



57-001

GE Nuclear Energy

ABWR

Date 5/15/92

Fax No. —

To

Clare Goodman

This page plus 17 page(s)

From

Jack Fox

Mail Code —

175 Curtner Avenue
San Jose, CA 95125

Phone (408) 925- 4824

FAX (408) 925-1193
or (408) 925-1687

Subject ABWR SSAR Chapter 18

Message A new Subsection 18.4.3 has
been added per your request.
Subsection 18.4.1 has been
modified accordingly. All other
portions are unchanged.

Daso
1/1

CHAPTER 18

TABLE OF CONTENTS

18.1 INTRODUCTION

18.2 DESIGN GOALS AND DESIGN BASES

18.3 PLANNING, DEVELOPMENT AND DESIGN

18.3.1 Introduction

18.3.2 Standard Design Features

18.3.3 Inventory of Controls and Instrumentation

18.3.4 Detailed Design Implementation Process

18.4 CONTROL ROOM STANDARD DESIGN FEATURES

18.4.1 Introduction

18.4.2 Standard Design Features

18.4.2.1 Listing of Features

18.4.2.2 Main Control Console

18.4.2.3 Process Computer Driven VDUs

18.4.2.4 Process Computer Independent VDUs

18.4.2.5 Dedicated Function Switches

18.4.2.6 Automation Design

18.4.2.6.1 Automatic Operation

18.4.2.6.2 Semi-Automated Operation

18.4.2.6.3 Manual Operation

TABLE OF CONTENTS

(Continued)

18.4.2.7	Large Display Panel
18.4.2.8	Fixed-Position Display
18.4.2.9	Large Variable Display
18.4.2.10	Supervisors' Console
18.4.2.11	Safety Parameter Display System
18.4.2.12	Fixed-Position Alarms
18.4.2.13	Alarm Processing Logic
18.4.2.14	Equipment Alarms
18.4.2.15	Control Room Arrangement
18.4.3	Control Room MMI Technology
18.5	REMOTE SHUTDOWN SYSTEM
18.6	SYSTEMS INTEGRATION
18.6.1	Safety Systems
18.6.2	Non-Safety Systems
18.7	DETAILED DESIGN OF THE OPERATOR INTERFACE SYSTEM

18.1 INTRODUCTION

This chapter describes the ABWR man-machine interface system (MMIS) design goals and bases, the standard MMIS design features and the detailed MMIS design and implementation process, with embedded design acceptance criteria, for the ABWR standard plant operator interface. The inventory of instrumentation and controls needed by the control room staff for the performance of emergency operating procedures is also described. The incorporation of human factors engineering principles into all phases of the design of these interfaces is provided for as described in this chapter.

Design goals and design bases for the instrumentation and control systems and operator interfaces in the main control room and in remote locations are established in Section 18.2. The overall design and implementation approach is described in Section 18.3. Section 18.4 contains a description of the main control room standard operator interface design features. The remote shutdown system is described in Section 18.5. Section 18.6 discusses how the systems which make up the operator interface are integrated together and with the other systems of the plant. Section 18.7 discusses the detailed design implementation process. The ABWR Emergency Procedure Guidelines, which provide the basis for a human factors evaluation of emergency operations, are contained in Appendix 18A. Appendix 18B discusses the differences between the ABWR emergency procedure guidelines and the U.S. BWROG Emergency Procedure Guidelines, Revision 4. Appendix 18C presents a characterization of a main control room operator interface equipment implementation that incorporates the ABWR standard design features discussed in Section 18.4. The input data and results of calculations performed during the preparation of the ABWR Emergency Procedure Guidelines are contained in Appendix 18D. A general description of the design and implementation process for the ABWR operator interface and supporting plant systems is presented in Appendix 18E. Appendix 18F contains the results of an analysis of information and control needs of the main control room operators during emergency operations.

18.2 DESIGN GOALS AND DESIGN BASES

The primary goal for operator interface designs is to facilitate safe, efficient and reliable operator performance during all phases of normal plant operation, abnormal events and accident conditions. To achieve this goal, information displays, controls and other interface devices in the control room and other plant areas are designed and shall be implemented in a manner consistent with good human factors engineering practices. Further, the following specific design bases are adopted:

- (1) During all phases of normal plant operation, abnormal events and emergency conditions, the ABWR shall be operable by two reactor operators. In addition, the operating crew will include one assistant control room shift supervisor, one control room shift supervisor, and two or more auxiliary equipment operators. During accidents, assistance is available to the operating crew from personnel in the Technical Support Center. Four licensed operators shall be on shift at all times, consistent with the staffing requirements of 10CFR50.54m.
- (2) Promote efficient and reliable operation through expanded application of automated operation capabilities.
- (3) The operator interface design shall utilize only proven technology.

- (4) Safety-related systems monitoring displays and control capability shall be provided in full compliance with pertinent regulations regarding divisional separation and independence.
- (5) The operator interface design shall be highly reliable and provide functional redundancy such that sufficient displays and control will be available in the main control room and remote locations to conduct an orderly reactor shutdown and to cool the reactor to cold shutdown conditions, even during design basis equipment failures.
- (6) The principle functions of the Safety Parameter Display System (SPDS) as required by Supplement 1 to NUREG-0737, will be integrated into the operator interface design.
- (7) Accepted human factors engineering principles shall be utilized for the operator interface design in meeting the relevant requirements of General Design Criterion 19, and
- (8) The design bases for the Remote Shutdown System shall be as specified in Section 7.4.

18.3 PLANNING, DEVELOPMENT AND DESIGN

18.3.1 Introduction: An integrated program plan to incorporate human factors engineering principles and to achieve an integrated design of the control and instrumentation systems and operator interfaces of the ABWR was prepared and implemented. The program plan presents formal decision analysis procedures to facilitate selection of design features which satisfy top level requirements and goals of individual systems and the overall plant. Also included is a comprehensive, synergistic design approach with provisions for task analyses and human factors evaluations.

Specific procedures developed as parts of the implementation of the program plan are:

- (a) Implementation Procedure for Development of System Functional and Performance Requirements
- (b) Implementation Procedure for Analysis of Tasks and Allocation of Functions,
- (c) Implementation Procedure for Evaluation of Human Factors and Man-Machine Interfaces,
- (d) Implementation Procedure for the Design of Hardware and Software, and
- (e) Implementation Procedure for the Verification and Validation of Hardware and Software.

The program plan and the associated procedures provided guidance for the conduct of the ABWR control and instrumentation and man-machine interface system design development activities including:

- (a) Definition of the standard design features of the control room MMIS (see Subsections 18.3.2 and 18.4.2).
- (b) Definition of the inventory of controls and instrumentation necessary for the control room crew to follow the operation strategies given in the ABWR Emergency Procedure Guidelines and to complete the important operator actions described in the Probabilistic Risk Assessment (see Subsection 18.3.3 and Appendix 18F).

In addition, the program and associated procedures will be transmitted to the team responsible for the definition of the detailed process by which the control room man-machine interface and control and instrumentation systems are implemented; this process includes provisions for NRC conformance reviews where the process or equipment-specific design will be tested against specific acceptance criteria and is discussed further in Subsection 18.3.4, Section 18.7 and Appendix 18E).

18.3.2 Standard Design Features

The ABWR control room man-machine interface design contains a group of standard or basic features which form the foundation for the detailed MMIS design. These features are described in Subsection 18.4.2.

The development of the control room MMIS standard design features was accomplished through consideration of existing control room operating experience; a review of trends in control room design and existing control room data presentation methods; evaluation of new MMI technologies, alarm reduction and presentation methods, and validation testing of two full-scale prototypes. The prototypes were evaluated using test scenarios especially developed for the purpose and utilizing experienced nuclear plant control room operators. Following the completion of the prototype tests and employing their results, the basic control room MMIS standard design features were finalized.

18.3.3 Inventory of Controls and Instrumentation

The ABWR Emergency Procedure Guidelines (EPGs), presented in Appendix 18A, and the important operator actions identified in the Probabilistic Risk Assessment (PRA), presented in Chapter 19, provided the bases for an analysis of the information and control capability needs of the main control room operators based upon the operation strategies. This analysis defines a minimum set of fixed displays and a minimum set of controls which will enable the operating crew to perform the actions that would be specified in the emergency operating procedures. Appendix 18F contains the tabulated results of this analysis. Tables 18F-1 through 18F-11 in Appendix 18F contain detailed descriptions of the steps of the EPGs and the information, alarms and controls needed by the operators to perform and validate the completion of those steps. Table 18F-12 contains the same type of information for the important operator actions identified in the PRA.

Another set of three tables in Appendix 18F provide convenient summaries of the control, display and alarm listings developed in the previous tables. These latter tables are numbered 18F-13.1, 2 and 3, respectively. The listings in Tables 18F-13.1 through 3 are an inventory of the controls, displays and alarms which define the minimum control, information and alarm requirements on any ABWR control room design implementation.

18.3.4 Detailed Design Implementation Process

The process by which the detailed equipment design implementation of the ABWR control and instrumentation and man-machine interface will be completed is discussed in Section 18.7 and in Appendix 18E. This process builds upon the standard MMIS design features which are discussed in Subsection 18.4.2. Embedded in the process, which is illustrated in Figure 18E.1-1, are a number of NRC conformance reviews in which various aspects and outputs of the process are evaluated against the established acceptance criteria which are presented in Tables 18E.2-1 through 18E.2-x.

18.4 CONTROL ROOM STANDARD DESIGN FEATURES

18.4.1 Introduction

This section presents, in Subsection 18.4.2, the standard design features of the operator interface in the control room. These basic design features are based upon proven technologies and have been demonstrated, through broad scope control room dynamic simulation tests and evaluation, to satisfy the ABWR operator interface design goals and design bases as given in Section 18.2. The specific technologies utilized in the main control room operator interface are listed in Subsection 18.4.3. Appendix 18C presents an example of a control room operator interface design implementation which incorporates these design features. Validation of the implemented main control room design will include evaluation of the standard design features and will be performed as part of the design implementation process as defined by the acceptance criteria presented in Tables 18E.2-1 through 18E.2-4.

18.4.2 Standard Design Feature Descriptions

18.4.2.1 Listing of Features

The ABWR control room operator interface design incorporates the following standard features:

- (a) A single, integrated control console staffed by two operators; the console has a low profile such that the operators can see over the console from a seated position.
- (b) The use of plant process computer system driven on-screen control video display units (VDUs) for safety system monitoring and non-safety system control and monitoring.
- (c) The use of a separate set of on-screen control VDUs for safety system control and monitoring and separate on-screen control VDUs for non-safety system control and monitoring; the operation of these two sets of VDUs is entirely independent of the process computer system. Further, the first set of VDUs and all equipment associated with their functions of safety system control and monitoring are divisionally separate and qualified to Class 1-E standards.
- (d) The use of dedicated function switches on the control console.
- (e) Operator selectable automation of pre-defined plant operation sequences.
- (f) The incorporation of an operator's selectable semi-automated mode of plant operations, which provide procedural guidance on the control console VDUs.
- (g) The capability to conduct these all plant operations in an operator manual mode.
- (h) The incorporation of a large display panel which presents information for use by the entire control room operating staff.
- (i) The inclusion on the large display panel of fixed-position displays of key plant parameters and major equipment status.

- (j) The inclusion in the fixed-position displays of both 1E-qualified and non-1E display elements.
- (k) The independence of the fixed-position displays from the plant process computer.
- (l) The inclusion within the large display panel of a large video display unit which is driven by the plant process computer system.
- (m) The incorporation of a "monitoring only" supervisor's console which includes VDUs on which display formats available to the operators on the main control console are also available to the supervisors.
- (n) The incorporation of the safety parameter display system (SPDS) function as part of the plant status summary information which is continuously displayed on the fixed-position displays on the large display panel.
- (o) The use of fixed-position alarm tiles on the large display panel.
- (p) The application of alarm processing logic to prioritize alarm indications and to filter unnecessary alarms.
- (q) A spatial arrangement between the large display panel, the main control console and the shift supervisors' console which allows the entire control room operating crew to conveniently view the information presented on the large display panel.
- (r) The use of VDUs to provide alarm information in addition to the alarm information provided via the fixed-position alarm tiles on the large display panel.

The remainder of this subsection provides further descriptions of these standard design features.

18.4.2.2 Main Control Console

The main control console comprises the work stations for the two control room plant operators. It is configured such that each operator is provided with controls and monitoring information necessary to perform their assigned tasks and allows the operators to view all of the displays on the large display panel (see Subsection 18.4.2.7) from a seated position.

The main control console, in concert with the large display panel, provides the controls and displays required to operate the plant during normal plant operations, abnormal events and emergencies. These main control console controls and displays include the following:

- (1) On-screen control VDUs for safety system monitoring and non-safety system control and monitoring which are driven by the plant process computer system (see Subsection 18.4.2.8).
- (2) A separate set of on-screen control VDUs for safety system control and monitoring and separate on-screen control VDUs for non-safety system control and monitoring; the operation of these two sets of VDUs is entirely independent of the process computer system. Further, the first set of VDUs and all equipment associated with their functions of safety system control and monitoring are divisionally separate and qualified to Class 1E standards (see Subsection 18.4.2.4).

(8) Dedicated function switches (see Subsection 18.4.2.5).

The main control console is also equipped with a limited set of dedicated displays for selected functions (e.g., the standby liquid control system and the synchronization of the main generator to the electrical grid).

In addition to the above equipment, the main control console is equipped with both intra-plant and external communications equipment and a laydown space is provided for hard copies of procedures and other documents required by the operators during the performance of their duties.

18.4.2.3 Process Computer Driven VDUs

A set of on-screen control VDUs is incorporated into the main control console design to support the following activities:

- (1) monitoring of plant systems, both safety and non-safety related,
- (2) control of non-safety system components,
- (3) presentation of system and equipment alarm information.

This set of VDUs is driven by the plant process computer system. Thus, data collected by the process computer is available for monitoring on these VDUs. All available display formats can be displayed on any of these VDUs.

18.4.2.4 Process Computer Independent VDUs

A set of VDUs which are independent of the process computer are also installed on the main control console. These VDUs are each driven by independent processors. They are divided into two subsets:

The first subset consists of those VDUs which are dedicated, divisionally separated devices. The VDUs in this group can only be used for monitoring and control of equipment within a given safety division. The VDUs are qualified, along with their supporting display processing equipment, to Class 1E standards.

The second subset of process computer independent VDUs are used for monitoring and control of non-safety plant systems. The VDUs in this subset are not qualified to Class 1E equipment standards.

18.4.2.5 Dedicated Function Switches

Dedicated function switches are installed on the main control console. These devices provide faster access and feedback compared to that obtainable with soft controls. These dedicated switches are implemented in hardware, so that they are located in a fixed-position and are dedicated in the sense that each individual switch is used only for a single function, or two very closely related functions (e.g., valve open/close).

The dedicated function switches on the main control console are used to support such functions as initiation of automated sequences of safety and non-safety system operations, manual scram and reactor operating mode changes.

18.4.2.6 Automation Design

The ABWR incorporates selected automation of the operations required during a normal plant startup/shutdown and during normal power range maneuvers.

Subsection 7.7.1.5 describes the power generation control system (PGCS) which is the primary ABWR system for providing the automation features for normal ABWR plant operations.

18.4.2.6.1 Automatic Operation: When placed in automatic mode, the PGCS performs sequences of automated plant operations by sending mode change commands and setpoint changes to lower-level, non-safety related plant system controllers. The PGCS cannot directly change the status of a safety-related system. When a change in the status of a safety-related system is required to complete the selected operation sequence, the PGCS provides prompts to guide the operator in manually performing the change using the appropriate safety-related operator interface controls provided on the main control console.

The operator can stop an automatic operation at any time. The PGCS logic also monitors plant status, and will automatically revert to manual operating mode when a major change in plant status occurs (e.g., reactor scram or turbine trip). When such abnormal plant conditions occur, PGCS automatic operation is suspended and the logic in the individual plant systems and equipment directs the automatic response to the plant conditions. Similarly, in the event that the operational status of the PGCS or interfacing systems changes (e.g., equipment failures), operation reverts to manual operating mode. When conditions permit, the operator may manually re-initiate PGCS automatic operation.

18.4.2.6.2 Semi-Automated Operation. The PGCS also includes a semi-automatic operational mode which provides automatic operator guidance for accomplishing the desired normal changes in plant status; however, in this mode, the PGCS performs no control actions. The operator must activate all necessary system and equipment controls for the semi-automatic sequence to proceed. The PGCS monitors the plant status during the semi-automatic mode in order to check the progression of the semi-automatic sequence and to determine the appropriate operator guidance to be activated.

18.4.2.6.3 Manual Operation: The manual mode of operation in the ABWR corresponds to the manual operations of conventional BWR designs in which the operator determines and executes the appropriate plant control actions without the benefit of computer-based operator aids. The manual mode provides a default operating mode in the event of an abnormal condition in the plant. The operator can completely stop an automated operation at any time by simply selecting the manual operating mode. The PGCS logic will also automatically revert to manual mode when abnormal conditions occur.

18.4.2.7 Large Display Panel

The large display panel provides information on overall plant status with real-time data during all phases of plant operation. The information on the large display panel can be viewed from the main control console and the supervisors' console. The large display panel includes fixed-position displays (see Subsection 18.4.2.8), a variable display (see Subsection 18.4.2.9) and spatially dedicated alarm windows (see Subsection 18.4.2.12).

18.4.2.8 Fixed Position Display

The fixed-position portion of the large display panel provides key plant information for viewing by the entire control room staff. The dynamic display elements of the fixed-position displays are driven by dedicated microprocessor-based controllers which are independent of the plant process computer system.

Those portions of the large display panel which present safety-related information are qualified to Class 1E standards.

The information presented in the fixed-position displays includes the critical plant parameter information, as defined by the SPDS requirements of NUREG-0737, Supplement 1, and the Type A post-accident monitoring (PAM) instrumentation required by Regulation Guide 1.97, Revision 3 (refer to Section 18.4.2.11 for a discussion of the SPDS and to Section 7.5 for a discussion of the PAM variables).

18.4.2.9 Large Variable Display

The large variable display which is included on the large display panel is a VDU which is driven by the plant process computer system. Any screen format resident in the process computer system can be shown on this large variable display.

18.4.2.10 Supervisors' Console

A console is provided for the control room supervisors which is equipped with VDUs on which any screen format resident in the process computer system and available to the operators at the main control console is also available to the shift supervisor. The location of this console in the control room is discussed in Subsection 18.4.2.15.

18.4.2.11 SPDS

NUREG-0737 provided guidance for implementing Three Mile Island (TMI) action items. NUREG-0737, Supplement 1, clarifies the TMI action items related to emergency response capability, including item I.D.2, "Safety Parameter Display System" (SPDS). The principal purpose of the the SPDS is to aid control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to prevent core damage. During emergencies, the SPDS serves as an aid in evaluating the current safety status of the plant, in executing symptom-based emergency operating procedures, and in monitoring the impact of engineered safeguards or mitigation activities. The SPDS also operates during normal operation, continuously displaying information from which the plant safety status can be readily and reliably assessed. The ABWR does not provide a separate SPDS, but rather, the principal functions of the SPDS (as required by NUREG-0737, Supplement 1) are integrated into the overall control room display capabilities. Displays of critical plant variables sufficient to provide information to plant operators about the following critical safety functions are provided on the large display panel as an integral part of the fixed-position displays:

- (1) Reactivity control.
- (2) Reactor core cooling and heat removal from the primary system.
- (3) Reactor coolant system integrity.
- (4) Radioactivity control, and
- (5) Containment conditions.

Displays to assist the plant operator in execution of symptom-based emergency operating procedures are available at the main control console VDUs. Examples of these VDU displays are trend plots and operator guidance. Information regarding entry conditions to the symptomatic emergency procedures is provided through the fixed-position display of the critical plant parameters on the large display panel. The critical plant parameters on the large display panel are also viewable from the control room supervisors' monitoring station. The supplemental SPDS displays on the VDUs on the main control console are also accessible at the control room supervisors' monitoring station and may be provided in the technical support center (TSC) and, optionally, in the emergency operations facility (EOF), which are the responsibility of the applicant referencing the ABWR design to provide.

Entry conditions to the symptomatic EOPs are annunciated on the dedicated hardware alarm windows on the large display panel. The large display panel also displays the containment isolation status, safety systems status, and the following critical parameters:

- (1) RPV pressure.
- (2) RPV water level.
- (3) Core neutron flux (startup range and power range instruments).
- (4) Suppression pool temperature.
- (5) Suppression pool water level.
- (6) Drywell temperature.
- (7) Drywell pressure.
- (8) Drywell water level.
- (9) Control rod scram status.
- (10) Primary containment oxygen concentration.
- (11) Primary containment hydrogen concentration (when monitors are in operation).
- (12) Containment radiation levels.
- (13) Secondary containment differential pressure.
- (14) Secondary containment area temperatures.
- (15) Secondary containment HVAC cooler differential temperature.
- (16) Secondary containment HVAC exhaust radiation level.
- (17) Secondary containment area radiation levels, and
- (18) Secondary containment floor drain sump water level.

The oxygen monitoring instrumentation system is normally in continuous operation and hence the large display panel also includes continuous fixed-position display of wetwell and drywell oxygen concentrations. The hydrogen monitoring instrumentation is automatically started on a LOCA signal and hence continuous display is not required. Additional post accident monitoring parameters, such as effluent stack radioactivity release (Refer to Section 7.5 for a list of post accident monitoring parameters), may be displayed at the large variable display or at the main control console VDUs on demand by the operator.

The SPDS is required to be designed so that the displayed information can be readily perceived and comprehended by the control room operating crew. Compliance with this requirement is

assured because of the incorporation of accepted human factors engineering principles into the overall control room design implementation process (Refer to Subsection 18.7 for a discussion of the design implementation process).

All of the continuously displayed information necessary to satisfy the requirements for the SPDS, as defined in NUREG-0737, Supplement 1, is included in the fixed-position displays listed in Table 18F-13.1. Table 18F-13.1 also includes other displays, beyond those required for the SPDS.

18.4.2.12 Fixed-Position Alarms

Fixed-position alarm tiles on the large display panel announce the key, plant-level alarm conditions that potentially affect plant availability or plant safety, or indicate the need of immediate operator action.

18.4.2.13 Alarm Processing Logic

Alarm prioritizing and filtering logic is employed in the ABWR design to enhance the presentation of meaningful alarm information to the operator and reduce the amount of information which the operators must absorb and process during abnormal events.

Alarm prioritizing is accomplished in the ABWR through the designation of three categories of alarm signals. The first of these is the important alarms. These are defined as those alarms which notify the operators of changes in plant status regarding safety and include those items which are to be checked in the event of accidents, principle events or transients. The important alarms are displayed on the fixed-position tiles discussed in Subsection 18.4.2.12.

The second category is the system-specific alarms which are provided to notify the operators of system-level abnormalities or non-normal system statuses. Examples of these are:

- (a) main pump trips caused by system process, power sources or control abnormalities,
- (b) valve closures in cooling or supply lines,
- (c) decreases in supply process values,
- (d) loss of a backup system,
- (e) system isolation,
- (f) safety systems are being bypassed,
- (g) systems are undergoing testing

The system-specific alarms are also shown on the fixed-position tiles discussed in Subsection 18.4.2.12.

Equipment alarms make up the third category of alarms in the prioritizing scheme and are discussed in Subsection 18.4.2.14.

Alarm suppression in the ABWR is based upon the following concepts:

- (1) Suppression based on the operating mode. The plant operating mode is defined on the basis of the hardware or process status, and alarms which are not relevant to the current operating mode are suppressed. For example, alarms which are needed in the "RUN" mode but are unnecessary in the "SHUTDOWN" mode are suppressed.
- (2) Suppression of subsidiary alarms. Alarms are suppressed if they are logically consequent to the state of operation of the hardware or to the process status. For example, scram initiation (a plant-level alarm condition announced with a fixed-position alarm tile on the large display panel) will logically lead to an FMCRD hydraulic control unit scram accumulator low pressure (also an alarm condition). Such subsidiary alarms are suppressed if they simply signify logical consequences of the systems operation.
- (3) Suppression of redundant alarms. When there are overlapping alarms, such as "high" and "high-high" or "low" and "low-low", only the more severe of the conditions is alarmed and the others are suppressed.

Operators may activate or deactivate the alarm suppression logic at any time.

18.4.2.14 Equipment Alarms

Alarms which are not indicated by fixed-position alarm tiles on the large display panel (i.e., those alarms of nominally lower level importance such as those related to specific equipment status) are displayed to the control room operating staff via the main control console VDUs. The supplemental alarm indications and supporting information regarding the plant-level alarms which are presented on the large display panel are also presented on the VDUs.

18.4.2.15 Control Room Arrangement

In the ABWR main control room arrangement, the main control console is located directly in front of the large display panel for optimum viewing efficiency by the plant operators seated at the main console. The shift supervisor's console is also placed in front of the large display panel, but at a somewhat greater distance than the main control console. The shift supervisor is, thus, in a position behind the control console operators. This arrangement allows all control room personnel to view the contents of the large panel displays.

18.4.3 Control Room MMI Technology

The ABWR main control room standard design features described in Subsection 18.4.2 include equipment which utilizes a variety of technologies to control and monitor the plant processes. This subsection provides a summary listing and description of the technologies which are utilized to support personnel execution of these control and monitoring functions. For this purpose, the term "technology" is taken to have the following definition:

"the equipment, including both hardware and software, employed to directly accomplish the functions of control and monitoring of the plant processes".

Hardware such as consoles, panels, cabinets, control room lighting and HVAC and plant communication equipment which has a supporting role but is not directly involved in the control and monitoring processes is excluded.

The scope of this section is limited to the main control room and the remote shutdown station areas of the plant and includes all human-system-interface (HSI) equipment technologies which may be applied, regardless of use in prior designs.

1. Hardware switches such as multi-position rotary, push-button, rocker, toggle and pull-to-lock types.
2. Soft switch, the functions of which may be changed through the execution of software functions.
3. Continuous adjustment controls, such as rotary controls and thumbwheels.
4. Visual display units with full color screens, including large reverse projection screens, cathode ray tubes and flat panel display screens.
5. On-screen control utilized with the cathode ray tubes and flat panel display devices.
6. VDU screen formats such as large screen optical projection display formats, text displays, including menus and tabular information and graphical displays including Trend Plots, 2-D Plots, P & IDs and other diagrams and pictorial information.
7. Analog Meters which employ a hardware medium to pictorially or graphically present quantitative and qualitative information concerning plant process parameters. This includes analog meters using digitally controlled LEDs and digital readouts.
8. Fixed-Position Digital Displays which present alphanumeric information in a hardware medium. These can be back-lit.
9. Fixed-position hardware mimic displays which schematically represent plant systems and components and their relationships utilizing pictorial elements, labels and indicator lights.
10. Fixed-Position alarm tiles which use light to indicate the alarm state.
11. An Audio Signal system which is coordinated to the fixed-position alarm tiles and utilizes prioritization and alarm reduction logic and pre-defined set points to alert operators to plant status changes.

12. Printers and Printer/Plotters used to provide hard copy output in the form of plots, logs and text.
13. Keyboards which are composed of alphanumeric and/or assignable function keys and function as computer input devices.

18.5 REMOTE SHUTDOWN SYSTEM

The remote shutdown system (RSS) provides a means to safely shutdown the plant from outside the main control room. It provides control of the plant systems needed to bring the plant to hot shutdown, with the subsequent capability to attain cold shutdown, in the event that the control room becomes uninhabitable.

The RSS system design is described in Subsections 7.4.1.4 and 7.4.2.4. All of the controls and instrumentation required for RSS operation are identified in Subsection 7.4.1.4.4 and in Figure 7.4-2.

The RSS uses conventional, hardwired controls and indicators to maintain diversity from the main control room. These dedicated devices are arranged in a mimic of the interfacing systems process loops.

18.6 SYSTEMS INTEGRATION

18.6.1 Safety Systems

The operator interfaces with the safety-related systems through dedicated hardware switches for system initiation and logic reset; hardware switches for system mode changes; safety related VDUs for individual safety equipment control, status display and monitoring; non-safety VDUs for additional safety system monitoring and the large fixed-position display for plant overview information. Instrumentation and control aspects of the microprocessor-based safety systems and logic control (SSLC) are described in Appendix 7A.

Divisional separation for control, alarm and display equipment is maintained. The SSLC processors provide alarms signals to their respective safety-related alarm processors and provide display information to the divisionally dedicated VDUs. The SSLC microprocessors communicate with their respective divisional VDU controllers through the essential multiplexing system (EMUX). The divisional VDUs have on-screen control capability.

Divisional isolation devices are provided between the safety-related systems and non-safety related communication networks so that failures in the non-safety related equipment will have no impact on the ability of the safety systems to perform their design functions. The non-safety-related communication network is part of the non-essential multiplex system (NEMS) described in Subsection 7.7.1.9.

Operation controls through dedicated hardware switches and master sequential switches communicate with the SSLC logic units through conventional hardwire signal transmission (i.e., not multiplexed). Communications between the SSLC logic units and alarm panels and the safety-related fixed-position displays is through multiplex data links.

Safety system process parameters, alarms and system status information from the SSLC are communicated to the NEMS through isolation devices for use by other equipment connected to the communication network. Selected operator control functions are performed through dedicated hardware control switches which are I-E qualified and divisionally separated on the main control console. These hardware switches communicate with the safety-related systems logic units through hardwire transmission lines.

The divisionally dedicated VDUs are classified as safety-related equipment. These VDUs provide control and display capabilities for individual safety systems if control of a system component is required. Normally, such control actions are performed for equipment surveillance purposes only, as the normal method of system control is through the mode-oriented master sequence switches.

18.6.2 Non-Safety Systems

For non-safety systems, operation control is accomplished using master sequence switches, on-screen control via the non-safety VDUs. The hardware switches for non-safety equipment on the main control console communicate with the non-safety related systems logic units through hardwire transmission lines.

The non-safety systems communicate with other equipment in the operator interface through the NEMS network. The non-safety related portion of the large display panel fixed-position displays is driven by a controller separate from the process computer system. Alarm processing microprocessor units separate from the process computer perform alarm filtering and suppression and also drive dedicated alarm tiles on the large display panel. The alarms for emergency conditions into the symptomatic emergency operating procedures are provided by the alarm processing units, both safety and non-safety related. Equipment level alarm information is presented by the process computer on the main control console VDUs.

An additional set of non-safety related on-screen control VDUs are provided on the main control console for control and display of non-safety systems. These VDUs are independent of the process computer system. In the unlikely event of loss of the process computer system, these independent VDUs, in conjunction with the large display panel safety-related displays, have sufficient information and control capability to allow the following operations to be performed:

- (1) steady-state power operation,
- (2) power decrease,
- (3) plant shutdown to hot standby conditions, and
- (4) plant shutdown to cold shutdown conditions.

Without the plant process computer system, control is carried out through the master sequential switches and the process computer-independent, on-screen control VDUs. Monitoring is accomplished with the independent VDUs and the fixed-position display on the large display panel. Power increases cannot be performed in the absence of the process computer system because core thermal margin limit information provided by the process computer to the automatic thermal limit monitor (described in Subsection 7.7.2.2) would not be available.

18.7 DETAILED DESIGN OF THE OPERATOR INTERFACE SYSTEM

The standard design features of the ABWR main control room MMIS, discussed in Subsection 18.4.2, provide the framework for the detailed equipment hardware and software designs that will be developed following a design and implementation process such as that typically described in Appendix 18E. This typical design and implementation process is presented in flow chart form in Figure 18E.1-1 and described in more detail in Table 18E.1-2.

As part of the Appendix 18E discussion of typical man-machine interface systems (MMIS) design and implementation activities, detailed acceptance criteria are specified that shall be used to govern and direct all ABWR MMIS design implementations which reference the Certified Design. These detailed acceptance criteria, presented in Section 18E.2 of Appendix 18E, encompass the set of necessary and sufficient design implementation related activities required to maintain the implemented MMIS design in compliance with accepted human factors principles and accepted digital electronics equipment and software development methods.

As part of the detailed design implementation process described in Appendix 18E, operator task analyses will be performed as a basis for evaluating details of the design implementation and MMIS requirements will be specified. These MMIS requirements will include the instrumentation and controls listed in Tables 18F-13.1 through 3 as a subset. The evaluation of the integrated control room design will include the confirmation of the ABWR main control room standard design features.