Be Depressurized~~
~~16. Should Reactor Vessel Head Be Vented~~
~~17. Evaluate Long-Term Status~~

~~Table 18.9.8-7~~

## ~~AP600 ES-1.1 SI TERMINATION~~

~~1. Control Charging Flow To Maintain CMT And PRZR Level~~
~~2. Reset All SI Related Signals~~
~~3. Realign CMTs To Pre-SI Configuration~~
~~4. Verify SI Not Required~~
   ~~a. RCS Subcooling Exists~~
   ~~b. CMT Level Stable Or Increasing~~
   ~~c. PRZR Level Stable Or Increasing~~
   ~~d. If Required, Go To E-1, Loss of Reactor or Secondary Coolant~~
~~5. Realign Other Components To Pre-SI Configuration~~
   ~~a. PRHR Heat Exchanger~~
   ~~b. Other Components~~
~~6. Verify All Control Rods Fully Inserted~~
   ~~a. If Any Rods Stuck Out, Borate As Necessary~~
~~7. Check If Passive Containment Cooling Should Be Stopped~~
~~8. Transfer Condenser Dump To Pressure Control Mode~~
~~9. Stabilize RCS Temperature~~
~~10. Control PRZR Pressure~~
~~11. Control SG Levels~~
~~12. Verify AC Busses Energized By Offsite Power~~
~~13. Check If DGs Should Be Stopped~~
~~14. Re-establish CCS Cooling To RCPs~~
~~15. Restart RCPs~~
~~16. Check If Source Range Detectors Should Be Energized~~
~~17. Shut Down Unnecessary Plant Equipment~~
~~18. Maintain Stable Plant Conditions~~
   ~~a. RCS Pressure~~
   ~~b. RCS Temperature~~
   ~~c. PRZR Level~~
   ~~d. SG Level~~
~~19. Go To Appropriate Plant Procedure~~

~~Table 18.9.8-8~~

## ~~AP600 - ES-1.2 POST-LOCA COOLDOWN AND DEPRESSURIZATION~~

~~1. Verify AC Busses Energized By Offsite Power~~
~~2. Control Charging Flow To Maintain CMT Level~~
~~3. Control Intact SG Levels~~
~~4. Initiate RCS Cooldown At Maximum Plant Spec Rate~~
~~5. Place All PRZR Heaters In OFF Position~~
~~6. Depressurize RCS To Refill Pressurizer~~
~~7. Check CCS Cooling To RCPs~~
~~8. Should An RCP Be Started~~
~~a. If No Subcooling, Go To Step 10~~
~~b. If No Pressurizer Level, Return To Step 6~~
~~9. Depressurize RCS To Minimize RCS Subcooling~~
~~10. Verify ADS Actuation Not Necessary~~
~~11. Check Shutdown Margin~~
~~12. Should Accumulators Be Isolated~~
~~13. Should DGs Be Stopped~~
~~14. Should Source Range Detectors Be Energized~~
~~15. Stop Unnecessary Equipment~~
~~16. Should RCPs Be Stopped~~
~~— Normal RCP Operating Limits~~
~~17. Should RHR Be Placed In Service~~
~~— If Not, Go To Step 18~~
~~18. Is RCS At Cold Shutdown~~
~~— If Not, Return To Step 2~~
~~19. Evaluate Long Term Status~~

~~Table 18.9.8-9~~

~~**AP600 - E-2 FAULTED STEAM GENERATOR ISOLATION**~~

~~1. Check Main Steam Line Isolation And Bypass Valves Of Affected SG(s) Closed~~
~~2. Check If Any SG Is Not Faulted~~
~~3. Identify Faulted SG~~
~~4. Isolate Faulted SG~~
~~5. Check SFW Water Supply~~
~~6. Check Secondary Radiation~~
~~7. Go To E-1, Loss of Reactor or Secondary Coolant~~

Table 18.9.8-10 (Sheet 1 of 2)

## AP600 – E-3 STEAM GENERATOR TUBE RUPTURE

1. Identify Ruptured SG
2. Isolate Flow From Ruptured SG
3. Maintain Ruptured SG Level Above U-Tubes
4. Control Charging Flow To Maintain CMT Level
5. Check If SGs Are Not Faulted
6. Control Intact SG Level
7. Verify AC Power Energized By Offsite Power
8. Check Cooldown Rate Should Be Maximized But Not Exceed Plant Spec Limit
   a. Ruptured SG Pressure Decreasing
   b. Low RCS Subcooling
   c. CMT Level Decreasing
9. Initiate RCS Cooldown To Cold Shutdown
10. Depressurize RCS To Refill Pressurizer
11. Verify ADS Actuation Not Necessary
12. Check CCW Cooling To RCPs
13. Should An RCP Be Started
    a. If No Subcooling, Go To Step 14
    b. If No Pressurizer Level, Return To Step 10
14. Depressurize RCS To Stop Primary-To-Secondary Break Flow
15. Control RCS And Ruptured SG Pressure To Minimize Primary-To-Secondary Leakage
16. Should DGs Be Stopped
17. Check If Passive Containment Cooling Should Be Stopped
18. Minimize Secondary System Contamination
19. Operate Pressurizer Heaters To Saturate Pressurizer
20. Check Shutdown Margin
21. Should Accumulators Be Isolated
22. Should Source Range Detectors Be Energized
23. Stop Unnecessary Equipment
24. Depressurize RCS And Ruptured SG
    a. Depressurize RCS Using Normal Spray, Auxiliary Spray, Or One ADS Valve In That Order
    b. Depressurize Ruptured SG Using Either Backfill, Blowdown, Or Steaming
25. Maintain Ruptured SG Level Above Top Of U-Tubes
26. Should RCPs Be Stopped
    a. Normal RCP Operating Limits

~~Table 18.9.8-10 (Sheet 2 of 2)~~

~~**AP600 - E-3 STEAM GENERATOR TUBE RUPTURE**~~

~~27. Should RHR Be Placed In Service~~
~~a. If Not, Go To Step 9~~
~~28. Is RCS At Cold Shutdown~~
~~a. If Not, Return To Step 9~~
~~29. Evaluate Long-Term Status~~

Table 18.9.8-11

## AP600 ECA 0.0 LOSS OF ALL AC POWER SOURCES

1. Verify Reactor Trip
2. Verify Turbine Trip
3. Verify PRHR In Service
4. Check If SI Should Be Actuated
5. Verify RCS Isolated
6. Try To Restore AC Power
7. Check If Main Steam Line Isolation And Bypass Valves Should Be Closed
8. Verify SG Blowdown Valves Closed
9. Check If SG Tubes Are Not Ruptured
10. Check If ADS Is Required
11. Check DC Bus Loads
12. Determine If RCS Cooldown Is Required
13. Check SI Signal Status
14. Verify Containment Isolation
15. Verify Containment Ventilation Isolation
16. Check If Passive Containment Cooling Is Required
17. Check Containment Radiation
18. Check If AC Power Restored
    a. If Not, Return To Step 3
19. Stabilize SG Pressures
20. Load Necessary Equipment On AC Busses
21. Determine Appropriate Recovery Guideline
    a. If SI Signal Exists, Go To E-1, Loss Of Reactor Or Secondary Coolant
    b. If SI Signal Does Not Exist, Go To ES-0.1, Reactor Trip Response

~~Table 18.9.8-12~~

~~**AP600 - ECA 1.1 LOCA OUTSIDE CONTAINMENT**~~

~~1. Try To Identify And Isolate Break~~
~~2. Check If Break Is Isolated~~
~~a. If Not Isolated, Start Making More Borated Water For Charging Pumps~~
~~3. Go To E-1, Loss Of Reactor or Secondary Coolant~~

Table 18.9.8-13

## AP600 – ECA-2.1 UNCONTROLLED DEPRESSURIZATION OF ALL STEAM GENERATORS

1. Check Secondary Pressure Boundary
2. Determine If Both SGs Should Be Isolated
3. Control Feed Flow To Minimize RCS Cooldown
4. Check Secondary Radiation Normal
   a. If Not, Go To E-3, Steam Generator Tube Rupture
5. Control Charging Flow To Maintain CMT And PRZR Level
6. Check If ADS Should Be Actuated
7. Check If Passive Containment Cooling Should Be Stopped
8. Check If Accumulators Should Be Isolated
9. Check RCS Hot Leg Temperatures Stable Or Decreasing
10. Check Narrow Range Level In All SGs Less Than 50%
11. Control Pressurizer Pressure
12. Verify AC Busses Energized By Offsite Power
13. Check CCW Cooling To RCPs
14. Check If An RCP Should Be Started
15. Check If Source Range Detectors Should Be Energized
16. Check If DGs Should Be Stopped
17. Shut Down Unnecessary Plant Equipment
18. Maintain Plant Conditions Stable
19. Verify ADS Actuation Not Necessary
20. Check If Accumulators Should Be Isolated
21. Check If RCS Hot Leg Temperatures Less Than RHR Cut-in Temperature
22. Check If RCS Pressure Less Than RHR Cut-in Pressure
23. Check If RHR Can Be Placed In Service
24. Continue Cooldown To Cold Shutdown
25. Check RCS Temperatures Less Than Cold Shutdown
26. Evaluate Long-Term Plant Status

~~Table 18.9.8-14~~

## ~~AP600 – F-0.1 SUBCRITICALITY~~

~~1. Go To FR-S.1 On RED Path If:~~
~~a. Power Range Less Than 5% – NO~~
~~2. Go To FR-S.1 On ORANGE Path If:~~
~~a. Power Range Less Than 5% – YES~~
~~b. Intermediate Range SUR Zero Or Negative – NO~~
~~3. Go To FR-S.2 On YELLOW Path If:~~
~~a. Power Range Less Than 5% – YES~~
~~b. Intermediate Range SUR Zero Or Negative – YES~~
~~c. Source Range Energized – NO~~
~~d. Intermediate Range SUR More Negative Than -0.2 DPM – NO~~
~~4. GREEN Path If:~~
~~a. Power Range Less Than 5% – YES~~
~~b. Intermediate Range SUR Zero Or Negative – YES~~
~~c. Source Range Energized – NO~~
~~d. Intermediate Range SUR More Negative Than -0.2 DPM – YES~~
~~5. Go To FR-S.2 On YELLOW Path If:~~
~~a. Power Range Less Than 5% – YES~~
~~b. Intermediate Range SUR Zero Or Negative – YES~~
~~c. Source Range Energized – YES~~
~~d. Source Range SUR Zero Or Negative – NO~~
~~6. GREEN Path If:~~
~~a. Power Range Less Than 5% – YES~~
~~b. Intermediate Range SUR Zero Or Negative – YES~~
~~c. Source Range Energized – YES~~
~~d. Source Range SUR Zero Or Negative – YES~~

~~Table 18.9.8-15~~

## ~~AP600 – F-0.2 CORE COOLING~~

~~1. Go To FR-C.1 On RED Path If:~~
~~a. Core Exit TCs Less Than 1200°F – NO~~
~~2. Go To FR-C.2 On ORANGE Path If:~~
~~a. Core Exit TCs Less Than 1200°F – YES~~
~~b. RCS Subcooling Based On Core Exit TCs Greater Than Predetermined Value – NO~~
~~c. Core Exit TCs Less Than Predetermined Value – NO~~
~~3. Go To FR-C.3 On YELLOW Path If:~~
~~a. Core Exit TCs Less Than 1200°F – YES~~
~~b. RCS Subcooling Based On Core Exit TCs Greater Than Predetermined Value – NO~~
~~c. Core Exit TCs Less Than Predetermined Value – YES~~
~~4. GREEN Path If:~~
~~a. Core Exit TCs Less Than 1200°F – YES~~
~~b. RCS Subcooling Based On Core Exit TCs Greater Than Predetermined Value – YES~~

Table 18.9.8-16 (Sheet 1 of 2)

**AP600 – F-0.3 HEAT SINK**

1. Go To FR-H.1 On RED Path If:
   a. Narrow Range Level In At Least One SG Greater Than On Span – NO
   b. Total Feed Flow To SGs Greater Than Predetermined Value – NO
   c. PRHR Flow Greater Than Predetermined Value – NO
2. Go To FR-H.2 On YELLOW Path If:
   a. One Of The Following:
      1. Narrow Range Level In At Least One SG Greater Than On Span – YES; Or
      2. Total Feed Flow To SGs Greater Than Predetermined Value – YES; Or
      3. PRHR Flow Greater Than Predetermined Value – YES
   b. Pressure In All SGs Less Than Highest Safety Valve Setpoint – NO
3. Go To FR-H.2 On YELLOW Path If:
   a. One Of The Following:
      1. Narrow Range Level In At Least One SG Greater Than On Span – YES; Or
      2. Total Feed Flow To SGs Greater Than Predetermined Value – YES; Or
      3. PRHR Flow Greater Than Predetermined Value – YES
   b. Pressure In All SGs Less Than Highest Safety Valve Setpoint – YES
   c. Narrow Range Level In All SGs Less Than Top Of Span – NO
4. Go To FR-H.2 On YELLOW Path If:
   a. One Of The Following:
      1. Narrow Range Level In At Least One SG Greater Than On Span – YES; Or
      2. Total Feed Flow To SGs Greater Than Predetermined Value – YES; Or
      3. PRHR Flow Greater Than Predetermined Value – YES
   b. Pressure In All SGs Less Than Highest Safety Valve Setpoint – YES
   c. Narrow Range Level In All SGs Less Than Top Of Span – YES
   d. Pressure In All SGs Less Than Lowest Safety Valve Setpoint – NO
5. Go To FR-H.2 On YELLOW Path If:
   a. One Of The Following:
      1. Narrow Range Level In At Least One SG Greater Than On Span – YES; Or
      2. Total Feed Flow To SGs Greater Than Predetermined Value – YES; Or
      3. PRHR Flow Greater Than Predetermined Value – YES
   b. Pressure In All SGs Less Than Highest Safety Valve Setpoint – YES
   c. Narrow Range Level In All SGs Less Than Top Of Span – YES
   d. Pressure In All SGs Less Than Lowest Safety Valve Setpoint – YES
   e. Narrow Range Level In All SGs Greater Than On Span – NO

Table 18.9.8-16 (Sheet 2 of 2)

**AP600 – F-0.3 HEAT SINK**

6. GREEN Path If:
   a. One Of The Following:
      1. Narrow Range Level In At Least One SG Greater Than On Span – YES; Or
      2. Total Feed Flow To SGs Greater Than Predetermined Value – YES; Or
      3. PRHR Flow Greater Than Predetermined Value – YES
   b. Pressure In All SGs Less Than Highest Safety Valve Setpoint – YES
   c. Narrow Range Level In All SGs Less Than Top Of Span – YES
   d. Pressure In All SGs Less Than Lowest Safety Valve Setpoint – YES
   e. Narrow Range Level In All SGs Greater Than On Span – YES

Table 18.9.8-17

**AP600 - F-0.4 INTEGRITY**

1. Go To FR-P.1 On RED Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - NO
   b. All RCS Pressure-Cold Leg Temperature Points To Right Of Limit-A Curve - NO
2. Go To FR-P.1 On ORANGE Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - NO
   b. All RCS Pressure-Cold Leg Temperature Points To Right Of Limit-A Curve - YES
   c. All RCS Cold Leg Temperatures Greater Than T1 - NO
3. Go To FR-P.2 On YELLOW Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - NO
   b. All RCS Pressure-Cold Leg Temperature Points To Right Of Limit-A Curve - YES
   c. All RCS Cold Leg Temperatures Greater Than T1 - YES
   d. All RCS Cold Leg Temperatures Greater Than T2 - NO
4. GREEN Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - NO
   b. All RCS Pressure-Cold Leg Temperature Points To Right Of Limit-A Curve - YES
   c. All RCS Cold Leg Temperatures Greater Than T1 - YES
   d. All RCS Cold Leg Temperatures Greater Than T2 - YES
5. Go To FR-P.1 On ORANGE Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - YES
   b. RCS Temperature Greater Than Cold Overpressure Cut-in Temperature - NO
   c. RCS Pressure Less Than Cold Overpressure Limit - NO
   d. All RCS Cold Leg Temperatures Greater Than T1 - NO
6. Go To FR-P.2 On YELLOW Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - YES
   b. RCS Temperature Greater Than Cold Overpressure Cut-in Temperature - NO
   c. RCS Pressure Less Than Cold Overpressure Limit - NO
   d. All RCS Cold Leg Temperatures Greater Than T1 - YES
7. GREEN Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - YES
   b. RCS Temperature Greater Than Cold Overpressure Cut-in Temperature - NO
   c. RCS Pressure Less Than Cold Overpressure Limit - YES
8. GREEN Path If:
   a. Temperature Decrease In All RCS Cold Legs Less Than Plant Spec Limit - YES
   b. RCS Temperature Greater Than Cold Overpressure Cut-in Temperature - YES

Table 18.9.8-18

## AP600 – F-0.5 CONTAINMENT

1. Go To FR-Z.1 On RED Path If:
   a. Containment Pressure Less Than Design Limit – NO
2. Go To FR-Z.1 On ORANGE Path If:
   a. Containment Pressure Less Than Design Limit – YES
   b. Containment Pressure Less Than Setpoint – NO
3. Go To FR-Z.2 On ORANGE Path If:
   a. Containment Pressure Less Than Design Limit – YES
   b. Containment Pressure Less Than Setpoint – YES
   c. Containment Sump Level Less Than Flooding Level – NO
4. Go To FR-Z.3 On YELLOW Path If:
   a. Containment Pressure Less Than Design Limit – YES
   b. Containment Pressure Less Than Setpoint – YES
   c. Containment Sump Level Less Than Flooding Level – YES
   d. Containment Radiation Less Than Predetermined Value – NO
5. GREEN Path If:
   a. Containment Pressure Less Than Design Limit – YES
   b. Containment Pressure Less Than Setpoint – YES
   c. Containment Sump Level Less Than Flooding Level – YES
   d. Containment Radiation Less Than Predetermined Value – YES

~~Table 18.9.8-19~~

~~**AP600 – F-0.6 INVENTORY**~~

~~1. Go To FR-I.3 On YELLOW Path If:~~
~~a. Pressurizer Level Less Than Top Of Span – NO~~
~~b. Pressurizer Level Behavior Indicates Upper Head Void – YES~~
~~2. Go To FR-I.1 On YELLOW Path If:~~
~~a. Pressurizer Level Less Than Top Of Span – NO~~
~~b. Pressurizer Level Behavior Indicates Upper Head Void – NO~~
~~3. Go To FR-I.2 On YELLOW Path If:~~
~~a. Pressurizer Level Less Than Top Of Span – YES~~
~~b. Pressurizer Level Greater Than On Span – NO~~
~~4. Go To FR-I.3 On YELLOW Path If:~~
~~a. Pressurizer Level Less Than Top Of Span – YES~~
~~b. Pressurizer Level Greater Than On Span – YES~~
~~c. Pressurizer Level Behavior Indicates Upper Head Void – YES~~
~~5. GREEN Path If:~~
~~a. Pressurizer Level Less Than Top Of Span – YES~~
~~b. Pressurizer Level Greater Than On Span – YES~~
~~c. Pressurizer Level Behavior Indicates Upper Head Void – NO~~

~~Table 18.9.8-20~~

## ~~AP600 FR S.1 RESPONSE TO NUCLEAR POWER GENERATION/ATWS~~

~~1. Verify Reactor Trip~~
~~2. Verify Turbine Trip~~
~~3. Verify PRHR Actuated~~
~~4. Initiate Emergency Boration Of RCS~~
~~5. Verify SFW Pumps Running~~
~~6. Check If The Following Trips Have Occurred~~
~~a. Reactor Trip~~
~~b. Turbine Trip~~
~~7. Check SG Levels~~
~~8. Verify All Dilution Paths Isolated~~
~~9. Check If Reactivity Insertion Is From An Uncontrolled Cooldown~~
~~a. If Not, Go To Step 13~~
~~10. Check Main Steam Line Isolation And Bypass Valves Closed~~
~~11. Identify Faulted SGs~~
~~12. Isolate Faulted SGs~~
~~13. Verify Reactor Subcritical~~
~~14. Return To Guideline And Step In Effect~~

~~Table 18.9.8-21~~

## ~~AP600 FR S.2 RESPONSE TO LOSS OF CORE SHUTDOWN~~

~~1. Check Intermediate Range Flux~~
~~2. Check Source Range Channel Startup Rate~~
~~3. Return To Guideline And Step In Effect~~

~~Table 18.9.8-22~~

## ~~AP600 FR-C.1 RESPONSE TO INADEQUATE CORE COOLING~~

~~1. Check SI Valve Alignment~~
~~2. Establish Charging Flow~~
~~3. Check SI Accumulator Isolation Valve Status~~
~~4. Check If ADS Should Be Manually Actuated~~
~~5. Check Core Exit TCs Less Than 1200°F~~
~~a. If Not, Go To Step 6~~
~~b. If Less Than 1200°F, Return To Guideline And Step In Effect~~
~~6. Check RCP Support Conditions~~
~~7. Check Containment Hydrogen~~
~~8. Check Intact SG Levels~~
~~9. Check RCS Vent Paths Closed~~
~~10. Depressurize All Intact SGs To Inject Accumulators~~
~~a. If Not, Use PRHR~~
~~11. Check If Accumulators Should Be Isolated~~
~~12. Stop All RCPs~~
~~13. Depressurize All Intact SGs To Atmospheric Pressure~~
~~14. Check If Core Cooling Re-established~~
~~a. If Not, Go To Step 15~~
~~15. Go To E-1, Loss Of Reactor Or Secondary Coolant~~
~~16. Check If RCPs Should Be Started~~
~~17. Continue To Try To Depressurize All Intact SGs~~
~~18. Check If Accumulators Should Be Isolated~~
~~19. Check If Core Cooling Re-established~~
~~a. If Not, Return To Step 15~~
~~20. Go To E-1, Loss Of Reactor Or Secondary Coolant~~

Table 18.9.8-23

**AP600 FR C.2 RESPONSE TO DEGRADED CORE COOLING**

1. Check CMT Valve Alignment
2. Establish Charging Flow
3. Check RCS Vent Paths Closed
4. Check Core Exit TCs Less Than Predetermined Value
   a. If Not, Go To Step 5
   b. If Less Than Predetermined Value, Return To Guideline And Step In Effect
5. Check If One RCP Should Be Stopped
6. Check Core Cooling
   a. If Adequate, Return To Guideline And Step In Effect
7. Check SI Accumulator Isolation Valve Status
8. Check Intact SG Levels
9. Depressurize All Intact SGs To Inject Accumulators
   a. If Not, Use PRHR
10. Check If Accumulators Should Be Isolated
11. Stop All RCPs
12. Depressurize All Intact SGs To Atmospheric Pressure
13. Check If Core Cooling Re-established
    a. If Not, Return To Step 8
14. Go To E-1, Loss Of Reactor Or Secondary Coolant

~~Table 18.9.8-24~~

## ~~AP600 FR-C.3 RESPONSE TO SATURATED CORE COOLING~~

~~1. Check RHR System Not Placed In Service~~
~~2. Check CMT Valve Alignment~~
~~3. Establish Charging Flow~~
~~4. Check RCS Vent Paths Closed~~
~~5. Return To Guideline And Step In Effect~~

Table 18.9.8-25

**AP600 - FR-H.1 RESPONSE TO LOSS OF HEAT SINK**

1. Check If PRHR Is Required
   a. If Not Required, Return To Guideline And Step In Effect
2. Verify PRHR Actuated
3. Check If Secondary Heat Sink Is Required
   a. If Not Required, Return To Guideline And Step In Effect
4. Try To Establish SFW Flow To At Least One SG
5. Check If Heat Sink Is Restored
   a. If PRHR Actuated OR SFW Flow Restored To At Least One SG, Return To Guideline And Step In Effect
6. Stop All RCPs
7. Try To Establish Main FW Flow To At Least One SG
8. Check SG Levels
   a. If SG NR Level Restored In At Least One SG, Return To Guideline And Step In Effect
9. Try To Establish Feed Flow From Condensate System
10. Check SG Levels
    a. If SG NR Level Restored In At Least One SG, Return To Guideline And Step In Effect
11. Check For Loss Of Heat Sink
    a. If Heat Sink Is Not Lost, Return To Step 1
12. Actuate ADS
13. Go To E-1, Loss of Reactor or Secondary Coolant

Table 18.9.8-26

**AP600 - FR H.2 RESPONSE TO STEAM GENERATOR OVERPRESSURE**

1. Identify Affected SGs
2. Verify FW Isolation To Affected SG
3. Check Affected SG Narrow Range Level Less Than Full
4. Try To Dump Steam From Affected SG
5. Check Affected SG Pressure
6. Isolate AFW To Affected SGs
7. Isolate All FW To Affected SG
8. Check RCS Hot Leg Temperatures
9. Continue Attempts To Manually Or Locally Dump Steam From Affected SGs
10. Return To Guideline And Step In Effect

~~Table 18.9.8-27~~

~~**AP600 FR H.3 RESPONSE TO STEAM GENERATOR HIGH LEVEL**~~

~~1. Identify Affected SG~~
~~2. Verify FW Isolation~~
~~3. Isolate AFW To Affected SGs~~
~~4. Check Affected SG Level~~
~~5. Close Affected SG Main Steam Line Isolation And Bypass Valves~~
~~6. Check Affected SG Radiation Normal~~
~~a. If Not, Go To E-3, Steam Generator Tube Rupture~~
~~7. Establish Blowdown From Affected SGs~~
~~8. Return To Guideline And Step In Effect~~

~~Table 18.9.8-28~~

## ~~AP600 FR H.4 RESPONSE TO LOSS OF NORMAL STEAM RELEASE CAPABILITIES~~

~~1. Try To Restore Normal Steam Release Capability Of Affected SGs~~
~~2. Check SG Pressure Less Than Safety Valve Setpoint~~
~~3. Return To Guideline And Step In Effect~~

~~Table 18.9.8-29~~

## ~~AP600 - FR-H.5 RESPONSE TO STEAM GENERATOR LOW LEVEL~~

1. ~~Identify Affected SG~~
2. ~~Verify Blowdown Isolation Valves From Affected SGs Closed~~
3. ~~Check If Affected SGs Not Faulted~~
   a. ~~If Faulted, Go To E-2, Faulted Steam Generator Isolation~~
4. ~~Check FW Flow To Affected SGs Greater Than Predetermined Value~~
5. ~~Continue To Fill Affected SG~~
6. ~~Return To Guideline And Step In Effect~~

~~Table 18.9.8-30~~

## ~~AP600 FR P.1 RESPONSE TO IMMINENT PRESSURIZED THERMAL SHOCK CONDITION~~

~~1. Check RCS Cold Leg Temperatures Stable Or Increasing~~
~~a. If Not, Try To Stop Cooldown~~
~~2. Check RCS Hot Leg Temperature Stable~~
~~3. Check If Accumulators Should Be Isolated~~
~~4. Depressurize RCS To Decrease Subcooling~~
~~5. Check Pressurizer Level Not High~~
~~a. If High, Reestablish Letdown To Reduce Level~~
~~6. Check If Subcooling Has Been Reduced~~
~~a. If Not Return To Step 4~~
~~7. Control RCS Pressure~~
~~8. Determine If Temperature Soak Is Required~~
~~9. Return To Guideline And Step In Effect~~

~~Table 18.9.8-31~~

~~**AP600 – FR-P.2 RESPONSE TO ANTICIPATED PRESSURIZED THERMAL SHOCK CONDITION**~~

~~1. Check RCS Cold Leg Temperatures Stable Or Increasing~~
~~a. If Not, Try To Stop Cooldown~~
~~2. Check RCS Pressure Within Plant Spec Limits~~
~~a. If Not, Depressurize RCS To Within Plant Spec Limits~~
~~3. Determine If Additional Cooldown Restrictions Are Required~~
~~4. Return To Guideline And Step In Effect~~

~~Table 18.9.8-32~~

## ~~AP600 FR-Z.1 RESPONSE TO HIGH CONTAINMENT PRESSURE~~

~~1. Verify Containment Isolation~~
~~2. Verify Containment Ventilation Isolation~~
~~3. Check if Passive Containment Cooling Is Required~~
~~4. Verify Main Steam lines Isolated~~
~~5. Check If Feed Flow Should Be Isolated To Any SG~~
~~6. Check Hydrogen Concentration~~
~~7. Check If Hydrogen Concentration Should Be Reduced~~
~~a. If Hydrogen Concentration Low, Go To Step 9~~
~~8. Notify Plant Engineering Staff Of Hydrogen Concentration~~
~~9. Return To Guideline And Step In Effect~~

~~Table 18.9.8-33~~

## ~~AP600 FR Z.2 RESPONSE TO CONTAINMENT FLOODING~~

~~1. Try To Identify Unexpected Source Of Water To Sump~~
~~2. Check Containment Sump Activity Level~~
~~3. Notify Plant Staff Of Sump Level And Activity Level To Obtain Recommended Action~~
~~4. Return To Guideline And Step In Effect~~

~~Table 18.9.8-34~~

~~**AP600 FR-Z.3 RESPONSE TO HIGH CONTAINMENT RADIATION LEVEL**~~

~~1. Verify Containment Ventilation Isolation~~
~~2. Check If SI Signal Should Be Actuated~~
~~3. Notify Plant Engineering Staff To Obtain Recommended Action~~
~~4. Return To Guideline And Step In Effect~~

~~Table 18.9.8-35~~

## ~~AP600 FR I.1 RESPONSE TO HIGH PRESSURIZER LEVEL~~

~~1. Check If Charging Flow Has Been Established~~
~~2. Establish Letdown~~
~~3. Turn On Heaters~~
~~4. Check Pressurizer and Auxiliary Spray Valves Closed~~
~~5. Control Charging And Letdown Flow As Necessary To Maintain Stable RCS Pressure~~
~~6. Check Pressurizer Pressure Less Than High Value~~
~~a. If Not, Return To Step 4~~
~~7. Return To Guideline And Step In Effect~~

~~Table 18.9.8-36~~

## ~~AP600 FR-I.2 RESPONSE TO LOW PRESSURIZER LEVEL~~

~~1. Verify Letdown Isolated~~
~~2. Increase Charging Flow To Establish Pressurizer Level~~
~~3. Check Pressurizer Level On Span~~
~~a. If Not, Increase Charging Flow And Return To Step 2~~
~~b. If Charging Flow At Maximum, Initiate SI And Go To E-1, Loss of Reactor Or Secondary Coolant~~
~~4. Operate Pressurizer Heaters As Necessary~~
~~5. Return To Guideline And Step In Effect~~

~~Table 18.9.8-37~~

## ~~AP600 - FR-I.3 RESPONSE TO VOIDS IN REACTOR VESSEL~~

~~1. Check If Charging Flow Has Been Established~~
~~2. Check If Letdown In Service~~
~~3. Establish Stable RCS Conditions~~
~~4. Check All RCPs Stopped~~
~~5. Check If RCS Pressure Should Be Increased~~
~~6. Control Charging And Letdown To Maintain Pressurizer Level~~
~~7. Determine If Reactor Vessel Is Full~~
~~a. If Full, Return To Guideline And Step In Effect~~
~~8. Try To Start One RCP~~
~~9. Determine If Reactor Vessel Is Full~~
~~a. If Full, Return To Guideline And Step In Effect~~
~~10. Obtain Containment Hydrogen Concentration Measurement~~
~~11. Record RCS Pressure~~
~~12. Establish Desired RCS Conditions~~
~~13. Prepare Containment For Reactor Vessel Venting~~
~~14. Determine Maximum Allowable Reactor Vessel Venting Time~~
~~15. Review Reactor Vessel Venting Termination Criteria~~
~~16. Vent Reactor Vessel~~
~~17. Determine If Reactor Vessel Is Full~~
~~a. If Not, Return To Step 14~~
~~18. Check Pressurizer Level Stable~~
~~19. Return To Guideline And Step In Effect~~