ADVANCED LIGHT WATER REACTOR REQUIREMENTS DOCUMENT

CHAPTER 10 - MAN-MACHINE INTERFACE SYSTEMS

Prepared For
Electric Power Research Institute
Palo Alto, California

Revision 0, Issued October 1989

LEGAL NOTICE

This report was prepared by the organizations named below as an account of work sponsored by the Electric Power Research Institute, Inc. (EPRI). Neither EPRI, members of EPRI, the organizations named below, nor any person acting on behalf of any of them: (a) makes any warranty, express or implied, with respect to the use of any information, apparatus, method, or process disclosed in this report or that such use may not infringe privately owned rights; or (b) assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

Prepared by:

Combustion Engineering, Inc.
Windsor, Connecticut

Duke Power Company
Charlotte, North Carolina

General Electric Company
San Jose, California

MPR Associates, Inc.
Washington, DC

S. Levy Incorporated
Campbell, California

Science Applications International Corporation
Los Altos, California

Westinghouse Electric Corporation
Monroeville, Pennsylvania

P. Wyckoff, Consultant
Hayward, California

Dr. R. Kinkade, H. F. Consultant
San Diego, California

W. Esselman, Consultant
Mountain View, California

Electric Power Research Institute
Palo Alto, California

LIST OF CHAPTERS IN THE ALWR REQUIREMENTS DOCUMENT

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 10: MAN-MACHINE INTERFACE SYSTEMS

Paragraph No. *Requirement* *Rev.*

1 INTRODUCTION 0

This chapter establishes requirements for instrumentation and control systems for ALWR plants. These requirements are consistent with the principles and objectives of the ALWR program. These systems, which perform the monitoring, control, and protection functions, are referred to as Man-Machine Interface Systems (M-MIS). 0

Each M-MIS is comprised to some degree of the following functions: 0

- Data gathering equipment which monitors equipment and process variables; 0
- Data communication equipment which transmits equipment and process variables between data processing equipment and plant equipment; 0
- Data processing equipment which manipulates data for use by plant operations personnel and/or automatic protection and control equipment; 0
- Plant information display and control equipment which provides alarm and display media for plant personnel to access plant processes and equipment status, and controls to operate plant equipment; 0
- Output processing equipment which provides the necessary interfaces between plant controls and plant equipment actuators. 0

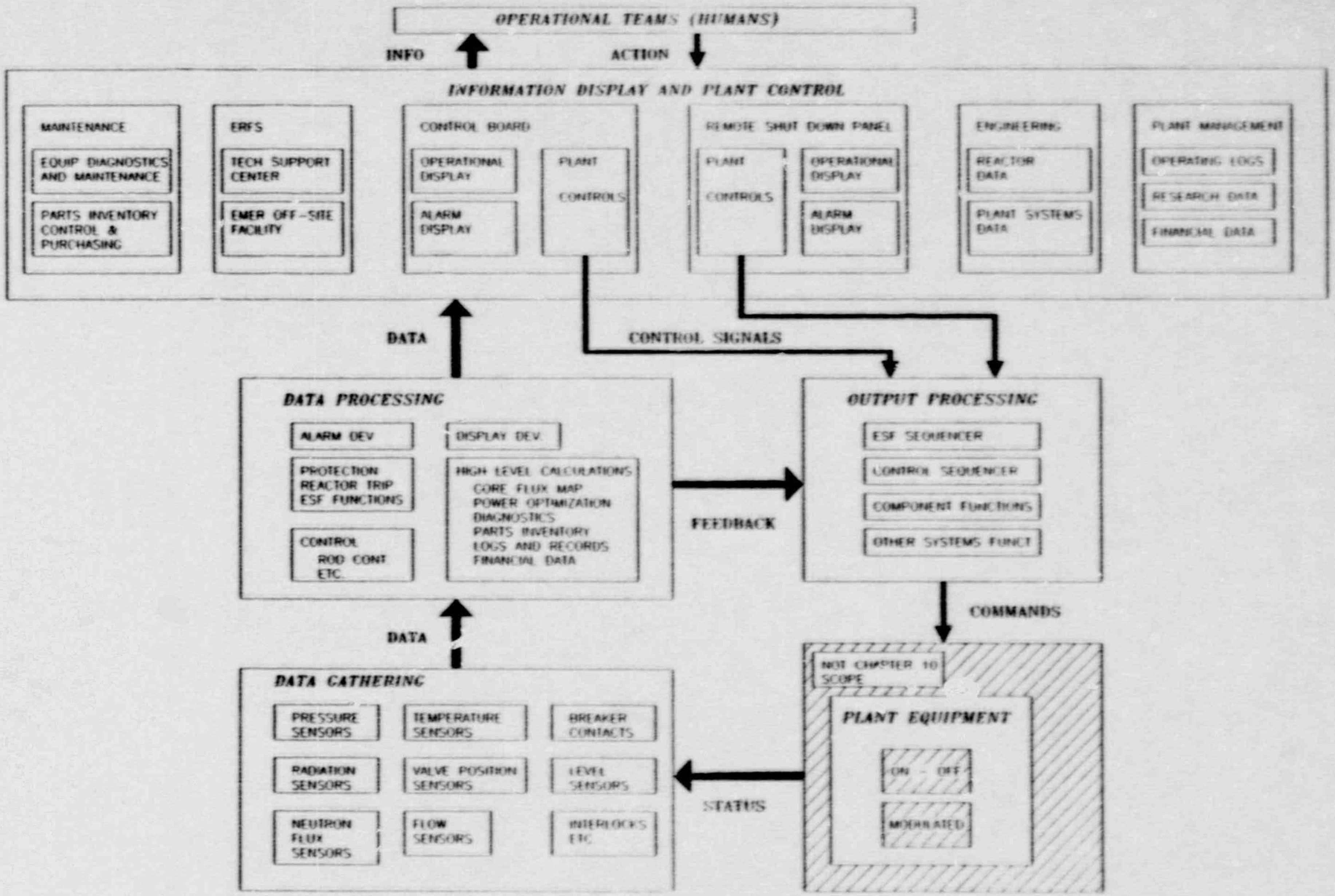
The scope and interfaces for a typical M-MIS integrated system architecture, showing the above functions, are shown in Figure 10.1-1. 0

The M-MIS requirements of this chapter address PWR and BWR plants and, in general, they are not dependent on plant size (although 1100 MWe is generally used as the reference plant size in the Requirements Document). These requirements incorporate technological improvements and human factors considerations that will resolve problems experienced by today's operating LWRs. M-MIS requirements in this revision of Chapter 10 have been developed for ALWRs of evolutionary design although the requirements which are not plant system specific have been developed to be applicable to the passive design as well. 0

1.1 SCOPE 0

The M-MIS encompass all instrumentation and control systems provided as part of an ALWR plant which perform the requisite monitoring, control, and protection functions associated with all modes of plant operation (i.e., startup, shutdown, standby, power operation, and refueling). The requirements of this chapter are applicable to all equipment supplied as part of these M-MIS regardless of the supplying agency or organization (e.g., NSSS vendor, AE, or other third party subvendors). 0

FIGURE 10.1-1 ADVANCED LIGHT WATER REACTOR
M-MIS INTEGRATED SYSTEM ARCHITECTURE



As in the case of the other ALWR Requirements Document chapters, the requirements of Chapter 10 are not all inclusive. Rather, the requirements are tailored in level of detail and specificity to assure utility objectives are met and/or existing problems are eliminated. As a result, in some cases the requirements are quite specific, whereas in other cases, they are more general and rely on invoking standards and acceptable design practices. 0

The M-MIS covered by Chapter 10 requirements include. 0

- Instrumentation, including sensors and local instruments, for all safety and non-safety systems throughout the plant. 0
- Automatic and manual controls for all safety and non-safety systems. 0
- Protection systems including safety and non-safety systems. 0
- Diagnostic systems, including loose parts monitoring systems, rotating machinery diagnostics, and neutron noise monitoring. 0
- Monitoring and control stations for the plant systems including the main control room, remote shutdown control station, technical support center, emergency operations facility, and local control stations. Not every local control panel is specified but requirements are provided regarding when local controls should be provided and for the consolidation and arrangement of these local controls into panels. 0
- Instrumentation and control power supplies, grounding, and environmental compatibility. 0
- Computer systems for control, data acquisition, display, storage and retrieval, monitoring and alarms, technical support, and operations support. 0
- Plant communications systems including data, visual, and voice intraplant communication associated with plant operation and maintenance. 0
- Although the plant simulator/training center complex is not within the scope of the ALWR Requirements Document, this chapter does specify the use of a simulator as a design tool and this simulator may eventually be used as the training simulator. The scope of the simulator requirements defined in this chapter is limited to the simulator's use in the design, verification, and validation of the M-MIS. 0

1.2 INTERFACES WITH OTHER CHAPTERS 0

The M-MIS chapter covers the integration of the instruments and controls into overall systems, control stations, etc., so that a fully satisfactory interface is achieved between the plant staff, e.g., operations and maintenance personnel, and the plant equipment and systems. As a result, this chapter has numerous interfaces with other chapters of the ALWR Requirements Document. For example, many of the functional and performance requirements of the M-MIS are constrained by the functional and performance requirements set by the designers for the systems and equipment covered in other chapters. Thus, the other chapters include specific M-MIS requirements related to the systems described in these chapters. The particular chapter interfaces within the ALWR Requirements Document are discussed below. 0

1.2.1 Interface with Chapter 1 0

Chapter 1 is an umbrella chapter which covers many requirements generally applicable to the ALWR. Chapter 10 is consistent with Chapter 1 and the requirements in Chapter 1 are not restated here. 0

1.2.2 Interface with Fluid Systems Chapters 0

The fluid systems chapters include the specific requirements for instrumentation and controls that relate to the fluid systems meeting their functional and performance requirements. These are Chapters 2 through 5, 7 through 9, 12, and 13 of the ALWR Requirements Document. They cover interfaces with the power generation systems (Chapter 2), the reactor coolant system (Chapter 3), the reactor system (Chapter 4), the safety systems including containment systems (Chapter 5) and the heating, ventilating, and air conditioning systems (Chapter 9), etc. The reader is referred to the overall table of contents for the ALWR Requirements Document for the location of the requirements for any specific system. Overall, plant-wide functional requirements for instrumentation and control, and hardware and software requirements related to the controls and instruments themselves are defined in Chapter 10. 0

The interface between the fluid system and the instrumentation is defined as the connection of the sensor to the system piping or components. For example, lines to a pressure sensor are part of the fluid system design while the pressure sensor is part of the control and instrumentation design. The interface between the system and the controls is the connection of the final actuator wiring or tubing through which power or control signals are transmitted. In some cases, certain characteristics of the actuators and final control components will be specified by the M-MIS designer to satisfy control system design requirements. All final actuators are part of the systems to which they are attached. As indicated above, an iterative, cooperative design effort among the fluid systems designers and the M-MIS designer will be required to ensure these interfaces are treated properly. 0

1.2.3 Interface with Electric Power Distribution System Chapter 0

Chapter 11 includes the specific functional and performance requirements for the electric power distribution system which affect the instrumentation and controls provided. The electric power distribution system scope is defined in detail in Chapter 11. It includes the normal and emergency AC distribution system and sources as well as the normal and emergency DC distribution system and sources. Chapter 10 covers requirements on the design of the instrumentation, controls and power supplies that relate to remotely monitoring and controlling the alignment and performance of the electrical distribution system inside the plant, and for the plant power output up through the generator output breakers. (Specific requirements for monitoring and control of the main power distribution/transmission system beyond the generator output breakers to the grid are not included as it is expected that these will be utility and site specific.) Chapter 10 also covers the instruments and controls necessary to remotely monitor and control the on-site power sources that provide input to the distribution system. Finally, as part of the overall M-MIS verification, Chapter 10 requirements assure the electrical system automatic transfers, etc., are acceptable and compatible from the standpoint of overall plant operation. 0

Chapter 11 covers the local (at or near the equipment) instruments and controls for the electrical systems. Sensors and actuators are covered by Chapter 11. The interface between Chapter 10 and Chapter 11 equipment shall be at the field termination of instrument or control cabling carrying the remote monitoring or control signal. Electrical system automatic control devices such as automatic transfer switches and protective devices are covered in Chapter 11. 0

1.2.4 Interface with Plant Arrangements Chapter 0

Chapter 6, Building Design and Arrangement provides overall requirements and interfaces for the M-MIS with regard to the physical plant arrangement. Specific M-MIS arrangements are defined in Chapter 10. In particular: 0

Chapter 6 provides requirements regarding location of major M-MIS control areas within the plant complex and with respect to location of other equipment. The M-MIS designer defines requirements as to size of the M-MIS areas based on functional needs and defines requirements for arrangement and configuration of M-MIS equipment and systems within these areas. 0

Chapter 6 and Chapter 9 provide requirements on services provided by balance of plant systems to M-MIS areas, such as the need for HVAC, fire protection, etc. Chapter 10 provides the functional and performance requirements for these interfaces as well as specifying the interface requirements for these systems as discussed in Section 1.1.3. HVAC performance requirements and active fire protection requirements are covered in Chapter 9. M-MIS performance requirements with full and degraded HVAC performance are covered in Chapter 10. 0

Chapter 6 provides requirements on arrangements of cableways, conduit, etc. to assure adequate separation for fire protection, defense against common mode failures, etc. Chapter 10 provides any needed requirements on the instrumentation and control cable itself. 0

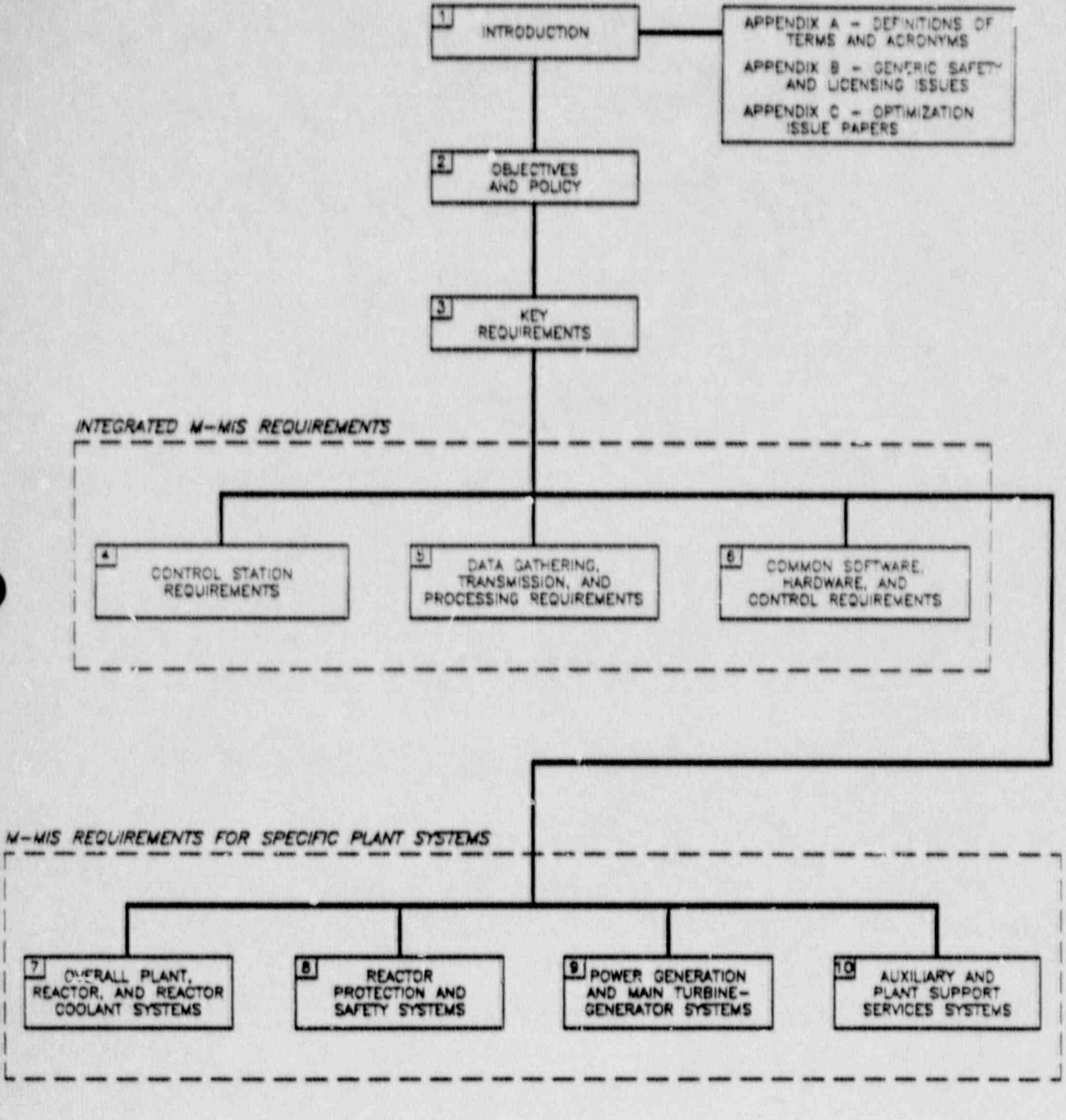
Chapter 10 provides requirements on color coding, labelling, and local equipment arrangement throughout the plant to assure good human factors to reduce operator and maintenance personnel errors. 0

1.3 CHAPTER ORGANIZATION 0

Figure 10.1-2 illustrates the hierarchical organization of Chapter 10. Section 2 contains objectives and policy statements which provide overall direction and guidance for the M-MIS design development and implementation and address specific issues which have arisen out of the utility experience with present M-MIS. 0

Section 3, Key Requirements, provides top level design requirements for the M-MIS. These requirements cover the M-MIS design organization, the responsibilities of the M-MIS Designer, the process for design development and implementation, and the verification and validation of the M-MIS design. The high level design requirements cover functional requirements relating to level of automation, proven technology, availability, simplification and standardization, etc, and provide the key requirements necessary to implement the guidance stated in the policies of Section 2. 0

MPR ASSOCIATES
F-140-31-226
07/10/89


1 INTRODUCTION
APPENDIX A – DEFINITIONS OF TERMS AND ACRONYMS
APPENDIX B – GENERIC SAFETY AND LICENSING ISSUES
APPENDIX C – OPTIMIZATION ISSUE PAPERS
2 OBJECTIVES AND POLICY
3 KEY REQUIREMENTS
INTEGRATED M-MIS REQUIREMENTS
4 CONTROL STATION REQUIREMENTS
5 DATA GATHERING, TRANSMISSION, AND PROCESSING REQUIREMENTS
6 COMMON SOFTWARE, HARDWARE, AND CONTROL REQUIREMENTS
M-MIS REQUIREMENTS FOR SPECIFIC PLANT SYSTEMS
7 OVERALL PLANT, REACTOR, AND REACTOR COOLANT SYSTEMS
8 REACTOR PROTECTION AND SAFETY SYSTEMS
9 POWER GENERATION AND MAIN TURBINE-GENERATOR SYSTEMS
10 AUXILIARY AND PLANT SUPPORT SERVICES SYSTEMS

CHAPTER ORGANIZATION AND STRUCTURE

FIGURE 10.1-2

Sections 4, 5, and 6 are the top level common requirements applicable to the overall, integrated M-MIS. They are applicable to all equipment, systems and hardware within the scope of the M-MIS. This group of requirements has been subdivided into three major areas. 0

Section 4, Control Station Requirements, contains requirements for control facilities staffing, control facilities, and the information displays, plant controls and alarms. The staffing requirements of Section 4 define the minimum operating staff continuously available for all modes of operation on which the M-MIS design shall be based and the maximum operating staff that must be accommodated within the main control room during emergency conditions. The control facilities' requirements address the capabilities and environment of the main control room, remote shutdown station, technical support center and emergency operations facilities. These include the general arrangement and auxiliary features (work stations, offices, etc.), general requirements for local control stations and communications capabilities for plant operations personnel. The information display and plant controls requirements address control room alarms, displays and controls, and the physical arrangement of controls and displays. 0

Section 5, Data Gathering, Transmission and Processing Requirements, contains requirements for the advanced data system which is at the heart of the M-MIS. It provides both hardware and software requirements for the necessary equipment such as computers, multiplexers, fiber optic and hardwired data transmission, self diagnostics, etc., as well as design requirements on overall functions, numbers of channels, data rate, failure modes, etc. 0

Section 6, Common Software, Hardware and Control Requirements. This section provides the common requirements for M-MIS equipment not covered specifically in either Section 4 or Section 5. These include items such as general control system requirements, general protection system requirements, overall reliability and availability requirements, maintainability requirements, environmental requirements, requirements to protect against common cause failures, test requirements, simplification and standardization requirements, contractibility and expandability requirements, grounding, protection against electrical and electromagnetic noise, etc. 0

Sections 7, 8, 9, and 10 provide specific requirements for M-MIS systems needed to carry out plant functions. To the extent practical, these requirements have been grouped to match with the scope of other chapters in the ALWR Requirements Document. This will facilitate referencing between chapters and the tracking of interfaces. These sections invoke but do not repeat the requirements from other chapters. These sections also identify any constraints or requirements that the needs of the specific system impose on use of the overall M-MIS, e.g., separation and redundancy requirements for safety systems. 0

1.4 DEFINITIONS AND ABBREVIATIONS 0

A list of terms and abbreviations used in this chapter, along with their definitions, is included in Appendix A. 0

1.5 REGULATORY STABILIZATION 0

Consistent with the overall ALWR program approach, regulatory stabilization for the ALWR is achieved via plant optimization subjects and resolution of generic safety and licensing issues. 0

1.5.1 Generic Safety and Licensing Issues 0

The ALWR is committed to providing a resolution for all applicable unresolved generic safety and licensing issues identified prior to July 1, 1986, as well as those new issues identified after that date which satisfy a defined screening process. The proposed elements of resolution for these issues are contained in topic papers transmitted separately to the NRC for review and comment. The requirements identified in this chapter are consistent with the proposed elements of resolution for the topic papers and issues included as Appendix B. 0

Paragraph No.	Requirement	Rev.
2	**OBJECTIVES AND POLICY**	0
2.1	**OBJECTIVES**	0
2.1.1	**Utilization of Operators**	0
	The M-MIS design shall take full advantage of operator capabilities but shall not challenge operator limitations. The human component in the man-machine interface system shall be explicitly included to correct the problem of insufficient focus on the operator in previous designs.	0
2.1.2	**Coordination With Overall Plant Design**	0
	The M-MIS design shall be coordinated with the overall ALWR plant design in order to allow the M-MIS Designer to interact with the plant systems and civil-structural designers. Such coordination shall provide for iteration in the overall design process and shall prevent unrealistically restrictive or complex requirements from being placed on either the M-MIS or the plant equipment designs.	0
2.1.3	**Consistent, Integrated Design**	0
	The control, protection, and monitoring functions of the M-MIS shall be designed with a consistent, integrated approach so that they work together to enhance plant operation and reduce operator burden. All control stations shall be integrated so that they perform as a coordinated whole and provide a consistent, easily understood and manipulated man-machine interface for plant operations and maintenance personnel.	0
2.1.4	**High Reliability**	0
	The M-MIS shall achieve very high reliability. To that end, the M-MIS shall be constructed of highly reliable components and equipment, be well analyzed, and be tested prior to and during installation and operation. Furthermore, the M-MIS shall be designed so that failures or problems in one function are incapable of propagating into other functions so that the extent of the upset is minimized and the operator burden is not increased.	0
2.1.5	**Designed for Maintenance**	0
	The M-MIS equipment shall be designed and built from the outset in full recognition of the need for maintenance and extensive testing and inspections on the installed M-MIS equipment throughout its life cycle. This includes specific consideration in the design of the need to provide for replacements and upgrades of the equipment during the life of the plant.	0

2.2 ALWR M-MIS POLICY STATEMENT 0

Policy statements provide overall direction and guidance and form the basis for many of the requirements in the following sections. The policy statements are intended to give the reader a summary view of the direction to be taken in the requirements which follow Section 2. 0

2.2.1 M-MIS Systems Approach 0

The M-MIS will employ modern digital technology to implement the monitoring, control and protection functions for the ALWR. Robust system design, including segmentation of major functions, separation of redundant equipment within a segment, and fault tolerant equipment will be used to achieve high reliability and protection against the propagation of failures. Application of signal validation to selected parameters will be used to assure the operators have data of high quality and reliability. Where it is appropriate and demonstrated, multiplexed data communications will be used for any function, including safety functions, to reduce the cost and complexity of the instrumentation and control cable runs throughout the plant. The high accuracy and drift free operation of the digital systems will reduce the overall maintenance calibration burden. Where appropriate, the use of fiber optic cables for data transmission will be used to provide high data transmission rates with electrical isolation and protection from electromagnetic interference at reduced costs. 0

Standardization of hardware and software and modularity of design will be used to simplify maintenance and provide protection against obsolescence. Built-in test features are to be provided to perform continuous self-diagnosis of digital hardware and communication paths and annunciate detected failures. Built-in test features will provide computer-aided, periodic functional testing capabilities that automatically verify system functionality once they are manually initiated, locate failures upon detection, and record test results. Most M-MIS equipment is to be located in compartments with controlled environments, maintained by reliable HVAC systems. All M-MIS equipment will be selected to be compatible with its environment under normal conditions and under casualty conditions as appropriate to meet functional requirements. 0

2.2.2 Design Process 0

The M-MIS design process will be directed by a single organization responsible for the entire M-MIS design, will be carried out by a multi-disciplined design team and shall include direct utility involvement, including engineering and maintenance personnel and operations staff familiar with plant normal, abnormal, and emergency operating procedures. The process forces coordination of the design by ensuring the M-MIS design team and the plant systems designers work together and take into account operation/maintenance inputs. In addition, a continuous verification and validation effort is performed in parallel to the design by an independent team (see Section 3.1.4) particularly in the difficult software area to assure the final product meets the requirements, and is robust and resistant to inadvertent errors. Formal documentation of the M-MIS design is achieved by including it in the plant-wide design documentation and configuration control process. 0

2.2.3 Reliability Inherent in Design 0

The M-MIS design should possess sufficient defense against the propagation of faults through segmentation, independence, and other measures so that a failure or upset in one plant control function cannot propagate to other plant control functions and thereby overburden the operators due to complex transient events. Further, the M-MIS design should be sufficiently robust to prevent a single random failure of M-MIS equipment from causing a forced outage. This is expected to require, for example, multiple computers as well as extensive use of distributed microprocessors. The emphasis is to be on assuring failures are accommodated gracefully, operators will not become over-burdened, and that no loss of essential capability results. 0

2.2.4 Testing of Man-Machine Interface Systems 0

Significant improvements in the area of system testing are to be provided with the ALWR M-MIS design. Accordingly, the equipment should be designed and configured to readily support in-service testing by incorporating good human factors principles, avoiding the use of undesirable features such as addition of test jumpers or lifting of leads, and providing built-in test features, including self diagnostics for continuous on-line testing and automated functional testing for periodic surveillance testing. 0

During design development and implementation, extensive tests are to be performed in accordance with documented test plans. Pre-installation testing is to confirm that hardware and software performance satisfies design requirements. The pre-installation test procedures should serve as the basis for post-installation validation tests and the long-term surveillance and maintenance which confirm installed system operability. 0

2.2.5 Proven Technology 0

Due to the advantages that recently available digital technology offers over some of the technology found in current LWRs, the incorporation of modern digital technology is encouraged to solve existing problems and to make significant improvements over previous designs. Introduction of new problems will be prevented by adhering to the ALWR principle of the use of proven technology. A technology will be considered proven it if has documented, successful experience in similar power plant or process industry applications, or if it has undergone extensive testing. 0

2.2.6 Cost 0

The engineering effort required to design and implement the first ALWR M-MIS will cost considerably more than if conventional technology were directly adopted. An improved M-MIS, however, will provide a major contribution to achieving significant cost savings over the plant life cycle through the achievement of higher plant availability factors. For example, the number of inadvertent plant trips will be reduced by improving the man-machine interface and control system stability (e.g., low power feedwater level control), and enhancing the testability of the M-MIS to reduce the number of testing errors. 0

2.2.7 Operating Staff 0

The size, education, and training of the operating staff, which is continuously available for plant control, influences the degree of automation, the sizing of control facilities, and the selection and arrangement of controls and displays. The adequacy of the operator staffing levels will be verified during the design process through the use of mockups and dynamic simulation. 0

It is anticipated that a single reactor operator (RO) will be able to control major plant functions performed from the main control room during normal power operation. However, this goal should not be achieved by the M-MIS Designer at the expense of overly automating the M-MIS to the point where it is difficult for the control room personnel to be cognizant of the processes being performed. During startup, shutdown, transient and emergency situations, the main control area will need to accommodate a larger operating staff. The operational tasks for these plant evolutions should be divided among this larger staff which is continuously available and is expected to be two or three operators. In order to provide a basis for the M-MIS design and to insure the main control area can accommodate a larger operating staff when necessary, a maximum operating staff and observer capacity, which must be accommodated, is defined: 0

Number	Position	License	0
1	Shift Supervisor	SRO	0
1	Senior Reactor Operator	SRO	
3	Reactor Operators	RO	
1	Technical Advisor	–	
2	Equipment Operators	–	
1	NRC Observer	–	
1	Utility Management Observer	–	

2.2.8 Human Factors Engineering 0

Nuclear utilities have spent considerable effort in backfitting good human factors into existing plant designs. In the ALWR, human factors will not be accomplished after the fact through redesign - it will be firmly entrenched in the design from the start. Human factors engineering principles will be applied as a formal part of the M-MIS design process and the design verification process. 0

It has generally been recognized that human factors and potential for human error are significant contributors in achieving necessary plant safety and availability. Therefore, the ALWR M-MIS design will place particular emphasis on: 0

- Elimination of potential sources of human error - eliminating as many potential sources of error as possible based on the current state of the art in applied psychology and on review of experience with existing designs, application of function and task analysis in the design, and use of mockups and simulation in verifying and validating the design; 0

- Reduction in the probability of human error through careful selection and allocation of tasks, proper support of defined tasks through detailed evaluation of information and control needs, and vigorous enforcement of consistency and integration among the task analyses, the hardware and software implementation of the design, the operating procedures, main control room environment, and personnel training requirements; reduction of human error potential will be a priority consideration in the design both for the operators and the plant maintenance personnel; 0

- Provision for detection and recovery from human errors should they occur - provide a robust design that takes advantage of the operating team concept and allows operators and supervisors to work together and back each other up and employs modern data processing and display technology to provide automatic checks and alerts, to detect errors before they affect the plant and help recover from them if they do occur. 0

The intent is to ensure that human factors criteria are consistently reflected throughout the M-MIS design and that human factors problems such as those identified by control room design reviews for existing plants do not occur. 0

2.2.9 Level of Automation 0

The M-MIS Designer is to evaluate each monitoring, control, and protection function as part of the design process and determine the appropriate level of automation for each with due consideration of operator workload, including potential failures of automatic equipment. This evaluation is to include considerations of system response requirements, complexity of operation, operator burden, level and duration of attention required, etc. In the selection of the level of automation, the M-MIS Designer must address the need to maintain the operators in the loop and cognizant of the plant status so that the operators remain alert and can intervene in plant operations as required. The M-MIS Designer must also recognize that the operator role changes from one of direct operation to one of management or supervision as the level of automation increases and that this, in turn, changes the type and level of plant data which must be provided to the operators. The effect of failures of automatic control systems must also be addressed as part of the process of selecting automated or manual controls. Automatic control systems should employ, wherever possible, fail safe features. 0

2.2.10 Main Control Room 0

At the center of the ALWR man-machine interface will be the main control room (MCR). The MCR will be designed as a coordinated whole, by a dedicated interdisciplinary control room design team, which is a subset of the overall M-MIS design team, and includes operations and maintenance personnel for walk-throughs and other assessments of M-MIS systems and control facilities designs. The design process, coupled with the use of current information and communications technology, will lead to a major update in control room design from existing U.S. LWRs. 0

The location and appropriate layout of the MCR will be based on reducing the need for access to the MCR by other plant personnel, yet maintain the necessary capability for the MCR staff to interface effectively with the field equipment operators and maintenance staff. The MCR environment is to be designed using human engineering principles to provide a comfortable, professional atmosphere for the operators that enhances their effectiveness. Attention will also be given to the use of colors and lighting levels to enhance operator alertness and minimize operator fatigue. 0

The layout of the MCR and the inventory of alarms, displays and controls will be selected as part of the design process to explicitly, comprehensively, and consistently support a top down, functionally based, decision making approach for investigating, planning, executing and verifying control for all plant conditions. Furthermore, the MCR equipment and information will be integrated and coordinated with other plant functions: engineering, maintenance, management and emergency response facilities (Technical Support Center and Emergency Off-Site Facility). 0

The operators and supervisor in the MCR will interface the plant through redundant compact workstations with multiple, electronic, display and control devices that provide organized, hierarchical access to alarms, display and controls. They will also use large, upright integrated plant status panels and top level alarm displays viewable from anywhere in the MCR. 0

The selection and arrangement of the display and control features for the redundant workstations shall be established during the design process described in Section 3. The design shall consider the use of multi-functional display and control features to obtain an integrated, compact workstation design which provides a consistent interface for all conditions and actions. This includes, for example, the use of a multi-functional control device for the operation of redundant safety trains and for the operation of both safety and non-safety equipment. 0

The display and control features shall be designed to satisfy existing regulations, for example: separation and independence requirements for Class 1E circuits (IEEE Standard 384); criteria for protection systems (IEEE Standard 279); and requirements for manual initiation of protective actions at the system level (Regulatory Guide 1.62). The designer shall use existing defensive measures (e.g., segmentation, separation, independence, diversity, fault tolerance, signal validation, self-testing, error checking, supervisory watchdog programs) as appropriate to insure that the alarm, display, and control functions provided by the redundant workstations meet these standards. 0

The supervisor's workstation will be identical to the operators workstations except that all of its plant equipment control functions shall be normally disabled. A means of readily obtaining hardcopy output of the workstation displays will be provided for operating staff. 0

Each workstation will include the following features: 0

- Electronically displayed normal, abnormal, and emergency operating procedures. The procedures should be consistent, use diagrammatic presentation modes, minimize the use of lengthy text, provide appropriate imbedded dynamic indication and alarm information, be coordinated with use of controls required for the procedures and provide means for flagging and logging actions taken by the operators which deviate from the set of recommended procedural options. 0

- Electronically displayed presentations of plant operational parameters and technical data based on operator tasks and event categories in graphical and diagrammatical format showing present values, trends over various operator selected intervals, acceptable ranges, set points, control bands, correlations and other explanatory information. 0

  Electronically displayed piping and instrument diagrams (P&IDs) generated from computer-aided design (CAD) software, providing multiple diagrams at different levels of detail, logically organized for easy access and dynamically updated with equipment status information.

  Access to this information should be coordinated with the decision making approach, the large displays and the other functions of the workstation and enable the operator to readily select different displays expeditiously without losing understanding of their logical organization.

- Electronically displayed alarms, designed specifically (based on plant conditions) to minimize nuisance alarms. Alarm messages should be organized and coordinated with the top level alarms as well as workstation displays and controls to support the decision-making approach. The workstation should provide alarm reflash capability and access to electronically displayed alarm data sheets to provide basic causal and recommended recovery action information. Diagnostic aids should be employed to help operators investigate problems and plan recovery actions. 0

- Plant equipment controls that are well coordinated with the decision-making approach; large, upright plant status panels and alarm displays; and workstation presentations. The controls need not be spatially dedicated, however, each control shall be clearly labeled and be organized into functional groups as appropriate using systematic and consistent arrangements. The controls shall be designed to promote efficient and reliable actuation and demonstrably preclude inadvertent mis-actuation. 0

A series of non-redundant, integrated upright displays and alarms shall be placed on or near MCR walls to provide a mimic with plant status information for essential equipment operated from the MCR and key parameter values such as water levels, temperature, pressure, power levels and the presence of flow. The alarms will provide a set of top level, spatially dedicated alarms visible throughout the MCR. 0

The large, upright displays and alarms will provide a spatially dedicated, continuously viewable, integrated mimic presentation of the plant status in a direct manner to a level of detail beyond that of summary information to enable the operators to confidently assess the status of essential equipment operated from the MCR. These spatially dedicated displays will supplement and compliment the serial presentations of subsets of this information at the workstation. Thus, these displays will enhance coordination among MCR personnel during normal, abnormal and emergency situations, and provide a clear, concise and continuous point of reference for operators to frequently and quickly assess plant status while performing tasks at the workstation. They will also be a useful aid during shift turnover, for assessing plant maintenance activities and for training activities in the MCR. 0

2.2.11 Other Control and Monitoring Stations 0

The same rigorous approach to the man-machine interface will be taken toward the design of the technical support center, emergency operations facility, remote shutdown station, local control stations, and other monitoring facilities for advisors and managers. An important part of the M-MIS design will be definition of the data communications and display needs of the technical support center and the emergency operations facility. The remote shutdown station will have the capability to control and monitor the safe shutdown of the plant, including the capability to initiate and control residual heat removal indefinitely. Control from the remote shutdown station will rely on local operation of some selected equipment. 0

The communications requirements of the operators will be included in the task analyses and the needed communications equipment will be integrated into the workstations. This will include in-plant communications as well as special communications for such needs as emergency notifications, accident management, etc. 0

Local control stations will be consistent with the remainder of the ALWR M-MIS. The availability and arrangement of indicators and displays, lighting, access, communications and special equipment needs of the operator will be considered during the design stage by analysis of the functions and tasks of the station. Where appropriate, the design will be verified by mock-ups. Operators will have ready access to local control stations and these control stations will be easy to use. The best human factors principles will be followed to enhance the operators effectiveness and reduce errors. Consistent color coding, use of mimics, labeling and demarcation will be applied as for the main control board. Finally, the environment at the local control stations will protect the operator and the equipment and reduce stress-induced failures in both normal and casualty operation. 0

Paragraph No.	*Requirement*	*Rev.*
	Monitoring provisions for technical advisors as well as plant and site management will be provided considering their needs and tasks and be made consistent with the ALWR M-MIS.	0
2.2.12	**Protection from Obsolescence**	0
	The state-of-the-art in instrumentation and control is constantly changing and obsolescence of equipment is of continuing concern. In order to minimize the impact of obsolescence of M-MIS equipment throughout the ALWR plant life, the M-MIS design should be modular in construction (hardware and software) and use standardization of M-MIS equipment to ease maintenance training, simplify spare parts requirements and support ready replacement and upgrading of the M-MIS equipment.	0
2.2.13	**Regulatory Stabilization**	0
	It is expected that the ALWR M-MIS will meet existing regulatory requirements. It is noted, however, that many existing regulatory guides and IEEE standards applicable to man-machine interface systems and equipment do not account for the potential use of modern digital technology. Thus, evolution of the detailed M-MIS design may necessitate new implementation of the intent and purpose of existing guides and standards.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3	**KEY REQUIREMENTS**	**KEY REQUIREMENTS**	0
3.1	**M-MIS DESIGN PROCESS REQUIREMENTS**	**M-MIS DESIGN PROCESS REQUIREMENTS**	0
	The M-MIS design shall be established by a defined process which begins at the same time as the rest of the plant design process and which meets the requirements of this section and the overall design process requirements of Chapter 1.	Experience has shown that conventional design methods cannot be expected to provide good interfaces between the operators and the plant. Even if all the design requirements are identified, it is unrealistic to expect them to be met in a simple and practical manner, unless the design process is systematic and consistent.	0
3.1.1	**Overall Design Process Requirements**	**Overall Design Process Requirements**	0
	The process for the development of the detailed M-MIS design shall ensure that the functional requirements of the plant systems and other design requirements are met: • Without unnecessary complexity; • Without using unproven or highly developmental instrumentation or control strategies.	This requirement addresses two problems which have occurred in the past. In previous designs, instrumentation and control requirements often were identified by the plant systems designers with little or no interaction with the M-MIS Designer. In some cases, this has led to unnecessarily restrictive or complex requirements on the M-MIS design (e.g., very tight calibration requirements). In other cases, the M-MIS Designer unnecessarily complicated the design by providing "enhancements" that could be achieved with the available (or emerging) instrumentation and control technology, but were not justified by the fundamental requirements arising from the physical plant systems. These "enhancements" have led to unneeded complexity in M-MIS, increasing their maintenance burden and reducing plant availability.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.1.1	**Functional Design Approach**	**Functional Design Approach**	0
	The M-MIS design process shall be structured to emphasize the functional division of the plant, rather than the traditional divisions based on physical systems. In particular, the design process shall address the overall control of the reactor from the viewpoint of the basic functions of: • Reactivity control; • Reactor coolant pressure control; • Reactor coolant inventory and chemistry control; • Reactor core heat removal; • Steam generator water level control (PWR only).	The M-MIS Designer will have to adopt a more global outlook than has been past practice in order to make other than minor improvements in the man-machine interface. The compartmentalization of the instrumentation and control design to match the boundaries of individual physical systems tends to ignore the natural and essential sharing of functions between systems. Ignoring these interrelations distorts the design toward detail tasks and ignores the overall functions which need to be accomplished.	0
	For other parts of the plant a similar function-based viewpoint shall be applied, for example, to the functions of: • Control of energy flow; • Control of the local plant environment; • Control of the release of material to the environment; • Providing services of water, air, and electric power.	Eventually, the M-MIS Designer must address each physical system; however, that should not occur at the beginning of the design process. The requirements in the sections which address the requirements on individual systems (Sections 7 through 10) although addressing individual physical systems, have an overall organization based on functions. It is the intent that this overall function-based outlook be fundamental to the M-MIS design process.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.1.1.2	**Coordination and Provisions for Iteration**	**Coordination and Provisions for Iteration**	0
	The M-MIS design process shall fully integrate the M-MIS design with the design processes of the remainder of the plant. In particular, it shall provide for the iteration of system requirements and M-MIS requirements so that balanced and practical designs are achieved. The process shall also assure that all modes of operation are considered, e.g., startup, shutdown, power operation, refueling, expected transients, and emergencies, including severe accidents, and that essential activities such as surveillance testing and maintenance are provided for in the design.	Iteration of the requirements between the M-MIS and the plant systems is essential to assure a balanced design, i.e., one which minimizes the total complexity not just the plant system complexity or just the M-MIS complexity. Existing LWR plants provide numerous examples where failure to coordinate the design of the M-MIS with the rest of the plant, or failure to consider how equipment will be maintained, has produced a less than desirable result – e.g., poorly laid out, congested control stations, inadequate space for maintenance or testing, insufficient HVAC, etc. Existing designs also provide examples of inadequate consideration in the design of all modes of operation, e.g., numerous bypasses and overrides may be required when changing modes of operation.	0
3.1.1.3	**Consistency**	**Consistency**	0
	The M-MIS design process shall be applied to all the interfaces between the plant and its operators and support staff. That is, the M-MIS design process shall not depend on the system involved, e.g., nuclear steam supply (NSS) or balance-of-plant (BOP), nor the classification, e.g., safety or non-safety, nor location, e.g., main control room or local control station.	Non-uniformity in the design approach across different systems (NSS and BOP, safety and non-safety) has resulted in poor operator interfaces, employing different conventions, different alarm and display philosophies, non-standardized hardware, etc. This requirement is intended to prevent this in the ALWR.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.1.2	**M-MIS Design Organization and Plan**	**M-MIS Design Organization and Plan**	0
3.1.2.1	**Design Responsibility**	**Design Responsibility**	0
	The M-MIS design effort shall be formally organized and directed by a single organization, the M-MIS Designer, who is responsible for the entire M-MIS. The individual or group charged with overall responsibility for the M-MIS shall be highly experienced in nuclear plant systems, i.e., not limited in experience to just the instrumentation and control disciplines.	In order to effectively coordinate the M-MIS design development process, single-point responsibility is required. It is important that the M-MIS Designer have broad experience that encompasses systems design and operation as well as instrumentation and control system design.	
3.1.2.2	**Design Teams**	**Design Teams**	0
	As part of the overall M-MIS design group, the M-MIS Designer shall organize and direct individual design teams for particular major interfaces. At least one of these shall be established for the overall coordination of the design of the main control room (MCR). In addition to instrumentation and controls engineers and designers, the MCR design team should include at least the following:	The total scope of the M-MIS design is large, and the need to correct the design deficiencies of existing control rooms is a major part of that undertaking. Therefore, it is essential that a dedicated design team be formed for the MCR.	0
	• Engineers and designers for the nuclear steam supply system;		0
	• Engineers and designers for the balance-of-plant systems;		0
	• Human factors specialists;		0
	• Utility engineering, operations, and maintenance staff representatives.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.2.3	**Independent Review**	**Independent Review**	0
	The M-MIS design process shall include independent review of all aspects of the M-MIS design throughout the process. This shall include the verification that individual stages of the process are correct and that the transfer of information from stage-to-stage has been properly accomplished. The independent review shall also validate that the overall M-MIS will accomplish the intended functions. The M-MIS Designer shall establish an independent review team which meets the requirements of Section 3.1.4	An independent team is necessary to provide rigorous, objective review during all stages of the design, in order to ensure that the final design meets all its requirements. This is consistent with recent industry practice in performing review of additions to existing plants' man-machine interfaces (e.g., see NSAC-39, *Verification and Validation for Safety Parameter Display Systems*).	0
3.1.2.4	**Design Plan**	**Design Plan**	0
	The M-MIS Designer shall prepare a comprehensive plan for the development and implementation of the M-MIS design which includes at least the following:	A documented plan for development and implementation of the M-MIS design is necessary because of the large scope of the M-MIS and the number of organizations involved.	0
	• An M-MIS design development and implementation schedule, which includes specific milestones, updating and tracking capability, and which is consistent with the overall ALWR plant schedule;	• This is needed to ensure coordination among the various organizations and teams and to meet the aggressive overall ALWR plant design and construction schedule.	0
	• A plan for controlling the configuration of the design and design tools, e.g., computer analysis software and program compilers;	• Configuration management is required for the entire ALWR plant. See the corresponding Chapter 1 requirements and rationale.	0
	• A plan for accomplishing the interaction between the M-MIS design team and the various plant systems designers, including formal methods for communicating and controlling system interfaces;	• In order to achieve a coordinated design and to provide for the iteration of requirements and design features, a formal method for establishing and maintaining interaction and communication among the M-MIS Designer and the plant systems designers will be needed.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Provisions for engineering, operations, health physics, and maintenance personnel representing the utility user to actively participate throughout the entire design development and implementation, testing and installation.	• User participation and input throughout the entire M-MIS design process is necessary to assure a satisfactory design and adherence to proven human factors engineering principles.	0
3.1.3	**Required Design Process Features**	**Required Design Process Features**	0
3.1.3.1	**Resolution of Past Problems**	**Resolution of Past Problems**	0
	The M-MIS design process shall ensure that problems with the existing LWR M-MIS designs are identified and that features are incorporated in the ALWR M-MIS which provide satisfactory solutions to those problems. To implement this requirement, the M-MIS Designer shall include the following in the design process: • At the beginning of the design process, a comprehensive review of existing LWR plant M-MIS designs shall be made to identify problems which have led to low plant availability and high maintenance burdens. • The final M-MIS design shall specifically identify how each of the problems has been solved.	The solution of existing problems is a basic objective of the ALWR program. The obvious first step is the identification of the problems to be solved. There is substantial information on these problems available from such sources as License Event Reports, Nuclear Power Experience, the Nuclear Plant Reliability Data Systems, and from the Institute of Nuclear Power Operations. Additionally, this review will aid in identifying those parts of the M-MIS design which will benefit from the application of new technology. The M-MIS Designer is required to explicitly address each of the problems so that the merit of the solutions can be independently evaluated and so that the basis for the design features which represent solutions are maintained for the Utility to evaluate future changes.	0

Paragraph No.	Requirement	Rationale	Rev
3.1.3.2	**Simplification and Standardization**	**Simplification and Standardization**	0
	The design process shall include the following features directed at achieving the ALWR goals of a simple, plant-wide standardized design:	The development of the detailed guidelines for design practices has several purposes:	0
	• The design process shall provide for the preparation of guidelines for standard design practices for the M-MIS. These design practices shall include identification of common configurations and components (control and I/O modules, for example). The control station design practices (see 4.1.5) shall be included as part of these guidelines.	• It forces the M-MIS Designer to think in terms of standard approaches; • It provides criteria which can be used by reviewers to identify and, therefore, question non-standard configurations; • It should reduce the total design effort; • Provide a basis for future changes and modification of the M-MIS.	0
	• The design process shall provide for the development and use of standard component and systems designations and nomenclature which are compatible with Configuration Management System, the control station human factors and common usage.	• In many plants the designation of components is not uniform and the designations in design documents, in procedures, and on the panel labels may be different. Some systems are arbitrary numbers with no mnemonics which burden the operator's memory and lead to errors and confusion.	0
	• The design process shall actively track the numbers of components and numbers of different types of components in the M-MIS. This shall include tracking the number of different types of small replaceable items such as fuses and light bulbs. These summaries shall be regularly made available to management and independent reviewers to support assessments of the overall acceptability of the design against the overall simplification and standardization requirement.	• Numbers of components or numbers of component types are not the only indicator of the success of efforts to simplify and standardize. They will, however, provide some means to quantify the efforts, but more importantly, they will assist reviewers in focusing on the parts of the design where numbers of components are high or where non-standard components have been specified.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.3.3	**Identification of Functions and Tasks of the M-MIS**	**Identification of Functions and Tasks of the M-MIS**	0
	The M-MIS design process shall result in the explicit identification of the functions of the M-MIS needed to support the plant systems and the overall operation of the plant. The design process shall also result in the explicit identification of the individual tasks, mental and physical, necessary to perform these functions.	The identification of functions and tasks has been widely used to review existing control room designs and it has had some limited use in the design of backfits. For existing plants, it has shown major disconnects between the functions and tasks and the actual plant hardware. This requirement is intended to make the function and tasks central to the M-MIS design so that they can be used in all aspects of the M-MIS design process and provide consistency of approach as well as a defined basis for use in any future modifications.	0
3.1.3.3.1	**Scope of Functions and Tasks**	**Scope of Functions and Tasks**	0
	The functions and tasks shall include all of those which affect the design of the M-MIS. The design process shall provide for the addition of functions and tasks in the course of the M-MIS design development as well as the modification of the initial set. It is required that the functions and tasks be kept current as the design progresses so that when the design is complete, the functions and tasks will accurately reflect the basis for the M-MIS design.	By applying the identification of functions and tasks to all parts of the M-MIS, it will permit a consistency of approach which should simplify review. In particular, it should make it easier to identify the features which are not needed and inappropriate assignments of functions to the operators.	0

Paragraph No.	Requirement	Rationale	Rev.
3.1.3.3.2	**Analysis of Function and Tasks**	**Analysis of Functions and Tasks**	0
	The design process shall provide for analysis and validation of the functions and tasks by such techniques as walk-throughs in mockups of control stations using experienced utility operators or other personnel, dynamic modeling and simulation using limited-purpose simulators, and a full-scale plant simulator. In particular, the allocations of functions to automatic control systems or to particular control stations shall be validated and, if necessary, the allocation changed and reanalyzed.	Since the functions and tasks are the fundamental basis for the entire M-MIS design, they must be rigorously and carefully evaluated for correctness. They must also be subject to modification and iteration as the design progresses so that optimum and practical design of the M-MIS can be achieved.	0
3.1.3.3.3	**Uses of Functions and Tasks**	**Uses of Functions and Tasks**	0
	The M-MIS design process shall provide for the use of the identified functions and tasks in at least the following activities: • Allocation of functions between automatic and manual control; • Allocation of tasks among work stations; • Development of control and operation strategies; • Assignment of responsibilities of the operating crew; • Assessment of operator workload, both mental and physical; • Arrangement of work stations; • Selections of types of displays and their detailed characteristics; • Selections of types of controls;	The purpose of this requirement is to emphasize that the functions and tasks are to be an integral and central part of the entire M-MIS design process, i.e., they are not an after-the-fact exercise which is used only to validate the system design or to verify the adequacy of the process. They will obviously be a fundamental part of the formal verification and validation of the design, however.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Selection and arrangement of alarms and their integration into the control station designs;		0
	• Development of operating procedures and training requirements;		0
	• Evaluation of the effects of credible M-MIS equipment failures;		0
	• Verification and validation reviews.		0
3.1.3.3.4	**Documentation of Functions and Tasks**	**Documentation of Functions and Tasks**	0
	The M-MIS design process shall provide for the controlled documentation of the identified functions and tasks. This documentation shall include the bases for the allocation of functions or tasks between automatic systems and the operators and the detailed information and action requirements for each task.	Since the functions and tasks are the fundamental basis for the M-MIS design and will be the basis for reviews and evaluation, they need to be carefully documented as befits their importance. This will involve some effort not normally involved in plant control system design; however, it should greatly simplify validation of the design, preparation of operating procedures, and any future plant modifications.	0
3.1.3.4	**Consideration of Potential Equipment Failures**	**Consideration of Potential Equipment Failures**	0
	The M-MIS design process shall explicitly consider the potential for and the consequences of failures of plant and M-MIS system components. That is, functions and tasks which result from the operator coping with equipment failures shall be identified as part of the M-MIS design bases. The analysis and validation testing of the M-MIS shall include the postulated failures and recovery from them.	Experience shows that major challenges to an M-MIS design come from failures or malfunctions of equipment. Unless the design specifically considers these malfunctions, the availability and reliability of the ALWR will probably be adversely affected, i.e., tolerance of the system to faults needs to be designed into the system.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.1.3.5	**Analysis Requirements**	**Analysis Requirements**	0
3.1.3.5.1	**Plant Dynamic Models**	**Plant Dynamic Models**	0
	The M-MIS design process shall include the development of digital computer based dynamic models for the overall plant response as well as individual control systems. These dynamic models shall be: • Suitable for analyzing both steady state and transient behavior; • Used to confirm the adequacy of control schemes; • Used to confirm the allocation of control to an automatic system or an operator; • Used to develop and validate plant operating procedures; • Validated against tests on actual plant behavior, wherever practical; • Developed early enough in the design process that modifications of the systems themselves can be made, if shown to be needed by the analysis; • Incorporated, as directly as possible, into plant general purpose or limited use simulators; • Completely documented and the documentation provided as part of the final M-MIS design.	Digital computer modeling techniques are current state-of-the-art and techniques are available to model the entire plant process systems and associated control systems. The early development and use of these models allows control strategies to be evaluated under a variety of upset and off normal conditions. The early identification of any problems with the ability of the M-MIS to cope with these occurrences will improve ease of making the needed changes.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.3.5.2	**Control System Analysis**	**Control System Analysis**	0
	All control systems shall be analyzed to assure they are stable and provide the required steady-state and transient response for all operating conditions. Control system analyses shall assume the maximum expected M-MIS signal propagation delays for all data communications paths. These analyses shall be made part of the M-MIS documentation.	Experience in existing plants shows that a significant number of control problems are traceable to a lack of basic design analyses. This requirement is intended to ensure that debugging, extensive adjustment, and modifications are not required on the final systems in the field.	0
3.1.3.6	**System and Component Testing**	**System and Component Testing**	0
3.1.3.6.1	**Test Plans**	**Test Plans**	C
	The M-MIS design process shall define the test requirements for both systems and components in formal test plans. All testing required to justify the M-MIS design, prepare the systems for operation, and tests required after the systems are in service and after maintenance shall be included. As a minimum, each test plan shall: • Identify the items to be tested, including their version or revision where appropriate; • Identify all features of the system under test which are not to be tested and the reasons why; • Describe the overall test approach; • Specify the test case specifications; • Specify the acceptance criteria; • Specify test environment;	Many problems in existing plants can be traced to inadequate testing before, during or after installation. Often, where testing has been performed, the requirements for the tests were developed independent of the designer, with little or no feedback of the results. Since the designer is most familiar with the functional requirements for the equipment, the details of the design and the potential problems areas, the designer should be the one to define the test requirements and document them in formal test plans to ensure that the tests match the intent of the design and to provide a means for independent review of the adequacy of the testing and the results of the testing.	0
	• Specify the test equipment;		0

Paragraph No.	Requirement	Rationale	Rev
	• Identify group responsible for performing the test, e.g., manufacturer, special test group, startup test organization, etc.;		0
	• Identify the test staffing needs and associated skill levels;		0
	• Specify a test sequence and provide an estimate of the time to carry out the tests.		0
3.1.3.6.2	**In-Service Surveillance Testing**	**In-Service Surveillance Testing**	0
	The design process for the M-MIS shall include the explicit identification of all in-service surveillance testing of plant components and M-MIS components which is required to ensure satisfactory long term operation of the equipment and to meet all appicable regulatory requirements. The functions and tasks to accomplish this testing shall be included in the design basis of the M-MIS and shall be fully accounted for in the design process, e.g., generic procedures for these tests shall be prepared and used in walkthroughs in control station mockups.	In-service surveillance testing of plant equipment and the components of the M-MIS are a necessity to assure satisfactory operation as well as, in some cases, being a regulatory requirement. In existing plants, these tests are often difficult to perform and represent major challenges to operator skill and training. They have been the source of many operational errors, plant trips, and unplanned outages. These tests need to be treated in the same rigorous manner as other plant functions and tasks so that the M-MIS will adequately support their performance.	0
3.1.3.6.3	**Installation and Startup Testing**	**Installation and Startup Testing**	0
	The M-MIS design process shall include the preparation of test plans and generic procedures for the testing to be performed on the M-MIS components and systems after they are installed in the plant and the testing to be performed by the utility operating staff as part of the initial plant startup.	Testing after installation and as part of the first actual operation is crucial to satisfactory future operation. The M-MIS Designer has the total responsibility for the design from conception to operation. This testing also needs to be carefully planned since problems can directly impact the first commercial plant operation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.4	**Independent Review of Design Process**	**Independent Review of Design Process**	0
	The M-MIS design process shall provide for independent review of all its activities and the resulting design of the M-MIS. Three levels of independent review shall be provided: • Overview of the entire M-MIS design process; • Independent validation that the system and its components will perform their intended functions; • Independent verification that the individual steps in the process of design have been properly carried out. These independent reviews shall be such that they will fulfill the quality assurance requirements for design reviews for both the hardware and software in the M-MIS. The scope of the independent overview review shall include any issue or area of inquiry which the review team considers may affect the suitability of the M-MIS.	The continuous and parallel review of the M-MIS will improve the quality of the end product design and its reliability, availability, and cost effectiveness. Independent review of the design from the beginning will allow correction of design deficiencies early in the design process. The requirements go beyond what would be considered verification and validation (V&V) in that provision is made for an independent overview of the entire process. This is intended to assure that the independent review does not consist entirely of detail checks of documentation, etc. but also adds the discipline of an independent, knowledgeable review to this overall approach and progress of the M-MIS design.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.4.1	**Qualification of Reviewers**	**Qualification of Reviewers**	0
	The independent review team(s) shall be comprised of individuals who have comparable technical qualifications to those of the M-MIS design team. These reviewers shall be independent of the M-MIS design team for that aspect of the design they are tasked to review.	The qualification of the reviewers needs to be on a par with the designers so that an effective review can be performed. Similarly, independence from the design team is also essential.	0
3.1.4.2	**Review Plan**	**Review Plan**	0
	The M-MIS Designer shall establish a preliminary plan for the independent reviews prior to initiating the design process; however, the final review plan shall be established jointly by the independent review teams and the M-MIS Designer.	The review plan must be considered in the scheduling and planning of the entire design effort. This will assure that adequate time is provided in the schedule and that the designers can plan and produce work products which facilitate review. The plan should not be totally controlled by the designers or the reviewers and, therefore, the final plan should be a joint responsibility.	0
3.1.4.3	**Timing of Reviews**	**Timing of Reviews**	0
	The independent review shall begin as soon as the design process is started and shall continue through the testing of the completed system.	The reviewers need to be a part of the entire design process to achieve maximum effectiveness.	0
3.1.4.4	**Verification and Validation Reviews**	**Verification and Validation Reviews**	0
	The following requirements define the minimum scope of the independent review for the purpose of verification and validation of the M-MIS design process.	These requirements are based on the current experience in the verification and validation of designs (both hardware and software) by a consistent, systematic approach.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.1.4.4.1	**Functional Requirements Reviews**	**Functional Requirements Reviews**	0
	The review team shall review the M-MIS system functional requirements and system functional designs and provide concurrence that plant systems functional requirements are met.	The M-MIS functional requirements form the basis for the design, implementation and acceptance of the completed system. The principal objective of the verification process at the initial stages of the design process is to confirm that the functional requirements are complete, correct, consistent, feasible and testable.	0
3.1.4.4.2	**Specification Reviews**	**Specification Reviews**	0
	The review team shall review hardware and software specifications and confirm that these specifications will obtain a satisfactory implementation of the functional design. The reviews of the functional design and hardware and software specifications shall confirm that the design is a correct, effective, and efficient translation of the functional requirements. These reviews shall also consider system architecture, interfaces, testability, maintainability, reliability, and human factors aspects of the design.	The preparation of specifications which accurately reflect the functional requirements is essential to ensure that the final M-MIS design is satisfactory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.1.4.4.3	**Review of Design Choices and Alternatives**	**Review of Design Choices and Alternatives**	0
	The reviews of system functional requirements, system functional design, and hardware and software specifications shall include evaluation of the alternatives and trade-offs considered by the M-MIS Designer and others in establishing these requirements and specifications, and that they address the correction of system and equipment problems experienced with previous plant designs. The reviews shall address all aspects of the design, including:	All stages of review should confirm that the functional requirements and functional design appropriately address and correct systemic and equipment related problems with previous systems.	0
	• Simplicity;		0
	• Standardization;		0
	• Reliability and availability;		0
	• Protection against common mode failures;		0
	• Power supply failures and their effects;		0
	• Compatibility with the environment, including:		0
	– Temperature,		0
	– Humidity,		0
	– Radiation,		0
	– Radio frequency interference (RFI),		0
	– Electromagnetic interference (EMI),		0
	– Vibration and seismic loadings,		0
	– Fire and fire suppression systems,		0
	– Flood,		0
	– Electrical transients and surges;		0
	• Maintainability;		0
	• Human factors for operators and maintenance personnel;		0
	• Protection against obsolescence;		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• Flexibility and expandability;		0
	• Constructibility.		0
3.1.4.4.4	**Review of Testing**	**Review of Testing**	0
	The review team shall review system and component test plans for factory and startup testing, shall witness the testing, and review the test results.	Review of the test program is required to ensure its effectiveness. Witnessing the testing by the review team will help ensure that the testing is performed in accordance with the test plan. Review of the test results is required to ensure satisfactory completion of the testing program.	0
3.1.4.4.5	**Review of M-MIS Design Documentation**	**Review of M-MIS Design Documentation**	0
	The team shall review the completeness and accuracy of the documentation of the M-MIS design.	Sufficient and accurate documentation of the M-MIS design is important to the long term maintenance of the M-MIS.	0
3.1.4.4.6	**Documentation of Reviews**	**Documentation of Reviews**	0
	The review team shall document all of their reviews. The documentation shall identify deficiencies identified by the reviews. Documentation shall contain sufficient information to enable a third party to repeat the review and understand the results obtained from the review. The results of the reviews shall be provided to the M-MIS Designer on a schedule such that any needed changes can be made without delaying the overall M-MIS and plant schedule.	Documentation of the reviews is necessary to provide traceability and to support the ability to review later changes.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.2	**PROVEN TECHNOLOGY**	**PROVEN TECHNOLOGY**	0
	In accordance with Section 2.2.A of Chapter 1, the ALWR shall use proven technology; however, some advanced technology appropriate for the M-MIS may have had no prior use in LWR plants. In those cases, the use of the advanced systems and equipment may be justified if proven in other applications as defined in this section.	It is expected that the use of advanced M-MIS technologies will realize significant improvement in plant availability, reliability, constructibility, maintainability, operability, etc. The ALWR cannot, however, be a test facility for developmental technology. These requirements are intended to ensure that advanced technology is not ruled out, but that it is fully utilized consistent with assuring its solid technical basis.	0
3.2.1	**Criteria for Proven Technology for Equipment**	**Criteria for Proven Technology for Equipment**	0
	In addition to the definition of proven technology in Chapter 1, Section 2.2.A, M-MIS equipment shall be considered proven if: • It has at least three years of documented, satisfactory service as modules of subsystems in power plant applications similar to that in LWRs or it has at last three years of documented, satisfactory service in other than power plant applications which are similar to the use in the ALWR M-MIS. • It has satisfactorily completed a defined program of prototype testing which has been designed to verify its performance in the ALWR M-MIS application.	Because of the extended hiatus in the construction of new nuclear power plants in the United States, some advanced technologies in the M-MIS area have not been applied in LWRs. However, they have been used in other applications such as fossil power plants, defense, or process industries. The ALWR should make use of technology improvements based on similarity of application or extensive testing. This will allow the gains to be achieved without using the ALWR as a test vehicle to develop and debug new equipment and processes. The primary emphasis of the ALWR is reliable power production.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.2.2	**Criteria for Use of Unproven Equipment**	**Criteria for Use of Unproven Equipment**	0
	For any component or system which is not yet proven in accordance with 3.2 or 3.2.1 and which is apparently needed to obtain a defined gain in simplicity or performance, the M-MIS design may include such equipment if: • A detailed plan has been developed for the testing or collection of experience which would meet the criteria of 3.2.1; • A specific alternate approach has been defined and included in the M-MIS design process to the extent necessary so that the limiting requirements for the ALWR can be met if the component or system were not to be adequately proven; • The needed testing or experience data collection can be completed and assessed and the choice made between alternatives without impacting the overall ALWR schedule.	This requirement is intended to make the M-MIS Designer justify the need to use the unproven equipment, have a defined program to establish its acceptability, and to have a fall-back position if the attempts to prove out the equipment were to fail. Meeting the minimum or limiting ALWR requirements should not depend on the development of advanced M-MIS hardware nor should these developments and their potential benefits be precluded. It is particularly important that the M-MIS Designer accept the risk for including such developmental items and the Utility not be forced to accept the developmental items because by the time the problems become apparent it is too late to change without impacting the overall schedule.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.3	**COST**	**COST**	0
	The costs of the M-MIS design shall be consistent with the specific ALWR cost goals and economic evaluation input assumptions of Chapter 1. In particular, the M-MIS design shall be based on the evaluation of the costs to the owner over the total life of the plant. Cost evaluations of alternate M-MIS designs shall adequately and consistently include consideration of the costs to the owner of such items as: • Operation, maintenance and repair, including radiation exposure and contamination control; • Scheduled and unscheduled plant shutdowns; • Training of operators and technicians; • Startup and surveillance testing; • Analysis and simulation; • Replacement.	The initial cost of many parts of the M-MIS is only a small part of the eventual cost to the owner. Improvements in reliability, operability, testability, and maintainability will be reflected in higher plant availability throughout the plant life and designs which have improvements in these areas may well be the least cost option for the owner. There has been a tendency to focus cost comparisons on the initial hardware costs, since these are relatively easy to establish. This requirement is intended to emphasize that the simplistic view of costs in terms of only the initial hardware is not acceptable for the ALWR M-MIS design.	0
3.4	**OPERATOR ACTIONS**	**OPERATOR ACTIONS**	0
	The M-MIS design shall explicitly consider the actions of the operators and other members of the plant staff to operate and control the plant. These actions shall be within the capability of all operators. These defined actions or tasks shall be identified as required in 3.1.3.3.	Experience has repeatedly shown that operator actions have been a major factor in most reactor incidents. This requirement and the remainder of this section are intended to ensure that the operator's part in the plant control and operation is as carefully planned as the electronic hardware and that the actions are well within the capability of all the probable operators.	0

Paragraph No.	Requirement	Rationale	Rev.
3.4.1	**Operator Workload**	**Operator Workload**	0
	The M-MIS design shall not require the operators to perform tasks which over-burden their capabilities, especially during emergency or upset conditions.	The workload of operators has not been specifically identified and evaluated as part of the design process of existing plants. Consequently, the workload tends to be excessive for upsets and too low for adequate attentiveness during normal operations. It is intended that the ALWR operator workload be engineered from the beginning of the M-MIS design to be compatible with expected operator capabilities and defined staffing levels (see 4.2).	0
3.4.2	**Operator Vigilance**	**Operator Vigilance**	0
	The M-MIS design shall include features which facilitate operator activities which tend to maintain the operators alert and attentive. These features shall be based on the available information at the time the M-MIS is designed on methods which have been proven to be effective in assuring operator vigilance. This shall include application of the guidance developed by EPRI on operator vigilance and alertness (RP-2184-7). The basis for these features, including a review of experience and practice at the time the M-MIS is designed shall be part of the M-MIS design documentation.	In periods of low workload, it is expected that the most determining factor in operator alertness will be operating practices – the duties, both technical and administrative, assigned to the operators, shift rotation schedule and duration, motivational factors and incentives, etc. However, the operators' workload (and therefore ability to remain attentive) during routine operation will be affected by decisions the M-MIS Designer makes in selection of automatic versus manual and remote versus local for specific control and monitoring functions performed during steady-state power operation. Also, design features of the control room and operator workstations will affect operator alertness – lighting levels, temperature, background noise, seating, etc. These decisions should reflect consideration of operator alertness. Utilities and others are presently engaged in work to investigate the factors which affect operator vigilance. It is expected that at the time th M-MIS is designed, additional guidance on methods to assure operator vigilance will be available.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.4.3	**Selection of Automatic or Manual Control**	**Selection of Automatic or Manual Control**	0
	Design choices on automatic versus manual control or monitoring shall be based on evaluations which specifically include consideration of: • Operator workload, including parallel or potentially concurrent emergency activities; • Operator capability, including time to respond, skill, and precision; • Past experience with automatic or manual controls or monitoring in similar applications; • Operator vigilance and the need to keep the operator involved and knowledgeable as to the plant status; • Amount and complexity of M-MIS equipment (including software) and the resulting maintenance and testing burden; • The consequences of and potential for malfunctions of the automatic equipment and for operating errors; • Regulatory requirements.	It is intended that the choices for manual or automatic designs be based on consistent technical bases that will result in an acceptable tradeoff of operator workload and system complexity so that a balanced design is obtained. The technical bases for these choices needs to be documented, not only to allow adequate review, but also to provide the input for operator training and guidance for future changes to the plant. The choice of automatic versus manual monitoring will be expected to be based on balancing the regulatory and accuracy of records which can be achieved if done automatically to the need to assure the operators are aware of the status of critical parameters.	0
	Sections 7 through 10 state the constraints on the selection of automatic or manual control which shall be applied to specific parts of the M-MIS. The M-MIS design documentation shall specifically identify those cases where a specific choice between automatic and manual control was made and include the bases for the choices.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.4.4	**Selection of Remote or Local Control**	**Selection of Remote or Local Control**	0
	Design choices on remote versus local control and monitoring shall be based on evaluations which specifically include consideration of: • Operator workload, including the effect of the time to access local equipment and the other parallel or potentially concurrent operator tasks; • Operator capability, including the need for feedback or monitoring as a control action is taken; • The local environmental conditions, such as access difficulty, temperature, radiation and contamination level, leaks, and other personnel hazards; • The need for the operator to monitor local conditions which are difficult to do remotely, e.g., the detection of small leaks, damaged parts, unusual noises, etc.; • The amount and complexity of M-MIS and plant system equipment and the resulting maintenance and testing burden; • The consequences of malfunctions of remote equipment; • Past experience with remote or local controls in similar applications.	In current plants remote controls and displays are provided where local components would be completely adequate. This is particularly the case for main control rooms where controls and displays are provided for operations which are not directly related to the safe and reliable operation of the power generation. This distracts the operators from their main duties and impairs their performance. It is intended that the ALWR focus the main control room on its primary functions. Unnecessary remote controls or displays also increase the amount of equipment and the resulting maintenance burden. It also tends to discourage actual observation of the equipment and the early detection of degradation such as leaks, loose parts, or improper maintenance.	0

Paragraph No.	Requirement	Rationale	Rev
	Sections 7 through 10 state specific constraints on the selection of remote or local control and monitoring which shall be applied to specific aspects of the M-MIS. In addition, Section 4.9.1.2 specifically prohibits controls and displays in the main control room unless they support a defined task for the control room operators.		0
3.4.5	**Operator Aids**	**Operator Aids**	0
	The M-MIS design shall include the definition of the features which are provided to assist the operator in carrying out specific tasks. These operator aids shall be considered as an integral part of the overall M-MIS design and shall be included in all evaluations of control station and M-MIS designs. These operator aids shall include:	Operator aids can provide valuable assistance for the operator; however, they may be more distracting than useful unless they are directly tied to some important task. This requirement is intended to ensure and encourage useful operator aids but avoid those which may be distracting for the operators.	0
	• Computer-aided CRT displays at convenient terminals which provide information which consolidates and processes data so that it is presented in a form which is directly usable by the operator to carry out defined functions and tasks. For example, calculating a total inventory from the levels in various tanks or determining control rod motion programs or critical rod positions.		0
	• Permanently posted information, instruments, or cautions which reduce the memory burden on the operators. (See also 4.8.4.)		0
	In addition to the above operator aids, the M-MIS Designer shall evaluate the incorporation of active systems which will predict for the operator the consequences of a potential action. If such operator aids are incorporated in the M-MIS design, the M-MIS Designer shall identify the conditions under which they would be used and shall demonstrate that they do not distract the operators from their other duties.		0

Paragraph No.	Requirement	Rationale	Rev.
3.5	**AVAILABILITY AND RELIABILITY**	**AVAILABILITY AND RELIABILITY**	0
	The M-MIS Designer shall establish quantitative reliability and availability criteria for the component parts and subsystems of the M-MIS which are consistent with the overall ALWR requirements of Chapter 1. In addition, the M-MIS design shall meet the requirements on availability and reliability of this section as well as Sections 7 through 10 for specific parts of the M-MIS.	The systematic setting of reliability criteria provides a means to ensure that the overall ALWR objectives will be met. Individual requirements in the remainder of this section are intended to ensure that the M-MIS Designer considers a number of specific issues which are expected to contribute to meeting the overall goals.	0
3.5.1	**Effects of Postulated M-MIS Failures**	**Effects of Postulated M-MIS Failures**	0
3.5.1.1	**Preferred State After Failure**	**Preferred State After Failure**	0
	The M-MIS Designer, together with the Plant Designer, shall select the appropriate failure state of plant equipment (e.g., pumps and valves) upon loss of motive power (electric, pneumatic, or hydraulic) on a case-by-case basis during the design process. For protection systems, the preferred failure state typically should be the safe condition. For control systems, the preferred failure state typically should be the most stable state. Upon restoration of power to control systems, the M-MIS shall not change the state of the controlled components and shall initialize in the manual mode.	In many current plant designs, the requirement to "fail safe" is implemented in such a way that the plant is in a "safe" mode from a limited, regulatory perspective. Further, these failure states typically only addressed protection equipment and did not address failures in control grade and information systems. As a result, transients and upsets were unnecessarily initiated or complicated. The intent of this requirement is to address this problem and assure that the M-MIS Designer considers the failure conditions of all M-MIS systems.	0

Paragraph No.	Requirement	Rationale	Rev.
3.5.1.2	**Effect of a Single Failure**	**Effect of a Single Failure**	0
	M-MIS equipment, together with the plant systems design, shall be designed such that, to the extent practical, no single random failure of any of the M-MIS equipment or its supporting equipment will cause a forced plant outage. This criterion shall be met for all normal operating and test modes of the M-MIS equipment, including on-line self-diagnostic testing and periodic functional testing modes. This criterion shall apply to automatic shutdowns that may be caused by a failure, and shutdowns the operator must perform due to conditions produced by a failure.	Required to meet the overall plant availability target specified in Chapter 1. It is intended that the M-MIS Designer significantly reduce the number of single failures or operator errors which will shut down the plant. Some events, obviously, will lead to shutdown; however, this set of failures and operator errors should be reduced to the practical minimum which assures adequate protection and safety actions can be executed.	0
3.5.2	**Top Level Reliability Requirements**	**Top Level Reliability Requirements**	0
3.5.2.1	**Forced Outage Frequency**	**Forced Outage Frequency**	0
	Mean time between forced outages caused by multiple random failures of M-MIS equipment shall be greater than fifty reactor operating years. This requirement shall apply over the entire design life of the M-MIS equipment. For the purpose of this requirement, forced outages shall include shutdowns that result directly from the failures, and shutdowns the operators must perform to avoid violation of plant Technical Specifications due to these failures.	Current experience shows that forced outages caused by M-MIS failures are in excess of one occurrence per plant per year. This is a major initiating event in PRA studies. Improving this figure by a factor of 10 can reasonably be achieved by the application of modern technology, good design practices and through surveillance/maintenance procedures to reduce equipment failure rates and reduce the time for detecting, bypassing, or repairing the failure. An additional improvement of 5 is expected through simplification, the procurement of high quality components, rigorous testing and improved environment compatibility of components. Since the M-MIS is always in series with the plant equipment, the combined failure rate for the system will be higher than either of the individual contributors. Therefore, in order to meet the overall ALWR plant availability goal, significant improvement in the forced outage rate due to M-MIS equipment failures will be necessary.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.2.2	**Loss of Availability**	**Loss of Availability**	0
	The mean time between M-MIS equipment failures, which result in a reduction in plant availability, shall be greater than 5 years over the entire design life of M-MIS equipment. For the purpose of this requirement, a loss of plant availability is defined as a condition in which the plant is unable to achieve or maintain steady state operation at any point within the warranted plant output range.	The probability of a failure in the M-MIS resulting in loss of plant availability during the plant fuel cycle should be minimized in order to meet the overall ALWR plant availability goal.	0
3.5.2.3	**Maintenance Frequency**	**Maintenance Frequency**	0
	Corrective maintenance of the following major parts of the M-MIS shall not be required more frequently than every 14 days over the entire design life of the M-MIS equipment, i.e., the mean time between failures which require corrective maintenance shall be greater than 14 days.	Even though the system may be configured so that the failures do not impact the overall availability, corrective action still involves Utility effort and needs to be limited. .	0
	• Protection system;		0
	• Plant control system;		0
	• Plant information and monitoring systems.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.3	**Design Requirements for Availability and Reliability**	**Design Requirements for Availability and Reliability**	0
3.5.3.1	**Segmentation of Major Functions**	**Segmentation of Major Functions**	0
	The M-MIS control and monitoring systems shall be designed to protect against failures of M-MIS equipment degrading the performance of more than one major control or monitoring function. The functional and physical designs of these systems shall be segmented or explicitly incorporate other functional defensive measures to inhibit the propagation of failure across major functions. The major control and monitoring functions that shall be segmented or incorporate functional defensive measures in the design include, as a minimum, those listed in Table 10.3-1. In those cases where strict segmentation of the major control functions is not practical or the designer can identify alternative design approaches which will achieve the same functional requirement – defense against propagation of unforeseen failures across major functions – the designer shall specifically identify and justify the alternative design approaches. Dependence on redundancy alone as a substitute for segmentation is not acceptable. The areas of the design where strict segregation of major functions have not been maintained shall be specifically identified in the design documentation and the alternative design criteria to maintain functional separation shall also be documented.	Availability and reliability of the M-MIS is of paramount importance in the ALWR. Since it is expected that newer technologies will be applied in the M-MIS, including use of computers and multiplexed data transmission for which it is easy and cost-efficient to perform many functions in a single piece of equipment, the requirements need to ensure that the design is as "forgiving" as possible in terms of the probability and consequences of failures of this potentially shared equipment. Existing regulatory requirements enforce segmentation and separation on the safety and protection systems; however, there are no such requirements for the major plant control and monitoring functions. The intent of the requirements given here is defense-in-depth: to give the utility a greater degree of assurance that failures, in particular, failures not initially foreseen in the design, will be limited in their effects such that, if they occur, they cannot propagate across more than one major control function. These segmentation requirements also aid in ensuring simplicity in the design by precluding complex combinations or interconnections of functions. This, in turn, promotes better understanding of the systems and equipment by the plant operators and maintenance technicians and is expected to reduce operator burden and errors.	0

TABLE 10.3-1

CONTROL AND MONITORING FUNCTIONS REQUIRED TO BE SEGMENTED

PWR SEGMENTS	SEGMENT SCOPE
Reactivity Control	Automatic and manual control and monitoring of rod positions and manual control and monitoring of boron concentrations and neutron flux.
Steam Generator Inventory Control	Control and monitoring of main feedwater flow, main feed pumps and steam generator inventory.
Turbine Steam Demand Control	Control and monitoring of turbine throttle valves and bypass valves.
Pressurizer Pressure Control	Control and monitoring of the pressurizer heaters and spray and reactor coolant system pressure.
Reactor Coolant System Inventory Control	Control and monitoring of makeup and letdown, reactor coolant system inventory and CVCS inventory.

BWR SEGMENTS	SEGMENT SCOPE
Control Rod Position Control	Control and monitoring of rod position.
Neutron Flux Monitoring	Monitoring of neutron flux.
Reactor Recirculation Flow Control	Control and monitoring of recirculation flow.
Reactor Feedwater Control	Control and monitoring of main feedwater flow, main feed pumps and reactor water level.
Reactor Steam Pressure Control	Control and monitoring of turbine throttle valves and bypass valves and reactor steam pressure.

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
		It is recognized that there may be situations in which strict segmentation may not be practical. In those few instances when it is not practical, alternate design approaches are allowed. Depending solely on redundancy is not allowed since: (1) a failure in one of the redundant paths could cause a heavy work-load and possible confusion for the operator by indicating there is a problem in more than one major function, and (2) unforeseen or unexpected failures (e.g., maintenance errors) which affect more than one redundant path could cause large-scale upsets threatening more than one major process function.	0
3.5.3.1.1	**Segmentation of Sensors and Data Transmission**	**Segmentation of Sensors and Data Transmission**	0
	The functional designs shall be such that each segmented function uses different process variables for performing the control function. For each segmented function, different sets of sensors and transmitters, and data communication paths from sensors and transmitters to data processing equipment, shall be used whenever practical. This is not intended to preclude signals from a measured variable used in one control function from being used for signal validation, signal cross-checking, or calibration/compensation in another control function. However, if measured variables are used for this purpose, the designer shall ensure that a complete failure of instrumentation for the variable used for cross-checking will not prevent the receiving control/monitoring function from being performed adequately.	This requirement minimizes use of common sensing instrumentation for more than one major control function, reducing the possibility of a single problem causing a large-scale upset that would be difficult for the operators to handle or causing multiple indications to the operator of problems in more than one major control and monitoring function which are confusing to the operator.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.3.1.2	**Segmentation of Processing and Power Supplies**	**Segmentation of Processing and Power Supplies**	0
	Each segmented function (i.e., major control and monitoring functions) shall use different processors and power supplies (but not necessarily different power feeds or sources) whenever practical even if redundancy is employed. That is, to the degree practical, functions of one segment shall not be combined with functions of another segment in a single processor or set of processors, or power supply.	This requirement minimizes the use of common processors or power supplies for more than one major control function reducing the possibility that a single problem will cause a large scale upset that would be difficult for the operators to handle or causing multiple indications to the operator of problems in more than one major control and monitoring function which are confusing to the operator.	0
3.5.3.1.3	**Physical Separation of Equipment**	**Physical Separation of Equipment**	0
	Data processing and data communication electronic equipment for the different segments (i.e., major control and monitoring functions) shall be housed in separate enclosures, whenever practical. Equipment for segmented functions may share a common room or cubicle and be subject to a common ambient environment. The data communication links for segments shall not share a conduit or other communication pathway enclosure, unless there are redundant pathways also carrying the data which are not in the same conduit or pathway enclosure.	This requirement extends the segmented design philosophy to the data communications and data processing components of the M-MIS equipment. The intent is to prevent a local environmental upset such as a loss of ventilation to a single cabinet, or a fire in a single cabinet, or perhaps a saboteur damaging a single cabinet, from causing problems in more than one major function.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.3.1.4	**Physical Separation of Segments**	**Physical Separation of Segments**	0
	For the different segmented functions (i.e., major control and monitoring functions), signal communication paths, multiplexers and demultiplex units for transmitting information to the main control room displays and alarms, and for transmitting control commands from the control room to the data processing or output processing equipment shall have separate power supplies and shall be housed in separate enclosures outside the control room to the maximum degree practical.	This requirement is to prevent propagation of failures originating in the data communication paths between the control room and data processing equipment, or originating in the multiplex/demultiplex equipment at either end. The requirement is limited to enclosures outside the control room because for the control panels, human engineering considerations and task analysis will determine the location and arrangement of alarms, displays and controls for the different functions. The Remote Shutdown Station provides backup in case of major failures of control room control panels (e.g., fire in a panel) and for events requiring evacuation of the control room entirely.	0
3.5.3.1.5	**Segmentation Within Major Functions**	**Segmentation Within Major Functions**	0
	To the maximum degree practical, segmentation within major functions of the M-MIS shall mimic the segmentation within the mechanical systems being monitored and controlled.	This requirement is intended to prevent single failures or problems in the M-MIS which can result in a loss of control or monitoring of the intra-function segments provided by the mechanical portion of the system. An example would be a single failure within the pressure control function of the M-MIS which would result in a loss of control of all banks of pressurizer heaters.	0
3.5.3.1.6	**Segmentation of Safety-related M-MIS**	**Segmentation of Safety-related M-MIS**	0
	In addition to meeting applicable regulations, the M-MIS Designer shall, to the extent practical, apply a segmented approach for safety-related systems similar to that specified above for non-safety control and monitoring systems. This shall include segmentation within the safety divisions as well as between divisions as required by present regulations.	Since the ALWR intends that the normal control systems, as well as the safety systems, have very high reliability, it is advantageous to use similar approaches for both.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.3.2	**Environmental Conditions**	**Environmental Conditions**	0
	M-MIS equipment must be designed to survive and meet all reliability and availability requirements in the environment in which it is located for both normal and off-normal conditions. The M-MIS and other plant system designers shall iterate their respective designs so that the applicable requirements are met in the simplest, most robust manner. Strong preference shall be given for passive environmental protection techniques, e.g., natural circulation cooling, robust hardware operated far below rating, etc.	In the ALWR M-MIS, equipment will likely be more distributed than it has been in the past. As a result, special attention is needed to assure the equipment and the environment in which it is placed are compatible. Furthermore, a strong coupling is needed between the M-MIS Designers and those responsible for the environmental design to assure a balanced, economic design is achieved which is the simplest approach needed to assure adequate performance.	0
3.5.3.3	**Indication of Loss of Environmental Control**	**Indication of Loss of Environmental Control**	0
	A means shall be provided to alert plant operators when loss of environmental control has occurred in an M-MIS equipment cabinet and to locate promptly the affected cabinet.	The reliability of M-MIS equipment is sensitive to temperature and humidity. Some instances of loss of environmental control can be expected over the life of the plant. In order to mitigate the consequences of such events the plant operators must be alerted to the condition and the affected cabinet must be located to assure timely correction by the maintenance staff.	0
3.5.3.4	The design of the M-MIS equipment, including the quality level of the components, shall be such that if appropriate action is taken within one hour following a loss of environmental control in an M-MIS cabinet, no temporary or permanent loss of function (e.g., inability to generate a signal or the generation of spurious signals or unintended operation of equipment) will occur, i.e., restoration of proper environmental conditions will permit the equipment to be returned to service without replacing components.	Instances of loss of environmental control can be expected to occur over the life of the plant. This requirement is intended to prevent major failure of M-MIS equipment under these events and to provide a quantitative requirement for the margin to be imposed.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.4	**Reliability and Maintainability Analysis**	**Reliability and Maintainability Analysis**	0
3.5.4.1	**Reliability Analyses**	**Reliability Analyses**	0
	The M-MIS Designer shall perform analyses to predict the reliability of the Man-Machine Interface System (M-MIS) and subsystems. These analyses, termed "reliability analyses," shall be performed using consistent, systematic and traceable methods and appropriate analytical tools. These analyses shall be generally consistent with the guidelines provided in MIL-HDBK-338, *Electronic Reliability Design Handbook*, and MIL-HDBK-217E, *Reliability Prediction of Electronic Equipment*. The analyses shall consider the expected normal operating and environmental conditions and credible abnormal operating and environmental conditions. This shall include assessment of the probability of excursions to the most limiting environmental conditions, including consideration of failures of HVAC systems or components, and accounting for these excursions in the analyses. These analyses shall be documented and independently reviewed in the M-MIS design process.	Reliability analyses are required to demonstrate that the M-MIS design meets the quantitative reliability and availability goals. Since environmental conditions are important contributors to mean failure rate (or MTBF) of electronic equipment, it is important that environmental conditions resulting from possible HVAC system failures and upsets, as well as normal conditions, be considered explicitly in the assessments.	0

Paragraph No.	Requirement	Rationale	Rev.
3.5.4.1.1	**Component Reliability Basis**	**Component Reliability Basis**	0
	For the reliability analyses, the M-MIS Designer shall use the component reliability data available in MIL-HDBK-217E, *Reliability Prediction of Electronic Equipment*, or other equivalent published sources. M-MIS components for which reliability data is not available in MIL-HDBK-217E or other equivalent published sources shall have their reliability based on the results of reliability testing and statistical analyses as required by 3.5.4.1.2. The quantitative values of the mean failure rate, or MTBF, of M-MIS components and their bases shall be documented and independently reviewed in the M-MIS design process.	A consistent base of reliability data is necessary to ensure that the reliability of all components used in the M-MIS equipment reliability analyses are such that the results of the analyses can be compared. The MIL-HDBK-217E database is extensive and represents a great deal of experience with complex electronic systems and components. However, reliability data does not exist in MIL-HDBK-217E or other equivalent published sources for all components.	0
3.5.4.1.2	When adequate reliability data is not available in MIL-HDBK-217E, *Reliability Prediction of Electronic Equipment*, or other equivalent published sources, the M-MIS Designer shall perform reliability tests to determine the mean failure rate, or MTBF, of M-MIS components. Statistical analyses of the results of the reliability testing can be used to determine the one-sided, low end 95 percent confidence interval for the mean failure rate or MTBF of the components tested which shall then be used in the reliability analyses. These reliability tests shall be performed using methods which are generally consistent with the guidelines provided in MIL-STD-781, *Reliability Test Methods, Plans, and Environments of Engineering Development, Qualification, and Production*; furthermore, the statistical analyses shall be consistent wit the guidelines provided in MIL-HDBK-338, *Electronic Reliability Design Handbook*. The tests and analyses shall be documented and independently reviewed in the M-MIS design process.	In order for meaningful reliability analyses to be performed, reliability data is needed for all components. Some components may not have adequate, published reliability data. For such components, reliability testing and statistical analyses are required in order to generate reliability data. The use of the one-sided, low end 95 percent confidence interval ensures that "reliability" based on reliability testing and statistical analyses compares well with "reliability" based on published data. The one-sided, low end 95 percent confidence interval of the MTBF represents the MTBF for which there is 95 percent confidence that 95 percent of any additional samples of the population of the item tested will have an MTBF greater than or equal to the one-sided low end 95 percent confidence interval.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.4.2	**Sneak Circuit Analyses**	**Sneak Circuit Analyses**	0
	The M-MIS Designer shall perform analyses of all M-MIS hardware and software to identify unplanned operational modes, including the inhibition of desired functions and the actuation of unwanted functions. These analyses, termed "sneak circuit analyses" (SCA), shall be performed using consistent, systematic methods and appropriate analytical tools. These analyses shall be generally consistent with the guidelines provided in MIL-HDBK-338, *Electronic Reliability Design Handbook*, and shall be documented and independently reviewed in the M-MIS design process.	A "sneak circuit" is the term applied to a latent path or condition in a system potentially resulting in unexpected operational modes which are not caused by component failures but are due to design oversight. Sneak circuit analysis (SCA) identifies these latent and largely hidden shortcomings of the system design. SCA focuses on the interconnections, interrelationships, and interactions of system components; therefore, SCA necessarily considers the complete system configuration. Due to the complexity and size of many systems in the M-MIS, system testing to identify the "sneak circuits" is neither an economical nor a logistically feasible alternative to analysis. (However, an SCA does not replace system functional testing; system testing is performed to demonstrate that the system is constructed and operates as designed.) Due to the nature of "sneak circuits," they are often evidenced as spurious operational modes and can appear in mature, thoroughly tested systems even after long periods of field use.	0
3.5.4.3	**Failure Modes and Effects Analyses**	**Failure Modes and Effects Analyses**	0
	The M-MIS Designer shall perform analyses to identify significant effects which result from the credible failures of individual M-MIS components. These analyses, termed "failure modes and effects analyses" (FMEA), shall be performed using consistent methods and appropriate analytical tools and shall generally be consistent with the guidelines provided in MIL-STD-1629A, *Procedures for Performing a Failure Modes Effects and Criticality Analysis*, and MIL-HDBK-338, *Electronic Reliability Design Handbook*. These analyses shall be documented and independently reviewed in the M-MIS design process.	An FMEA addresses each credible failure mode (e.g., failure of motor control logic), determines the possible effects from such failures (e.g., shutdown of a reactor coolant pump), and classifies each failure mode according to its effects (e.g., loss of plant availability). The results of the FMEA are used to demonstrate that the M-MIS design meets the quantitative reliability and maintainability design goals. FMEA can also assist in the identification and elimination of common mode failures and may suggest areas where improvements in reliability can be achieved. Finally, the FMEA results are also useful for maintenance planning analysis.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.5.4.4	**Maintainability Analyses**	**Maintainability Analyses**	0
	The M-MIS Designer shall perform analyses of all M-MIS hardware to predict the amount of time that an M-MIS subsystem or component will be inoperative due to maintenance activities. These analyses shall be performed using consistent, systematic methods and appropriate analytical tools. These analyses shall be generally consistent with the guidelines provided in MIL-HDBK-472, *Maintainability Prediction*, and shall be documented and independently reviewed in the M-MIS design process.	These analyses will provide the quantitative measure of whether the maintainability requirements of Section 3.7 have been met and will provide input for maintenance planning.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.6	**TESTABILITY REQUIREMENTS**	**TESTABILITY REQUIREMENTS**	0
3.6.1	**Continuous On-line Testing**	**Continuous On-line Testing**	0
	The capability for continuous on-line self testing of hardware integrity shall be provided for as much of the M-MIS as is practical. This testing shall not affect the system functionality and shall be performed on the module, as opposed to the system basis. These tests may include, but are not limited to, RAM and ROM failure checks, arithmetic processing unit failure checks, data link buffer checks, and CPU reset of watch-dog timers.	Continuous on-line self testing provides continuous monitoring overall system availability by rapid identification of hardware failures. This requirement also provides guidance as to the minimum coverage of the tests.	0
3.6.2	**Periodic Testing**	**Periodic Testing**	0
	The capability for periodic functional testing of the systems shall be provided. This periodic testing shall be manually initiated, but automatically performed once initiated, and shall meet the requirements of Regulatory Guides 1.22 and 1.118 and IEEE Standard 338. Automatic initiation of periodic testing may be provided where the testing does not degrade the system functionality.	Automated periodic functional testing improves overall system reliability through identification of system failures.	0
3.6.3	**Reliability of Testing Features**	**Reliability of Testing Features**	0
	The mean time between failures of M-MIS continuous on-line self-test features and periodic functional test features shall be equal to or greater than the equipment they are designed to test.	The benefits gained by built-in test features should not result in a significant increase maintenance burden.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.6.4	**Reconfiguration After Failure Detection**	**Reconfiguration After Failure Detection**	0
	Upon detection of a failure in the M-MIS, a system shall be designed so that it can be placed in a configuration such that an additional single failure will not prevent system-level protection or safety action. This reconfiguration shall be automatic in the case of continuous on-line self testing with notification of the new reconfiguration given to the operator. Where the system configuration has sufficient redundancy to meet the reliability goals without automatic reconfiguration, such automatic reconfiguration need not be provided; however, the operators must be alerted to any failures detected by on-line self-testing.	The ability to reconfigure a system improves overall system reliability. It is not the intent of this requirement to have the entire M-MIS have the capability to accept two failures.	0
3.6.5	**Failure Location Identification**	**Failure Location Identification**	0
	The M-MIS test features shall identify the location of a detected failure down to the lowest replaceable module.	Replacement of the lowest replaceable module will reduce the mean time to repair and reduce the risk of replacing non-defective hardware during a protracted troubleshooting exercise.	0
3.6.6	**Classification of Automatic Test Circuits**	**Classification of Automatic Test Circuits**	0
	The automatic testers for M-MIS Class 1E shall be classified as associated Class 1E circuits and shall meet the requirements for associated circuits as described in IEEE 384 and the reliability requirements of this Chapter.	Since the automatic testing inherently affects the reliability of the circuits being tested, the testing circuits must have a high reliability to be effective in finding failures and to avoid false failure indications.	0
3.6.7	**System Reconfiguration for Testing**	**System Reconfiguration for Testing**	0
	Built-in, automated test features shall be provided for periodic, functional testing as necessary to eliminate physical reconfiguration of systems (e.g., adding jumpers, lifting leads, swapping cables) to accomplish the required tests. However, manual initiation shall be required for any periodic, automated functional tests.	Built-in test features to eliminate system reconfiguration will be expected to alleviate problems experienced in present LWRs that have resulted from designs with poor testability.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.6.8	**Safety-Related System Testing**	**Safety-Related System Testing**	0
	The Safety-Related Systems, e.g., reactor protection and engineered safety features actuation systems, shall have automatic test features that are sufficient to meet the Technical Specification requirements for periodic surveillance of the system's functionability as defined by Regulatory Guides 1.22 and 1.118 and IEEE Standard 338.	Manual initiation allows administrative control over initiation of automatic test sequences. This provides the operator with the ability to prevent testing if conditions do not warrant testing.	0
3.6.9	**Test Performance**	**Test Performance**	0
	Test features of the M-MIS shall be designed so that, to the degree practical, the tests can be performed with the plant at power without causing spurious actuation of reactor trip devices or safety system components. Where testing at power would upset plant operation or damage equipment, provisions shall be made to test the equipment with the plant operating at reduced power or in a shutdown condition. All tests required to be performed to keep the plant at power or increase power shall be capable of being performed without shutting down or reducing power.	The ability to perform functional tests at power eliminate the potential need to come off-line to meet technical specification testing segments. The ability to perform all tests at shutdown ensures full system functionality prior to startup.	0
3.6.10	**Automatic Bypass**	**Automatic Bypass**	0
	Once the functional tester is enabled and a test sequence is manually initiated, the testing shall not proceed unless proper bypasses have been established. The bypass conditions required for testing shall be established automatically.	Reduces the risks of potential operator error which could result in unintentional actuation of M-MIS equipment.	0
3.6.11	**Indicators for Test and Bypass Status**	**Indicators for Test and Bypass Status**	0
	For the periodic functional tests, the tester shall have indicators at the local cabinet to provide a quick indication of pass or fail status for the test and the status of bypasses.	Local indication of pass or fail status and the status of bypasses reduces time for system repair.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.6.12	**Test Result Records**	**Test Result Records**	0
	The M-MIS design shall provide an industry standard printer interface at the local cabinet to allow plant personnel to obtain a hard copy record of the automatic test results. As a minimum, the test results printed should include identification of each subtest and the pass or fail status of that subtest.	Printout of test results reduces time to repair or replace failed M-MIS modules or equipment. A standard printer is required to ensure ease of maintenance or replacement.	0
3.6.13	**Removal of Automatic Bypass**	**Removal of Automatic Bypass**	0
	Upon completion of a test sequence, the automatic tester shall remove all bypasses which were established to allow the automatic test to be performed. Positive indicating features shall be included within the design to allow plant personnel to determine that all test bypasses have been removed and that the system has been properly reconfigured for normal operation.	Reduces potential for error which could result in unintended activation of M-MIS equipment.	0
3.6.14	**Process Input Signals**	**Process Input Signals**	0
	During periodic functional tests, the reactor trip and safety system functional processors shall not depart from their normal execution paths. Therefore, all input and output functional testing performed by the automatic tester shall be done using simulated process input signals.	This is the preferred test method.	0
3.6.15	**Testing at Initialization of Processors**	**Testing at Initialization of Processors**	0
	Comprehensive self-diagnostic routines shall be performed upon initialization for all processors.	This is a preferred method; it provides a consistent level of readiness when equipment is powered-up, and reduces the need for back-tracing to find a problem.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.7	**MAINTAINABILITY**	**MAINTAINABILITY**	0
	The M-MIS shall be designed to simplify and reduce the amount and difficulty of the maintenance required over the lifetime of the plant.	Experience has shown that M-MIS maintenance can be a significant burden on the owner's staff or can be so difficult that errors are prevalent and the plant reliability is reduced. Ease of maintenance must be designed into the M-MIS – it cannot be added after the design is complete. The requirements of this section are intended to ensure that the M-MIS Designer has considered the need for practical maintenance as a fundamental part of the overall design.	0
3.7.1	**Maintenance Burden**	**Maintenance Burden**	0
	The M-MIS Designer shall quantify the expected aggregate maintenance burden of the M-MIS equipment in terms of the times and skills of the maintenance technicians and the operator's time which will be required. This shall be based on the mean time between failure and the mean time to repair, considering all the redundant channels and equipment. This shall also include preventive maintenance, periodic functional testing of safety related equipment required during plant operation, and planned replacements.	The maintenance requirements determine the minimum number and qualifications of maintenance personnel, as well as the maintenance related tasks which absorb operators' time and attention.	0
3.7.2	**Replacement of Equipment**	**Replacement of Equipment**	0
	It should be an objective that M-MIS equipment have a service life long enough that replacement during the plant life will not be required. Where this is not practical, e.g., no proven components are available, the M-MIS design shall include features to minimize the impact of the actual replacement and ensure that wearout does not reduce plant availability. The M-MIS design shall identify the service life of all equipment which must be replaced and outline the timing of the logistic support, e.g., equipment and manpower, which will be required on the part of the plant owner.	This information will be needed by the Utility to properly plan for maintenance over the life of the ALWR. This requirement is intended to apply to expected wearout; it is not intended to reduce the need to design all components for maintainability irrespective of whether they are expected to last for the design lifetime.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.7.3	**Modular Replacement**	**Modular Replacement**	0
	Repair of M-MIS equipment shall normally be accomplished by simple modular replacement in the field, i.e., rewiring or replacement of individual small components shall be done in the shop, not in the cabinets in the field.	The maintenance downtime will be reduced by modular replacement. Additionally, there will be less potential for miswiring or other repair related deficiencies with the system.	0
3.7.4	**Time to Detect and Repair a Failure**	**Time to Detect and Repair a Failure**	0
	The mean time to detect and repair failures down to the lowest replaceable module, averaged across all types of M-MIS equipment for the entire design life, shall be less than four hours. The maximum time to detect and repair failures of any M-MIS module shall be less than eight hours. This time shall include the time to detect the failure, gain access to the faulty equipment, determine the necessary repair, obtain necessary replacements or spares, make the repair or replacement, and verify that the repair has been successfully accomplished. The evaluation of the repair time shall assume that a technical with the necessary skill level will be available at the site.	These times are intended to be consistent with completing the average repair within a single shift by a single crew. It should also assure that no more than two shift crews will have to be involved in a single repair. This will minimize the need to exchange information between maintenance personnel and improve the accountability and, therefore, the quality of the work.	0
	This requirement applies to all M-MIS equipment with self-test capability. It shall be an objective to meet this requirement for other M-MIS equipment where practical. For example, it will probably be impractical to meet this requirement for cables which run from location-to-location within the plant or for sensors in systems which are not accessible to personnel when the plant is in operation.		0

Paragraph No.	Requirement	Rationale	Rev
3.7.5	**On-line Calibration**	**On-line Calibration**	0
	Any module that requires calibration more frequently than once per fuel cycle must provide for on-line calibration while maintaining adequate control, monitoring, and system performance.	Plant operation should not be disturbed if calibration must be performed between scheduled shutdowns.	0
3.7.6	**On-line Maintenance and Repair**	**On-line Maintenance and Repair**	0
	No activity associated with expected maintenance or repair of the M-MIS equipment shall prevent any plant safety or protection system from fulfilling its required function. In addition, the M-MIS system shall be designed to permit expected maintenance to be performed, to the greatest extent practical, while the plant is on-line. The design shall provide maintenance bypasses to allow for on-line repair including suitable lockouts or interlocks to ensure that operator errors will not lead to plant outages while repairs are in progress.	Maintenance obviously cannot be allowed to adversely affect safety or protection system operation. The ability to safely perform maintenance while the plant is operational allows reduction in plant outage maintenance burden and supports the ALWR availability requirements. The plant should operate correctly with a single safety-related channel in a test or bypass mode for repair without a significantly increased risk of shutdown. For example, during such an operation, the remaining safety-related channels should be designed to be locked out of test or bypass.	0
3.7.7	**Maintenance Human Factors**	**Maintenance Human Factors**	0
	The M-MIS shall be designed to recognized human factors standards and shall provide the specific features defined below.	A significant fraction of the problems with M-MIS maintenance have involved operator errors. Steps to make the maintenance easier should reduce the risk of errors as well as the time to effect the maintenance.	0
3.7.7.1	**Identification of Maintenance Tasks**	**Identification of Maintenance Tasks**	0
	The M-MIS Designer shall systematically identify the tasks required to maintain the M-MIS equipment, including definition of skills, tools, test equipment, access, etc. These tasks shall include any testing required to return the equipment to service after maintenance is complete. The results of this analysis shall be provided as part of the M-MIS design.	The Utility will need to know the qualifications of maintenance personnel and the support and test equipment necessary to maintain M-MIS equipment in operation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.7.7.2	**Evaluation of Maintenance Tasks**	**Evaluation of Maintenance Tasks**	0
	The M-MIS Designer shall evaluate the maintenance tasks to ensure that required maintenance actions are simple and well understood and within the expected capability of maintenance technicians. The evaluations shall use mockups or prototypes of typical M-MIS equipment and the performance of maintenance task walkthroughs. The evaluations shall be accomplished early enough in the design process to allow feedback to be incorporated into equipment design to resolve discrepancies discovered by the task evaluations. The results of the task evaluations shall be provided as part of the M-MIS design information.	Accessibility, adequate maintenance envelope and pull space requirements for equipment removal, maintenance related communication requirements and actual interface with equipment can best be demonstrated by evaluations conducted with mockups or prototypes of M-MIS equipment. The task evaluations will also provide information needed by the owner to prepare maintenance procedures.	0
3.7.7.3	**Equipment Design for Maintenance**	**Equipment Design for Maintenance**	0
	The M-MIS equipment (circuit boards, racks, terminations, etc.) shall be designed to facilitate maintenance and repair and to minimize confusion and the chance for error during these operations. This includes such features as:	Significant improvements in the ease of maintenance should be achievable by consistently considering maintenance as an integral part of the overall M-MIS design. Designing the M-MIS equipment for maintenance will reduce the maintenance time for the plant owner and, in addition, the incidence of maintenance errors.	0
	• Locations and arrangements which are functionally logical;		
	• Unambiguous, readable, and consistent labeling of components, both inside and outside of cabinets, in accordance with the general guidance contained in EPRI NP-6209, *Effective Plant Labeling and Coding*, and consistent with other plant labeling practices;	Existing experience indicates that many errors occur due to lack of or inadequate labeling on the inside and outside of panels. Installed communication features allow maintenance, operations, and test personnel to establish continuous communications without leaving the work area and eliminates the need to run communication cord through doors and across floors. (See also Section 4.6 for communication requirements.)	
	• Accessible and identified test points;		
	• Appropriate protection against inadvertent actuation, shorting out of terminals, dropping of parts, etc.;		0

Paragraph No.	Requirement	Rationale	Rev
	• Power for test equipment;		0
	• Posted cautions and critical instructions;		0
	• Provisions for communicating between locations where maintenance, observation, and testing is required.		0
3.7.7.4	**Access for Maintenance**	**Access for Maintenance**	0
	The M-MIS cabinets shall be designed to facilitate access by maintenance personnel. The design of M-MIS cabinets should allow specialized maintenance technicians to work on their particular equipment without interference with equipment serviced by other technicians.	Ease for access for maintenance of M-MIS cabinets will promote fewer maintenance related upsets caused by miswiring or difficulty experienced with returning the system to the correct configuration following the maintenance activity.	0
3.7.7.5	**Maintenance Location**	**Maintenance Location**	0
	For continuously manned control stations, particularly in the main control room, maintenance personnel shall be able to troubleshoot, perform related tests, and repair M-MIS equipment in an area which does not impair the operators' ability to access controls and displays or disrupt the operators' view of the control panels. The only exception shall be to allow maintenance personnel access to physical control switches or modules and front panel displays where front access is necessary to repair this equipment. The need for maintenance personnel to gain access to the control panel fronts shall be minimized.	Although the operators need to be aware of repair work in progress, additional personnel in the vicinity of the operating station is distracting. It is particularly distracting when the maintenance personnel are literally "under-foot."	0

Paragraph No.	Requirement	Rationale	Rev
3.7.7.6	**Operator Actions to Effect Repairs**	**Operator Actions to Effect Repairs**	0
	M-MIS equipment that normally receives input from controls on the main control panels or consoles and drives indicators or displays on the panels shall be capable of receiving signal inputs which simulate the controls and shall be capable of providing and monitoring outputs so that the control panel operator is not required to take action to provide the inputs or monitor displays and indicators during repairs, except in those cases when the front panel components themselves are being repaired. The operators, however, shall be provided with an indication when testing is in progress which affects the operability of equipment or systems or makes that equipment or system more susceptible to unusual events, e.g., spurious trips.	Although the operator at the control panel will need to know that repairs are in progress, his active participation in the repair operation itself will distract him from his other responsibilities.	0
3.7.7.7	**Controls and Displays for Maintenance**	**Controls and Displays for Maintenance**	0
	Controls and displays which are used only by technicians in the course of maintenance and repair, i.e., are never used by the operators, shall not be on the front of panels unless they are covered and do not crowd the operators' controls and displays. This includes such items as programming controls, test connections, calibration controls, various test lights, and some set point adjustments.	Displays and controls which are not used by the operator crowd the panels and distract the operator. In some cases, these controls can affect operation if inadvertently actuated. For example, some stock, general purpose controls or displays include front mounted programming or calibration controls which are used only for maintenance.	

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
3.8	**CONSTRUCTIBILITY**	**CONSTRUCTIBILITY**	0
	The M-MIS design shall incorporate features to reduce the time and effort to fabricate and install the M-MIS equipment; however, these features shall not adversely impact the ability to operate, test, maintain, and repair the equipment. This section identifies some of the specific requirements for these features.	Ease of construction and installation of the M-MIS is important to meeting the ALWR cost and schedule goals; however, these must not overshadow the owner's long term needs for ease of operation and maintenance.	0
3.8.1	**Use of Proven Techniques**	**Use of Proven Techniques**	0
	The fabrication and installation of M-MIS equipment shall be based on proven manufacturing, assembly, and installation techniques.	For the ALWR, it is the intent that the plant incorporate, to the maximum extent practical, the latest construction technologies. These technologies must, however, be proven in order to ensure installation costs and schedule for M-MIS equipment are predictable.	0
3.8.2	**Minimization of Field Operations**	**Minimization of Field Operations**	0
	The M-MIS shall be designed to incorporate features which minimize the amount and difficulty of the operations which are required in the field to install the M-MIS equipment. These features shall include the items identified below.	Field operations tend to be more difficult to control than shop operations, particularly for detailed operations or those where a clean or controlled environment is needed. Field labor is also typically relatively high cost, particularly for the skilled technicians needed for M-MIS equipment.	0
3.8.2.1	**Modular Design**	**Modular Design**	0
	The components of the M-MIS shall be designed to allow installation and functional checkout of each module separately, prior to complete system integration. Control systems cabinets and panels should be fabricated, wired, and functionally tested before they are installed as modules in the plant.	The capability to perform installation and functional checkout on a modular basis permits these operations to commence before all M-MIS subsystems become completely available. This will result in an earlier M-MIS availability. Since the availability of the M-MIS is essential to the plant startup test program, early availability of a working M-MIS is important to the overall ALWR startup schedule. In addition, shop fabrication of modules or subassemblies of M-MIS type equipment has proven to be cost effective.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
3.8.2.2	**Field Wiring**	**Field Wiring**	0
	The M-MIS design should limit the amount of wiring which is done in the field. Maximum use of multi-conductor connectors and pre-assembled wiring harnesses should be made. Where connectors are used, means to ensure proper indexing and ensure against shorts or inadvertent contacts shall be provided. Single wire-to-wire or wire-to-terminal connections should be avoided.	Shop wiring provides more controlled assembly conditions which can reduce costs and should reduce wire connection errors. Additionally, shop testing can validate wiring installations and make corrections before delivery of the equipment to the site. Use of wire harnesses reduces field installation labor and field miswiring.	0
3.8.2.3	**Modular Design**	**Modular Design**	0
	Wire harnesses and cable shall include spare conductors, where practical. These spares shall be used to replace wire damaged during equipment shipment, installation, and other construction activities as well as providing flexibility for plant repair or modification per 3.9.	Damage of wiring during equipment shipping or installation could require stringing replacement wiring. Spare conductors in a wiring harness could eliminate the time necessary to run wiring to replace wiring damaged during equipment shipment or installation.	0
3.8.3	**Standardized Designs for Construction**	**Standardized Designs for Construction**	0
	The features incorporated in the M-MIS which impact the field operations shall be standardized, where practical. This includes such items as: • Sizes and types of connectors and harnesses; • Cabinet handling, shipping, and mounting hardware; • Labeling and identification of modules and components.	Differences in designs result in different techniques for the field operations. It complicates the control of field work and can lead to errors in installation.	0

Paragraph No.	Requirement	Rationale	Rev.
3.8.4	**Schedule for Construction**	**Schedule for Construction**	0
	The M-MIS Designer shall ensure the construction, fabrication, installation and checkout schedule of the M-MIS equipment to the site is such that it fully supports the aggressive construction and startup testing schedule of the ALWR plant. In particular, the M-MIS Designer shall plan on the basis that the permanently installed plant instruments and controls are used for plant testing and startup to reduce the amount of temporarily installed instrumentation and the amount of rework required to correct and retest systems because the plant equipment and the associated instruments and controls are not adequately coordinated.	In the current plants, instruments and controls are often not installed and operational at the time that plant equipment is ready for initial testing. As a result, temporary instruments and controls are jury-rigged to support these tests. Then, some of these tests must be repeated once the permanent controls and instruments are installed and checked out. The intent of this requirement is to prevent the recurrence of this problem and to facilitate meeting the aggressive ALWR construction and startup schedule requirements.	0

Paragraph No.	Requirement	Rationale	Rev.
3.9	**DESIGN FLEXIBILITY**	**DESIGN FLEXIBILITY**	0
	The M-MIS design shall provide flexibility to accommodate design changes and the ability to replace equipment due to aging, wear, or obsolescence. Specifically, the M-MIS design shall include design features such as: • A modular design, both functionally and physically, to accommodate replacements and upgrades gracefully; • Physical spare capacity in instrument panels, control consoles, terminal strips, wire ways, etc.; • Spare input and output capacity (both logical and physical) in computer systems; • Spare capacity in alarm and display systems for both information processing and physical presentation; • Spare capacity in data communication (system loading, etc.); • Spare capacity in power supply and HVAC.	Existing plant experience demonstrates the necessity for the M-MIS design to accommodate design changes, additions and upgrades. The state-of-the-art in M-MIS equipment is constantly changing, and obsolescence of equipment is a continuing concern. As a result, the M-MIS design must be flexible to allow for design changes and replacement of obsolete equipment without major disruption to overall ALWR plant availability.	0
	The plant configuration and design documentation shall specifically identify these features and outline how they could be utilized.	The documentation of these special features will assure that they can be reviewed for adequacy and that they will be fully recognized in the planning for any future plant modifications.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4	**CONTROL STATION REQUIREMENTS**	**CONTROL STATION REQUIREMENTS**	0
4.1	**CONTROL STATION DESIGN PROCESS REQUIREMENTS**	**CONTROL STATION DESIGN PROCESS REQUIREMENTS**	0
	The M-MIS Designer shall establish a process to ensure a consistent design approach for all the plant control stations in the M-MIS. The requirements for this process are in this section and in Section 3.1.	It is important that all the control stations in the plant be workable and consistent with each other. Unless a process specifically directed at achieving this goal is used, the control stations will be developed largely independent of each other, they may not be workable as a total system, and it is unlikely that they will be consistent.	0
4.1.1	**Utilization of Functions and Tasks**	**Utilization of Functions and Tasks**	0
	The Control Station design process shall be based on and integrated with the overall identification of functions and tasks required in 3.1.3.3	The direct coupling of the control station design to the overall M-MIS functions and tasks will assure that the control stations are compatible with the tasks which they are expected to support.	0
4.1.2	**Control Station Conceptual Designs**	**Control Station Conceptual Designs**	0
	The design process shall include the early preparation of conceptual designs for each control station based on the initial definition of tasks. These conceptual designs shall be complete enough to permit reviews as defined in 4.1.3 and include: • Layout drawings of the station; • Identification of the controls and displays and their major characteristics; • Specific listing of tasks in sequence and their requirements for information and control; • Preliminary procedures for the operation of the control station.	The early conversion of the functions and tasks to real hardware designs will assure that realistic verification and validation of the assignment of functions and tasks and the capability for their performance can be made. They will also allow any limitations imposed by the availability of hardware to be identified. The preliminary procedures will be used in the review process, e.g., in walkthroughs in mockups.	0

Paragraph No.	Requirement	Rationale	Rev
4.1.3	**Review of Conceptual Designs**	**Review of Conceptual Designs**	0
	The design process shall provide for the interdisciplinary review of each conceptual control station design and the functions and tasks assigned to the control station for compatibility.	Interdisciplinary review of the conceptual designs under conditions which approximate the control stations actual use is essential to the selection of a final configuration.	0
4.1.3.1	**Makeup of Review Team**	**Makeup of Review Team**	0
	The review team for each control station, as a minimum, shall include personnel with operational experience and human factors specialists in addition to engineering disciplines, specifically:	The control station designs have diverse impacts; consequently, the review team needs to represent a diversity of viewpoints.	0
	• Current or previously licensed, experienced operator (preferably an individual who has experience at the unlicensed level, the RO level, and the SRO level);		0
	• An I&C engineer;		0
	• A systems engineer familiar with the systems controlled at the control station;		0
	• A human factors specialist;		0
	• Individuals familiar with other disciplines appropriate to the functions of the particular control station, for example, maintenance, testing, procedures, lighting, radiation protection, communication, and licensing.		0
4.1.3.2	**Use of Mockup Control Stations**	**Use of Mockup Control Stations**	0
	The design process shall provide for the fabrication of a static mockup of each control station for use in the review process.	Although some initial reviews with drawings can be made, it is essential that accurate pictorial mockups be made at an early stage. This improves the quality of any reviews.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.1.3.3	**Use of Active Simulators**	**Use of Active Simulators**	0
	The control station design review process shall provide for the use of active simulation of the control stations.	Although static mockups can provide a review of some features, they inherently lack the time input which is important in some tasks. For such tasks, the early use of a simulator helps to avoid unreasonable demands on the operators.	0
4.1.4	**Iteration of Functions, Tasks, and Designs**	**Iteration of Functions, Tasks, and Designs**	0
	The design process shall provide for the iteration of the control station design with the functions and tasks assigned to the control station. That is, the design process shall specifically provide for feedback from the design of the individual control stations to the overall identification of functions and tasks and their assignment to particular control stations.	The design process needs to be such that difficulties found in the course of the review can result in reassignment of tasks. Otherwise,there is no mechanism to correct initial assignment of functions and tasks which lead to unsatisfactory control station designs.	0
4.1.5	**Definition of Design Practices**	**Definition of Design Practices**	0
4.1.5.1	The design process shall provide for the definition of the specific detail design practices as they evolve in the course of design development. These practices shall be based on published guidance on human factors practice, such as EPRI NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development*, and EPRI NP-6209, *Effective Plant Labeling and Coding*. These practices include:	Detailed design practices must be defined to ensure consistency from station-to-station. Much of the guidance on control station design, e.g., EPRI NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (see 4.4.1, 4.5.1, etc.), identifies the subjects which must be considered and some approaches; however, the detailed practice must be selected by the designer.	0
	• Types of controls and displays;		0
	• Labeling;		0
	• Color coding;		0
	• Demarcation;		0
	• Nomenclature;		0
	• Convention for locations;		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• Mimic conventions and symbols;		0
	• Abbreviations and acronyms.		0
4.1.5.2	Where the M-MIS Designer selects new technology (e.g., "soft" controls) for which published guidance on human factors practice is limited, the M-MIS Designer shall develop the necessary design practices based on the best available information. This design practice shall then be verified by experimentation, including active simulation, and explicitly included in the design review process. The review team shall specifically determine the need for further review of the design practices by human factors specialists.	The intent of this requirement is to assure that new technology is applied with proper consideration of the importance of its human factors impact.	0
4.1.6	**Documentation of Final Designs**	**Documentation of Final Designs**	0
	Detailed documentation of the final design of all control stations shall be provided. As a minimum, the requirements below shall be met.	The detailed documentation of the final design is needed by the Utility to support the training of operators, the preparation of the operating procedures, and to design future plant modifications.	0
4.1.6.1	**Design Configuration**	**Design Configuration**	0
	Complete definition of the configuration of each control station shall be provided. This shall include: • Arrangement of panels and other equipment; • Types of controls;	Design configuration control of control stations has typically been poor. Drawings of control panels tend to be directed at the fabrication (particularly wiring) rather than the presentation to and use by the operators. Consequently, incorrect or awkward configurations are not discovered until the plant is built. In addition, the information is often fragmented and difficult to use for training or for planning modifications.	0
	• Types of displays;		0
	• Colors, finishes, and materials;		0
	• Labels and operation aids.		0

Paragraph No.	Requirement	Rationale	Rev.
	The drawings shall provide a pictorially correct representation of the control station.		0
4.1.6.2	**Definition of Functions and Tasks**	**Definition of Functions and Tasks**	0
	The design documentation for each control station shall define the functions and tasks to be performed at the station in their probable sequence.	The functions and tasks for a control station provide a defined interface between the Plant Designer and the plant operator.	0
4.1.6.3	**Design Practices**	**Design Practices**	0
	The design documentation shall define the common design practices for all control stations. Any deviations from the common design practices and the basis for these differences shall also be documented.	The use of standard design practices will ensure consistency. It will also simplify training of operators and evaluating any future changes. Deviations from standard practices will need to be covered in training programs or operating procedures.	0
4.1.6.4	**Generic Operating Procedure**	**Generic Operating Procedure**	0
	The design documentation for each control station shall include its generic operating procedures. These procedures shall be reviewed as an integral part of the control station design review required by 4.1.3. This review shall include their validation using mockups and active simulation.	Although some modifications of these procedures by the Utility to conform to their individual practices will be required, these procedures will substantially reduce the effort needed by the plant staff. They will also help assure that the plant is, in fact, operated in the manner intended by its designer.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.2	**OPERATING CREW**	**OPERATING CREW**	0
4.2.1	**Normal On-Site Staffing**	**Normal On-Site Staffing**	0
	The M-MIS design shall be based on the staffing defined in this section for normal operation, i.e., the functions and tasks for normal plant operations may be carried out by these individuals within the constraints of qualifications and locations. The following normal shift operational staffing shall be accommodated by the M-MIS design:	This staffing is intended to comply with the applicable regulatory requirements. It provides for augmentation of this minimum staffing to assure adequate manning for emergencies is available and to assure routine and administrative tasks do not distract the operators actually at the plant controls from the plant operation. It provides for an additional RO to take much of the burden of contact with other plant personnel from the operators actually operating the plant. It also provides specifically for a clerk for the shift supervisor to assist with handling the administrative load.	0
	• One shift supervisor will be included in each shift. This individual will be responsible for overall plant operation and will have a senior reactor operator (SRO) license. This individual's normal station will be the shift supervisor's office which is adjacent to the main control room (MCR); however, at any time the shift supervisor may be anywhere within the plant boundary.		
	• One other individual with an SRO license will be part of each shift. This individual will be responsible for the direct supervision of the operators in the MCR. This individual's normal station will be in the main controlling area of the MCR; however, at any time the individual may be anywhere in the MCR.		0
	• Two individuals with reactor operator (RO) licenses will be part of each shift. These individuals will be responsible for the operations of controls in the MCR. These individuals will normally be located at the controls in the main controlling area of the MCR. One of these individuals (or another individual with an SRO or RO license) will be at the controls at all times. The other individual will be in the MCR at all times.		0

Paragraph No.	Requirement	Rationale	Rev
	• One other individual with an RO license will be part of each shift. This individual will be responsible to assist the operators in the controlling area of the MCR by interfacing with other members of the plant staff, e.g., switching and tagging for maintenance personnel. This individual's normal location will be in an area immediately adjacent to the controlling area of the MCR; however, the individual may be in the controlling area to relieve or assist another RO or anywhere within the plant boundary.		0
	• One individual qualified to provide engineering support as a shift technical advisor (STA) will be part of each shift. This individual will normally be located in an office immediately adjacent to the main controlling area of the MCR; however, the individual may be anywhere within the plant boundary.		0
	• Two individuals qualified as necessary to operate equipment in the plant at local stations shall be part of each shift crew. These individuals will not normally be located in the MCR but will be at various locations throughout the plant as operations require. The M-MIS Designer shall specifically evaluate whether two such equipment operators (EOs) are an adequate staff. If they are not adequate or if meeting this requirement adds substantial specialized automatic control or equipment, so that a change in the number of EOs is required, the basis shall be included in the M-MIS design documentation.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• One individual appropriately qualified and trained will be available on each shift to assist the Shift Supervisor with administrative details, e.g., obtaining references, handling correspondence, etc. This individual will normally be located in or adjacent to the shift supervisor's office; however, the individual may be located anywhere within the plant boundary.		0
4.2.1.1	**Operating Crew Responsibilities**	**Operating Crew Responsibilities**	0
	The M-MIS Designer shall specify the responsibilities assumed in the design for each member of the operating crew. This includes responsibility for supervision and should consider all plant operating modes.	This information is needed by the Utility in staffing the plant and planning for training.	0

Paragraph No.	Requirement	Rationale	Rev
4.2.2	**Staffing During Emergencies**	**Staffing During Emergencies**	0
4.2.2.1	The analyses of plant transients and emergencies performed as part of the M-MIS design process specified in Section 3.1.3.3.2, shall be based on the following assumptions: • At least one licensed operator will be in the controlling area of the MCR at all times during normal power operations, and will be available at the controls immediately to respond to any off-normal situation; • Two additional licensed operators (at least one of which is an SRO) will be available in the controlling area of the MCR within one minute when called upon; • Two equipment operators will be available via voice communication to respond immediately to commands from the control room operators; • The shift supervisor, the STA, and an additional RO will be available via voice communication to respond immediately to the control room operators and can be available in the controlling area of the MCR within ten minutes.	The intent of this requirement is to establish a firm, uniform design basis assumption for the analyses of operator workloads and adequacy of response to off-normal events. Since not all of the personnel listed in 4.2.1 above can be stationed continuously in the control room, it is important that the designer be given a clear statement on minimum availability of personnel for handling off-normal situations. Past experience has shown that the minimum manning level required for the operating staff is set not by normal operating conditions but by upset or emergency conditions, particularly situations in which equipment failures occur. In these situations, an operating team approach for monitoring and controlling the plant is considered the best approach, for several reasons: • Studies have shown that the best human operator can effectively track about five dynamic processes simultaneously. In the ALWR, it is expected that up to 8 to 10 dynamic processes could be running simultaneously during a design basis event. Although the automated systems expected to be applied in the ALWR could help track and control these processes, credible failures of plant equipment will still result in the need for more than one operator to monitor, make decisions and take action in upsets.	0
		• With the team approach, there will be multiple human minds available to "brainstorm" and develop optimum solutions to plant problems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
		• With the team approach, operators can back each other up. Human error will never be totally eliminated. Therefore, it is important to provide as much capability as possible to detect and correct human errors. Availability of multiple, trained individuals in the control room is beneficial in this regard.	0
4.2.2.2	In accordance with Chapter 1, Section 2.3.A, the required time for an operator to act in an emergency shall not be less than 20 minutes; however, the M-MIS Designer shall not preclude operator actions before that time. That is, the M-MIS design shall provide for operator actions on a realistically achievable timescale in an emergency in addition to the extreme case of no operator action for 20 minutes. The operating crew available following evacuation of the control room is defined in 4.9.3.4.	It is expected that operator actions in an emergency can materially reduce the seriousness of almost any event. It is not the intent of the requirement in Chapter 1 that the operators be reduced to mere observers.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.2.3	**Maximum Crew Size**	**Maximum Crew Size**	0
	The control room design (size, environment, layout, number, and design of workstations, etc.) shall support operation during emergencies in the main controlling area of the MCR by a maximum crew complement consisting of the following: • Two individuals with SRO licenses; • Three individuals with RO licenses; • One STA; • Two equipment operators. Provision shall also be made for two active observers in the main controlling area of the MCR. • One from the NRC; • One from the Utility management.	The control room should accommodate a range of crew sizes to allow for variation in utility practices, yet some bounds must be placed on this to help achieve a level of standardization and to prevent the control room design from becoming such a compromise that it does not effectively handle any crew size. The previous requirement on minimum assumed manning, and this requirement on accommodating a maximum complement of personnel, are intended to establish these bounds and provide a sufficiently firm design basis for off-normal or emergency conditions.	0
	These provisions shall include the identification of specific areas where these individuals can be located and observe activities without impeding the normal, maximum crew complement.		0
4.2.4	**Operators Required for Normal Operation**	**Operators Required for Normal Operation**	0
	The M-MIS shall be designed such that a single licensed operator can adequately perform the monitoring and control functions needed to bring the plant from a hot standby condition to full power, maintain operation at power, and bring the plant down to hot standby.	It is not within current regulatory requirements to startup with only a single operator and that is not the intent of this requirement. It is expected that if the operations are capable of being performed under nominal, routine circumstances by a single individual, then the additional personnel who will actually be available can be assured to be free to handle upsets and emergencies.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.2.5	**Operators Required for Heatup and Cooldown**	**Operators Required for Heatup and Cooldown**	0
	For startup from cold shutdown to hot standby and for shutdown from hot standby to cold iron, the M-MIS shall be designed such that the necessary control and monitoring functions can be accomplished by the normal shift crew defined in 4.2.1.	To achieve cold shutdown, and to startup from a cold condition, there are many control actions that must be taken locally in the plant. It is not expected that these actions will be made remotely controllable from the control room of the ALWR since this would require addition of many remote actuators, motor operators, etc., which would be costly and would significantly increase the complexity of the plant. There is little incentive to do so since these evolutions are not performed very often, and the manpower will be available (as noted in the requirements above, the manning level is set by upset and failure conditions).	0
4.2.6	**Qualifications of Operators**	**Qualifications of Operators**	0
	Where practical, the training, qualification, and experience of the operating staff members which are used as the basis for the M-MIS design shall be typical of current operating practice. The M-MIS Designer shall specify, early in the design process, any levels of training, qualification, and experience of the operating staff members which are used as the basis for the M-MIS design which differ from typical utility training and operating practices. These differences and their bases shall be included in the M-MIS design documentation.	The M-MIS design will inherently be based on an assumed skill level for each member of the operating crew. The Utility must know the assumptions in order to provide an adequate staff, particularly if the skill level is different from current practice.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.3	**ALARMS**	**ALARMS**	0
4.3.1	**General Alarm System Requirements**	**General Alarm System Requirements**	0
	The M-MIS design shall include a main process alarm system for the main control room, as well as alarm systems for local control stations where needed to support the functions and tasks assigned to the local control station.		0
4.3.1.1	**Design Basis**	**Design Basis**	0
4.3.1.1.1	The ALWR alarm systems shall be designed to: • Alert the operators to off-normal conditions which require them to take action; • Guide the operators, to the extent possible, to the appropriate response; • Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions; • Minimize distraction and unnecessary workload placed on the operators by the alarm systems.	Existing power plant alarm systems have proven to exhibit a number of common deficiencies, in their human factors and in general in their effectiveness in plant operation, particularly during upsets or other situations involving many alarms. These deficiencies in part result from a lack of treatment of the alarms as a system, that should have well-defined objectives and should be engineered as a system. In addition to the traditional objective of alerting the operators to specific off-normal conditions in the plant, prompting them to take action, alarms have proven to be a useful continuous source of information in and of themselves, and in fact to be the first source the operators may use in a top-level sort of information to determine the state of the plant.	0
		While alarm systems have the potential to be effective sources of information, they also have the potential to be sources of unnecessary noise, distraction and workload for the operators. The designer must try to minimize these while meeting the design objectives for the systems. Audible nuisance and awkward or burdensome acknowledgement schemes have been problems with existing systems.	0

Paragraph No.	Requirement	Rationale	Rev.
4.3.1.1.2	The designer shall apply the guidance given in EPRI reports NP-3448, *A Procedure for Reviewing and Improving Power Plant Alarm Systems*, and NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development*, in the design of the alarm systems, in addition to meeting the specific requirements given below.	EPRI has developed practical design guidance, based on experience with present alarm systems and original research, which is being applied by utilities to improve existing systems and should be used by the M-MIS Designer in synthesizing the ALWR alarm systems.	0
4.3.1.2	**Incorporation in Function and Task Analysis**	**Incorporation in Function and Task Analysis**	0
	The function and task analysis required by Section 3.1.3.3 shall specifically include the identification of where and how alarm information will be used to perform a function or task, or where tasks will be initiated or modified in response to an alarm.	Although the alarms together should be treated and engineered as a system, as indicated above, they are also an integral part of the overall M-MIS and are utilized in carrying out specific functions and tasks at a control station.	0
4.3.1.3	**Testing**	**Testing**	0
	The alarm system shall provide the capability for the operators to periodically confirm that it is functioning properly. Any portions of the alarm system that are not continuously checked through built-in test features shall be checked through periodic functional testing by the operators. The test capability shall be easy to understand and easy to use. Human factors evaluations shall be performed for the test "task" to ensure that it is consistent with and reinforces normal use of the alarm system.	Since alarms are not normally active but are counted on to alert the operators to off-normal conditions, it is important for the operator to be able to test and confirm proper functioning of the alarm system, particularly the audible devices (horns or tone generators) and the lights or other visual displays. Periodic tests also serve to reinforce memory of audible coding schemes, annunciation sequences, etc.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.3.1.4	**Evaluation by Simulation**	**Evaluation by Simulation**	0
	The effectiveness of the alarm system shall be verified through real-time, dynamic simulation. Simulator evaluations shall include specific evaluations of the important alarm system design features and characteristics – the adequacy of the specific alarms chosen, the effectiveness of the audible and visual displays, and the methods and devices for interaction between the operators and the alarm system (acknowledgement, silencing, display selection, etc.). Evaluation of some of these design characteristics can be carried out with less than a full scope simulator. However, final verification of the entire alarm system's effectiveness shall be performed using the full-scope simulator and shall be integrated with overall verification testing of the M-MIS and control room on the simulator. The specific measures used to judge alarm system effectiveness shall be defined by the designer, and shall be based on the specific design goals for the alarm system. Accordingly, these measures shall be defined early in the design process, and will be heavily interactive with measures used to judge overall control room and workstation effectiveness.	The only way to effectively evaluate the performance of an alarm system is to conduct real-time, dynamic simulations. The effectiveness of the system hinges on its performance during upsets and emergencies involving many alarms, with multiple horns going off, indications flashing, etc., whose full effect can only be evaluated through realistic simulation. Evaluations specifically aimed at the use and effectiveness of alarms have proven to be feasible and beneficial in previous research (see EPRI NP-5693P, *An Evaluation of Alternative Power Plant Alarm Presentations*). Experience in this and other research efforts in the U.S. and internationally has shown that the evaluations must be directed specifically at the use of alarm information in order to provide useful data on alarm system performance. A simulation which only checks that the operator did or did not "do the right thing" does not provide sufficiently specific data to determine the effectiveness of the alarm system, since so many other variables enter into determining a correct response.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.3.2	**Selection of Alarm Conditions**	**Selection of Alarm Conditions**	0
4.3.2.1	**Approach**	**Approach**	0
	A consistent approach and philosophy shall be used in selecting plant conditions that are to be alarmed. The selection process shall be based on interaction between the plant system designers and the M-MIS Designer to ensure that individual system requirements are met, while at the same time ensuring that uniform criteria are applied and the resulting alarm systems are compatible with the operators' needs and capabilities.	In the past, alarms often have been chosen by the fluid, mechanical and electrical system or component designers, with little influence by the control room designers. The result has been that the operators are presented with alarms from the various systems that are too numerous, chosen on different bases, and together are not as effective as they would be if the alarm set were looked at by a single individual or group applying uniform criteria and evaluating the alarm system as a whole.	0
4.3.2.2	**Criteria for Selection**	**Criteria for Selection**	0
	The criteria used in selecting alarm conditions shall include the following:	Application of the "action" and "dark board" criteria has proven effective in review and improvement of existing plant alarm systems. Improperly chosen set points have been one source of nuisance alarms in existing designs. See the latest revision or edition of EPRI report NP-3448.	0
	• For each alarm there is a defined action the operator is to take in response.		
	• The alarm conditions shall be chosen based on a "dark board at power" concept – no alarms should be present when the plant is operating normally at full power, with all systems in their normal configuration.		
	• Each alarm set point shall be chosen such that the operator will be alerted early enough to give him time to take the appropriate action, but the set point is not so close to the normal operating range as to produce unnecessary or nuisance alarms.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Where practical, alarms should be provided such that the operator is alerted **before** a major system or component problem results in a condition which causes a loss of availability (e.g., plant trip), equipment damage, violation of Technical Specifications, or other serious consequences. The M-MIS Designer shall assure that these precursor or anticipatory alarms do not become nuisance alarms as described in Sections 4.3.3.1 and 4.3.3.2.		0
	• Where possible, alarms on process deviations shall be based on validated process signals rather than individual sensor indications.		0
4.3.2.3	**Alarm Response Procedure**	**Alarm Response Procedure**	0
	For each alarm condition, an alarm response procedure shall be outlined by the designer, defining the required operator action and giving other information needed to ensure an adequate response.	To ensure that the action criterion is properly thought out when the alarm is initially chosen, and to assist in development of needed alarm response procedures, it is good practice to outline the response procedure at the time the alarm condition is identified.	0
4.3.2.4	**Temporary, Operator-Defined Alarms**	**Temporary, Operator-Defined Alarms**	0
	The capability shall be provided for temporary, operator-defined alarms and operator-defined set points on specific conditions where such alarms are determined to be of assistance to the operators in selected evolutions (e.g., temporary alarms to support increased monitoring of a problem component, or at other times when the operator wants to know of drift or approach to a limit for a specific variable). These temporary operator-defined alarms would be in addition to the set of required alarms determined to be necessary per Section 4.3.2.2 above.	Capability for the operator to define temporary alarms and set points to support specific evolutions or monitoring tasks allows him to use the alarm system to greater advantage, tailoring it when necessary to suit his needs. Giving the operator more control over the alarm set would be expected to lead to greater acceptance and use of the alarm system and better capability to detect and correct problems in operation before they lead to a plant trip. (It is expected that strict administrative controls would be put in place to insure against the proliferation of such alarms so that they would be limited to specific needs and would be eliminated when no longer necessary.)	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.2.5	**Documentation of Basis for Alarm Selection**	**Documentation of Basis for Alarm Selection**	0
	The designer shall document, as part of the formal design basis of the alarm system, the bases for selection of each alarm condition, including definition of the action required, basis for the chosen set point, etc. The guidance given in EPRI NP-3448 shall be used as a basis for this documentation.	Experience in reviewing existing plant alarm systems has shown the benefit of having a documented design basis for each alarm and its set point, to support modifications that may be required over the operating life of the plant.	0
4.3.3	**Alarm Processing**	**Alarm Processing**	0
4.3.3.1	**Nuisance Alarms**	**Nuisance Alarms**	0
	The alarm system shall be designed to minimize the potential for nuisance alarms. To support elimination of potential nuisance alarms, the alarm system shall incorporate the following features: • Capability to apply time filtering and/or time delay to the alarm inputs to allow filtering of noise or eliminate unneeded momentary alarms; • Capability to apply logic to alarm inputs, combining an input alarm condition with other alarms, signals, calculated conditions, mode indications, etc., with flexible logic that allows alarms to be made more "intelligent" or "conditioned" to prevent unnecessary alarm occurrences.	Nuisance alarms have been a common problem in existing plant alarm systems. Often, the alarm system design does not provide easy capability to treat these problems. The ALWR alarm system should include features that prevent nuisance alarms in the initial design, and flexibility to treat nuisance alarm problems that may develop later in plant life.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.3.2	**Evaluation for Potential Nuisance Alarms**	**Evaluation for Potential Nuisance Alarms**	0
	Each individual alarm shall be evaluated to examine its potential for nuisance alarming – that is, the potential for the alarm to occur unnecessarily, when no operator action is required. The evaluation shall consider: • All modes of operation of the plant and the associated system. • Maintenance of the associated system or component (e.g., the potential for many alarms to come in due to a component being shutdown for extensive maintenance);	To ensure that nuisance alarms are prevented in the initial design, it is important for the designer to look for possible nuisance alarm problems early in the synthesis of the alarm conditions. A specific evaluation of nuisance potential for each chosen alarm condition will help ensure this. The elements of the evaluation specified here are based on experience with nuisance alarms in existing plants.	0
	• Possible momentary alarm occurrences due to equipment startup (e.g., a low discharge pressure alarm on a pump that is enabled when the breaker is closed but pressure takes some time to build).		0
	• System dynamic response to plant transients or upsets which induce temporary physical disturbances capable of setting off the alarm but which are not indicative of an actual alarm condition (e.g., pressure oscillations in steam lines following turbine trip of MSIV closure picked up by steam generator level instruments as spurious level swings, feedheater or tank level oscillations induced by plant power changes, etc.).		0
	• Potential sources of noise (electromagnetic, contact bounce, etc.) at the alarm input.		0
	• Unusual (but plausible) lineups for the associated system or component.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Other conditions that might lead to unnecessary occurrences of the alarm.		0
	On the basis of this evaluation, the alarm's set point, input filtering or delay, conditioning logic, and other features shall be chosen to prevent nuisance alarms to the greatest degree practical.		0
4.3.3.3	**Capability for Reflash**	**Capability for Reflash**	0
	For any alarm that is formed from the combination of more than one input alarm condition through "OR" logic (e.g., a TROUBLE alarm combining several potential problems with a piece of equipment or system, or a bearing temperature alarm covering many bearings on one or more components), the alarm logic system shall provide the capability to "reflash" – reactivate the visual and audible indication for the alarm – when subsequent conditions occur after a first has come in and been acknowledged. The need to implement this reflash capability for multiple-input alarms shall be evaluated on a case basis for each alarm, considering the need for the operator to be alerted to subsequent alarm conditions and the potential for nuisance alarms if reflash is applied unnecessarily. For any multiple-input alarm, the operator shall have the capability to determine which specific input alarm condition activated the alarm, in a timeframe that supports taking the required action.	Multiple-input alarms have proven to be a major source of problems and costly fixes in existing plants. Availability of the reflash feature for all multiple-input alarms will ensure the utility has the necessary flexibility to treat this issue in a cost-effective manner in the ALWR plant.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.3.4	**Reduction in Number of Alarms During Upsets**	**Reduction in Number of Alarms During Upsets**	0
	The alarm system shall be designed to minimize the number of alarms that occur in plant upsets and emergencies, consistent with providing the operators with the information they need to formulate correct responses. The number of alarms and the rate at which alarms occur shall be reduced as compared to present plants, through use of filtering, conditioning logic, and other processing to eliminate unnecessary alarms and make alarms that do occur as informative as possible. Reduction in the number and rate of alarm occurrences in upsets shall be achieved primarily through use of system- and component-based logic applied to individual alarms to make them more intelligent and less likely to occur unnecessarily (see 4.3.3.1 and 4.3.3.2 above). Other, more "global" or plant-wide alarm suppression schemes such as mode suppression (preventing sets of alarms from activating when the plant is in a particular operating mode) or event suppression (preventing sets of alarms from activating when signals such as reactor trip or safety injection occur) may be used. However, the Designer shall provide justification for all alarms suppressed in this manner, ensuring that the operators are not deprived of information under any circumstances in which they may need it. Also, where such global suppression schemes are used, the capability shall be provided for the operator to access the suppressed alarm information through a manually-initiated request.	Testing of alarm systems under simulated upset and emergency conditions has shown a definite relationship between operator errors (in terms of alarms missed) and the number of alarms occurring, and an even stronger relationship between errors and the rate at which alarms occur (see EPRI NP-5693P). These results and experience from operating plants in actual upsets indicate the importance of reducing the number and rate of alarm occurrences. Careful selection of alarm conditions initially should provide improvement in this area. Also, use of natural, process-based relationships to condition alarms and make them less susceptible to occurring unnecessarily should provide considerable reduction in the alarm avalanche presently experienced. Going further to provide suppression of large blocks of alarms on the basis of priority, plant mode, or event signals has proven more difficult to define and implement successfully. The difficulty (and the danger) of such schemes lies in the fact that they tend to be more artificial, not rooted in natural process relationships, and the difficulty of foreseeing all possible situations in which the suppressed alarms may be needed.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.3.4	**Alarm Presentation**	**Alarm Presentation**	0
4.3.4.1	**Location and Type**	**Location and Type**	0
	The locations and types of alarm displays, and the specific alarms displayed on each, shall be based on ensuring that: • Each operator has the alarm information he needs to perform his assigned tasks, recognizing that different operating crew members may use alarm information for different purposes. • The characteristics of each display used to present alarm information are consistent with the intended use of the information (e.g., in the short term for prompt response to off-normal conditions, for longer-term diagnosis of equipment problems, for post-event analysis, etc.). • The alarm displays support the entire crew's needs in maintaining an awareness of the state of the plant and its major systems. • Alarm information is well-integrated with the other process information presented to the operators, allowing the operators to use alarms with other displays in monitoring and diagnosing problems	EPRI research has shown that different members of the operating crew may use alarms for different purposes. Some alarms require short-term response by the control board operators to take action on specific off-normal conditions in the systems and components for which they are responsible. The response to other alarms is longer term, and may require assembling other information to formulate the appropriate action. Alarms also support diagnosis and response to plant upsets or emergencies and can be used by all members of the crew, particularly supervisors and advisors, in getting the "big picture" and maintaining an awareness of the plant and system states. The research further shows that characteristics of the alarm display affect the crew members' ability to use alarm information effectively. See EPRI report NP-5693P.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.4.2	**Presentation Characteristics**	**Presentation Characteristics**	0
	Alarms that require short-term response by the operators, and the main process alarms used by the operators in diagnosing and responding to plant upsets or other events involving many alarms, or to maintain an overview of plant and system status, shall be presented on displays having the following characteristics:	Testing of alternate types of alarm displays has shown that displays having the listed characteristics are more effective in transferring alarm information and allowing use of alarm information by operators in the short term in multiple-alarm events. See NP-5693P.	0
	• Spatial dedication – the alarm messages always appear in the same position on the display so that the operator can make use of position and pattern recognition and always find the alarm when he wants to check its status.		0
	• Continuous, parallel presentation – the alarm information is always available to the operator, as opposed to a serial presentation in which the operator must select the information he wants to see.		0
	• Co-location with controls and displays – alarms are presented near the related controls and displays, helping the operator to quickly relate the alarms to the affected system or functional area of the plant.		0
	• Presentation of both normal and alarm state – the display is such that the operator can quickly determine whether a given alarm is "in" (in the alarm state) or the condition is normal, so he can determine (based on which alarms are not "in") where he does **not** have problems, he can use alarms to test hypotheses about what is wrong, etc.	• This is not intended to imply creation of alarms on **normal** conditions, but rather refers to the characteristic of conventional window-type annunciators that allows the operators to easily glance up and determine whether a particular alarm is present, whether an entire system is free of alarms, etc.	0

Paragraph No.	Requirement	Rationale	Rev.
4.3.4.3	**Alarm Grouping**	**Alarm Grouping**	0
	The spatially-dedicated display of alarms shall organize the alarms in groups by plant system or function. System/functional groups shall be clearly delineated and labeled such that any member of the operating crew located anywhere within the primary operating area can easily determine which systems have standing alarms and which system is affected by an incoming alarm.	Research has shown that organizing alarms by system or function is beneficial in improving the operators' ability to use the alarm information, particularly during upset conditions. (See EPRI NP-5693 and NP-3448.) Many utilities are rearranging their existing alarms to obtain this benefit.	0
4.3.4.4	**Prioritization of Alarms**	**Prioritization of Alarms**	0
	Alarms shall be presented in a manner which prioritizes them so that the operator's response can be based on their relative importance or urgency and the time within which the operator must take action.	As used here, prioritization refers to a scheme for identifying, coding or ordering alarms based on their relative importance or urgency to help the operator determine which alarms to act on first in a multiple-alarm event. This is typically done by assigning each alarm to one of two or more discrete "priority levels." For spatially dedicated displays, ordering alarms by importance may be accomplished through the position in the display. The need for prioritization and the extent to which prioritization should be applied will depend on the type of alarm display and other coding or ordering schemes that may be used.	0
4.3.4.4.1	**Criteria for Assignment of Priorities**	**Criteria for Assignment of Priorities**	0
	The assignment of priorities shall be based on documented criteria which shall become part of the defined design practices required by 4.1.5.	Documentation of the criteria for prioritization is necessary to assure adequate review and consistency. In addition, the documentation provides a basis for evaluation of future plant modifications involving alarms.	0

Paragraph No.	Requirement	Rationale	Rev.
4.3.4.4.2	**Number of High Priority Alarms**	**Number of High Priority Alarms**	0
	The number of alarms assigned to the highest priority level shall be limited so that in credible upsets or accidents which result in multiple alarms, the operators are not presented with an excessive number of highest priority alarms.	The effectiveness of the prioritization becomes degraded as the number of alarms displayed of a given priority level increases. To ensure that the most important (highest priority) alarms are identified easily by the operators, the number of these that occur in a given event must be strictly limited.	0
4.3.4.4.3	**Prioritization of Display Lists**	**Prioritization of Display Lists**	0
	Where alarms are displayed in the form of a list on a CRT or similar device, the M-MIS Designer shall demonstrate that the number of highest priority alarms does not exceed the capacity of the display for credible accident scenarios. That is, paging shall not be required to view all the highest priority alarms.	For a message list display in which only a limited number of alarms can remain visible to the operator, the inability to identify all of the highest priority alarms without action on the part of the operator degrades the system's usefulness.	0
4.3.4.4.4	The prioritization and method of coding shall be evaluated by real-time simulation which specifically confirms their effectiveness in realistic upset and accident scenarios.	The evaluation under real-time conditions is needed to confirm that the prioritization scheme does, in fact, help the operator order or prioritize his response to alarms, allows him to easily pick out and assimilate the most important alarms, does not interfere with or detract from other ordering or grouping schemes (e.g., grouping by system or function), and does not inadvertently distort the plant situation for the operator by over-emphasis of some alarms while others are relegated to a minor status.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.4.5	**Alarm System Controls**	**Alarm System Controls**	0
	Alarm displays and the controls provided for the operators to interact with the alarms (acknowledge, silence, reset, etc.) shall be arranged and located such that: • The operating crew member who must respond to an alarm can access the alarm information in sufficient time to respond adequately. • The need for one person to read an alarm message only to recite it to another person, who will then respond, is avoided. • The alarm messages are readable by the operator when he is at the station from which they will be acknowledged. • The need for an operator to leave a station at which he is working, in order to acknowledge an alarm, is avoided to the extent practical.	Alarm displays and control stations should be located to eliminate unnecessary operator burden to read and acknowledge the alarms, and the possibility that the operator acknowledges an alarm that he has not read. With computer-based alarm systems it is expected that acknowledgment of alarms can be made more efficient – for example, by allowing alarms to be called up at more than one workstation to allow reading and acknowledging the alarms.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.3.4.6	**Audible Tones**	**Audible Tones**	0
	The alarm system shall be capable of driving multiple audible tones or signals to annunciate alarm conditions. The types and volumes of audible tones or signals provided shall be chosen such that: • The operator is alerted to the presence of the alarm condition. • The operator can, from the specific tone and/or the direction of the sound, quickly determine where the alarm originated (which functional area of the plant, or which workstation) and therefore where he should direct his attention. • The amount of distraction and added stress on the operators owing to the audible alarm signals is minimized, through choice of the alarms, design of the audible annunciation scheme, and provision for silencing audible tones. • The tones used for incoming alarms are separate and distinct from tones used to signify "clearing" alarms, and the latter are momentary or "self-silencing."	Nuisance associated with audible devices has been a problem with existing plant alarm systems, particularly during plant upsets. This can be alleviated to a degree through proper choice of audible tones and volumes, by minimizing the number of unnecessary alarms, and by good design of the silence/acknowledge scheme.	0
4.3.4.7	**Integration with Control Station Design**	**Integration with Control Station Design**	0
	The alarms provided at a control station shall be treated as an integral part of the panel design of that control station, e.g., they shall be included in any mockup or simulation.	The alarms at a control station are an important part of the operator's field of attention. Adequate evaluation of the design of the station requires consideration of the alarms with the other displays and controls at the control station.	0

Paragraph No.	Requirement	Rationale	Rev
4.3.4.8	**Time Sequence of Alarms**	**Time Sequence of Alarms**	0
	As part of alarm processing, the alarm system shall tag each alarm with the time of its occurrence so that information on the time sequence of alarms is obtained, resolved to within 2.0 seconds or less. For alarms that are designated as sequence-of-events points, the time resolution shall be 4 milliseconds or less, except in specific cases where the M-MIS Designer demonstrates that coarser time resolution is adequate based on the operator's needs for time sequence information.	The sequence of alarm occurrences has proven to be crucial to understanding and diagnosing major plant upsets. Problems experienced in existing plants with loss of information in upsets, insufficient coverage of the alarms in the sequence, and lack of sufficient time resolution to obtain a correct sequence, should be prevented in the ALWR.	0
4.3.4.8.1	The operators shall be provided with capability to access at any time, via an on-line display and in printed form, the time sequence of alarms that have occurred over a pre-defined historical time period, covering at least four hours. The alarm system hardware and software shall have sufficient computational speed and capacity, buffer capacity, etc., to be sure that no alarm information is lost from this historical record for the worst-case upset or emergency the plant may suffer, including events involving losses of power and others that bring in many alarms. This alarm sequence information shall also be available at supervisors' and engineers' workstations, and in the technical support center (TSC).	See rationale for 4.3.4.8 above.	0
4.3.4.8.2	The time sequence of all alarms shall be included as part of the permanent historical records of plant operation.	See rationale for 4.3.4.8 above.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4	**DISPLAYS**	**DISPLAYS**	0
	The M-MIS Designer shall develop specifications for the displays at control stations which are consistent with the guidance in EPRI NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (particularly Chapter 6), EPRI NP-3701, *Computer-Generated Display Guidelines (Volumes 1 and 2)*, and the requirements of this section.	EPRI NP-3659 identifies the attributes which have to be considered when selecting the types of displays; however, it does not prescribe the design details. The M-MIS Designer will have to make specific choices and thereby develop the specific design practices (See Section 4.1.5).	0
4.4.1	**Consistent Presentations**	**Consistent Presentations**	0
	It shall be an objective of the M-MIS design to minimize the number of different types of displays which are used to present information to the operators. Differences in display type should be clearly related to differences in the character or use of the information by the operators. The Design Practices for the control stations should describe fully the logic for the selection of the display types.	In addition to the obvious practical advantages in maintenance and repair of minimizing the number of types of instruments, it is also important that the display not imply differences or similarities when that is not intended.	0
4.4.2	**Demand Indications**	**Demand Indications**	0
	Position or status indications provided to the operator shall be the actual component status or position. A "demand" indication, e.g., power to a solenoid valve or pressure to an air actuator, shall be supplied only if it provides the operator with needed information.	A so-called "demand" indication figured in the Three Mile Island, Unit 2, event. Unless these are considered early in the design, they may be very difficult to backfit. In some cases, both an actual and the demanded position or status may need to be displayed. It is not the intent of this requirement to substitute component status for process variables, e.g., an open valve signal is not a substitute for a flow signal.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4.3	**Indications of Disabled Display**	**Indications of Disabled Display**	0
	A display should provide a means to identify to the operator when its indication is properly erroneous, e.g., when it has no power or when the signal to it has been lost.	Some types of displays may still provide an apparently sensible indication to the operator even though there has been a failure in the system. A common example is the use of a mechanical meter to monitor a quantity with + and - voltage output which then "fails" to the center of the scale on loss of power or signal. This can result in considerable confusion for the operator.	0
4.4.4	**Position Indication for Valves**	**Position Indication for Valves**	0
	Position indication, i.e., open or closed, shall be provided for all valves at the location where they are controlled. Position indication shall be provided at other control stations where required by the analysis of functions and tasks. For control or throttling valves, a continuous indication shall be provided, i.e., open-closed is not sufficient. This continuous indication shall be located so that the operator has an immediate feedback of a control action.	In addition to the obvious need to show the valve's status, valve position indication provides an essential, immediate feedback of operator action; consequently, it must be provided at the same location as the control. This status may also be necessary for proper action at other stations. Control and throttle valves need more than open-closed indication to provide adequate immediate feedback. The feedback from the system response to a valve change, e.g., a change in level or temperature, may be relatively slow. This delay makes it difficult for the operator to detect promptly a nonfunctioning, e.g., stuck, valve.	0
4.4.5	**Current Indication for Motors**	**Current Indication for Motors**	0
	The operator should be provided with an indication of current draw for any major motor for rotating equipment (pumps and fans, for example) which can be started from the control station and for which motor current provides a meaningful indication of proper starting and running. This current indication shall identify to the operator the expected range of starting and running currents. Motors which operate only briefly, e.g., valve motor operators or breaker positioning activator motors, need not be provided with current draw instrumentation.	Motor current gives the operator immediate feedback of his control action as well as providing an immediate indication of abnormal operation of the motor and the component it is driving.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4.6	**Indicator Lights**	**Indicator Lights**	0
	Indicator lights which depend on a single light element (incandescent bulb, LED, etc.) shall not be used, i.e., the failure of a single light producing element shall not result in loss of information. Furthermore, any failure shall be evident and the replacement shall be easily performed by the operators themselves. In general, short-lived (less than 10,000 hour) light elements should be avoided.	The failure of indicator lights can result in erroneous information being supplied to the operators. Incandescent lights, in particular, are a maintenance burden, increase the heat load in the control room, and can result in shorts or shocks to personnel during replacement.	0
4.4.7	**Strip Chart Recorders**	**Strip Chart Recorders**	0
	Operational trend information shall be provided by displays which do not require paper, ink, etc., i.e., conventional strip chart recorders shall not be used. Similarly, multipoint chart recorders shall not be used to provide operational information.	Strip chart recorders have been a chronic maintenance problem in current plants. They have low reliability, take the operators' attention to change pens and paper, the chart time reliability is often poor, and their readability is usually not good. Multipoint recorders share the same problems as other chart recorders but have even worse readability. It is often necessary for the operator to watch the recorder go through the series of points or to manually select one of the points in order to reliably read its value. It is expected that the advanced technology of the ALWR M-MIS will provide operational trend information on displays such as CRTs or similar devices. The data recording function of chart recorders is expected to be provided by the plant data system.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4.8	**Integrating Displays and Mimics**	**Integrating Displays and Mimics**	0
	Where several individual control or work stations are provided in a room or work area, the M-MIS Designer shall evaluate the need for and, where necessary, provide integrated displays and mimics to coordinate the tasks at the various stations.	Providing key parameters and status indications independent of other displays provides information which would immediately be available to all operators and any supporting observers without burdening the normal display facilities and without any direct action by personnel other than to look up at the display.	0
4.4.8.1	**Incorporation of Integrating Displays in the Design Process**	**Incorporation of Integrating Displays in the Design Process**	0
	Any display shall be explicitly included in the process of developing the M-MIS design, especially the design of the work or control stations which it services. This shall include:	Any display needs to be an integral part of the design of the work stations which it serves; otherwise, the displays may distract or confuse the operators and degrade their performance.	0
	• The specific identification of the functions and tasks assigned to the overview displays;		0
	• The incorporation of the displays into simulators and mockups;		0
	• The specification of the use of the overview displays in the generic operating procedures.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4.8.2	**Main Control Room Integrating Display and Mimic**	**Main Control Room Integrating Display and Mimic**	0
	The M-MIS design shall include a display for the main control room which incorporates the following features:	This display is intended to support the "team" approach to control activities by providing a spatially dedicated, continuously available reference to the status of essential equipment controlled in the main control room.	0
	• Displays shall be provided of the values of a limited number of key operating parameters which are indicative of the state of the plant, for example:		0
	– Power level;		0
	– Reactor coolant system pressure;		0
	– Reactor coolant system temperatures;		0
	– Margin to saturation (PWR);		0
	– Reactor coolant flow rates;		0
	– Reactor vessel level;		0
	– Steam generator level (PWR);		0
	– Pressurizer level (PWR);		0
	– Steam pressure;		0
	– Steam flow.		0

Paragraph No.	Requirement	Rationale	Rev.
	• An integrated mimic and display shall be provided of the operational status, e.g., flow or no-flow, energized–de-energized, on-off or open-closed, of essential components controlled or monitored from the control room, for example: – Reactor coolant pumps (PWR); – Recirculation pumps (BWR); – Feedwater and condensate system pumps; – Isolation valves (e.g., main steam and feedwater); – Safety injection pumps and valves; – Decay heat removal pumps and valves; – Power supply breakers; – Auxiliary power generators; – Safety and relief valves; – Circulating water pumps.	• The displays and mimic will provide a spatially dedicated, continuously viewable, integrated presentation of the plant status in a direct manner to a level of detail beyond that of summary information to enable the operators to confidently assess the status of essential equipment operated from the MCR. These spatially dedicated displays will supplement and complement the serial presentations of subsets of this information at the workstation. Thus, these displays will enhance coordination among MCR personnel during normal, abnormal and emergency situations, and provide a clear, concise and continuous point of reference for operators to frequently and quickly assess plant status while performing tasks at the workstation. They will also be a useful aid during shift turnover, for assessing plant maintenance activities, and for training activities in the main control room.	0
	• Displays of higher level derived quantities, such as availability of functions or systems, shall be considered by the M-MIS Designer and included if they can be shown to improve the operators' performance and to be unambiguous.		0
	• These displays shall be visible and usable from the workstations in the main control room as well as from the probable locations of observers or support personnel.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.4.9	**Audio-Visual Monitoring**	**Audio-Visual Monitoring**	0
	The M-MIS design shall provide for audio-visual monitoring of conditions in areas which are not normally accessible to the operators because of high radiation or other hazards. The displays shall be provided at the control or work station where specific functions and tasks are identified which depend on the audio-visual monitoring.	Monitoring of activities through audio-visual observation (closed circuit television) can reduce the personnel accumulated dose.	0
4.5	**CONTROLS**	**CONTROLS**	0
	The M-MIS Designer shall develop specifications for the controls at control stations which are consistent with the guidance in EPRI NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (particularly Chapter 6) and the requirements of this section.	EPRI NP-3659 identifies the attributes which have to be considered when selecting types of controls; however, it does not prescribe the design details. The M-MIS Designer will have to make specific choices and thereby develop the specific design practices (see 4.1.5).	0
4.5.1	**Consistent Types of Controls**	**Consistent Types of Controls**	0
	It shall be an objective of the M-MIS design to minimize the number of different types of controls which are provided for the operators' use. However, differences in types of controls shall be provided to distinguish controls which have different characteristics or use. For example, the control for a motor should be different in appearance from the control for a valve, even though the basic requirements for control hardware are the same. The Design Practices (see 4.1.5) for the control stations should describe fully the logic and conventions for the selection of control types.	In addition to the advantages of maintenance and reductions in spares and training of having a minimum number of different control types, controls need to have different appearances when they perform different functions. This helps the operators avoid confusing controls.	0

Paragraph No.	Requirement	Rationale	Rev.
4.5.2	**Identification of Power Sources**	**Identification of Power Sources**	0
	The M-MIS design shall provide a consistent and effective method to provide, as part of each control, information as to the source of power for each controlled device. This method shall be specifically designed to support the operators in coping with losses of electric power, control power, or instrument air or other upsets which affect the power to a controlled device.	Although design requirements on the electric power systems and air systems are intended to substantially reduce the instances of power loss and their potential effects, it is considered that there will still be situations under which the operator will need to know the source of a control's power and whether a control is functional.	0
4.5.3	**Identification of Normal Control Position**	**Identification of Normal Control Position**	0
	The M-MIS design shall provide a consistent method to identify a defined normal position(s) for each control, where this is appropriate. This need not be an active system which covers various plant operating modes; however, such a system should be considered if adequate hardware and software can be devised.	Although a "green board" scheme may not be feasible, the provision of features for operators to identify unusual lineups is valuable to the operators in reviewing the plant condition as they assume their station.	0
4.5.4	**Inadvertent Actuation and Locking of Controls**	**Inadvertent Actuation and Locking of Controls**	0
	The prevention of inadvertent actuation of controls shall be achieved by selection of the type and location of controls or simple guards. The use of key locked controls shall be eliminated, if practical. In particular, key locked controls shall not be used when a control must be actuated on a timely basis in the course of an emergency event.	The use of keys for emergency controls introduces another way for a component to be out-of-service or delayed in actuation. It requires space for key lockers as well as the need to review access and traffic patterns and inevitably takes the time and attention of an operator, and probably the supervisor, to physically get the key and perform the control actuation.	0

Paragraph No.	Requirement	Rationale	Rev.
4.6	**VOICE COMMUNICATION SYSTEMS**	**VOICE COMMUNICATION SYSTEMS**	0
4.6.1	**Scope**	**Scope**	0
	This section covers requirements related to systems and equipment for:		0
	• Voice communications within the plant to support operations and maintenance;		0
	• Voice communications with outside organizations including the utility load dispatcher as well as other agencies for which communication is needed to support emergency operations.		0
4.6.2	**Required Capabilities**	**Required Capabilities**	0
	Voice communication systems and equipment shall be provided to support all phases of operations and maintenance, including emergency operations. The voice communications capabilities shall include as a minimum: • *Portable , Wireless Communication Capability.* Capability shall be provided for communication among operators and maintenance technicians using portable, wireless communication equipment supported by appropriate base stations, antennas, amplifiers and/or repeaters. This shall be designed as the primary, dedicated means of communication among control room operators, equipment operators, and maintenance technicians for routine and emergency operations, including surveillance tests, startup and shutdown operations, refueling, and emergency or accident conditions.	Existing plants have experienced numerous problems with communications among operating and maintenance personnel. In many plants, the plant paging system has been relied upon to support this communication and it has proven to be over-used and insufficient for this purpose. The ALWR should have communications capability that is dedicated to operations and maintenance personnel and designed to support their needs. Since they need to be able to communicate from any part of the plant, not just near fixed telephone stations, this system should support portable, wireless communication devices.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• *Plant-wide Paging and In-plant Telephone System.* A page system shall be provided to give capability of plant-wide paging of personnel. This paging system shall reach all areas of the plant, i.e., no dead areas are permitted. Also, fixed telephone stations shall be provided and located strategically throughout the plant to support general communications. The combination of the page and the in-plant telephone system shall support general communication needs and shall supplement and back up the dedicated wireless communication system for operations and maintenance. The in-plant telephone system shall have conferencing capability.	It is expected that general plant-wide paging and telephone communication will be needed, although it is the intent in the ALWR to reduce the burden on this system and to support operations and maintenance without relying directly on the page system.	0
	• *Dedicated External Communication Links.* Dedicated communication links shall be provided for communication with external organizations and facilities, including NRC, local fire and law enforcement agencies, off-site emergency facilities, and the utility load dispatcher.	Dedicated emergency communication links are required by regulation. Dedicated communication with the utility load dispatcher is required to support coordination of the plant with the grid, including load following, availability of off-site power, etc.	0
	These systems or capabilities may be supplemented with additional communication systems such as sound-powered phones, two-way radios, etc., provided that these additional systems are properly integrated into the overall communications system design as outlined in the requirements below.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.6.2.2	**Communications Analysis and Definition of Specific Needs**	**Communications Analysis and Definition of Specific Needs**	0
	The functions and tasks which involve communication among the operators or with other members of the plant staff or public will be identified, analyzed and documented per Section 3.1.3.3. Using the identified overall communication tasks, the communication system designer shall determine the specific communication needs and the specific design requirements for the various communication systems. This shall be included as part of the design basis documentation of the M-MIS and shall include the following as a minimum:	Problems experienced with present communication systems in many cases would have been prevented if specific needs for communications had been defined and these had been used in the communications system design. Voice communication is an integral part of the tasks that the operators and maintenance technicians must perform. The purpose of this requirement is to ensure that these identified communication needs give rise to specific evaluations by the communication system designers to define design requirements for the communication systems.	0
	• Detailed evaluation of the specific communication tasks that must be performed by operations and maintenance personnel (including specific locations, ambient noise levels, etc.) to determine the specific communication equipment and systems needed and the characteristics and features required of the equipment.		0
	• System analyses to define overall system design — numbers of channels, locations of communication stations, interfaces between various systems, dynamic range and frequency response characteristics, noise suppression, etc. The guidance given in EPRI NP-3659 shall be applied.		0
	• Development of a communications frequency allocation plan — defining the frequencies to be used by all wireless transmission systems, insuring that there is no interference between M-MIS communication systems and other transmission/communication systems on or off site, insuring compatibility with EMI/RFI protection measures taken by electronic/computer equipment designers for M-MIS and other on-site equipment, etc.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• Human factors evaluations of the designs of individual communication devices and stations, including use of mockups to walk through or talk through communication tasks, verify adequacy of equipment controls, labeling, and operating procedures, in the actual environment (noise, protective masks or clothing, etc.).		0
4.6.3	**Specific Requirements - Dedicated Wireless Communication System**	**Specific Requirements - Dedicated Wireless Communication System**	0
4.6.3.1	**Point-to-Point and Open-channel Communication Capability**	**Point-to-Point and Open-channel Communication Capability**	0
	It is preferred that the dedicated wireless communication system be based primarily on telephone-type, point-to-point communications (similar to cellular telephones), so that any fixed or remote (portable) unit can be "dialed up" and a conversation initiated between two points. However, the system shall also provide the capability for open channel, or "party line" communication in which up to [5?] at different stations can maintain continuous communication on an open line in situations that require this (e.g., a fire brigade or other emergency response team).	Telephone type communication is beneficial in allowing conversations to take place without interference from open-line noise and distraction such as have been experienced with page systems and radios. However, open channel communication will be needed for certain situations and should be provided in the ALWR.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.6.3.2	**Adequate Transmission/Reception Capability**	**Adequate Transmission/Reception Capability**	0
	Adequate antennae, amplifiers, repeaters, etc., shall be provided to ensure that clear, intelligible communication can be achieved from any locations at which operations and maintenance personnel may need to communicate, including locations inside the containment. The Designer shall carry out an experience review with existing systems and assure that problem areas identified will not recur in the ALWR. Verification of adequate transmission/reception capability shall be included as part of the plant start-up program.	Existing plants have experienced problems with two-way radio systems lacking the power to penetrate thick concrete walls, preventing communication from areas inside containment or in and out of the control room. This should be prevented in the ALWR communications system design by providing appropriate antennae, repeaters, etc., and the associated containment penetrations.	0
4.6.3.3	**Communications Effectiveness in High Noise Areas**	**Communications Effectiveness in High Noise Areas**	0
	The communication system designer shall consider potential ambient noise levels in the analysis of task requirements and the communication system design, and shall provide suitable equipment that allows communication from high-noise areas (e.g., at the diesel generators or turbine hall) consistent with performing other tasks in those areas. The designer shall also provide adequate means of alerting personnel to use communication equipment — for example, provision of visual and/or vibra-tactile alerting as well as audible signals for hand-held communicators.	Ineffectiveness of communications in areas of high ambient noise has been a problem with existing systems. The Designer should ensure that the ALWR communications systems do not exhibit these problems.	0
4.6.3.4	**Integration with Personnel Protective Equipment**	**Integration with Personnel Protective Equipment**	0
	The design of portable communication equipment and personnel protective equipment, including respirators, shall be such that personnel wearing protective gear can adequately communicate. The guidance developed by EPRI on voice communication systems compatible with respiratory protection (RP-2705-7) shall be applied.	Inability to communicate while wearing protective gear has been a problem in existing plants. EPRI has been developing guidance for utilities on integrating communications equipment with protective equipment, which should be applied by the M-MIS designer in the ALWR.	0

Paragraph No.	Requirement	Rationale	Rev
4.6.3.5	**Adequate Capacity/Channels**	**Adequate Capacity/Channels**	0
	An ample number of communication channels shall be provided, sufficient to accommodate the expected message load based on the network analysis including task requirements in critical or emergency situations, plus allowing margin for expansion and contingency. The wireless system shall be dedicated to operations and maintenance, and use by operators and maintenance technicians in critical situations shall take precedence of any other functions or uses of the system.	Lack of sufficient communication channels to handle message loads has been a problem in existing plants. There have been too few phone lines and too few page channels. By dedicating a wireless communication system to operations and maintenance, so that the page system need not be relied upon for most communications, and ensuring adequate capacity/channels of the dedicated wireless system, problems with inadequate capacity should no occur in the ALWR.	0
4.6.3.6	**Interference with Electronic Equipment**	**Interference with Electronic Equipment**	0
	The design of the communications equipment and all M-MIS electronic, computer and instrumentation equipment shall be such that there is no interference between the communication systems and the M-MIS equipment. The communication system designers and the M-MIS monitoring, control and protection system designers must work together to ensure this,including the following specific requirements: • The communication system designers shall define worst-case emissions from the communication equipment – type and magnitude, frequency content, and locations based on the task analyses and consideration of all potential uses of the communications gear.	Existing plants have experienced problems with interference, including spurious trip signals, resulting from use of two-way radios. Since the ALWR M-MIS will include even more electronics, including computers and data transmission equipment that could be susceptible to EMI/RFI, and at the same time the wireless voice communications systems wil be designed to be used more extensively, from more locations, and with stronger transmission capability (addressing problems with pool communication in present plants), it is imperative that stringent measures be taken to protect against interference between these systems. This will require close coordination among the communications system designers and the M-MIS electronic equipment designers.	0

Paragraph No.	Requirement	Rationale	Rev
	• The M-MIS equipment designers shall evaluate all M-MIS equipment for susceptibility to interference from use of the communication systems. Adequate protection shall be provided for electronics, computers, instruments, and data transmission equipment to ensure that they are unaffected by the voice communication systems. This shall include consideration of maintenance and troubleshooting activities which may involve technicians working at M-MIS equipment cabinets or instruments, with access panels or doors open, communicating with operators or other technicians using hand-held communication equipment. If adequate protection is afforded only when cabinet or enclosure doors or panels are closed, the designer shall specify this and provide appropriate cautions on use of hand-held communicators when working on the equipment. In such cases, any indicators needed to visually check status of the equipment, determine fault locations, etc., shall be provided external to the cabinet or enclosure so that they may be inspected without opening doors.		0
	• The communications equipment shall be designed such that it is not susceptible to interference or noise from the M-MIS electronics or data transmission systems, or other electrical or electronic equipment near which communication equipment must be used. Intelligibility of voice communications must be maintained at all locations from which operators or technicians need to communicate.		0

Paragraph No.	Requirement	Rationale	Rev
4.6.3.7	**Reliability and Analysis of Failure Modes**	**Reliability and Analysis of Failure Modes**	0
	Credible communications system failures shall be considered in the design. The system shall be designed to be highly reliable and resistant to failures. No single failure shall prevent communications from more than one device or location.	Since voice communication is an integral part of the tasks that operators and technicians must perform, it is crucial that the communication systems and equipment be highly reliable and resistant to failures, applying the same care and attention as for other M-MIS equipment.	0
4.6.3.8	**Reliable Power Sources**	**Reliable Power Sources**	0
	All electrical power required to maintain full functioning of the wireless system, including maintaining clear and intelligible voice transmission to all areas normally covered, shall be provided from reliable, backed-up sources of on-site power such that the communication system will function properly during all credible abnormal, accident and emergency situations, including loss of off-site power.	Loss of power to portions of communication systems has resulted in a lack of needed communications or degraded communications during events at some existing plants, particularly in loss of off-site power events. Communications systems have been powered from busses that have lost power in situations when good communication is desperately needed. This must be prevented in the ALWR. This means that the central communications equipment, and all repeaters, amplifiers, etc., must be provided with robust sources of power that ensure the entire system will remain functional in credible scenarios.	0
4.6.4	**Specific Requirements - Communication Stations and Devices**	**Specific Requirements - Communication Stations and Devices**	0
4.6.4.1	**Communication Station Arrangement**	**Communication Station Arrangement**	0
	Communication stations provided in the main control room shall be such that the operator can use more than one communication system, channel or line effectively, without requiring awkward manipulations – for example, use of multiple handsets, tangled cords, etc. Also, the communication equipment and stations shall be designed to accommodate simultaneous use by more than one operator or supervisor, based on needs defined by analysis of control room tasks.	Use of multiple phones has been difficult in some existing plant control rooms. Modern communication equipment should allow provision for a communication station that gives access to more than one system/channel/line in an effective manner. Also, use by more than one individual should be facilitated.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.6.4.2	**Communication Consistent with Other Ongoing Tasks**	**Communication Consistent with Other Ongoing Tasks**	0
	Communication stations and equipment shall be designed to be consistent with ongoing tasks that need to be performed by the user of the communication equipment and by others nearby. Use of communication equipment shall not interfere with monitoring or access to controls and indicators, or cause personnel hazards – for example, due to long cords. Mock-ups, walkthroughs, and simulations shall be used as necessary to verify design adequacy both for local control stations and the main control room.	Interference with other tasks has been a problem in using present communication equipment. The design should be such that this is prevented in the ALWR.	0
4.6.4.3	**Alerting Devices**	**Alerting Devices**	0
	Alerting devices, e.g., tones, rings, lights, etc., associated with multiple communication systems or devices at a station shall be selected such that the operator or other user can determine easily which communications instrument is to be answered. These devices shall be easily distinguishable from other signals and alarms at the control/communication station.	Confusion resulting from mixtures of different instruments has been a problem in existing main control rooms. This should be prevented by proper selection of audible tones or rings.	0
4.6.4.4	**Identification of Communication Lines, Locations and Devices**	**Identification of Communication Lines, Locations and Devices**	0
	Clear, unambiguous and easily readable identification shall be provided for all communication devices, selectable lines or channels, and locations or stations so as to avoid confusion and errors by users trying to initiate communication in a hurry. The labeling and color coding shall be consistent with the overall scheme adopted for the entire plant. See Section 4.1.5.	Poor identification of phone lines has been reported as a problem in existing plants.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.6.4.5	**Communication Between Operators and Technicians in Control Room**	**Communication Between Operators and Technicians in Control Room**	0
	The design of the control room and the communications equipment shall be such that there is adequate means for voice communication between operators at the controls and technicians working on equipment anywhere in the control room. This capability shall be ensured even for maintenance tasks that would not normally require the maintenance technician to communicate with an operator in order to complete the task – it is important that the operator be able to communicate with anyone who at any time is working on M-MIS equipment, including work that may go on behind or inside control panels.	Some existing control rooms have exhibited poor verbal communication between operators at the boards and technicians doing maintenance behind the boards or at other locations in the control room. Operators must maintain continuous awareness of any ongoing work that may affect the M-MIS, and be able to communicate with anyone performing such work.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.7	**ARRANGEMENT, ENVIRONMENT, AND EQUIPMENT**	**ARRANGEMENT, ENVIRONMENT, AND EQUIPMENT**	0
	The M-MIS Designer shall develop designs and arrangements and provide environment and equipment for control stations which are consistent with the guidance in EPRI-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (particularly Chapter 3), and the requirements of this section.	EPRI NP-3659 identifies the items which need to be considered in selecting the arrangement, environment, and equipment at a control station; however, it does not prescribe the design details. The M-MIS Designer will have to make specific choices and thereby develop the design practice (see Section 4.1.5).	0
4.7.1	**Compatibility with Functions and Tasks**	**Compatibility with Functions and Tasks**	0
	All control stations shall be arranged and have an environment and equipment which are suitable for the functions and tasks which have been assigned to that control station. This includes specific consideration of traffic patterns, access to support material, communications among the operators at the station and communications to personnel at other locations, and potentially degraded environmental conditions, such as the use of emergency lighting. These tasks also include any periodic testing which must be performed at or supported by the control station.	The control stations need to be specifically designed to support all activities which must be performed at the control station.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.7.2	**Ancillary Operator Tasks and Duties**	**Ancillary Operator Tasks and Duties**	0
	Each control station design shall specifically provide for the operators to perform those functions and tasks of a largely administrative nature which are not directly involved in operating the plant equipment, but which are essential to their duties. Each control station design shall specifically identify those tasks and the features in the control station design which facilitate their performance. For example,	A significant fraction of an operator's time may be involved in activities which will not appear in the tasks identified to operate the plant equipment. If these other duties are difficult, they can distract the operator from the plant's operating condition and adversely affect the operator's performance.	0
	• Switching and tagging involved in taking equipment out of service and returning it to service;		0
	• Completion of logs;		0
	• Preparation of reports;		0
	• Shift turnover activities;		0
	Specific requirements related to access for these kinds of tasks for the MCR are covered in Sections 4.9.1.2.1 and 4.9.1.2.2.		0

Paragraph No.	Requirement	Rationale	Rev
4.7.3	**Test and Maintenance**	**Test and Maintenance**	0
	Each control station design shall specifically provide for the test and maintenance operations which may have to be performed at the station. The tasks involved in these operations shall be identified and included in the function and task analysis of the station. This shall include: • Access to the components on the panels for repair, removal, or replacement; • Separation of controls and displays used only for test and maintenance from those used for operations; • Contingency space for special test equipment or repairs. The design documentation for the control station shall identify any special factors or assumptions used to arrange the control station to meet this requirement.	Unless provisions are made for test and maintenance activities and space is reserved for these special uses, tests, repairs, or modifications may be difficult or may so crowd or disrupt the operations at a control station that operator performance is substantially degraded and there is a substantial risk of operator error. Note that this requirement is related to the need to have the designed-in capability for modification and upgrading (see Section 3.9).	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.7.4	**Lighting**	**Lighting**	0
	Control stations shall be provided with lighting which can be adjusted by the operators to provide uniform illumination in the range of 10 to 50 foot-candles.	EPRI is currently engaged in research to define lighting levels appropriate to control station tasks. Initial results (EPRI-5989, *Effects of Control-Room Lighting on Operator Performance, A Pilot Empirical Study*) indicate relatively low light levels (10 foot-candles) may be completely adequate and may be preferred by some operators. Adjustability will provide the operators the ability to adjust the lighting levels to the values which provide the best balance between brightness and glare.	0
4.7.5	**Material Storage**	**Material Storage**	0
	Each control station design shall include a detailed list of the material which will be stored at the control station or in the surrounding area for use at the control station. This includes: • Reference materials, e.g., procedures, manuals, and drawings; • Spare parts, e.g., bulbs or fuses; • Operators personal equipment; • Emergency equipment; • Logs and records.	The operators use a great number of items at a control station which are not controls or displays in the usual sense. Storage and access to this material is a chronic problem at many plants. The lack of planning in this realm leads to makeshift and often awkward schemes to store the material and then later find it and use it. Advanced information handling techniques may reduce the burden in handling "hard copy".	0

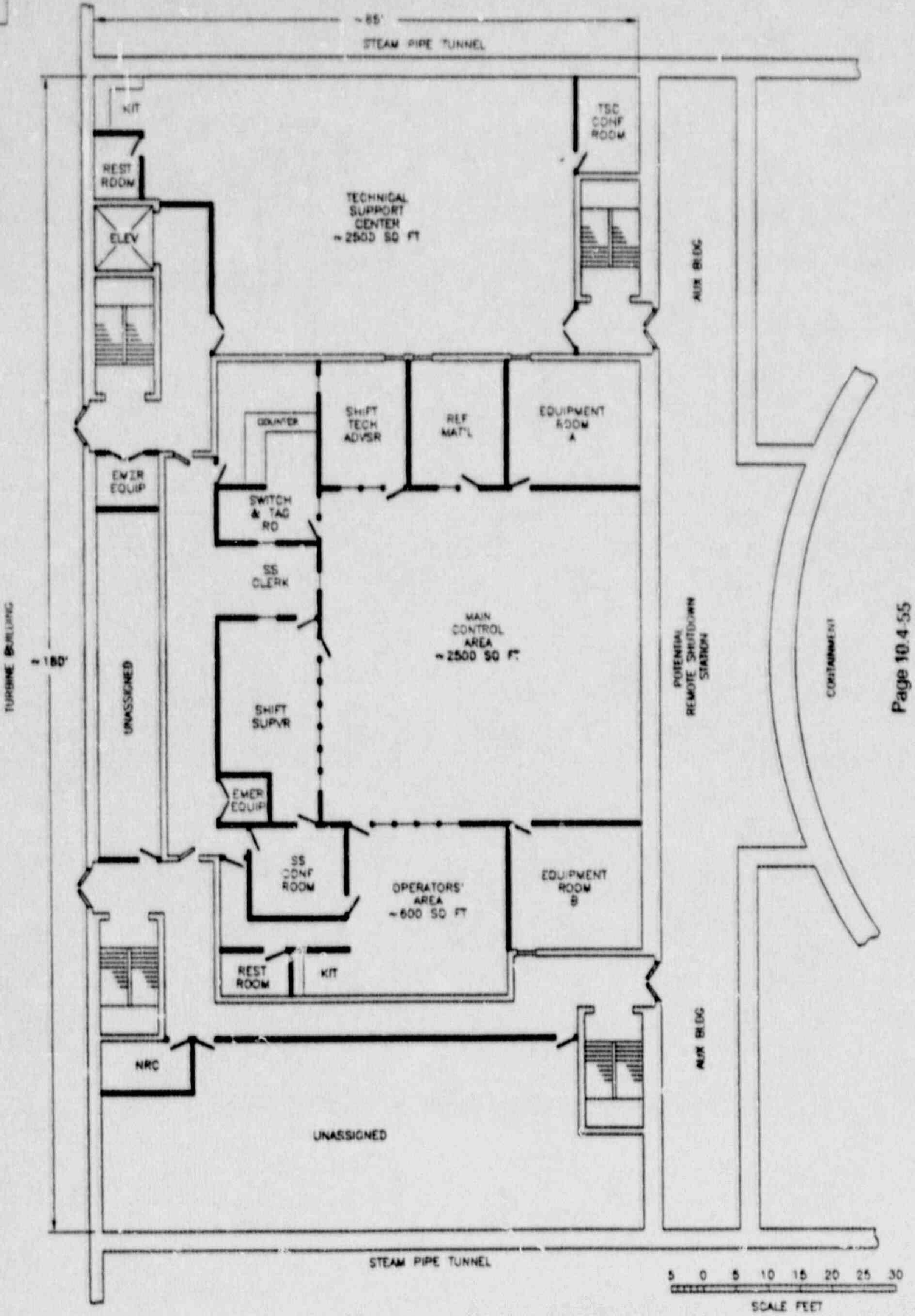
Paragraph No.	*Requirement*	*Rationale*	*Rev*
	The space required to use these materials, e.g., laydown space for procedures or drawings, and the personnel movement to and from storage locations shall be identified as part of the control station design. The control station design shall also include definition of the methods to be used to identify the stored material, e.g., the labeling of reference materials, spare parts, and stored emergency equipment.		0
4.7.6	**Noise Levels**	**Noise Levels**	0
	All control stations which are continuously manned on a routine basis, e.g., the main control room, the technical support center, and the emergency operations facility, shall have an ambient noise level no greater than 60 dB(A) from installed equipment in the immediate neighborhood of the control station and plant equipment which may operate for long periods. This limit shall be met for all normal or emergency HVAC system lineups in all areas of those control stations where communication between operators is necessary.	Low ambient noise levels will facilitate communication at the control stations. It will also allow audible alarms to be at low sound levels so that they have less potential to affect communications. The current practice (see EPRI NP-3659, page 73) is to accept noise levels as high as 65 db(A), however, as indicated by Exhibit 3-15 of NP-3659, this results in "easy" communication only at face-to-face (2 to 3 feet) distances and voice communication across more than about 25 feet would be difficult. Experience indicates that noise levels under 60 db(A) are achievable. This level would assure "easy" communication at a distance of up to about 8 feet as well as practical voice communication up to 30 feet, i.e., completely across the main controlling area of the control room. It is intended that brief plant transients, such as safety valves lifting, could be allowed to raise the ambient noise level.	0
4.7.7	**Surface Finishes**	**Surface Finishes**	0
	All control stations which are continuously manned on a routine basis, e.g., the main control room, the technical support center , and the emergency operations facility, shall be provided with carpeting and sound absorbing walls and ceilings. These materials shall be selected for fire resistance, ease of upkeep, durability, and appearance in addition to their sound absorption.	Proper selection of surface finishes can markedly improve the environment at control stations. This, in turn, will result in less operator fatigue and increased vigilance in addition to improving communication among the operators.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.8	**CONTROL PANELS**	**CONTROL PANELS**	0
	The M-MIS Designer shall develop designs for the panels at control stations which are consistent with the guidance in EPRI-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (particularly Chapter 4) and the requirements of this section.	EPRI NP-3659 identifies the attributes of panel arrangements which need to be considered, however, it does not prescribe specific arrangements. The M-MIS Designer will have to make specific choices and thereby develop the design arrangement practices (see 4.1.5).	0
4.8.1	**Relations Among Panel Mounted Components**	**Relations Among Panel Mounted Components**	0
	The M-MIS Designer shall base the locations of controls and displays on the panels at control stations on the functions and tasks identified for the control station (see 3.1.3.3). In particular, the design shall determine which controls and displays must have a definite and consistent location and which need be available only at the operator's request. Arrangements shall be assessed as required in 4.1.3 by reviews in mockups which utilize walk-throughs and talk-throughs. Final arrangements of the MCR shall be selected after review in a full-scope simulator.	Although hardware and software may permit the flexible location of controls and displays, i.e., the operator may be able to call up a particular control, display, or set of controls or displays; this may not be the most effective way to present some critical or frequently used information or control. Accordingly, the M-MIS Designer will be required to make a decision based on analysis of the actual tasks under realistic conditions to pick a workable arrangement.	0
4.8.2	**Identification of Panels and their Components**	**Identification of Panels and their Components**	0
	The M-MIS Designer shall establish a comprehensive and consistent method to identify the functional divisions of the control panels and the individual components. This method shall be completely described as part of the Design Practices for the control stations. In this connection, the M-MIS Designer shall establish a list of abbreviations, symbols, and acronyms which shall be used at control stations. This list, as well as other nomenclature used on the panels at the control stations, shall be consistent with that used in the Configuration Management System (Chapter 1, Section 2.2.c).	Experience has shown that special effort is necessary to get consistent and sensible identification of systems and components. This consistency reduces the burden on the operator's memory, simplifies the preparation of procedures, and reduces the potential for errors by operators and other plant personnel.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.8.3	**Provisions for Modification**	**Provisions for Modification**	0
	The panels in the control areas shall be designed to facilitate their future modification as required by 3.9. The features included in the designs to meet this requirement shall be identified in the conceptual designs of the stations and summarized in the Design Practices document.	Modifications of the plant hardware often involve changes at control stations. Unless the panels are flexible and can readily accept changes, the modification can degrade the existing arrangements and result in operator confusion. The location and character of the feasible changes need to be specifically identified to assist planning for plant modifications which exploit the flexibility.	0
4.8.4	**Space for Posted Operator Aids**	**Space for Posted Operator Aids**	0
	The panels shall have defined space for the incorporation of posted operator aids. These areas shall be defined on the design configuration drawings. The M-MIS Designer shall identify any specific posted operator aids that are assumed and they shall be considered part of the control station design.	The operators often add information, e.g., cautions, special instructions, lists, figures, diagrams, etc., to the panels so that they have quick access to reference information. This reduces the burden on the operator's memory and can reduce his response time or the potential for errors. Planning for such posted operator aids will assure they are compatible with the tasks performed at the control station and assures they will be evaluated as part of the review process.	0

Paragraph No.	Requirement	Rationale	Rev
4.9	**REQUIREMENTS FOR SPECIFIC CONTROL STATIONS**	**REQUIREMENTS FOR SPECIFIC CONTROL STATIONS**	0
4.9.1	**Main Control Room**	**Main Control Room**	0
	The main control room (MCR) design shall be consistent with the guidance in EPRI NP-3659, *Human Factors Guide for Nuclear Power Plant Control Room Development* (particularly Chapter 3) and the requirements of this section.	EPRI NP-3659 includes detailed checklists of issues which need to be addressed in the MCR design. It is expected that the specific ALWR implementation will be defined in the Design Practices document and the detailed design configuration of the MCR.	0
4.9.1.1	**Utilization of Functions and Tasks**	**Utilization of Functions and Tasks**	0
	The control stations in the MCR shall provide for the performance of the tasks assigned to them. Controls and displays which are not necessary to perform the defined tasks shall not be included in the MCR.	Unnecessary information provided to the operators or controls which are not used can distract them from their essential tasks.	
4.9.1.2	**Main Control Room Location and Access**	**Main Control Room Location and Access**	0
	The general location of the MCR is addressed in Chapter 6, 4.6.5. The analyses of functions and tasks shall specifically include evaluation of the traffic patterns from the MCR to other parts of the plant. Additional requirements on MCR access are given below. Figures 10.4-1 and 10.4-2 illustrate layout arrangements which address many of these requirements. Figures 10.4-3 and 10.4-4 show how the particular illustrative sample layouts address personnel access to and from the MCR. These layouts are not requirements, but are provided only to illustrate potential approaches to satisfying access requirements.	The MCR is the focus for essentially all plant activities. Access to and from the MCR plays an important part in many normal and emergency operations.	0

MPR ASSOCIATES
7-140-31-205
07/13/89



GURL 10.4-1

PWR MAIN CONTROL ROOM
SAMPLE L'YOUT

MPR ASSOCIATES
F-148-31-208
07/13/88

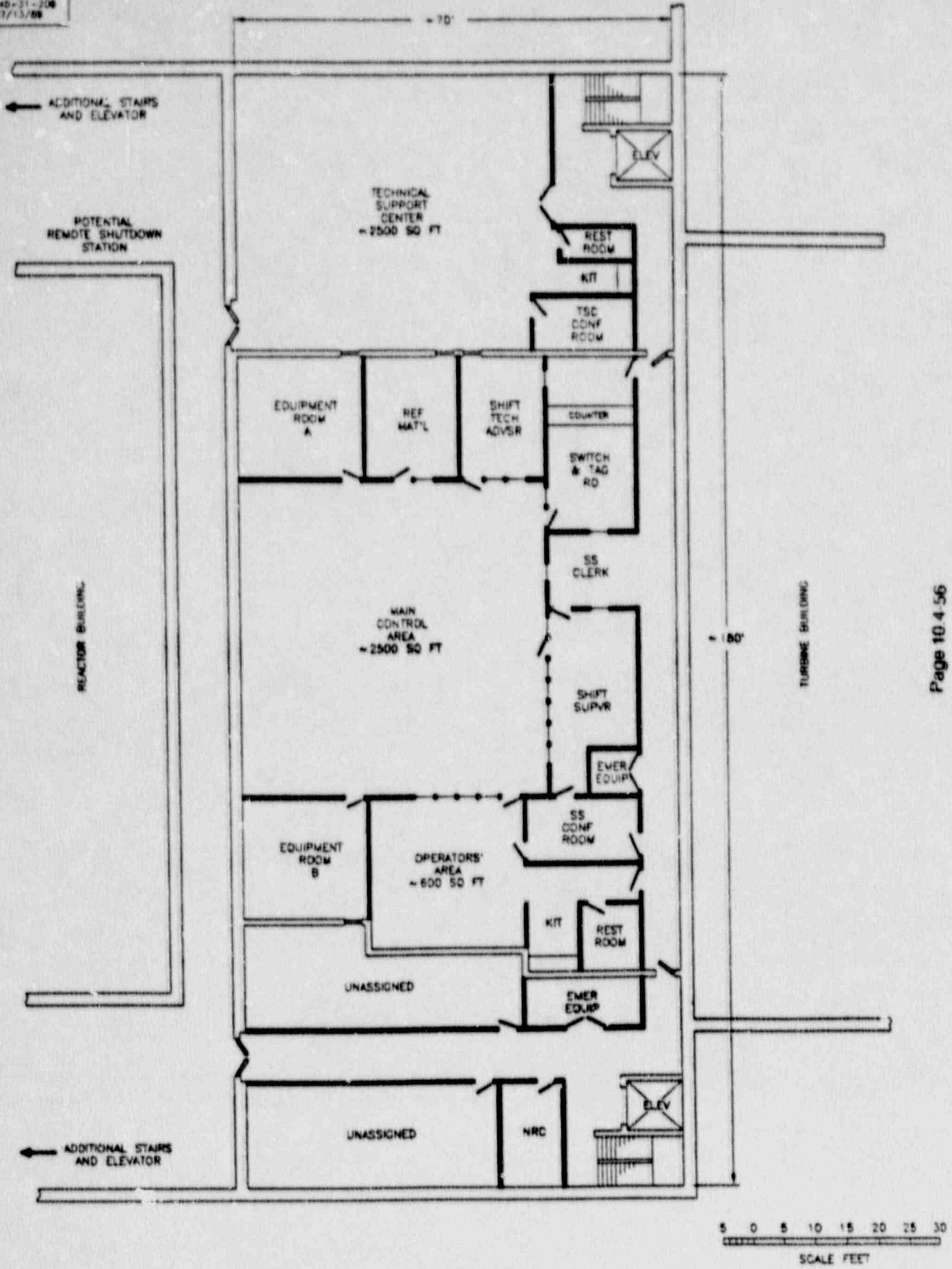


FIGURE 10.4-2
BWR MAIN CONTROL ROOM
SAMPLE LAYOUT

MPR ASSOCIATES
F-140-31-207
07/13/89

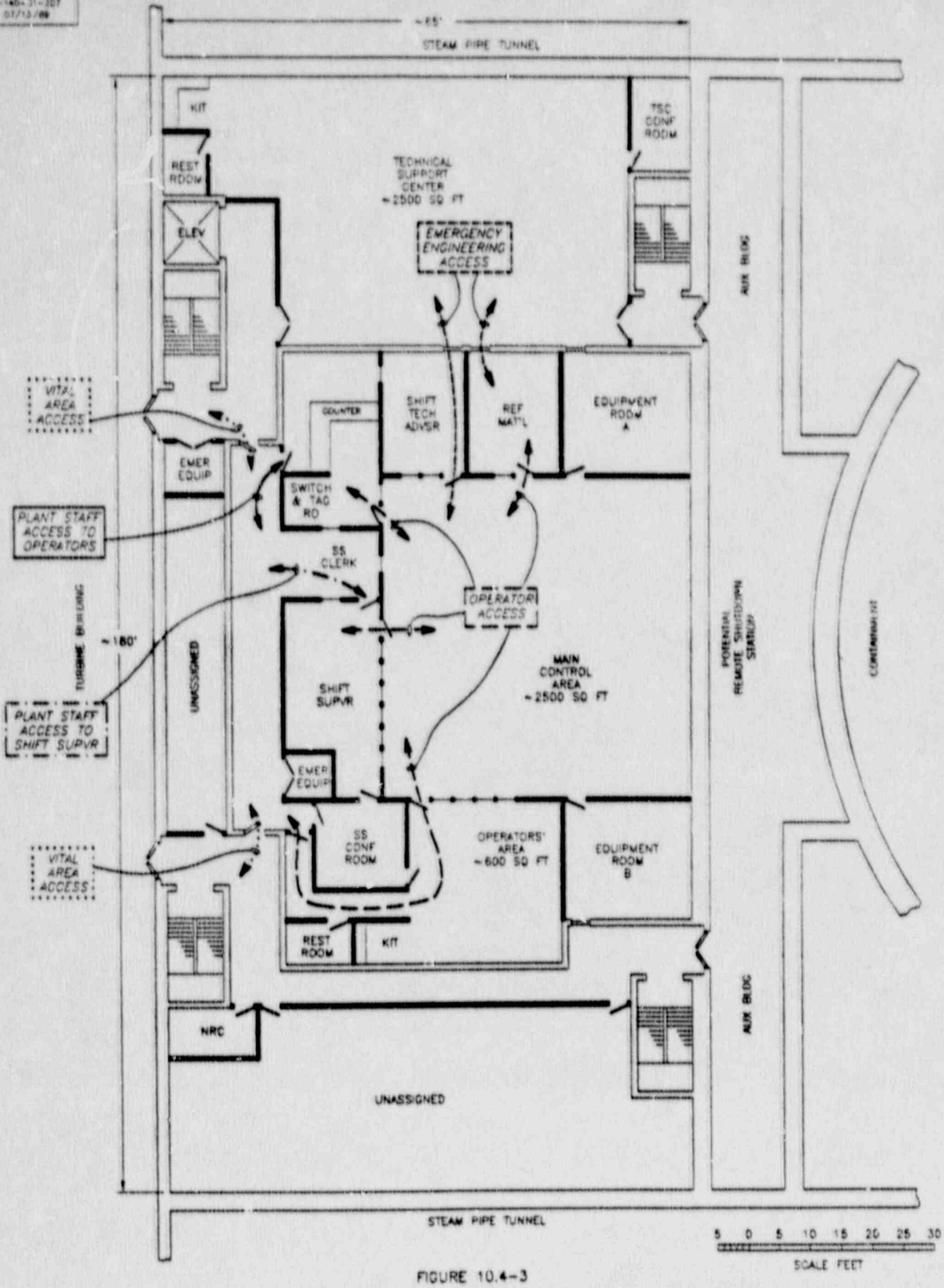


FIGURE 10.4-3
PWR MAIN CONTROL ROOM
PERSONNEL ACCESS ROUTES

MPR ASSOCIATES
F-140-31-206
07/13/89

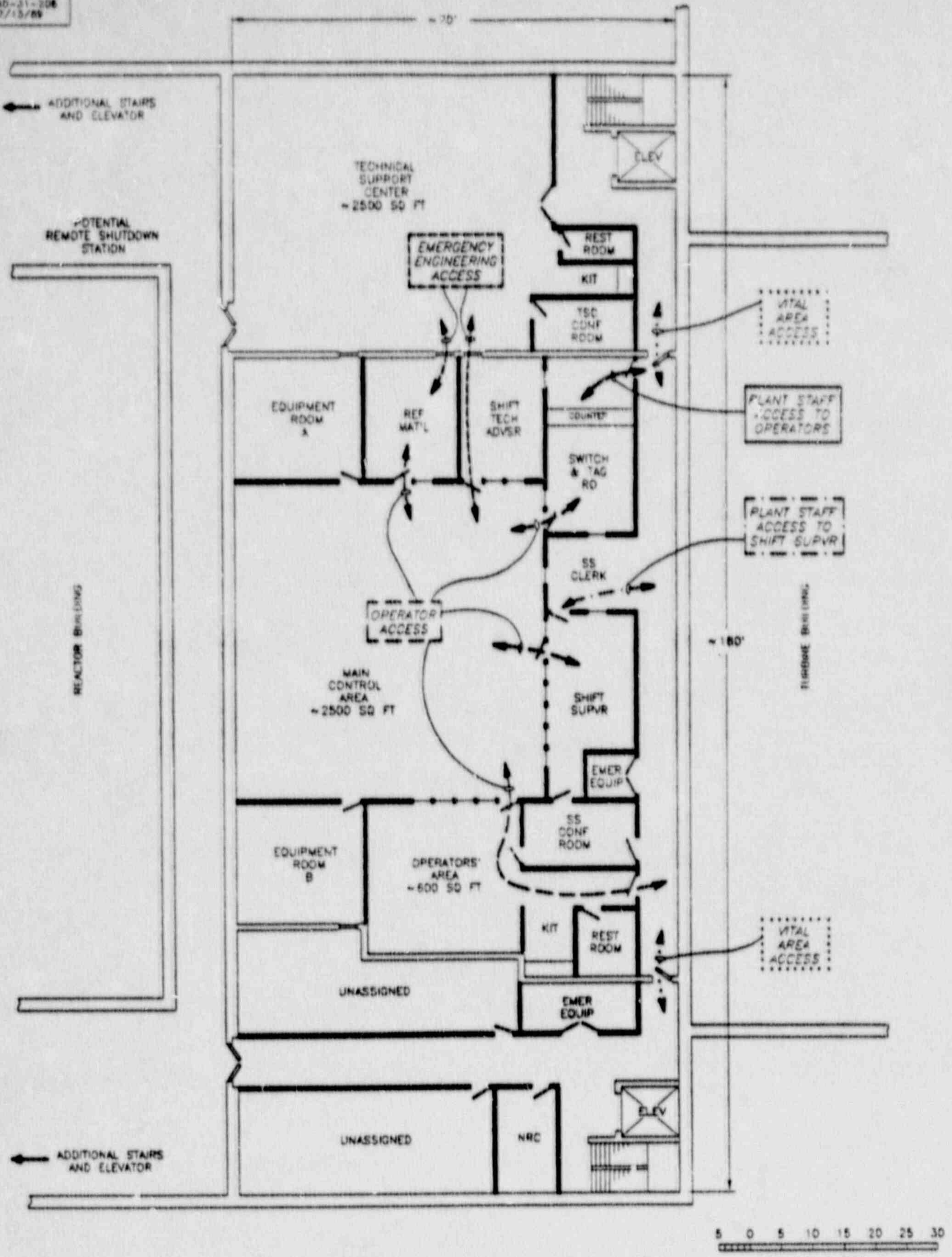


FIGURE 10.4-4
BWR MAIN CONTROL ROOM
PERSONNEL ACCESS ROUTES

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.1.2.1	**Access by Operating Staff**	**Access by Operating Staff**	0
	The M-MIS design shall specifically identify the access paths to and from the MCR by the operators for specific tasks. In addition, the MCR shall provide for the following more general access requirements: • Access from various parts of the plant to the MCR by equipment operators so that they may consult directly with the control room operators. • Access from the MCR to locations in the plant where local operator actions may be needed because of abnormal conditions. This access shall not disrupt the actions of the operating team in the main controlling area of the MCR unless it is necessary for efficient communication. Specifically, in addition to adequate space in the main controlling area for visiting plant staff, space for consultation shall be provided outside the main controlling area and access to that space shall not require passage through the main controlling area.	It is difficult for the operators to get access to other parts of the plant or for the operators to come to the control room, the control room may become isolated and get out of touch with the plant. It should be recognized that the control room personnel tend to be more highly experienced than the equipment operators who are out in the plant at equipment or local stations. Isolation of the operators in the control room makes it difficult to use their experience and expertise. Some activities, consulting drawings, for example, and instructing equipment operators may best be accomplished by one-on-one discussion between the EO and the RO or SRO. The access to the control room should support such discussion and consultation. Ideally, it should not be necessary for control room operators to go to a local station or equipment. However, the operators, particularly the SROs, tend to have more experience than the equipment operators and full assessment of a local condition may need their direct observation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.1.2.2	**Access to MCR by Non-Operating Plant Staff and Others**	**Access to MCR by Non-Operating Plant Staff and Others**	0
	The location, arrangement and equipment in the MCR shall facilitate the necessary interaction between the operators in the control room and other personnel, even though these contacts do not appear explicitly in the tasks assigned to the operators in the MCR. The MCR design shall identify all such interactions or contacts which have been considered in the design basis. The objective of the MCR arrangement shall be to limit the contacts of these non-operating personnel so that normally they do not distract the operators at the controls in the main controlling area of the MCR. In particular, routine contacts with the Shift Supervisor, the Shift Supervisor's Clerk, the RO assigned to switching and tagging, or the Shift Technical Advisor shall not require personnel to pass through the main controlling area of the MCR.	The MCR is in essentially continuous use and is the focus of the majority of plant activities; consequently, it has contact with more than the operators. These other needs may not adequately be covered by the M-MIS design unless they are defined.	0
	Some specific items which shall be included are the following:		0
	• Access by NRC inspectors and provisions for them to communicate with their headquarters, with the Shift Supervisor, or with the Utility management without disrupting MCR activities;		0
	• Access by maintenance personnel related to operators actions and tagging needed to accomplish maintenance;		0
	• Access by plant staff such as engineering or radiological protection when the operators request assistance;		0
	• Access for maintenance of control room equipment;		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• Access to the Shift Supervisor for administration functions;		0
	• Access by fire brigades;		0
	• Access by administrative support personnel, e.g., to distribute mail and update reference material.		0
4.9.1.2.3	**Main Control Room Evacuation**	**Main Control Room Evacuation**	0
	The main control room shall have at least two independent exits which can be used in case the control room must be evacuated. The remote shutdown station(s) shall be accessible to the operators from either exit without the use of security devices such as keys or key cards or electric power.	Although control room evacuation is very unlikely, it is also unpredictable and more than one choice for exiting the control room is needed to have assurance that evacuation can be effected. The operator may have exited the control room very suddenly and may not have been able to pick up keys or may have lost his keycard or other security device.	0
4.9.1.3	**Operator Relief Area**	**Operator Relief Area**	0
	The layout of the MCR shall include an area of at least 600 square feet, which is designated as an operator relief area. This area should be adjacent to the kitchen and restroom facilities as well as being immediately accessible to the main controlling area of the MCR.	Studies in operator alertness may show that brief periods of relief away from the main part of the control room in an area where an operator may relax, move around and even engage in physical activity, are desirable.	0
4.9.1.4	**Restroom**	**Restroom**	0
	A restroom adequate for both men and women shall be provided. This restroom shall not be shared with areas outside the main control room.	A shared restroom increases the traffic into the control room.	0
4.9.1.5	**Kitchen Facilities**	**Kitchen Facilities**	0
	Convenient kitchen facilities with provisions for heating food, e.g., microwave oven, hot water and drinking water, and refrigeration, shall be provided.	It is impractical for the operators to leave the control room to eat. Adequate kitchen facilities are important to operators' comfort.	0

Paragraph No.	Requirement	Rationale	Rev.
4.9.1.6	**Shift Turnover Area**	**Shift Turnover Area**	0
	The layout of the MCR shall specifically provide for the operations involved in shift turnover. In particular, a location where the personnel for a shift may meet without disturbing the activities in the main part of the control room shall be provided. This area may be combined with operators relief area (see 4.9.1.4)	Proper transfer of information from one shift to another is essential to plant operation. Special provisions to make the turnover convenient can reduce the potential for operator errors.	0
4.9.1.7	**Emergency Equipment**	**Emergency Equipment**	0
	The MCR shall include defined storage space for emergency equipment, e.g., breathing apparatus or protective clothing, which could be needed by personnel in the control room. The MCR design shall identify all such equipment and the assumptions upon which their need is based.	Storage space in the MCR is premium space and equipment should not be stored there unless a need for the equipment inside the rooms is established. Furthermore, the upkeep of such equipment leads to traffic to check and maintain it. It may not be appropriate to store some emergency equipment in the control room, for example, fire protection equipment used to enter the control room.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.2	**Local Control Stations**	**Local Control Stations**	0
	The local control stations shall be part of the M-MIS design process and shall meet the same requirements as the MCR except as required by this section.	Many important operator actions in both normal and abnormal conditions will take place at local control stations. Consistent high standards of design will assure the overall ALWR requirements are met.	0
4.9.2.1	**Local Override of Main Control Room**	**Local Override of Main Control Room**	0
	It should normally not be possible to override the controls in the MCR from a local control station or to take actions which generate a false display signal. However, where it is impractical to design the M-MIS on this basis, because of the need for maintenance or testing, the M-MIS Designer shall specifically provide for these operations. In those cases, the control room operators shall either have a control which permits the override or have a positive means to inform them that they do not have control or that they have an inoperative display.	Since the MCR is the focus of plant activity, the loss of control capability or the display of status can significantly complicate the operator's response to an emergency condition, especially if the operator is not aware of the condition.	0
4.9.2.2	**Environment, Equipment, and Access**	**Environment, Equipment, and Access**	0
	For local control stations which are not used routinely and will not be manned for more than a few hours at a time, somewhat less stringent environmental requirements, more limited equipment, and more limited access are acceptable; however, in no case shall the conditions be predicted to prevent the operators from carrying out the assigned tasks under accident as well as normal operating conditions. For example, lighting must be sufficient to support task performance, noise levels shall permit adequate communication, and access shall not involve personnel or equipment hazard. The M-MIS design shall specifically identify the relaxed requirements and document the basis for their acceptability.	At some local control stations, which are used infrequently, it may be impractical to provide all the attributes of a control station which is used continuously.	0

Paragraph No.	Requirement	Rationale	Rev.
4.9.2.3	**Staffing of Local Control Stations**	**Staffing of Local Control Stations**	0
	Local control stations shall be designed to be operated by one person. However, the space shall not be so limited that two persons are precluded from the station.	A strictly one-person control station can result in undesirable limitations. There are instances where the performance of an operation may require the presence of a checker, an assistant, or a supervisor. For example, on-the-job training or special tests which require a data recorder or observer.	0
4.9.2.4	**Inadvertent Actuation**	**Inadvertent Actuation**	0
	Local control stations shall be designed to eliminate inadvertent actuation of any controls in so far as practical. This shall consider the potential for plant personnel to be in the area of the local control panels.	Because local control stations may not be continuously manned, operating personnel may not be immediately available to recover from an inadvertent actuation. A higher level of concern for inadvertent actuation should be applied to local control stations than in the main control room or a continuously manned station.	0

Paragraph No.	Requirement	Rationale	Rev.
4.9.2.5	**Unauthorized Use**	**Unauthorized Use**	0
	The M-MIS Designer shall identify those controls at normally unmanned local control stations which have serious consequences if activated by unauthorized persons. Serious consequences are:	Although security against unauthorized use is prudent, such measures can easily impede the operators' actions in an emergency. The M-MIS design must balance these considerations.	0
	• Violation of plant technical specifications;		0
	• Immediate trip of the plant;		0
	• Actuation of safety systems;		0
	• Damage of expensive equipment or repairs that require an extended outage.		0
	For such controls, the M-MIS Designer shall provide positive means to prevent unauthorized actuation, except where such means would interfere with emergency use of the control. Where no positive means is practical, the M-MIS Designer shall assure that the conditions caused by the unauthorized action will be adequately annunciated in the main control room.		0
4.9.3	**Remote Shutdown Control Stations**	**Remote Shutdown Control Stations**	0
	The M-MIS design shall provide for control stations outside the main control room which have the capability to bring the reactor to hot standby and maintain it in that condition indefinitely. The M-MIS design shall also allow the plant to be brought to cold shutdown within 72 hours using these control stations as well as local controls.	It is the intent that the ALWR have a capability to meet applicable regulations with regard to control room evacuation.	0

Paragraph No.	Requirement	Rationale	Rev.
4.9.3.1	**Use of Functions and Tasks**	**Use of Functions and Tasks**	0
	The M-MIS Designer shall identify all the functions and tasks involved in the remote shutdown operations. Tasks at any other local control stations as well as those at dedicated remote shutdown control stations shall be included. The functions and tasks defined for the remote shutdown station shall be used in selecting the specific controls and displays to be provided at that station.	It is generally not practical to include all controls or displays at the remote shutdown stations (particularly those needed to cool down the plant). However, in order to assure that the remote shutdown capability is available, all these other local controls and displays must be evaluated.	0
4.9.3.2	**Conditions of Evacuation**	**Conditions of Evacuation**	0
	The design of the M-MIS for remote shutdown shall be based on evacuation of the main control room without an opportunity to carry out any tasks involved in the shutdown. However, it shall also establish that the remote shutdown control stations are compatible with the operators performing a few tasks, e.g., reactor trip or initiation of emergency feed, prior to evacuating the control room. Any limitations or assumptions on these tasks shall be defined and documented in the design basis for the remote shutdown control stations.	The conditions under which evacuation is required are unpredictable. The remote shutdown stations should not have to assume a particular scenario for the evacuation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.3.3	**Simulation of Remote Shutdown Stations**	**Simulation of Remote Shutdown Stations**	0
	The plant simulator shall include any remote shutdown control stations and permit shutdown using the remote shutdown facilities to be realistically simulated.	Although the arrangement of the remote shutdown station will be functionally identical to the main control room, training on the operation using only the normal control room stations may not properly prepare the operators. The use of the remote shutdown station will necessarily involve a great deal of stress and a high level of training will be needed to overcome this stress and achieve adequate operator performance. It is also essential that the operators have sufficient confidence in their capability to use the remote shutdown station that they will not delay their evacuation and risk incapacitating all available personnel. Simulator training will help to establish that confidence.	0
4.9.3.4	**Staffing of Remote Shutdown Stations**	**Staffing of Remote Shutdown Stations**	0
	The remote shutdown operations shall be based on a reduced number of operators, specifically, only two licensed operators (SRO or RO) and two EOs shall be assumed to be available in the short term, i.e., for bringing the reactor to hot standby. For the subsequent operation, a normal crew shall be assumed to be available.	It is prudent to assume that the same event which makes it necessary to evacuate the control room may result in incapacitation or unavailability of some of the control room crew. In the first few minutes the personnel may have to work short handed. It is only necessary that this crew get the reactor to a stable, controlled condition, i.e., hot standby. The cooldown can easily wait until a new shift or off-site replacements are available.	0
4.9.3.5	**Panel Arrangement and Design Practices**	**Panel Arrangement and Design Practices**	0
	The design of the remote shutdown station shall locate the display and control elements in an arrangement which is functionally identical to the arrangement of the similar elements in the main control room. Other design practices, e.g., labels, nomenclature, color codes, etc., shall be identical to the main control room.	The similarity of arrangement will reduce the potential of errors and minimize the training burden of the remote shutdown stations.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.9.3.6	**Use of Remote Shutdown Stations for Normal Operations**	**Use of Remote Shutdown Stations for Normal Operations**	0
	The M-MIS Designer shall evaluate the possible routine use of the remote shutdown station for testing, surveillance, or other operations. The routine operations assigned to the remote shutdown station as a result of this evaluation shall be defined and documented as part of the design basis for the remote shutdown station and the overall ALWR M-MIS.	The use of this station for some activities may avoid disruption in the main control room, provides a check of the operational readiness of the station, and keeps the operators familiar with the station and its layout.	0
4.9.3.7	**Reference Material**	**Reference Material**	0
	The analysis of the functions and tasks assigned to a remote shutdown station shall be used to identify the reference material which will be needed at the station. The remote shutdown station design shall specifically provide for the storage and use of these items.	The use of the remote shutdown station will involve operations which are inherently different from those normally encountered. The availability of up-to-date reference material will be important for the operators to cope with the situation, which may be complex. The availability of other reference material, e.g., from the TSC, may be limited in the short term.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.9.3.8	**Enabling of a Remote Shutdown Station**	**Enabling of a Remote Shutdown Station**	0
	No operator action or equipment failures in the main control room shall prevent a remote shutdown station from carrying out its function to shutdown the reactor. That is, the method used to enable a remote shutdown station shall use transfer devices which allow the remote shutdown station to exercise control irrespective of the failures which may have occurred in the main control room. In addition, these transfer devices shall not introduce points of common vulnerability which could lead to loss of both the main control room and remote shutdown station operability. However, any action taken to enable a remote shutdown station or transfer of control to it shall be annunciated in the main control room. The operations required to enable a remote shutdown station shall require a minimum of operator steps, consistent with the reliability (e.g., separation) requirements and the prevention of inadvertent or unauthorized use (see 4.9.2.5).	Because of the unpredictable nature of the evacuation, the operation from the remote shutdown station should have precedence; however, the operators in the main control room need to be alerted if they have been deprived of control of some parts of the plant or some components may be under the control of others.	0
4.9.3.9	**Location of Remote Shutdown Stations**	**Location of Remote Shutdown Stations**	0
	The remote shutdown stations shall not be located in the same building as the main control room nor shall it be possible to open a single door and connect a room containing a remote shutdown station with the main control room complex (e.g., the main control area, operators area, shift supervisor's office, shift technical advisor's office, etc., see Figures 10.4-1 and 10.4-2).	This degree of separation appears to be practical and provides added assurance that events which disable the main control room will not also disable a remote shutdown station.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.4	**Emergency Response Support Facilities**	**Emergency Response Support Facilities**	0
	The M-MIS design shall include those portions of the emergency support facilities which interface with personnel in the course of supporting emergency operations. The design of these facilities shall be consistent with the requirement standards of 10CFR Part 50, 50.47(b) as elaborated in 10CFR Part 50, Appendix E(IV); the criteria of NUREG-0696, *Functional Criteria for Emergency Response Facilities*; the requirements on these facilities in NUREG-0737 Supplement 1, Section 8, "Emergency Response Facilities"; and the additional requirements of this section.	It is intended that the ALWR design meet the currently applicable regulations. Although many aspects of these facilities involve issues other than the man-machine interface, they are fundamentally an extension of the MCR and part of the overall control of the plant during an emergency. Accordingly, it is appropriate to include them within the purview of the M-MIS Designer.	0
4.9.4.1	**Technical Support Center**	**Technical Support Center**	0
4.9.4.1.1	**Access Between MCR and TSC**	**Access Between MCR and TSC**	0
	The TSC shall be located so that the time for personnel to transit from the MCR to the TSC and vice versa will be less than two minutes. In an emergency, it shall be possible to modify normal security boundaries (using defined procedures) so that personnel can move between the two facilities without crossing a security boundary. Access to the MCR from the TSC shall be by a route which can be easily controlled administratively by the MCR staff and the plant management to avoid disruption of the MCR operations by personnel from the TSC.	In an emergency, good access between the TSC and the MCR will put less burden on voice communications and will tend to discourage people from congregating in the MCR and disrupting operations. Easy access between the TSC and the MCR raises concerns that this capability will be abused by personnel from the TSC and result in disruption of the MCR. However, easy access between the two spaces facilitates the support of the operators and the "team" approach to coping with emergencies. Deliberately making the access difficult between the mcr and the TSC to relieve some of the need to exercise administrative discipline in an emergency is not prudent.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.9.4.1.2	**Viewing of MCR Activities from TSC**	**Viewing of MCR Activities from TSC**	0
	The capability shall be provided to monitor visually the general activities in the MCR from the TSC. This may be accomplished by bullet resisting windows or by closed-circuit television.	The capability to establish the general level of activity and personnel present in the MCR from the TSC will reduce the need for personnel in the TSC to contact the MCR and reduce the potential to disrupt the work in progress in the MCR. It will not replace normal voice communication or the need to have ready access between the TSC and MCR.	0
4.9.4.1.3	**TSC Non-emergency Utilization**	**TSC Ncn-emergency Utilization**	0
	The M-MIS Designer shall evaluate the routine use of the TSC to support plant operations as long as it can be shown that these uses would not reasonably be expected to impair its use in an emergency. The routine uses assigned to the TSC as a result of this evaluation shall be defined and documented as part of the design basis of the TSC and the overall ALWR M-MIS.	Because of the extensive data handling capabilities and reference material available in the TSC, as well as the physical space convenient to the MCR. the TSC may be convenient for test data collection, shift or test crew meetings, etc., which would disrupt normal control room operation. Its regular use also helps to assure that its equipment is functional and that personnel are familiar with its facilities.	0
4.9.4.2	**Emergency Operations Facility (EOF)**	**Emergency Operations Facility (EOF)**	0
	The responsibility of the M-MIS Designer for the off-site emergency operations facility (EOF) is limited to the design of equipment intended to duplicate or to link the EOF to the plant process data base used to support the MCR, the TSC, or other plant control stations (remote shutdown stations, for example).	The actual structure, layout, or location of the EOF is considered to be outside the scope of the ALWR.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
4.9.4.3	**Data Handling and Computer Facilities**	**Data Handling and Computer Facilities**	0
4.9.4.3.1	**Availability of Data**	**Availability of Data**	0
	Personnel in the TSC and EOF shall have access to all monitoring data accessible to the control room operators on CRTs or similar computer interface devices and information on the MCR overview display. These personnel shall be able to display the data in a form which is the same, insofar as practical, as the displays used in the MCR.	To perform their support role, the personnel in the TSC and EOF should have access to the same data as the control room operators. By maintaining similar, or identical display systems in the control room, TSC and EOF, communication between personnel will be facilitated when referencing display data.	0
4.9.4.3.2	**Data Transmission Reliability**	**Data Transmission Reliability**	0
	The TSC and EOF data transmission paths shall be designed so that a single failure shall not eliminate a communication pathway.	Robustness of the communication interface design is necessary to assure reliable operation of emergency facilities.	0
4.9.4.3.3	**Processing Capabilities**	**Processing Capabilities**	0
	Data storage, processing, and display capability shall be provided for personnel in the TSC and EOF to recall from storage, manipulate, and display data.	This requirement is based on the following:	0
		1. During an emergency, it is imperative that neither the plant process computer, nor the data links are bogged down with data, computational and display requests from the emergency response facilities, and	
	These functions shall be performed without burdening the plant computer or data communication links between the control room and these facilities.		
		2. Technical analysis involving heavy usage of trending, comparing and calculating based on previous (historical) data, as well as real time data, is expected in the TSC and EOF during an emergency situation. These would potentially place a heavy burden on the plant computer at a time when it is most needed to perform its intended functions.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
4.9.4.3.4	**Access to Data by Other Users**	**Access to Data by Other Users**	0
	The design shall be compatible with the use of data by others, such as the utility management and groups both on and off the plant site.	Although the other uses of these data are not within the scope of the ALWR Requirements Document, the design should not preclude such use. Obtaining the data through the TSC/EOF should provide a reliable source and one which is separate from the control room. That is, it should reduce the potential for these other users to impact control room operations and use of the data.	0

Paragraph No.	*Requirement*	*Rev.*
5	**DATA GATHERING, TRANSMISSION, AND PROCESSING REQUIREMENTS**	0
5.1	**DEFINITION**	0
5.1.1	**Purpose**	0
	This section provides requirements that are needed to assure proper acquisition, processing, and distribution of the large amount of data used for plant control, monitoring, and protection. The scope of this section is from the outputs of sensors and other devices connected to the plant wide data highways to the presentation of data to the various utilizing devices and functions. Requirements for various systems that are primarily data processing functions are also included in this section. Figure 10.5-1 illustrates the scope and interfaces of this section.	0
5.1.2	**Functions**	0
	The functions covered in this section are those required to:	0
	• Provide adequate data quality;	0
	• Provide sufficient data handling capacity;	0
	• Provide a data system that meets overall plant requirements without unduly restricting the designers selection of equipment to meet the needs of a specific function;	0
	• Provide guidelines for maintaining a balance between too much and too little data;	0
	• Provide data requirements for various support functions (TSC, EOF) and operator aids.	0
5.1.3	**Interfaces**	0
	The data gathering, transmission, and processing functions interface to virtually every control, monitoring, and protection system in the plant. The data gathering function interfaces with sources of data (e.g., sensors, operator switches, controller outputs) and sinks of data (e.g., actuators, operator displays). The data transmission function interfaces with data multiplexers, controllers, control stations, etc. The data processing functions described in this section are those processing functions needed to provide consistent data formats and usage in the plant.	0

REV. E 6/01/89

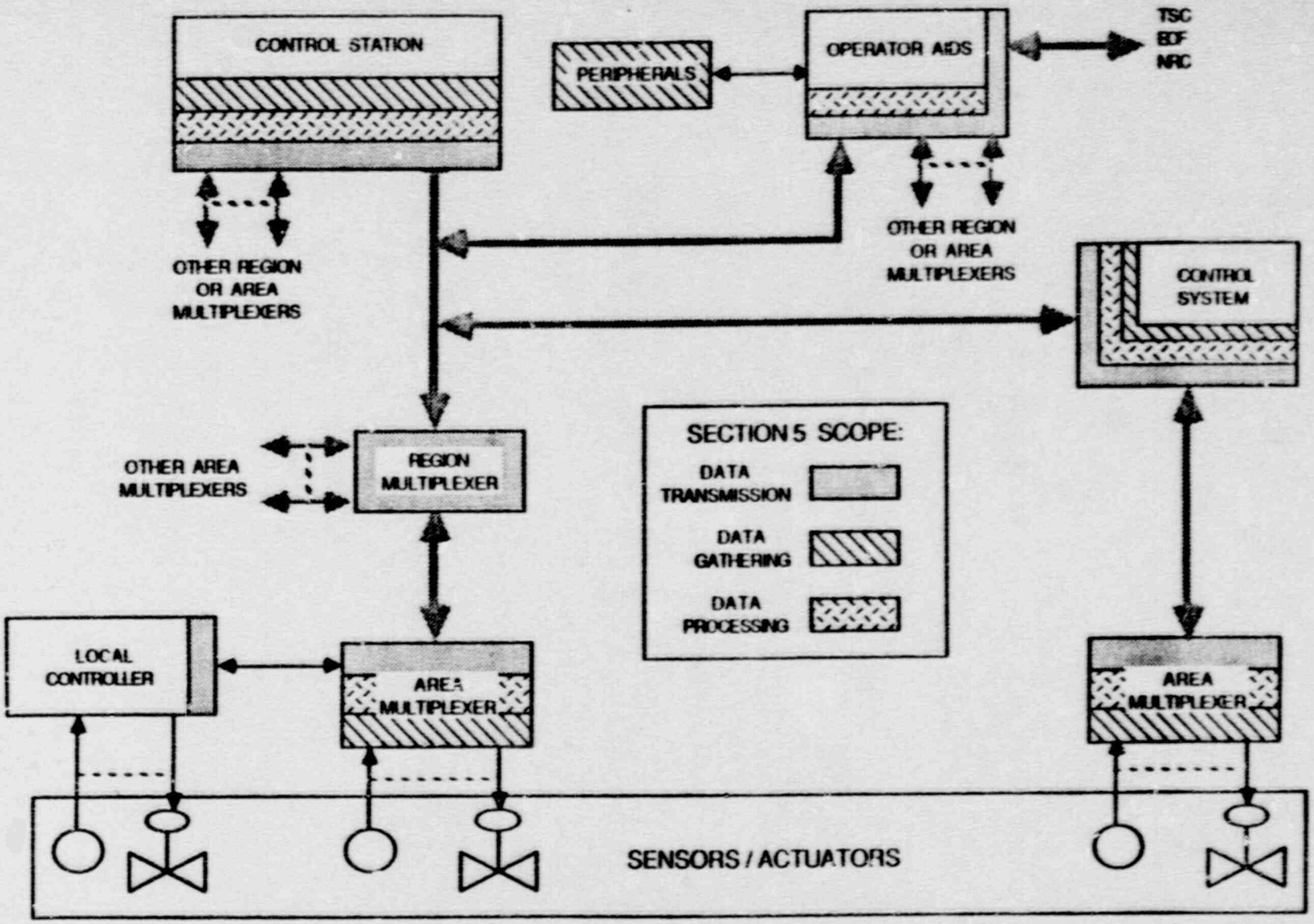


FIGURE 10.5-1: DATA GATHERING, TRANSMISSION, & PROCESSING SCOPE & INTERFACES

Paragraph No.	Requirement	Rationale	Rev
5.2	**GENERAL REQUIREMENTS**	**GENERAL REQUIREMENTS**	0
5.2.1	**Architecture**	**Architecture**	0
5.2.1.1	**Data System Structure**	**Data System Structure**	0
	The Plant Designer shall establish the data system structure. The data system design shall: 1. Minimize the plant wiring; 2. Consider the vulnerability of the plant control and monitoring to a single component failure which can affect more than one system or function; 3. Support the maintenance and test requirements; and 4. Minimize the disruption to the plant data base when a component, equipment, subsystem or system failure occurs. The requirement for layering does not preclude point-to-point hardwired or serial data transmission over long distances when needed to meet other requirements such as speed, diversity, etc.	The data system structure shall incorporate several "layers" of data acquisition and data distribution. The layers shall be structured so that the number of transmission paths between different areas of the plant decrease for each higher layer. The Plant Designer shall establish the number of layers and the number of paths required to minimize plant wiring while maintaining adequate redundancy, segmentation, and separation. There may be cases where point-to-point connections over long distances are required to meet separation, redundancy, and segmentation requirements so this type of connection must be permitted.	0
5.2.1.2	**Signal Interfaces**	**Signal Interfaces**	0
	In addition to providing for analog and discrete I/O, the structure shall provide for data acquisition and distribution using serial and parallel I/O.	There are many devices (e.g., "smart" sensors, programmable controllers, digital panel meters) available that have the capability to provide data or accept set points etc. using serial (e.g., RS232, RS422) or parallel (e.g., Binary Coded Decimal (BCD), IEEE 488) connections. The plant data system must accommodate the use of these devices.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
5.2.1.3	**Redundancy and Diversity**	**Redundancy and Diversity**	0
	The data system shall meet the diversity requirements given in Sections 3 and 6. The data system shall provide redundancy commensurate with the redundancy of the systems and functions that interface with it. The several divisions of safety related systems must use data paths that meet the redundancy and separation requirements of the systems as described in other sections of this chapter.	The independence of redundant systems must not be compromised by the data system.	0
5.2.2	**Design Process Requirements**	**Design Process Requirements**	0
	The design process for the data system shall meet the design process requirements of Section 3 and shall include:	With the application of multiplexing, a signal may be used in several places. The specifications for a signal must therefore support all of its intended applications. In some cases, the listed specific items will impose tighter specifications on a signal than the process monitoring and control requirements.	0
	• Features to assure that the characteristics of a signal will support all of its intended uses. Each characteristic of a signal (e.g., accuracy, resolution, data rate) shall meet the most restrictive requirement of all systems or functions that use the signal. Signal characteristics to support special applications such as operator displays, operator aids, maintenance aids, and the initial startup test program shall be included.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• A method of identifying cases where the signal characteristics required by special applications (e.g., initial startup test equipment) causes the selection of a sensor or other device that has performance characteristics which are much tighter than those required by process control and monitoring. Separate special purpose sensors shall be provided if the high performance requirements result in the selection of a device with lower reliability, higher drift, higher sensitivity to its environments, etc.	• High performance devices may have undesirable characteristics, such as lower reliability, higher susceptibility to noise and environmental changes, higher drift, etc. These characteristics are acceptable for the special applications that are not critical to plant operation or safety, but may not be acceptable for plant control and monitoring, particularly under abnormal conditions.	0
	• Guidelines for determining the method of transmission of a specific signal, extent of segmentation and/or redundancy, extent of distribution of a signal, acceptable transmission path loading and other data system characteristics that require judgment on the part of the designers.	• The data system application must be consistent on a plant-wide basis. Therefore, the design process must provide guidelines to assure that a reasonably consistent basis is used by the many designers.	0
5.2.3	**Performance Requirements**	**Performance Requirements**	0
5.2.3.1	**Multiplexer System Capacity**	**Multiplexer System Capacity**	0
	The multiplexer system shall be designed with sufficient performance margin to perform its designed function under conditions of maximum stress. Conditions of maximum stress shall be based on plant events that cause the highest data acquisition, data processing, and data transmission loading. Consideration of failures, operator actions, automatic test features, etc. shall be evaluated.	The multiplexer system should have enough capacity to perform its intended functions without skipping a function because there is insufficient idle time allotment. It is good engineering practice to have approximately 40 percent additional performance capacity when the system is fully stressed.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
5.2.3.2	**Multiplexer System Expansion Capacity**	**Multiplexer System Expansion Capacity**	0
	The multiplexer system shall be designed with reasonable expansion capability which would permit an Owner to add functions in the future. The system shall have, as a minimum, a 25 percent expansion capability.	There should be sufficient capacity to permit the Owner to expand the system. System expansion can be achieved by adding modules for most designs. Sometimes expansion by the addition of modules may require the addition of communication links which can be costly. Therefore, expansion capability within a common chassis is desirable. Requirement 5.2.3.1 should insure sufficient margin to accommodate the performance capacity impacts of expanding the system.	0
5.2.3.3	**Data Transmission Capacity**	**Data Transmission Capacity**	0
	Data communication links and network links shall be designed with sufficient performance margin to perform under conditions of maximum stress. The loading shall be based on plant transients and events that cause the highest transmission. Plant data, failures, operator actions, automatic test features, etc. shall be considered by the Plant Designer.	It is good engineering practice to have approximately 40 percent additional capacity. Ten percent is for the uncertainty of stressing the hardware to its limit, and 30 percent is for system expansion accommodation.	0
5.2.4	**Reliability and Availability**	**Reliability and Availability**	0
5.2.4.1	The reliability and availability of a particular data path shall meet the Section 3 requirements that are applicable to the systems and functions that use it.	In effect, the reliability and availability of the data system must be included in the analysis performed for a specific system or function.	0
5.2.4.2	When redundant data paths and signal selection are used, the reliability model of the data path shall include consideration of the failure rate and coverage provided by the selection device or algorithm. The coverage term as well as the reliability must be justified, particularly when complete coverage is used.	The failure rate of the selector may be a significant contributor to overall data path reliability. Coverage is an indication of the effectiveness of the selection device or algorithm. The reliability analysis must include consideration of cases where the selection algorithm or device will not detect all failures or data anomalies. This is of special concern when analytic redundancy is used because the effectiveness of the selector depends on the capabilities of the model used.	0

Paragraph No.	Requirement	Rationale	Rev.
5.2.5	**Signal Transport Delay**	**Signal Transport Delay**	0
5.2.5.1	The propagation time for multiplexed data shall be analyzed to demonstrate the prevention of significant degradation in performance of plant control and monitoring systems.	A multiplexed data system creates a finite deadtime in a control loop.	0
5.2.5.1.1	For closed loop controls, the combined propagation delay from a change in a signal to the results of the change being received at an actuator shall be considered in the analysis of the control loop to show stable operation.	For closed loop controls, deadtimes reduce system stability, so the control system design must adequately account for this deadtime.	0
5.2.5.1.2	For discrete control functions (reactor trips, ESF initiation, equipment protection, etc.) the signal transport delay shall be analyzed to show that the actions occur within the allocated time when the signal transport time is added to other delays.	For discrete control actions, the delay could be a significant portion of the time allowed to implement the action.	0
5.2.5.1.3	The propagation time shall include response degradation due to filters, the sampling rate of the signal, analog to digital (A/D) conversion time, signal processing time (if applicable), resampling rates (if applicable), data transmission time, and digital to analog (D/A) conversion times.	Various aspects of the data system which could contribute to the effective delay must be considered.	0
5.2.5.1.4	Operator control (e.g., joystick, trackball, etc.) feedback response to operation of the man-machine interface device shall be determined from human factors analysis. The process response delay time shall be established by the system requirements. When an operator control device causes a parameter to ramp, the display update must not be significantly greater than the operators perception time in order to prevent overshooting or undershooting the desired value.	With the operator in the control loop, care must be taken that the display system does not introduce delays which significantly destabilize the system. In addition to this functional requirement, there is an implied requirement that the operator perception of the delay be negligible.	0
5.2.5.2	The system design shall provide the operator acknowledgment of a requested action within 0.25-second of the operator request.	The operators are accustomed to and expect a prompt feedback that their requests have been received. This requirement is analogous to the snap action of a switch which is perceived as an acknowledgment.	0

Paragraph No.	Requirement	Rationale	Rev
	The system design shall not introduce more than a 1.5-second additional delay to the change of state of a display than is current experienced in a "hand-wired" system.	The equipment which is expected to be used in the M-MIS, in many cases, will add time delays to the acquisition, transport, and display of information. From the standpoint of operator perception, a maximum time limit needs to be established.	0
5.2.6	**Standardization**	**Standardization**	0
	The plant data system shall meet the standardization requirements given in Sections 3 and 6. The modules and algorithms for filtering, data conversion, data processing, error checking, etc. shall be standardized to the extent practical.	Standardization requirements given in other sections apply to the plant data system.	0
5.2.7	**Communication Protocols**	**Communication Protocols**	0
	Plant-wide data highway protocols and interfaces to controllers, sensors, actuators, etc. shall be based on widely used industry standards. Interfaces that are proprietary or have a small installed base shall not be used. Localized proprietary data highways, such as those in some programmable controllers, may be used if a clear benefit can be derived from their use; however, their interface to the plant-wide data highway must be of a standard type.	The interfaces to and communication between the plant data system and other plant equipment must be based on widely supported standards in order to achieve the flexibility, longevity, and standardization envisioned for the ALWR. Some control devices – in particular, programmable controllers – use proprietary buses. Use of these devices should not be precluded if they can interface to the plant data highway.	0

Paragraph No.	Requirement	Rationale	Rev
5.3	**DATA GATHERING REQUIREMENTS**	**DATA GATHERING REQUIREMENTS**	0
5.3.1	**Signal Specifications**	**Signal Specifications**	0
5.3.1.1	The data gathering hardware and software for analog input signals must assure that the signal provided meets the requirements of all the assigned uses of the signal. The signal characteristics to be considered shall include:	The data provided must meet all of the traditional signal quality requirements.	0
	• Accuracy;		0
	• Resolution;		0
	• Sample Rate;		0
	• Repeatability;		0
	• Response rate;		0
	• Safety Classification;		0
	• Range;		0
5.3.1.2	For discrete and pulse input signals, the data gathering process shall provide:	This requirement is to preclude the system from receiving fake or spurious signals.	0
	• Immunity against noise causing a false signal indication;		0
	• Sufficient response and sample rates to capture all transitions of the input signal;		0
	• Voltage supply for dry contact signals;		0
	• Switch debounce, where applicable.		0
	• All failure modes to be identifiable as soon as practical.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
5.3.1.3	The signal provided shall meet the most restrictive value of each requirement from all of the systems that utilize the signal.	Because each signal may be used in several places, each specification for the signal must meet the most restrictive of all the uses.	0
5.3.2	**Signal Filtering**	**Signal Filtering**	0
5.3.2.1	Each data acquisition channel shall contain appropriate filtering of the sensor output to reduce any noise on the signal to acceptable levels. The residual noise shall be small enough to prevent spurious trips and equipment actuation due to noise and to prevent excessive equipment wear due to "dithering". Filtering shall be held to a minimum in order to eliminate noise spikes or isolations. A capacitance circuit or similar approach should be used so as not to affect the general signal characteristics.	Any residual noise on sensor outputs should be reduced by filtering to a level that will not cause operational or maintenance problems. Filtering should not remove signal characteristics that could be used for sensor health monitoring.	0
5.3.2.2	When A to D conversion is used, the filters shall also reduce any signal noise aliased into the pass band to acceptable levels. Whenever a signal is resampled at a rate lower than the sample rate used in the A/D conversion process, appropriate digital filters shall be used to reduce aliasing and noise to an acceptable level.	In sampled data processes, high frequency noise can appear as a lower frequency signal. This is known as aliasing. Appropriate signal filtering must be used to reduce the aliasing. Resampling a previously sampled signal at a lower rate can also cause aliasing.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
5.4	**DATA TRANSMISSION**	**DATA TRANSMISSION**	0
5.4.1	**Data Signal Tagging**	**Data Signal Tagging**	0
5.4.1.1	All data on the plant-wide data buses shall have signal identification information associated with them. When a signal is to be used for post event analysis or other applications where precise timing information is required and the transport delay could be a significant portion of the time resolution, then time tagging shall be attached to the signal.	Some method of identifying the source of a signal is needed to assure that the correct data is used. Precise timing information is needed for some applications of data. Multiplexing data can cause some time slewing of the data, so timing information may be needed in some cases.	0
5.4.1.2	All data shall have a signal quality tag associated with it. The signal quality tag along with other troubleshooting aids must provide sufficient information to direct the troubleshooting process.	The multiplexing system can detect data and equipment errors and must flag the data when its quality is suspect. The data errors can occur at several levels in the system, so the tag must indicate where the problem has occurred. Other troubleshooting aids may be used to supplement the information provided by the tag.	0

Paragraph No	*Requirement*	*Rationale*	*Rev*
5.4.2	**Multiplexed Data Transmission Fidelity**	**Multiplexed Data Transmission Fidelity**	0
	The data transmission process shall provide sufficient inherent integrity and error checking to assure that random errors in the process will not degrade the availability and reliability of the systems and functions that utilize the data. The intent of this requirement is distinct from "hard" equipment failures. It is meant to address soft errors that result in one or more bits in a data stream to be in error for a single transmission. As a minimum, the data transmission process shall assure that the transient errors do not cause significant errors in the operator displays more frequently than once for every 10^{10} signal transmissions. The data transmission process shall assure that spurious trips, spurious actuation, equipment misoperation, etc., due to transient errors does not significantly degrade plant availability and capacity factor. These error evaluations must include consideration of errors in the device addressing data, handshaking data, signal data, error checking data, signal quality data, and signal identifier data. The effect of filters or switch debounce at the receiver that cause short term errors to be ignored and any signal redundancy used may be included as methods to reduce the effective error rate.	Multiplexed data consists of a large amount of data that can be corrupted by the line drivers, line receivers, and possibly the signal transmission conductor. The availability and reliability of data transmission is an integral part of the availability and reliability of the systems utilizing the data. If a plant contains 2000 multiplexed signals with an average sample rate of 3 per second, the total number of signals transmitted in a day is approximately 500 million. Note that the signals that must be considered are those from sensors, operator controls, switches, etc., and those to actuators, relays, displays, etc. Also, note that plant sensitivity to errors in discrete signals can be much higher than plant sensitivity to errors in analog signals because a single error can cause unwanted equipment actuation or shutdown. Errors in device addressing and signal identifiers are perhaps more critical than errors in the data because they can cause signals to go to the wrong destinations.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
5.5	**SIGNAL PROCESSING**	**SIGNAL PROCESSING**	0
	Any signal processing, such as scaling, amplification, linearization, rate of change calculations, etc., shall assure that: • The accuracy, resolution, precision, and rate of response of the results of the processing are consistent with those of the signal being processed and the applications of the signal. • Any coefficients or other factors used in the processing must retain their values for power interruptions and other events that could potentially corrupt them. In addition, provisions for periodically verifying them shall be incorporated. • If signal rate of change is determined, the rate of change method shall assure that noise in the signal does not unduly influence the rate.	Processing of signals can change the characteristics of a signal. The requirements are intended to assure that adequate consideration is given to the changes. The integrity of the parameters used in signal processing must be insured and confirmed in order to retain the desired signal characteristics. Special consideration must be used when rate is determined – as might be used in some signal validity checking algorithms.	0
5.5.1	**Signal Validity Checks**	**Signal Validity Checks**	0
	The data system signal processing shall provide appropriate signal validity checks. The validity checks shall assure that the data meets the reliability requirements of Section 5.2.3.	Signal validity checks are an important aspect of assuring reliable data.	0

Paragraph No.	Requirement	Rationale	Rev
5.6	**OPERATOR AIDS**	**OPERATOR AIDS**	0
	The operator aids are intended to provide information to the operator to help in monitoring and controlling the plant. All operator aid functions shall meet the requirements of Section 5.5 and provide the self diagnostics, signal fault detection, etc. to warn the operator whenever the system or specific sub-functions are unavailable.	Operator aids are processing functions, so the requirements of Section 5.5. are applicable. The operator must be made aware whenever the aid is unavailable so that alternative means may be used.	0
5.6.1	**Technical Specification Monitoring Function**	**Technical Specification Monitoring Function**	0
	The technical specification monitoring function shall have the following capabilities to warn the operator when a limiting condition of operation (LCO) is being approached or an LCO is being violated:	Technical specification monitoring can aid the operator in maintaining plant operation and thereby improve plant availability.	0
	• The system shall use appropriate information on equipment status, core limits and margins, and other appropriate data to determine the approach to an LCO. To the extent practical, the system shall also indicate appropriate action to avoid violating the LCO.	• In order to provide maximum aid to the operator, an indication of the approach to an LCO and information on how to avoid the LCO is required.	0
	• Provide for acquisition and processing of the information needed to determine the approach to and existence of an LCO. To the extent practical, the information shall be automatically acquired by the system. Any automatic testing that could impact LCOs shall be automatically acquired by the system.	• Failures, maintenance activities, and test operations are important data for establishing LCOs. Automatic acquisition of the information will relieve the burden on the operator and is required when the activity is not initiated by the operator.	0
	• Warn the operator when an LCO has been violated and identify the LCO. To the extent practical, the system shall also indicate the action needed to recover from the LCO. The system shall automatically log all LCO violations.	• A violation of an LCO must be indicated since this is a primary function of the system.	0

Paragraph No.	Requirement	Rationale	Rev.
	• Perform calculations to establish reactor and core parameters required for monitoring LCOs, such as thermal margins, power distributions, heat generation rates, etc. The results of these calculations shall be made available on operator displays.	• Various core and plant parameters are needed to establish approach to or existence of an LCO. The results of these calculations are useful for normal plant monitoring by the operator.	0
	• The system shall have manual input capability for limiting conditions of operation that cannot be monitored automatically by the system. An acknowledgment function for alarm conditions shall be included.	• Operator administrative burden for logging and tracking limiting conditions of operation is greatly reduced through the use of a computerized system for all limiting conditions of operation. Acknowledgment of alarm conditions will ensure operator awareness and verification of identified operational problems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
5.6.2	**Emergency Safety Features Availability Monitoring Function**	**Emergency Safety Features Availability Monitoring Function**	0
	The M-MIS shall provide the operator with the status of both the long term and short term availability of the ESF functions. If appropriate, this function may be considered a sub-function of the technical specification monitoring function. The M-MIS shall: - Monitor support services (e.g. voltages, cooling water, oil pressure and levels, etc.) that can affect the availability of the ESF functions. The availability of both the initiating equipment (sensors, control systems, etc.) and the implementing equipment (pumps, valves, etc.) shall be monitored. The availability of both primary and backup sources of services shall be monitored. - Monitor process parameters (reactor pressure, water storage tank levels, environment, etc.) that can impact the successful operation of an ESF. - Have provisions for acquiring the maintenance, calibration, and test data needed to establish ESF operability.	The status of the ESF functions is an important part of determining the plant status with respect to LCOs. The short term availability of the ESF functions is basically the ability of the functions to initiate properly. The long term availability of an ESF function is its ability to continue operation for extended periods using the available sources of water, power, etc. The status of support services, plant conditions, and the results of various test and maintenance operations are important for establishing ESF availability.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
5.6.3	**Computer Aided Plant Diagnostics, Maintenance, and Testing**	**Computer Aided Plant Diagnostics, Maintenance, and Testing**	0
	The plant shall contain features to aid in periodic surveillance testing, special testing, maintenance and inspection planning, and identifying potential equipment degradation. The functions shall provide for the data acquisition, data analysis, data base management, and operator interface to accomplish the following:	Because the ALWR is expected to utilize a large amount of multiplexed data, this provides the opportunity to use the data to aid in plant operations. Because many problems in operating LWRs can be attributed to inadequate maintenance and testing, the ALWR must capitalize on these opportunities.	0
	• Provide logs, historical information, logistics aids, etc., to support the periodic surveillance testing required or implied by the plant technical specifications. Provisions for tracking instruments used in the tests, procedures used in the tests, verifying pre-test and post-test conditions, and collecting and storing the results of the tests shall be provided.	• Surveillance tests to implement plant Technical Specification requirements is a significant plant activity. The ALWR should use the plant data base and other aids to enhance the performance, tracking, utility, and data storage for these tests.	0
	• Provide appropriate inspection planning aids. The inspection planning aids shall use information such as component design, results of previous inspections, repair history, operating history, regulatory guides, and service information to guide the plant inspections.	• Both site specific and industry wide data can be very useful in guiding special inspections (e.g., steam generator tubes, welds).	0
	• Provide temperature monitoring and logging of equipment for equipment qualification lifetime extension.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Monitor plant performance to identify possible degradation in plant equipment. The overall plant efficiency shall be periodically evaluated using NSSS and BOP data, such as reactor power level, feedwater temperatures and flows, turbine steam flows and steam conditions, condenser vacuum, energy consumed by auxiliaries, etc. The evaluations shall be compared against expected performance for the current plant conditions. These evaluations shall be used as an aid in determining degradations in overall plant performance and identify the parameters that are responsible for the degradation.	• The overall plant efficiency can be an indicator of degradation in performance of some plant equipment.	0
	• Provide features for monitoring and managing water chemistry. This feature shall provide appropriate sensors, data acquisition, data storage, and analysis tools to aid the plant chemist in the analysis, diagnosis, and correction of chemistry anomalies. Analysis tools to perform corrosion prediction shall also be provided.	• Water chemistry is an important factor in the lifetime of some components. Close monitoring and control of water chemistry can prevent premature failure of the components.	0
	• Provide for data acquisition and analysis to be used for identifying degradation in or failure of selected critical equipment. The system shall use both straightforward techniques (e.g., leak rate measurement) and special analysis techniques to identify potential equipment degradation. The special analysis techniques shall include noise analysis, analysis of the results of surveillance tests, and other techniques to identify degradation in the equipment, failure of equipment or the existence of foreign object inside of assemblies (e.g. vessel loose parts monitoring).	• In the past, various parameter measurements, such as relief valve discharge temperature, have been used to identify degradation of selected critical components. The continued application of some of these techniques may be appropriate. Various efforts by EPRI and others have used various analysis techniques [e.g., acoustical noise analysis, Fast Fourier Transforms (FFTs) on sensor signals] to both identify and predict component wear out. The ALWR should take advantage of these techniques.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Provide for sensors, data acquisition, data analysis, data storage, and data displays required to support initial plant startup testing. Logistics support, such as identifying and tracking special test equipment used, establishing pre- and post-test conditions and test initiation and termination shall also be provided. Special care must be used to assure that the data provided has sufficient accuracy, resolution, and response rate to satisfy the initial startup test requirements. The initial startup testing shall utilize permanent plant sensors and instruments to the maximum extent practical. The use of special connections shall be minimized, and disconnecting of plant wiring is not permitted unless there is a compelling reason to do so.	• The initial plant startup tests require the acquisition and analysis of large amounts of data. In addition, the test conditions must be carefully controlled to assure useful test results. Data available in the plant data base will, in many cases, be adequate for initial startup testing; however, test results must not be compromised in order to utilize existing sensors. Connecting and disconnecting leads always introduces the possibility of damaging equipment or causing improper restoration following the tests.	0
5.6.4	**Technical Support Center (TSC)**	**Technical Support Center (TSC)**	0
	A TSC for operator support personnel during a site emergency is provided near the control room. The data system for the TSC shall meet all applicable regulatory guides and standards.	A TSC is a regulatory requirement for LWRs. The requirements for the TSC are given in NRC regulations. The listed requirements are highlights of the regulations.	0
5.6.5	**Emergency Operations Facility (EOF)**	**Emergency Operations Facility (EOF)**	0
	An EOF to provide coordination and communication between on-site and off-site emergency management personnel shall be provided near the plant site. The EOF shall meet all applicable regulatory guides and standards.	An EOF is a regulatory requirement for LWRs. The requirements for the EOF are given in NRC regulations.	0

Paragraph No.	Requirement	Rationale	Rev
5.7	**HARDWARE**	**HARDWARE**	0
	The hardware used in the data system shall meet the applicable general hardware requirements given in Sections 3 and 6 and the applicable hardware requirements for all systems that interface to a particular portion of the data system. The hardware shall also contain the features needed to meet various key requirements for connected systems.	The general hardware requirements are applicable to all ALWR hardware. The quality and classification of the data system hardware must meet the requirements of all systems that utilize data from a particular portion of the data system. Some data system capabilities may be needed to meet testability, maintainability, etc. key requirements.	0
5.7.1	**Module Configuration**	**Module Configuration**	0
	The use of switches or other configuration selection mechanisms on the data system modules shall be minimized. Module configuration by back plane wiring is preferred. When on card configuration is used, the installation instructions shall provide clear instructions on configuration and appropriate post installation tests to assure proper configuration.	Module addressing, signal range selection, etc. are sometimes set using devices internal to the module. Providing configuration selection on the backplane will eliminate the need for configuring replacement modules, but is not always practical.	0
5.7.2	**Analog to Digital (A/D) Convertors**	**Analog to Digital (A/D) Convertors**	0
	The A/D convertors used in the plant, including those incorporated as part of purchased equipment shall:	These are the basic specifications of any A/D convertor. Minimum performance requirements should be applied, regardless of the application. The given minimum requirements are somewhat arbitrary but are easily met by most A/D convertors.	0
	• Provide accuracy, resolution, and speed suitable for the application.		0
	• Have a drift small enough so that a calibration interval of 18 months or more can be used. Automatic self-calibration may be used to achieve the 18-month interval, but provisions for checking and adjusting the reference used for self calibration shall be provided.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
5.7.3	**Digital to Analog (D/A) Convertors**	**Digital to Analog (D/A) Convertors**	0
	The D/A convertors used in the plant, including those incorporated as part of purchased equipment shall:	These are the basic specifications of any D/A convertor. Minimum requirements should be used regardless of the application. The given minimums are easily met by most D/A convertors.	0
	• Provide accuracy, resolution, distortion, and speed suitable for the application.		0
	• Have a drift small enough so that a calibration interval of 18 months or more can be used.		0
	• Any output glitches from the convertors shall not be permitted.		0

Paragraph No.	*Requirement*	*Rev.*
6	**COMMON SOFTWARE, HARDWARE AND CONTROL REQUIREMENTS**	0
	This section provides the common software, hardware, and control requirements for design, implementation, and installation of the M-MIS. The requirements, along with the requirements specified in Sections 3 and 4 and Sections 7 through 10, comprise the requirements necessary to design the M-MIS. The purpose of this section is to specify those requirements which are applicable to all systems contained in Chapter 10 to avoid repeating requirements in other sections.	0
6.1	**COMMON SOFTWARE REQUIREMENTS**	0
6.1.1	**Definition**	0
6.1.1.1	**Purpose**	0
	The purpose of this subsection is to define common requirements for design, selection, and installation of specific M-MIS software. This subsection does not repeat any requirements specified in Chapter 1 or other sections of this chapter, but complements those requirements by specific requirements.	0
6.1.1.2	**Scope**	0
	The M-MIS software includes all software and firmware required for operation and maintenance of the plant. The requirements do not necessarily apply to software utilized by the Plant Designer in the design of the plant. It includes both software prepared by the Plant Design organization, purchased software, and software supplied with the purchased system and equipment as part of the plant. Software means computer programs.	0

Paragraph No.	Requirement	Rationale	Rev
6.1.2	**Design Process**	**Design Process**	0
6.1.2.1	Software products prepared by the Plant Design organization, purchased software, and software supplied with the purchased system and equipment as part of the plant shall be covered by a Software Quality Assurance Program (SQAP). For safety-related software, the SQAP shall comply with the requirements specified in 10CFR50, Appendix B. The intent of this requirement can be met if NUREG/CR-4640, *Handbook of Software Quality Assurance Techniques*, applicable to the nuclear industry, is followed.	There are four types of software commonly used: application, support, test and maintenance, and training software. Application software includes computer codes used for plant design calculation and plant operating software. Support software includes those software items such as operating systems, compilers, assemblers, development stations, debuggers, editors, data bases, mathematical subroutines, system libraries, and utilities. Test and maintenance software is used to carry out testing, operation, and maintenance functions. Training software includes computer aided instruction, simulators, etc. which are used for training plant personnel.	0
6.1.2.2	For all software developed by the M-MIS Designer as a deliverable product, the M-MIS Designer shall establish a software life cycle which provides a systematic approach to the development, use, and operation of any software system. Strict adoption and use of a software life cycle shall be required.	Strict adoption and use of a life cycle ensures that software development will progress in a traceable, planned, and orderly manner. Quality must be designed into the software.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.2.3	The software life cycle, as a minimum, shall contain the following phases and activities:		0
	• Requirement Specification;	• Requirement Specification consists of identifying the requirements that the computer program must satisfy.	0
	• Functional Specification;	• Functional Specification determines the design for the software.	0
	• Detailed Software Design Specification;	• Detailed Software Design Specification continues to break down the functions identified in the software requirements specification.	0
	• Coding and Software Generation;	• Coding and Software Generation – the detailed software design is translated into a high level or assembly level programming language.	0
	• Testing, Installation, and Commissioning;	• Testing, Installation, and Commissioning include final testing by the developer, installation, acceptance testing, and commissioning (or certification) of the software system.	0
	• Transfer of Responsibility;	• Transfer of Responsibility is the turnover of the software for maintenance of the software from the developer to the user.	0
	• Operation/Maintenance;	• Operation/Maintenance is the final phase of the software cycle. The software is accepted for operational use.	0
	• Project Management.	• Project Management is a critical element of software quality assurance and covers the entire software life cycle, including both the development and operational phases.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.2.4	The M-MIS Designer shall develop a software requirement specification which clearly describes each software requirement (function, performance, design constraints, and attributes of the software and external interfaces). Each requirement shall be defined such that its achievement can be verified and validated objectively by a prescribed method (e.g., inspection, demonstration, analysis, or testing).	The software requirement specification is the most significant phase of the overall project in terms of its effect on quality of the final product. Critical errors need to be caught during the requirements analysis to avoid costly rework. This document is a technical description of how the software will meet the requirements set forth. It describes the major functions of the software such as data bases, diagnostics, external and internal interfaces, and the overall structure. The software design description involves detailed descriptions of the operating environment, monitors, timing, system throughput, tables, sizing, modeling, etc.	0
6.1.2.5	The M-MIS Designer shall specify the detail design which shall include the definition of algorithms and equations, the detailed control logic, and data operations that are to be performed within the software.	The detail software design provides a conceptual solution or blueprint for the implementation phase that follows. All ingredients that will ultimately make up final implementation are considered. Some of the specific considerations are defined at this time, including (1) the computer, (2) the computer resources to be used and the extent of use, (3) the computer language, (4) the modules, (5) the sequence of functions, (6) the data structures, and (7) other items specific to the software product.	0
		The primary output of this phase is a detailed design specification which may consist of words, flow charts, decision tables, program design language, or other choices.	0

Paragraph No.	Requirement	Rationale	Rev.
6.1.2.6	A Software Verification and Validation Plan (SVVP) shall be developed to describe each phase of the software life cycle: the verification and validation tasks; tools, techniques, methods and criteria; inputs and outputs; schedule; resources; risks and assumptions; and roles and responsibilities for accomplishing verification and validation of the software. The plan shall meet the requirements of ANSI/IEEE Std. 730 and ANSI/IEEE 829	The software quality assurance plan (SQAP) identifies the documentation to be prepared during the development, verification and validation, use, and maintenance of a software system. The SQAP should describe the following for each phase of the software life cycle: V&V tasks; tools, techniques, methods, and criteria; input and output; schedule; resources; risks and assumptions; etc. The software quality assurance plan shall demonstrate that the project has been thought out and that the QA activities are well defined before execution of the project. NUREG/CR-4640 is an acceptable SQA approach.	0
6.1.2.7	A Software Verification and Validation Report shall be developed which describe the results of the execution of the software verification and validation. This includes the results of all reviews, audits, and tests required by the SVVP.	The Owner can review the report and assess the quality of the software product. The Software Verification and Validation Reports should summarize the status of the software as a result of the execution of the software verification and validation plan. It describes any major deficiencies found; provides the results of reviews, audits, and tests; and recommends whether the software is ready for operational use.	0
6.1.2.8	The M-MIS Designer shall establish a design standard to be used during the design phase. The standard shall describe coding convention, color convention, code format, code documentation format, and all other standards which will ensure uniformity in the software design. Consideration shall be given to the use of graphical techniques, and structured analysis and design methodology.	The use of coding standards in the development of software permits reviewers to be on common ground when they are verifying a software module. If each software module throughout the project is formatted like every other, a reviewer will always be in familiar territory. A similar format expedites the review process and aids in the identification of errors and deficiencies in format.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.2.9	The software shall be designed with descriptive statements or comments incorporated into the source program.	Documentation internal to the program makes the verification and testing easier, and is a powerful incentive for proper maintenance and an assurance that documentation will be accessible to the user. In the case of scientific software commentary which references the source of the equations, the models and the logic are of great help to reviewers and users in verifying and validating the software or in establishing the adequacy or applicability of the software.	0
6.1.2.10	The M-MIS Designer shall perform code analysis to verify that the computer program, as coded, correctly implements the specified design.	Code analysts should examine the program's source language and its compiled or assembled object code, using a variety of techniques. The equations and logic of the source language program should be reconstructed, either manually or using automated aids, and compared to those specified in the design to identify errors made in translating the design into programming language.	0
6.1.2.11	The M-MIS Designer shall develop user documentation (e.g., operations and maintenance manuals, or guides) which specify and describe the required data, input sequences, options, program limitations, and other activities/items necessary for the execution of the software. All error messages shall be identified in text meaningful to the user, and possible corrective actions shall be described.	Sufficient documentation of the M-MIS software is required by the Owner prior to final acceptance.	0
6.1.2.12	The purchasing organization procuring "off-the-shelf" software shall perform acceptance tests (or verification and/or validation) on the computer configuration which the software is to be applied. The purchasing organization shall plan, design, and carry out the test in accordance with the software requirements specification.	The purchasing organization must be held accountable for commercially available software products in the same manner as for hardware components.	0
6.1.2.13	The purchase testing plan, specification, report and analysis shall be maintained and available for examination by the Owners if requested.	This requirement provides a document trail to permit the Owner to evaluate the quality of the software purchased.	0

Paragraph No.	Requirement	Rationale	Rev
6.1.2.14	After the code has been tested and/or verified on the purchasing organization's system, the software shall be placed under configuration management. From this point forward, the code shall be handled and treated as software developed by the organization, and the software life cycle is implemented.	All users and designers will be using the current version of software.	0
6.1.2.15	For purchases made from "software clearinghouses," for which the purchaser has read-only access to the software on a contractual basis, the purchaser must rely on the clearinghouse to provide configuration control of the software. However, the purchaser shall be responsible for the accuracy of calculational results, identification of software errors, and assessment of impacts caused by software errors identified by other users and controlling use of the software.	Self-explanatory.	0
6.1.2.16	The software designer shall maintain records of all commercially purchased software, the version numbers of the software used to perform calculations, the dates they were run, etc. In addition, the purchasing organization shall have a systematic means of informing all past code users of updates, of bugs that have been identified and fixed, and of planned changes to the software.	This is specified in order to meet the configuration control requirement.	0
6.1.2.17	Software which is developed specifically for the purchasing organization (M-MIS Designer) and is a new type of software shall be subjected to all the software requirements specified in this subsection. Applicable requirements specified in this subsection shall be required of the software developer. As a minimum, the requirements for documentation; standards, practices and conventions; review, audits, and controls; software configuration management; testing and verification shall be required of the software supplier.	The quality level of software delivered by the software developer should be comparable to the software delivered by the M-MIS Designer for new applications.	0

Paragraph No.	Requirement	Rationale	Rev.
6.1.3	**Software Design**	**Software Design**	0
6.1.3.1	A top-down structured design approach shall be required for the design of all software.	Quality must be designed into software. Quality through after-the-test testing or unstructured software testing is very costly, risky, and does not assure correctness or robustness of the software. The preferred top-down structured approach is the Yourdon methodology to structured design and analysis.	0
6.1.3.2	Software documentation shall be developed along with the software design. Documentation shall include hardware/software specifications that delineate the functional performance, design constraints, interfaces, and integration requirements involving hardware and software. This documentation is necessary to ensure that system hardware is coordinated with its control program.	This is essential to perform comprehensive verification and validation activities and for the V&V to be effective. The documentation is the basis for the test acceptance criteria.	0
6.1.3.3	Software design shall incorporate defensive techniques. Software design shall anticipate beyond the design basis because the software cannot discriminate between design basis and beyond design basis. The software shall include limits checks, assign default values to prevent software instability, out-of-range of design inhibits which prevent erroneous entries, logic check for erroneous input data due to communication errors, etc. to prevent software instability, erroneous calculation or control other adverse results.	The design basis of software is unlike that of hardware because it will accept nearly any input data. For example, if the design basis is to select an option of 1, 2 or 3 for an action and if the operator selects anything other than the three options, the software should be designed to ignore any other inputs. Selection of "99", "ABC", or any other illegal characters shall be ignored rather than hang up the software or cause any other adverse action.	0
6.1.3.4	Software design shall avoid convoluted control software structure.	Such design practices makes debugging very difficult and introduces the potential for errors.	0
6.1.3.5	Operating System software shall remain "as delivered" from the computer vendor or commercial software house. Modifications, alterations, or writing application software integral to the operating system shall not be permitted.	Portability and upward compatibility are ensured when updates and new releases are provided from the computer or software vendor.	0

Paragraph No.	Requirement	Rationale	Rev.
6.1.3.6	Software shall be portable and upward compatible to ensure that updates and new releases can be incorporated.		0
6.1.3.7	The software design shall use a hierarchical design structure and principles of modular design with coherent, cohesive modules.	The use of these design methodologies are known to result in high quality software because it is an easily verifiable product. The objective of these techniques is to reduce the complexity of the design and verification of the software by dividing the system into intellectually manageable components.	0
6.1.3.8	The software design phase shall explicitly identify assumptions, the violations of which would be critical. The designer shall specify how the program shall behave if any of these assumptions are violated. These assumptions shall include both hardware and software violations.	Fault-tolerant design enables software to continue to function successfully in spite of failures when faults occur.	0
6.1.3.9	A minimum number of different compilers, operating systems, programming languages, and other support software packages shall be used. A specific programming application should be restricted to one programming language and one operating system, wherever possible.	Minimizing the number of different programming languages and programming environments supports standardization and transportability, and facilitates testing and modification of software.	0
6.1.3.10	Compilers, operating systems, and other support software shall be chosen from commercially available proven software packages. New or untried compilers and operating systems shall be avoided.	While the compilers and operating system software will be tested functionally as part of verifying the application routines that use them, to achieve the highest reliability and minimize problems uncovered in testing, new software packages should be avoided. (Traditionally, it has taken some period of usage before all the "bugs" are worked out of even the best commercial software packages.)	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.1.3.11	Programming shall be done in a commonly accepted high level language (e.g., FORTRAN or 'C') appropriate for the algorithms to be programmed. Assembly language shall be used only where sufficient performance cannot be achieved through use of a high level language or where it is justified based on other requirements of this chapter. In any event, the use of assembly language should be restricted to low level routines.	Use of a high level language facilitates review, testing, debugging, and modification of the software. This does not preclude the use of low level programming where performance requirements dictate it for a particular design (e.g., programming at the microprocessor level for a customized board), but this adds to the burden on the designer to properly test and document the software in accordance with the requirements of this section.	0
6.1.3.12	Machine specific programming dependencies shall be restricted to low level modular routines unless justified by performance requirements. M-MIS software shall be as machine independent as possible.	Restricting machine specific routines to low level functions supports transportability of software by reducing the reprogramming effort required to transport applications from one machine to another.	0
6.1.3.13	The M-MIS Designer shall provide a plan for providing support of all software, including application programs as well as compilers, operating systems, and other support software; the plan shall indicate the time periods over which such support will be provided.	The Owner must be provided with assurance that the vendor will support the software in the sense of fixing problems discovered after the plant is delivered, as well as supporting the Owner in making later changes for the purpose of improving or adding additional features.	0
6.1.3.14	The M-MIS functions of protection, control, alarm, and display shall be based on digital technology (instrument display formats and sensor signal conditioning exempted). This technology shall have the following characteristics:		0
	• Software shall be capable of being verified and validated.	• Prescription for robust software design.	0
	• The final source program shall be readable from start to end.	• This aids in the verification of the software.	0
	• The software design shall include self-supervision of control flow and data.	• Self-explanatory.	0
	• A single high level language shall be used throughout the entire system to the extent feasible.	• The use of a common software language minimizes the potential for errors.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Assembly languages should not be used for protection and control systems programs except in those cases where they are required in order to meet timing or hardware interface constraints.	• An assembly language code is difficult to verify.	0
	• A standard software structure shall be used in all processors which provide protection functions.	• The use of a common software language minimizes the potential for errors.	0
	• A continuous-loop, non-interruptible software structure is preferred.	• A continuous-loop, non-interruptible software structure is very deterministic.	0
	• The use of public or global variables (those known to more than one software module) shall be located in a common region and defined.	• The use of public or global variables scattered throughout makes it difficult to follow the software logic.	0
6.1.3.15	Comprehensive diagnostic routines shall be performed during initialization. The diagnostic routines shall have provisions to be bypassed during maintenance.	The computer and its peripherals are stressed following shutdown and power-up, and failures can occur. For this reason, automatic diagnostic testing should be conducted before the system is put in service.	0
6.1.3.16	Programs shall be developed as a set of program modules and linked together into an absolute code module to be installed into the processor memory.	There is less chance of errors occurring in the linking of programs if all of the programs are compiled and linked together.	0
6.1.3.17	Constants which are used to tune the system or parameters which can be changed for a specific set of plant conditions shall not be hardcoded into the code.	Operational parameters should be capable of being changed without having to recompile the source program, thereby permitting qualification of the basic code to remain intact when operational parameters are changed. Changes to operational parameter do not require qualification of the complete program, only verification of the inputs.	0
6.1.3.18	The software designer shall consider defining a summation widely used in other parts of the software as "utilities" which can be shared by several other software modules.	This simplifies the verification of the modules. In addition, the amount of code is reduced because sharing of logic can be realized.	0

Paragraph No.	Requirement	Rationale	Rev.
6.1.3.19	Steps shall be taken to protect against software additions ("viruses") which are designed to propagate in the software systems. Specific steps to limit the opportunity for insertion, such as physically limiting access to input devices and independent verification of the validity of input, shall be employed. In addition, frequent checks of the software by checksum techniques and, when necessary, bit-by-bit comparisons with secure copies of the software, or similar techniques will be used to limit unauthorized software additions.	The problem of preventing and curing a "virus" infection in software been recognized fairly recently. Countermeasures are developing rapidly but have not yet stabilized. It is therefore premature to specify detailed requirements.	0
6.1.3.20	**Data Base Management**	**Data Base Management**	0
	The M-MIS Designer shall provide the data base management tools needed to support the various functions described in this and other sections. The data base management shall provide:	The large amount of data in an ALWR requires organization to assure appropriate storage, dissemination and utilization of the data. Data base management as used here includes the transient data storage used by on line systems as well as long-term storage for a variety of purposes.	0
	• Storage and retrieval of the data in an organized, easily cataloged fashion using standardized and completely described formats.	• In order to be useful, well organized data bases are required with all the information needed to access and store the data readily available to users and potential users.	0
	• Sufficient redundancy and diversity of data storage so that a single event or failure cannot cause the loss of critical data. Critical data is any data needed to maintain plant power operation, maintain plant safety, permit plant maneuvering, or establish operating limits and margin.	• Some of the data is critical to continued plant operation, plant safety and plant maneuvering. The availability and integrity of such data must be preserved.	0
	• Provide appropriate time tags, data quality tags, and data identification tags.	• All of these elements are needed in order to fully utilize the data.	0
	• Utilities for extracting, storing, sorting and copying the data.	• Some general housekeeping utilities are needed for managing the data bases.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.3.20.1	**Storage and Retrieval**	**Storage and Retrieval**	0
	Various types of storage media and environments suitable for the date and use of the data shall be provided:	• Process data that is updated periodically must have fast access time and the integrity of the memory must be assured, the executable code must be protected, and information on the existence of updated data may be needed to assure adequate control and monitoring. Also, a failure to receive updated data is an indication of a fault.	0
	• Process control and monitoring data that is updated frequently shall be stored in memory,such as RAM, with a fast access time. The integrity of the memory shall be periodically checked, facilities shall be provided to prevent the data from overwriting executable code portions of the memory, and facilities shall be provided to indicate that the data has been updated.		
	• Data that is used to define the plant, define operator displays, or is infrequently changed shall be stored in a reliable, long term non-volatile storage media with sufficient data integrity checks and redundancy to assure that the MTBF for corruption of the data is greater than 60 years. The data shall not be corrupted due to power interruptions and shall be automatically acquired on power-up, if needed. When the same data is used in redundant safety related systems, the redundant systems shall acquire the data from different physical devices.	• Some data, such as coefficients that describe a plant (e.g., plant dimensions), operating data generated during initial start up testing (e.g., tuning parameters) display format and text, etc., is infrequently changed but must be loaded to the utilizing devices at power up or loaded in for defined conditions. The integrity of this data must be very high and redundant safety related devices must not used the same data base.	0
	• Data that defines the operating state of the plant, such as set points, shall be stored in a non-volatile media with sufficient redundancy and error checking to assure that the plant availability, reliability, and capacity factor are not significantly degraded. Changes in the data shall be placed in the non-volatile media within 0.1 seconds after the change is made. On power-up, the data shall be automatically loaded and consistency checks shall be made on the data to assure that it is compatible with the current state of the plant and equipment.	• Data that defines the state of the plant must be stored in non-volatile media so that the correct values are available on power restoration following a momentary loss of power. For extended power outages, the plant state may not be consistent with the set points.	0

Paragraph No.	Requirement	Rationale	Rev
	• Historical data that is used for post event evaluation, fuel calculations, maintenance history, equipment degradation monitoring, and similar applications, shall be stored on reliable, non-volatile storage media. The data shall include appropriate time and date tags. The data shall be stored in a fashion that will prevent damage to a small portion of the media - including portions that contain file directories - from causing a loss of the ability to retrieve other data from the media. Appropriate storage facilities shall be provided to prevent damage to the media or loss of data when the media is stored for the useful life of the data.	• Some data must be archived for a variety of purposes. Typical mass storage media such as tapes, disks, and compact disks (e.g., write once read many) provide adequate reliability. However, care must be used to prevent corruption of a small amount of data from causing a loss of the ability to retrieve the remaining valid data. Long term storage facilities to protect the media and its contents are needed.	0
	• The use of rotating storage of data shall be discouraged unless compelling reasons for its use is demonstrated. The M-MIS Designer shall be responsible for substantiating the application.	• The use of rotary buffers or equivalent can be misleading to the plant operators because data can be overwritten without his/her knowledge. Data can be lost when the operator is expecting the historical data to be available.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.4	**Performance Requirements**	**Performance Requirements**	0
6.1.4.1	The computer system shall be designed with a sufficient performance margin to perform as designed under conditions of maximum stress. Conditions of maximum stress include data scan, data communication, data processing, algorithms processing, analytical computation, control request servicing, display processing, operator request processing, and data storage and retrieval, as a minimum; however, they are not limited to these functions. In addition, the computer system shall be designed with reasonable expansion capability which would permit an Owner to add some functions in the future.	The central processing unit and peripherals should have enough capacity to perform their intended functions without skipping a function because there is insufficient idle time allotment. There should be a sufficient margin in capacity to permit the Owner to expand the system. It is good engineering practices to have approximately 40 percent idle capacity when the system is fully stressed.	0
6.1.4.2	The System or M-MIS Designer shall measure the performance of the system to demonstrate the excess capacity of the system.	This measurement generally is part of the factory acceptance test program.	0
6.1.4.3	The computer system shall have as much on-line diagnostics as practical to detect fatal failures. Failures shall be annunciated to the plant operating staff. All diagnostic errors shall be recorded on the on-line printer with date and time tags.	Diagnostic messages alert the plant staff the status of the equipment.	0
6.1.4.4	The computer system shall have the capability of performing periodic testing to check the status of the hardware as well as performing comparative measurement of the software for malfunction or unauthorized changes to the software.	This is a verification tool needed to detect any unauthorized changes or errors which the on-line diagnostic test was unable to detect.	0

Paragraph No.	Requirement	Rationale	Rev
6.1.5	**Verification, Testing, and Qualification**	**Verification, Testing, and Qualification**	0
6.1.5.1	The M-MIS Designer shall develop tools and techniques to be used to develop/operate the software system or used in software quality assurance functions to improve the quality and reliability of the software.	The following tools can be used to develop software or used in software QA:	0
		• Interrupt analyzers;	0
		• Debuggers;	0
		• Data base analyzers;	0
		• Language processors;	0
		• Dynamic simulators;	0
		• Text editors;	0
		• Requirements tracers;	0
		• Decision tables;	0
		• Hardware monitors;	0
		• Structural test analyzers;	0
		• Logic analyzers;	0
		• Library handlers;	0
		• Cross reference generators;	0
		• Test drivers;	0
		• Timing analyzers;	0
		• Source comparitors;	0
		• Instruction tracers;	0

Paragraph No.	Requirement	Rationale	Rev.
		• Editors;	0
		• Dynamic analyzers;	0
		• Consistency checkers;	0
		• Test beds;	0
		• Standards analyzers;	0
		• Test result processors;	0
		• Flow charters;	0
		• Interface checkers;	0
		• Automated test generators;	0
		• Static analyzers;	0
		• Software monitors;	0
		• Management information systems.	0
6.1.5.2	The design, development, testing, and documentation of tools and techniques shall entail the same rigor and level of detail as other deliverable software.	This is to ensure that the quality level of the control or monitoring software/hardware is not degraded by using unqualified tools.	0
6.1.5.3	Tools and techniques shall be placed under configuration management control, and maintenance and documentation shall be required.	Quality of the product must be preserved.	0
6.1.5.4	Tools shall be coded in high level languages so that portability from one computer to another does not entail major rework—unless, due to the nature of the test, a lower level language is required to achieve the specific test objective.	As with the computer hardware, large investments can be made in software tools; therefore, the tools, as well as the application software, should be portable.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.5.5	The test program shall utilize both human-based testing (e.g.,source code walk-through team audits) and computer-based testing.	Software quality assurance relies heavily on the verification process. Source code walk-throughs, design reviews, etc. are essential parts of designing quality into the product.	0
6.1.5.6	The test program shall be designed and carried out, first, with the objective of finding programming errors and, second, with the intent to validate that the software performs correctly. Changes to the software shall be handled in accordance with the software configuration management program.	The classical testing of hardware is to test the system, equipment, or component in accordance with the design basis which is less than its failure point. Software differs from hardware because failures can occur both within the design basis as well as beyond the design basis. Both conditions must be tested. It is impractical to test all of the combination of conditions which can occur; hopefully, a reasonable amount of testing is conducted to provide a sufficient degree of confidence that the software is correct.	0
6.1.5.7	The individual or group responsible for development of the software to be tested shall not perform the testing of that software.	It has been found that verification and validation performed by an independent group or individual, not responsible for the development of the software, was more objective. Independence is essential for a quality product.	0
6.1.5.8	For each test, the expected results shall be predefined in order to avoid interpreting errors as correct results (e.g., the program executes successfully but the results or output data are incorrect).	The NRC also provides general guidance for developing and testing safety-related software in Regulatory Guide 1.152, which endorses ANSI/IEEE Std ANS-7.4.3.2. These documents emphasize an orderly, structured, development approach and the use of verification and validation to confirm the design. Independent verification must follow the quality assurance requirements of 10CFR50, Appendix B. An independent team of verifiers shall perform the checking process; the individuals must be other than those who performed the original design. Validation must verify a predictable and safe response to abnormal as well as normal test cases. NUREG/CR-4640 is another source of NRC guidelines for software development.	0

Paragraph No.	Requirement	Rationale	Rev
6.1.5.9	The testability, calibration, and bypass requirements of IEEE-279 shall be supported in a software-based design. Periodic testing shall exercise the hardware and software sufficiently to confirm operability of the system. Some level of continuous test capability (such as monitoring watchdog timers) should raside in the software to verify computer operation. The M-MIS Designer shall be responsible for identifying total errors and for designing continuous tests to detect the errors, to the extent practical.	Testability, calibration, and bypass requirements are dependent upon the software and hardware design. The M-MIS Designer must specify the requirements for the utility/owners to review and evaluate.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.1.6	**Availability and Reliability**	**Availability and Reliability**	0
6.1.6.1	Verification and validation shall be planned and shall include systematic quality assurance activities.	Verification provides assurance that the design is proceeding correctly from one stage to another, while validation assures that the design specifications for both hardware and software are necessary to provide confidence that the software and the associated hardware meet the functional requirements and will perform satisfactorily in normal service.	0
6.1.6.2	The M-MIS Designer shall evaluate the diversity and redundancy requirements of each computer-based system and specify the degree of redundancy and diversity it shall have. The M-MIS Designer shall consider the need for a hardwired backup system to the computer-based system, thereby eliminating the need for diversity in the software. Design requirements and validation testing acceptance criteria of the diverse approaches shall be the same.	There is a concern that software-based safety systems may contain subtle failure modes that occur only under an obscure set of conditions. These conditions may include environmental factors as well as internal hardware or software failures. If these conditions were not considered during software and testing, then safety-critical signal functions might be affected at some unpredictable future time. If the software failures were random, a multi-division safety system might be expected to provide the required redundancy to back up such failures; however, if standardized software is used to perform similar functions in similar computer hardware installed throughout the system, then common-mode failures could degrade overall safety system operation. This concern may require various forms of hardware and software diversity to be incorporated into the composite nuclear system design. A possible acceptable means of diversifying software is to use two different program languages and different programmers. Validation testing would be conducted against the same design requirement documents.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.1.6.3	A reliability evaluation shall be required to provide assurance that the final system design, including all modules, performs together with the hardware in accordance with system requirements. Software change procedures following installation shall require a rigorous set of review, testing, and qualification requirements before modifications can be approved. Software security, reliability, and maintenance are issues important to safety-related systems. The design shall incorporate software and hardware interlocks to prevent unauthorized tampering with the computer codes, which may not be readily detectable. Software reliability shall follow a modular approach for developing an independent and cohesive code that performs only its prescribed task.	Quality must be designed into the system. Upon completing design, validation testing against the design specification is essential to reliability.	0
6.1.6.4	The level of security protection shall be established in accordance with the application. Prevention of unauthorized tampering with the code, which may not be readily detectable in software, shall be incorporated in the design by hardware or software, or both. As a minimum, there shall be two levels of protection for plant operators, software engineers, and authorized software engineers.	It is important the unauthorized or inadvertent changes to software and data be prevented. Inadvertent or unauthorized software changes have led to failure and corruption of data.	0

Paragraph No.	Requirement	Rationale	Rev
6.1.6.5	Software-based safety systems shall satisfy basic nuclear plant design principles, such as defense-in-depth, redundancy, separation, independence, and diversity. The means of conforming to these principles shall be carefully examined, since the associated hardware shall also meet all design principles, but with inherently different failure modes.	The NRC has been concerned that existing regulatory criteria do not address the special design requirements of stored-program computers. Safety system hardware design has followed IEEE Std 603 for implementing functional and design criteria. Following a review of an integrated protection system, the NRC produced NUREG-0493, which imposed standard evaluation procedures on this safety system design, which uses software to perform safety system functions. NUREG-0493 provides guidelines for performing a defense-in-depth analysis, separation, independence, and stressed. A procedure is presented for postulating common-mode failures for the worst case among similar hardware and software components and analyzing the effects on safety-critical inputs and outputs.	0
		The use of extensive diversity to mitigate the effects of common-mode failures may be avoided by carefully allocating diverse system input signals and processing functions to software modules distributed among separated processing hardware. If the modules are simple enough, they can be validated with great confidence. The separated hardware demonstrates independence among systems.	0
6.1.7	**Maintainability and Serviceability**	**Maintainability and Serviceability**	0
6.1.7.1	The M-MIS Designer shall pass on the computer and peripheral equipment manuals provided by the vendor.	The Owner is the end user of the equipment and must maintain the system.	0
6.1.7.2	The M-MIS Designer shall provide all the required documentation (manuals and drawings), diagnostic tools, calibration tools, development stations, etc. required to maintain and modify the system.	The Owner is the end user of the equipment and must maintain the system.	0

Paragraph No.	Requirement	Rev.
6.2	COMMON HARDWARE REQUIREMENTS	0
6.2.1	**Definition**	0
6.2.1.1	**Purpose**	0
	The purpose of this subsection is to define common requirements for design, selection and installation of specific M-MIS hardware. This subsection does not repeat any requirements specified in Chapter 1 or other sections of this chapter, but complements those requirements by specific requirements.	0
6.2.1.2	**Scope**	0
	The requirements in this subsection apply to all M-MIS hardware and have been organized as follows:	0
	• General requirements.	0
	• Requirements for design and selection of specific M-MIS hardware for the following components:	0
	– Computer Systems;	0
	– Switches;	0
	– Sensors;	0
	– Isolation devices.	0
	• Valve requirements for design and selection of specific valve control and instrumentation features and requirements for valve operational surveillance.	0
	• Instrumentation and control (I&C) power supply requirements for conditioning of power supplies to M-MIS instrumentation.	0
	• Grounding requirements applicable to M-MIS equipment.	0
	• I&C penetrations and seals.	0
	• M-MIS equipment cables, fiber optics, and raceway requirements for design, selection, and installation.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.2	**General**	**General**	0
6.2.2.1	The control system shall meet the common systems and equipment requirements specified in Section 7.	Requirements are common to all sections which specify control functions.	0
6.2.2.2	The control system design shall be integrated with the reactor systems control (Section 7) to provide for smooth overall plant control to meet all design basis conditions.	Strong interactions between reactor and power generation control require an overall integ ated approach (i.e., use of an overall plant dynamic model fo system analyses).	0
6.2.2.3	The control system monitoring function shall provide the operator sufficient information on systems and equipment operation to monitor performance trends and take appropriate action in the event of system and/or equipment misoperation or malfunction.	Up-to-date information on system process parameters and equipment status and condition is essential for the operator to take corrective action in a timely fashion.	0
6.2.2.4	The system control design shall be integrated with the power generation control to provide for smooth overall plant control to meet all design basis conditions.	Strong interactions between reactor and power generation control require an overall integrated approach (i.e. use of an overall plant dynamic model for system analyses).	0
	The margins, as specified in Chapter 4, will be maintained for all design basis conditions.	Chapter 4 states that a minimum 15 percent margin shall be maintained.	0
6.2.2.5	All I&C required for operation shall "self-start" without human interaction upon reinstatement of power. Pumps, motors, valves, support systems and safety systems should not be automatically restarted or inappropriately initiated without the operator's action or authorization.	Microprocessor and computer-based systems should be self-starting; however, the actions to be taken require operator action or authorization.	0
6.2.2.6	Free-standing or wall-mounted instrument racks shall be provided for mounting process sensors, process signal transmitters, solenoid valves, when applicable, and associated wiring whenever possible to facilitate maintenance and testing of this type of equipment. All instrument tubing and electrical wiring on instrument racks shall be procured along with the rack.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.2.7	All rack electrical wiring requiring external connections shall be brought to a rack mounted terminal box or connector supplied by the vendor.	This requirement provides a convenient location for troubleshooting and maintenance.	0
6.2.2.8	Process instrument sensing lines shall not be run an excessive distance, thereby affecting the accuracy, response and sensitivity of the measured parameter.	Generally, they shall be run not more than 100 feet to minimize the degradation in response time of the instrument.	0
6.2.2.9	The instrumentation and control equipment and components shall be protected from potential hazards by their design, location, and the use of protective barriers or enclosures. The Plant Designer shall demonstrate that this equipment is protected against potential hazards by performing hazard analyses.	Potential hazards include, for example, failure of other equipment (e.g., transformers, seals, pressurized pipes and vessels), equipment and personnel associated with nearby maintenance activities, fire and flooding. The instrumentation and control equipment is compact and relatively vulnerable to hazards. Therefore, this equipment must be located to minimize damage from hazards and protected as required to ensure its availability.	0
6.2.2.10	Instrument ranges shall always cover the range of the variable over which the system utilizing the information is operable with reasonable margins. The established range shall consider the normal, transient, and accident operating conditions. The M-MIS Designer shall be responsible for establishing the margins.	Experience shows that improper specifications of instrument ranges has led to increased delays and costs due to field changes and retrofits. The design basis shall be available for review by the plant owner. An example of inadequate design specification is the requirement of Regulatory Guide 1.97 instrumentation.	0
6.2.2.11	Normal operating conditions shall be maintained at the midscale of the instrument range as much as possible when the instrument scale is uniform. Use of the lower and upper ranges should be avoided, where possible.	This is good practice in order to obtain the optimum readout of the displayed information.	0
6.2.2.12	All analog signals shall be either current inputs or differential voltage. Single-ended voltage (zero base systems) signals shall not be used unless there is a compelling reason to do so.	Reduces the potential for ground loops and other noise problems. Use of instruments which include zero in the span of the reading is discouraged because signal quality cannot be tested. Downscale failure cannot be distinguished from a true zero reading.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.2.13	Set point drift in instruments shall not cause violation of technical specification limits.	[The EPRI Contractor shall review the Draft Regulatory Guide and Value/Impact Statement, Task IC 010-5, "Proposed Revision 2 to Regulatory Guide 1.105, U.S. NRC 12/81" and NUREG-0993, pages 3.3-1 and 3.3-2, and ISA 67.15 recommended practice for set points and set point drift in instrumentation.]	0
6.2.2.14	All equipment and devices shall be inherently free from electromagnetic interference or shall be installed with appropriate shielding and isolation to reduce susceptibility to acceptable levels. The broadcasting of EMI shall be minimized.	EMI can affect the signal to produce erroneous inputs.	0
6.2.2.15	M-MIS equipment design, materials, and construction shall be chosen to reduce the potential for electrostatic discharge per DOD-HDBK-263, *Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies and Equipment.*	Electrostatic discharge is a major problem for digital equipment. Design requirements are needed to ensure the problem is adequately addressed.	0
6.2.2.16	M-MIS equipment outside containment shall be designed to operate between 40°F and 120°F. I&C equipment shall operate with 10 to 95 percent (non-condensing) humidity and 95°F maximum wet bulb temperature. Operation between 60°F and 105°F shall be used for reliability and availability assessment. M-MIS equipment in the control room is specified in Section 4. The HVAC (Section 9) servicing the equipment areas shall be designed to provide the required environmental control to assure the equipment conditions are maintained during all plant operation.	These are nominal values for M-MIS equipment. A requirement has been placed on the HVAC system to provide a normal environment of 60°F to 105°F and 10 to 95 percent (non-condensing) humidity and 95°F maximum wet bulb temperature. The M-MIS equipment needs to be designed to operate within the indicated limits to insure its functionality under favorable as well as all defined adverse conditions.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.2.17	The M-MIS equipment shall be capable of operating within performance limits when exposed to the expected variations of input voltage and frequency, including the margins of IEEE-323-1974. Use of power conditioners is an acceptable method of filtering the input voltage and frequency so that the equipment can perform over its design range. The M-MIS Designer shall evaluate the requirements for power conditioners.	The equipment may be commercially available equipment which cannot withstand the conditions specified for plant design. It will be the M-MIS Designer's decision either to provide equipment that will withstand the plant condition or provide equipment to limit the input to the commercially available equipment.	0
6.2.2.18	The M-MIS Designer shall provide features in the M-MIS design to protect the system against failure resulting from transients, sags, surges, and noise inputs (such as EMI) which may occur on the power input cabling from the external power system. M-MIS equipment shall withstand electrical surge (field wiring and power feeds) per IEEE-472-1974.	This is required in order for I&C equipment to function correctly during adverse conditions such as electrical storms and switchgear-induced electrical transients. This requirement enhances availability.	0
6.2.2.19	The design of the M-MIS equipment shall minimize the requirements placed on support systems such as power supplies and HVAC.	The M-MIS Designer should consider solid-state devices which require low power and minimum heat dissipation. This minimizes the power requirements as well as HVAC loads. The required amount of M-MIS equipment, such as video, workstations, printers, etc., shall be kept to a minimum.	0
6.2.2.20	Those control and instrument devices for which it is not practical to achieve a 60-year design life shall be identified by the M-MIS Designer, and provision shall be made for their replacement or repair, as appropriate, to achieve the overall plant availability and design life.	Refer to the rationale provided in Chapter 1.	0
6.2.2.21	Large and important control and instrumentation systems shall be pre-assembled to the maximum extent practical and tested in their final configuration. Testing shall include debugging and verification of performance requirements.	Integrated system testing and validation is required to ensure system reliability. This testing must be exhaustive and, therefore, it must be well planned.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.2.22	Hazardous areas, such as high voltage areas, shall be labeled and shielded in accordance to the Federal, State and Local electrical codes.	Protection of personnel is required by Federal, State, and Local safety codes.	0
6.2.2.23	If the M-MIS Designer uses circuit cards or modules in the design, the circuit cards and modules shall be replaceable during channel bypass without affecting system safety or reliability.	The maintenance features must help ensure that availability goals are met.	0
6.2.2.24	Signal validation shall be performed on all critical safety, control, and plant availability systems. The complexity of the signal validation shall be in accordance to the critical functions the signal serves. Simpler cost-effective validation techniques can and should be used for non-critical systems. The M-MIS Designer shall establish the level of complexity of signal validation to be used for each application.	Signal validation is a process by which signals are checked for accuracy, ensuring that the operator or process using this signal can achieve its goals and functions. Some of the rudimentary techniques being used today are: • Limit checking; • Auctioneering; • Instrument-loop-integrity checking; • Like sensor comparisons and calibration checking.	0
		New more complex methods of signal validation have been and are being developed. These include parity-space representation and analytic redundancy. Signal validation can be used to achieve highly reliable automatic control systems.	0
6.2.2.25	All I&C equipment shall have design provisions to perform diagnostics and troubleshooting down to the circuit board or module level.	This minimizes repair time so that system availability is not impacted.	0
6.2.2.26	The M-MIS Designer shall include provisions for testing circuit cards or modules while they are in the chassis. Extender boards, test points, or other suitable means shall be provided to permit diagnostics and testing.	Test and diagnostic provisions minimize system downtime.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.2.27	Standard three-connector 110VAC service power outlets shall be provided within cabinets, bays, and other equipment locations to facilitate maintenance activities in non-safety cabinets. For safety-related cabinets, service power outlets shall be provided close by. The M-MIS Designer shall consider personnel safety, impairment of plant operations, mobility, electromagnetic interference effects, and other hazards to operation when specifying the location. These service outlets facilitate the use of auxiliary lights and electrically powered equipment to perform the maintenance.	Convenient service outlets should be provided for maintenance activities; otherwise, extension cords would be used which can cause personnel safety hazards.	0
6.2.2.28	Permanent internal lighting shall be installed in cabinets to facilitate maintenance. In order to preclude the potential for leaving the service light on, the light shall be designed to be turned off when the cabinet is secured or, in the alternative, the cabinet shall not be secured until the light is extinguished.	Plant personnel have used flashlights and drop lights to maintain and service equipment within the cabinet. This practice results in a safety hazard to personnel and increased chance of disturbance to the equipment.	0
6.2.2.29	The instrumentation and control equipment and components shall be protected from nearby hazards. The Plant Designer shall perform hazard analysis to demonstrate that the instrumentation and control equipment design, location of the equipment and protective enclosure have considered the safeguards against consequences of nearby hazards.	Nearby hazards include transformers in the next room (potential fire hazard beneath bottom entry cables for the I&C cabinets), steam lines on the other side of the wall (potential impact, steam leak, etc. hazards). These types of hazards can be reduced or avoided by careful location of room containing the I&C equipment.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.3	**Computer Systems**	**Computer systems**	0
6.2.3.1	The different types of hardware and software used throughout the plant shall be standardized as much as practical.	This requirement supports the goal of standardization throughout the plant.	0
6.2.3.2	The M-MIS Designer shall specify the design life of the computer system and its peripheral equipment. Provisions shall be made to facilitate replacement of obsolete equipment.	The design life of the computer system is considerably shorter than the plant design life, and availability of spare parts from the manufacturer is a limiting factor. Therefore, a space and enclosure envelope sufficient to accommodate the replacement equipment must be provided. M-MIS Designer must make some assumptions to establish the envelope.	0
6.2.3.3	All equipment, including commercially purchased computer and peripheral equipment, shall meet the configuration management control requirements of Chapter 1. Configuration management control at the equipment, subassembly, and board level shall be required to maintain service contracts conditions.	The configuration and architecture of computer and peripheral equipment must be maintained by the Plant Designer if the service contract is to remain in effect. Changes and modifications to the system configuration, equipment, or boards can invalidate service contracts. For this reason, strict configuration control of the key equipment and subassemblies is required.	0
6.2.3.4	System testing and validation shall be performed with both software and hardware totally integrated.	The software and hardware interaction must be tested. Validation testing must demonstrate the integrated system performance as designed.	0
6.2.3.5	Comprehensive integrated testing and validation is required to ensure that interactive tasks are tested. All validation and testing shall be documented and retained for historical records.	The interaction of software and hardware must be tested to ensure that the software is robust and correct and that the hardware is able to respond to the operator's requests. This provides a benchmark measurement of the system which can be used for comparison if modificaitons are made to the system.	0
6.2.3.6	The M-MIS Designer shall evaluate and establish the need for redundancy and diversity of computer and peripheral hardware.	The M-MIS Designer can perform a reliability analysis of the equipment and establish the need for redundancy and diversity. Diversity may not be practical because standardization and diversity are sometimes mutually exclusive.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.3.7	All developmental, diagnostic, maintenance, and servicing hardware shall be provided to the Owner along with instructions for, documentation of, and training in its use. All of the equipment specified above shall be demonstrated to be identical to the suppliers' equipment which is used in development, verification, and testing.	The Owner shall have the capability to perform or obtain assistance in performing modifications, adding new functions, troubleshooting, and maintaining the delivered systems.	0
6.2.3.8	All software and hardware licences and warrantees from the computer or peripheral equipment manufacturer shall be passed on to the Owner.	These updates and services are part of the system purchased from the manufacturer, which is required to maintain and service the system. Therefore, they should be delivered as part of the system.	0
6.2.3.9	All equipment documentation and training credits from the computer or peripheral equipment manufacturer shall be passed on to the Owner.	These documents and training are part of the system purchased from the manufacturer, which is required to maintain and service the system. Therefore, they should be delivered as part of the system.	0
6.2.3.10	All computer-based systems required for operation shall have a battery-backed calendar clock.	In the event of a power interrupt, the clock time and calendar is preserved. Otherwise, the operator must input data to establish the correct time and date.	0
6.2.3.11	Maintenance and replacement of an auctioneered power supply system shall not disrupt operation of the system.	Assures minimization of system downtime.	0

Paragraph No.	Requirement	Rationale	Rev.
6.2.4	**Switches**	**Switches**	0
	The requirements specified in this subsection are applicable to, but not limited to the following types of switches:		0
	• Proximity;		0
	• Contact;		0
	• Level;		0
	• Pressure;		0
	• Position.		0
6.2.4.1	The M-MIS Designer shall specify the accuracy and repeatability requirements for each type of switch in accordance to its application and operation.	Self-explanatory.	0
6.2.4.2	The M-MIS Designer should encourage the use of integrated logic for switches to simplify M-MIS operator information. If integrated logic is used, the designer shall make provisions for the readout of individual switch positions in addition to the logic output.	The added information may be helpful to diagnose problems in the event of equipment failures.	0
6.2.4.3	The M-MIS Designer shall determine whether a "wet" or "dry contact shall be used in accordance with its application.	The type of contact would depend on whether high current would be experienced in the design application.	0
6.2.4.4	The M-MIS Designer shall specify the design life cycle and qualified life (margin for qualification) for each type of switch in accordance with its application and operation. The switches shall be qualified for the qualified life cycle, accuracy and repeatability.	Self-explanatory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.4.5	The M-MIS Designer shall consider intelligent logic design to detect failure of switches. Software algorithm (local microprocessor or central processor logic) or hardware logic are acceptable methods for performing the logic.	Equipment failure detection and alarming improves the equipment reliability.	0
6.2.4.6	All switches shall have provision for testing their performance. Test equipment connection and output signal provisions shall be provided by the M-MIS Designer.	Switches shall be required to be tested periodically; therefore, provision for testing is required to service the equipment.	0
6.2.4.7	Switches shall be of modular design to enable separate replacement.	Modular design permits replacement of the switch and replacement of the logic module with minimal disturbance to the system.	0
6.2.4.8	Switches shall be designed to permit position adjustment, if required.	Self-explanatory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.5	**Sensors**	**Sensors**	0
	The requirements specified in this subsection are applicable to, but not limited to the following types of sensors:		0
	• Temperature;		0
	• Pressure;		0
	• Acoustic;		0
	• Optical;		0
	• Vibration;		0
	• Flow;		0
	• Neutron;		0
	• Radiation;		0
	• Level;		0
	• Current;		0
	• Voltage.		

Paragraph No.	Requirement	Rationale	Rev
6.2.5.1	Reactor coolant system temperature sensors shall utilize ASME Code thermowells welded into the piping or temperature probes (or RTDs) strapped to the piping. Where temperature sensors are strapped to piping, insulation may be required to obtain accurate measurement and desirable response time. Direct immersion temperature sensors shall not be utilized. The temperature probe (or RTD) and thermowell combination shall be designed to allow easy removal and insertion, while minimizing response times. The plant control and protection systems shall be designed to accept the slower response time which is expected for temperature probe/thermowell combinations.	Use of thermowells facilitates replacement of temperature sensors without requiring that the reactor coolant system be drained. However, the plant control and protection system must be designed to accept the response time of the temperature sensor/thermowell combination. It is not the intent to require close-fitting temperature sensors with gold plating in order to minimize response times.	0
6.2.5.2	The M-MIS Designer shall select the temperature measuring device in accordance with its application, characteristics, and service. The M-MIS Designer shall be responsible to demonstrate that the selected device meets these requirements.	RTD and IR devices, etc. are standard devices presently used in industry. This does not preclude the M-MIS Designer using other devices, such as fiber optic sensors if he chooses as long as the requirements are met.	0
6.2.5.3	For temperature measurements in locations where temperature stratification may result in measurement uncertainty, a sufficient number of thermowells shall be provided and located to reduce measurement uncertainty to an acceptable level. The specific orientation of the thermowells shall be identified. In addition, an appropriate method of combining the temperature measurements shall be defined by the M-MIS Designer.	Two or more thermowells have been required to avoid thermal stratification problems in the hot leg of some PWRs.	0
6.2.5.4	The M-MIS Designer shall specify the accuracy and repeatability requirements of sensors in accordance with their application, design, and operation.	Self-explanatory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.5.5	The M-MIS Designer shall specify the calibration accuracy requirements for the sensors.	Review of current plant calibration history indicates there is an over-correction in calibration. There have been observations that the same sensor, from calibration to calibration, oscillated about the "true" value. This was caused by insufficient sensitivity in the calibration to preclude over-correction.	0
6.2.5.6	Flow nozzles, averaging pitot tubes, and vortex shedding may be used as required. If remote indication or recording is required, linear scales or charts shall be used.	These devices have signal output capability.	0
6.2.5.7	The M-MIS Designer shall consider the use of temperature measuring devices other than thermocouples or RTDs. Integrated circuit temperature devices are available with current outputs that do not require any reference junctions and provide voltage or milliamp outputs which can be used directly with data acquisition systems.	Traditionally, there have been numerous problems with reference junctions which are required with thermocouples and RTDs. These problems can be minimized by using ICTDs. In addition, ICTDs do not require any signal conditioners.	0
6.2.5.8	All sensors shall be qualified for the full range of operation, including normal, transient and abnormal operation. If it is not practical to perform qualification tests, the M-MIS Designer shall demonstrate by analysis the qualification of the sensors.	Qualification testing is the most desirable method of qualification. The M-MIS Designer can choose to perform by analysis; however, the M-MIS Designer is responsible for qualifying the sensor. A finite amount of risk is associated with the analysis approach.	0
6.2.5.9	All sensors shall have provisions for test equipment to receive a direct output to facilitate performing calibration using a microprocessor based system.	A direct output reading would reduce potential errors in handling the calibration data. In addition, it would expedite the calibration procedures to obtain direct data without having to hand record data.	0
6.2.5.10	The M-MIS Designer shall provide means to minimize improper arrangement of sensor isolation valves or leaving the valves in the incorrect position following calibration.	There have been numerous field reports of improper valve alignment and incorrect positions. It has been proven that procedures alone are not sufficient; design provisions must be considered.	0
6.2.5.11	If the sensor requires local logic, the logic module shall be replaceable without having to replace the complete sensor.	Self-explanatory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.5.12	All sensors shall have provisions to perform bench calibration as well as field calibration. They shall have direct output provisions to perform testing and diagnostics.	Self-explanatory.	0
6.2.5.13	Sensors shall have no undetectable failure mode.	Failures must be detectable to allow the plant staff to take mitigating action on the basis of present information.	0
6.2.5.14	Diversity shall include principle of operation as well as function.	To minimize common mode failures.	0
6.2.6	**Isolation Devices**	**Isolation Devices**	0
6.2.6.1	The engineered safety signal isolation devices shall provide Class 1E to non-Class 1E digital and analog signal isolation while maintaining Class 1E integrity in accordance with Regulatory Guide 1.75.	This requirement is based on regulatory requirements for electrical separation and successful experience.	0
6.2.6.2	Fiber optic cable is an acceptable isolator. Fiber optic isolation between multiplexers and other data acquisition equipment is an acceptable design.	It would be good engineering practice to provide isolation between multiplexers and other data acquisition equipment.	0
6.2.6.3	The M-MIS Designer shall select the type of isolators to be used in accordance with the design application and environmental requirements. Optically-coupled, transformer-coupled, or other suitable types, such as solid-state isolators, are acceptable types. The M-MIS Designer shall be responsible for demonstrating that the isolation device chosen for an application meets the input voltage protection requirements. Hot starts in the power distribution and interconnects on wire runs shall be considered.	The M-MIS Designer is responsible to demonstrate that input voltage protection considers hot shorts.	0
6.2.6.4	Use of analog isolators shall not degrade the accuracy of the safety-related portion of the instrument loop below that required for the safety analysis.	Self-explanatory.	0
6.2.6.5	Analog isolators' linearity and stability shall not decrease significantly as a function of time and temperature.	This requirement ensures high quality against long-term degradation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.6.6	**Ground Protection**	**Ground Protection**	0
	The M-MIS Designer shall select the type of isolator to be used for common mode rejection in accordance with its application. The M-MIS Designer shall demonstrate that the device selected meets the requirements for its application. As a minimum, the device shall provide 80 dB common mode rejection.	Required to minimize the ground loop noise.	0
6.2.7	**Valves (I&C Features)**	**Valves (I&C) Features**	0
6.2.7.1	Motor operated valves shall have the valve operational logic module separate from the position indicator module.	Separation of the logic and position indication modules permits replacement of one without the other.	0
6.2.7.2	If practical, all logic and position indication modules shall be interchangeable with all motor operated valves.	This requirement standardizes the stocking of spare parts and inventory control.	0
6.2.7.3	Valve operators shall have the following characteristics:		0
	• For motor operated valves, valve close and valve open positions shall be detected. The valves shall be protected against mechanical overload during full open or full close operation. The M-MIS Designer shall specify the type, accuracy, and repeatability, the number of indicators, etc. required for design in order to meet the reliability, serviceability, and maintainability requirements.	• An acceptable design is two torque switches, one in the open and one in the close valve position. The open torque switch provides protection against mechanical overload during opening operation. The closing torque switch provides protection against mechanical overload during the closing operation.	0
	• Air operated valves in safety-related systems shall always be fail-safe with respect to loss of air supply or control signal.	• Air operated modulating valves should also fail safe on loss of air supply or control signal; however, the valve should be provided with timed steps if a full open position causes excessive flow. Valves that fail as-is should be provided with motor operators.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• If functional task analyses show that intermediate valve position indication is required, four sets of geared limit switches (or other acceptable devices), each having four independent contacts, shall be incorporated. Two sets shall be factory adjusted, one for close and one for open; and two sets shall be field adjustable to operate at any position between the limits of valve travel (except valves for special application, e.g., floor valves).		0
	• Class 1E motor operated valves shall have their thermal overloads bypassed continually per Regulatory Guide 1.106. The only time the overload bypass shall be removed is during maintenance and testing of the valves.	• Self-explanatory.	0
	• All non-modulating valves used as shut-off or bypass valves shall have their control circuits designed to prevent reversal of the valve at any intermediate valve position unless the valve operator is de-energized in an intermediate position due to loss of power or operation of a torque switch. An exception to this criterion would be the situation where the valve opening is limited to 10 or 20 percent travel to limit water hammer during pump starting or pump loading, as specified by the M-MIS engineer. Safety-related valve control circuits shall be designed to ensure that the safety-related automatic signal overrides all other process control signals.	• Erroneous valve control cannot be tolerated. A valve shall continue in the direction it has been commanded without reversing.	0
	• The use of non-modulating type valves which may require the capability to reverse direction in mid-stroke shall be discouraged. The Plant Designer shall justify the need for such valves and take appropriate safety precautions to prevent inadvertent override of the valve during mid stroke.	• The main feedwater block valves in current plant designs have long stroke times. If the valve inadvertently or erroneously receives a close signal, the steam generator could boil dry before the valve is reopened. Such designs should be avoided if possible.	0

Paragraph No.	Requirement	Rationale	Rev
	• Where an air operated valve is required to move from its position after a loss of air supply, the valve shall be supplied with an air accumulator. The air accumulator shall be sized with sufficient capacity to permit moving the valve over the required range. The design shall preclude the division of the accumulator air preventing the moving of the valve during a loss of air supply event. Air accumulators are only needed if continued cycling or modulation after loss of air is required.	• The design needs to ensure that valves are moved to their required position despite loss of air.	0
	• Solenoids for pneumatic valves located in inerted or high radiation cells shall be located external to the cell to allow accessibility for service and maintenance.	• Self explanatory.	0
	• Air operated valves, whether of a modulating or non-modulating type, shall be provided with limit switches and a local terminal box. In the case of non-modulating AOVs, the solenoid valve shall also be wired to the local terminal box unless the solenoid valve is rack mounted.	• Local position indication is necessary for plant operation and maintenance.	0
	• The position limit switches for an air operated valve shall be of the double pole, double throw type or of other acceptable types.	• NAMCO Type EA170 is an example of an acceptable limit switch.	0
	• If valve position indication is required, the solenoid valve shall be provided with integral reed type position switches or other acceptable devices.	• These types of position switches have been demonstrated to be reliable.	0

Paragraph No.	Requirement	Rationale	Rev
	• For open loop fluid systems, the pump discharge valve shall be interlocked with the pump to prevent pump runout. The valve sequencing with the pump start and stop is an acceptable means of controlling the pump runout. The valve position indication shall be obtained directly from the valve shaft (stem) not from the control loop signal or pilot valve. This requirement is not needed if mechanical means such as cavitating venturis to prevent pump runout are provided.	• Good design practice to protect the equipment from damage.	0
	• The control and motive power for all electrically operated valve shall be supplied from the same Class 1E division for Class 1E loads. The electrically operated valves shall be supplied from the same non-class 1E system for non-class 1E loads.	• The failure mode for this event is unanalyzable. If power is supplied by several sources, the consequences of power failure can be complex.	0
	• Contact pairs that have a common wiper shall not be used in circuits of different phase, type, or voltage level.	• Certain considerations must be given when assigning contact usage to avoid contact arcing problems. To avoid contact arcing, either contacts from the other contact pair or an auxiliary relay should be used. To ensure that polarity is observed, the terminals that are suffixed with "C" shall always be connected to the "phase" side of an ac circuit and the "positive" side of a dc circuit.	0
6.2.7.6	All operated valves shall have local position indication provisions. All manually operated valves, if the application requires, shall have security locking devices.	This requirements allows plant personnel to visually verify the valve position. Local or remote control is permissible.	0
6.2.7.7	All valve designs shall have provisions for detecting external and internal leakage. External leakage shall be detected while the plant is operational. Internal leakage can be detected in-place and/or at the shop.	Self-explanatory.	0
6.2.7.8	Diagnostic, calibration, and any special tools required for troubleshooting shall be provided to the Owner.	Required to maintain and service the valves.	0

Paragraph No.	Requirement	Rationale	Rev
6.2.7.9	On loss of motive power, valves associated with reactor plant fluid system controls shall fail in a position such that the plant safety system is not challenged. Consideration should also be given to post-accident recovery actions required of the valve. If the plant safety system is not challenged and a specific valve position is not required by post-accident recovery actions, actuation devices shall fail in a position such as to allow the plant to remain at power and remain controllable.	If safety considerations do not require a specific failure mode, consideration should be given to a failure mode that allows the plant to remain at power.	0
6.2.8	**I&C Power Supplies**	**I&C Power Supplies**	0
6.2.8.1	The M-MIS equipment shall be capable of operating within performance limits when exposed to the expected variations of input voltage and frequency, including the margins of IEEE 323-1974.	Many of the power supplies can be powered from inverters or diesel generators so their input voltage and frequency may vary over a larger range. The M-MIS power supplies must operate properly over the expected variations.	0
6.2.8.2	The M-MIS shall be designed to operate within performance limits when the dc input is at the level required to charge the batteries. Low dc voltage when batteries are fully loaded and charge is depleted. The battery charging level shall not cause damage to equipment connected to this dc source.	The battery charging voltage will be higher than the nominal battery voltage while the battery voltage will be lower than nominal when the batteries are fully loaded and the charge is depleted.	0
6.2.8.3	Surge protection features on the power inputs shall be designed and tested to withstand the worst case surge limits of appropriate standards. Surges within the limits of the ANSI standard shall not cause damage to the power supply or to equipment connected to the power supply. After the surge is removed, the equipment shall perform all functions and meet all performance limits without repair or recalibration by plant personnel. The surge withstand requirements on power inputs only applies to power supply cabling which penetrates the cabinet assembly boundary.	Modern electronic equipment is vulnerable to voltage surges. The power supplies must contain features to prevent surges in ac power from damaging equipment.	0
6.2.8.4	Overcurrent protection shall be provided within the protection function cabinet assemblies for the ac input feeders.	To prevent shorts within a cabinet from causing a distribution breaker to trip and causing loss of power to several cabinets.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.8.5	Cabinet subsystem dc power supplies shall be provided with overvoltage and overcurrent protection. Operation of the power supply protective features shall not cause equipment damage. Once the fault condition has been removed, dc power restored, and the system has completed initialization, the equipment shall function properly within performance limits. This may require plant personnel to manually reset the subsystem power supply protective devices prior to restoring the subsystem to an operating condition.	Overvoltage protection is required to prevent damage to component receiving power from the supply. Overcurrent protection is required to protect the power supply against shorts in the driven equipment.	0
6.2.8.6	The ac and dc (i.e., batteries) power distribution from the ac input feeder termination point to the cabinet bays shall be internal to the cabinet assembly.	Power source input connection points must be within an enclosure and readily accessible.	0
6.2.8.7	All dc power used by the equipment within a cabinet bay shall be supplied by dc power supplies mounted within the same bay. DC power buses shall not be routed between bays within a cabinet assembly. Exceptions are permitted where justified.	Required to reduce vulnerability to shorts and power supply failure.	0
6.2.8.8	Cables from the power supply units to the loads shall be specified according to the projected loads within each cabinet bay.	The power supply output distribution must use cables that do not create excessive voltage drop or overheating of the conductors.	0
6.2.8.9	Non-class 1E system instrumentation and controls and all the equipment required to make them function, which is powered from a Class 1E division, shall be powered from the same division or system.	Must not mix Class 1E power from two divisions in a single non-1E function in order to maintain a high level of separation.	0
6.2.8.10	If an instrument loop is powered from an uninterrupted power supply bus, then its entire function (indication, alarm, etc.) shall be powered from a UPS bus.	The state and status of an instrument loop should be available whenever it is operable.	0

Paragraph No.	Requirement	Rationale	Rev.
6.2.8.11	The loss of power to an indicator and/or to equipment in the instrument loop required to function shall cause the indicator to read its lowest reading or read off-scale to distinctly indicate a loss of power.	An indicator should be provided to show a loss of power.	0
6.2.8.12	Where specific instruments require power supplies other than those specified, the subsystem requiring the power shall provide the power supply.	This requirement is intended to cover cases where equipment from a specific vendor needs a voltage level different than that supplied by the M-MIS Designer.	0
6.2.9	**Grounding**	**Grounding**	0
6.2.9.1	**Protective and Power Grounding**	**Protective and Power Grounding**	0
6.2.9.1.1	Protective power outlet ground wires shall be routed to the cabinet grounding point separately from signal ground.	To protect ground loops and excessive ground currents in signal ground wires.	0
6.2.9.1.2	Suitable means shall be provided for the grounding of all equipment, cabinet bays, and their doors to a cabinet ground point.	For personnel safety and EMI reduction.	0
6.2.9.1.3	Metal enclosed equipment and modules, where the operating voltage is 50 volts or greater or where ANSI C37.90a-1974 surge withstand test is a requirement, shall be provided with a protective ground.	For personnel safety.	0
6.2.9.1.4	Protective and power grounds shall be connected so that disconnection of any equipment from the ground shall not disconnect any other equipment.	To maintain protective grounds during maintenance.	0
6.2.9.1.5	All electrical equipment shall have provisions of grounding live parts when the equipment is out-of-service. This means shall consist of portable ground cables of sufficient length to reach from the furthest level part to the nearest ground grid tap or the equipment ground bus.	To assure personnel safety during maintenance.	0

Paragraph No.	Requirement	Rationale	Rev.
6.2.9.1.6	The cabinet ground bus network shall be designed to minimize common mode voltage between subsystems in a cabinet. The common ground bus shall be connected to an adequately sized earthing stud on the plant ground bus. It is preferred that the ground bus within the cabinet be connected directly to the main plant ground grid using a dedicated, adequately sized ground cable. A minimum of #4/0 AWG is preferred.	Common mode voltages must be minimized to maintain signal accuracy.	0
6.2.9.1.7	A power supply common shall be supplied to provide a path for low voltage currents returning from the load to the power supply common. The power supply common shall be connected to the cabinet ground bus at one point.	To prevent ground loops.	0
6.2.9.2	**Instrument Grounding**	**Instrument Grounding**	0
6.2.9.2.1	The grounding of wiring shields shall be independent from modules so that removal of a module from the circuit shall not disturb the shield connection.	To maintain shielding with a module removed to prevent potential disruption of other modules.	0
6.2.9.2.2	Shielded cables used within the cabinet assemblies shall provide for a minimum of 95 percent effective coverage by the shield.	Required to assure adequate shielding.	0
6.2.9.2.3	Analog signals shall be grounded only in one place to prevent circulating ground currents in the signal lead.	To prevent noise due to ground loops.	0
6.2.9.2.4	Instrumentation cable shields shall be grounded only at one point.	To prevent ground loops and excessive shield currents.	0
6.2.9.2.5	Instrumentation cable shields shall be terminated on terminal blocks adjacent to the signal conductors.	To avoid the need for long pigtails on shield drain wires and to prevent confusion.	0

Paragraph No.	Requirement	Rationale	Rev.
6.2.9.2.6	Shields shall be grounded so that the shield potential is as close as possible to the ground potential at the signal source. Also, shield currents shall not flow in either the ground reference or signal conductors. In general, instrument cable shields shall be grounded at the location of the power source for the instrument loop. In the case of thermocouples used to monitor processes, the thermocouples shall be of the ungrounded type and the shield shall be grounded at the receiving device.	To minimize leakage between shields and signal conductors.	0
6.2.9.2.7	Signal transmission between devices where there is the potential for ground potential differences shall be differential voltage, current, optical or ac coupled. There shall be sufficient isolation ground between system grounds to prevent ground loops.	To prevent ground loops and maintain signal quality.	0
6.2.9.2.8	The plant instrument grounds shall be designed so that the ground potential difference between systems does not damage the interface equipment due to excessive common mode levels. Signal connections between systems shall have isolators to protect the equipment from damage.	To prevent equipment damage.	0
6.2.9.2.9	The signal grounding scheme for assemblies, subassemblies and subsystems shall use a "branching" scheme arranged so that ground currents do not tend to flow between the various elements.	To prevent ground loops.	0
6.2.9.2.10	Connections to the instrument ground bus shall use materials and techniques that are designed to prevent corrosion.	Corrosion will degrade the integrity and reliability of the ground connection	0
6.2.9.2.11	Communication systems shall not share the instrument grounds.	To reduce coupling between I&C systems and communication systems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.10	**Electrical Penetrations and Seals**	**Electrical Penetrations and Seals**	0
6.2.10.1	If barrier penetration connectors are used, the I&C signals shall not be degraded. Splices are permitted providing they do not degrade the signal. Splices in fiber optic cables are discouraged.	Self-explanatory.	0
6.2.10.2	All barrier penetration connectors shall have spare connectors. The M-MIS Designer shall determine the number of spare connectors to be provided.	Field modifications are costly. Spare connectors for replacement in the event of a failure or for expansion capability is good engineering practice.	0
6.2.10.3	The design of the I&C penetrations shall consider the effects of EMI/RFI interference from other electrical wiring penetrations.	Other electrical wiring can degrade the I&C signals if the penetrations are placed too close to one another.	0
6.2.11	**Cables, Fiber Optics, and Raceways**	**Cables, Fiber Optics, and Raceways**	0
6.2.11.1	**Equipment Cables**	**Equipment Cables**	0
6.2.11.1.1	The M-MIS Designer shall determine the requirements for spare conductors, considering cable replacement cost, complexity, plant down time, etc.	There is an economic tradeoff of field installation cost and spare conductors in the event of a conductor failure.	0
6.2.11.1.2	All control and instrumentation cables shall be color coded and identification numbering assigned to them. The Designer shall establish standards for color coding and identification numbering. Industry standard color coding and identification numbering shall be followed as closely as possible.	Color coding and numeric identification permits serviceability of the wiring if required.	0
6.2.11.1.3	Conductors for multi-conductor control cables shall be identified as per IPCEA 5-61-402.	Same as above.	0
6.2.11.1.4	Shield twisted pair cables shall be in one sheath; each pair shall contain conductors which are color coded in accordance with ANSI C96.1.	The wires can easily be identifiable. To reduce the potential for erroneous installation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
6.2.11.1.5	The M-MIS Designer shall establish panel internal wiring standards in accordance to the color and identification numbering standards established for the entire plant design.	The standard permits the client to service the requirement rapidly.	0
6.2.11.1.6	All instrument and control cables shall be preassembled cables to the maximum extent practical.	Preassembled cables reduce the possibility of field installation and maintenance errors in misconnecting the wires.	0
6.2.11.2	**Raceways**	**Raceways**	0
6.2.11.2.1	**Raceway Shielding**	**Raceway Shielding**	0
	Low level control and instrumentation cable tray system shall be separated from the power cable tray systems to minimize any interference of signal. Grounded metal trays and air space separation are acceptable means of providing raceway shielding.	Self-explanatory.	0
6.2.11.2.2	**Power Cable Shielding**	**Power Cable Shielding**	0
	Power cables shall be shielded to minimize the potential for emitting EMI/RFI. The shield shall be grounded to minimize the ground noise.	Self-explanatory.	0
6.2.11.2.3	**Loading of Wiring Raceways**	**Loading of Wiring Raceways**	0
	Loading of wiring troughs inside panels shall not exceed 40 percent capacity as per NEMA Standard PBI 1977, Paragraph PBI-5 20.	Self-explanatory.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.2.11.2.4	The following separation criteria shall be used for internal panel wiring:	These requirement are specified to meet the intent of General Design Criteria (GDC) 22.	0
	• AC and DC circuits shall be kept separated.		0
	• Instrumentation signal wiring shall be run separate from power or control wiring. This separation shall be accomplished by the use of separate wireway runs. Lacing of instrumentation signal wires with power and control wiring is not permitted.		0
	• Separation between Class 1E circuits and Non-class 1E circuits and redundant Class 1E circuits shall be in accordance with IEEE Std. 384- 1974, NRC Branch Technical Position CMEB 9.5-1 and NRC Regulatory Guide 1.75.		0
	• The minimum separation distance between redundant Class 1E equipment and wiring internal to control switchboards shall be a minimum of six inches or that which can be established by analysis of the proposed installation. This analysis shall be based on tests performed to determine the flame retardant characteristics of the wiring, wiring materials, equipment, and any other material associated with the design. In the event that the separation distance cannot be achieved, barriers shall be installed between redundant Class 1E equipment and wiring.	• Required to meet the GDC physical separation criteria.	0
	• Non-class 1E wiring shall not be harnessed with Class 1E or associated Class 1E wiring.		0
	• Conduit opening in Class 1E panel boards shall be sealed.		0

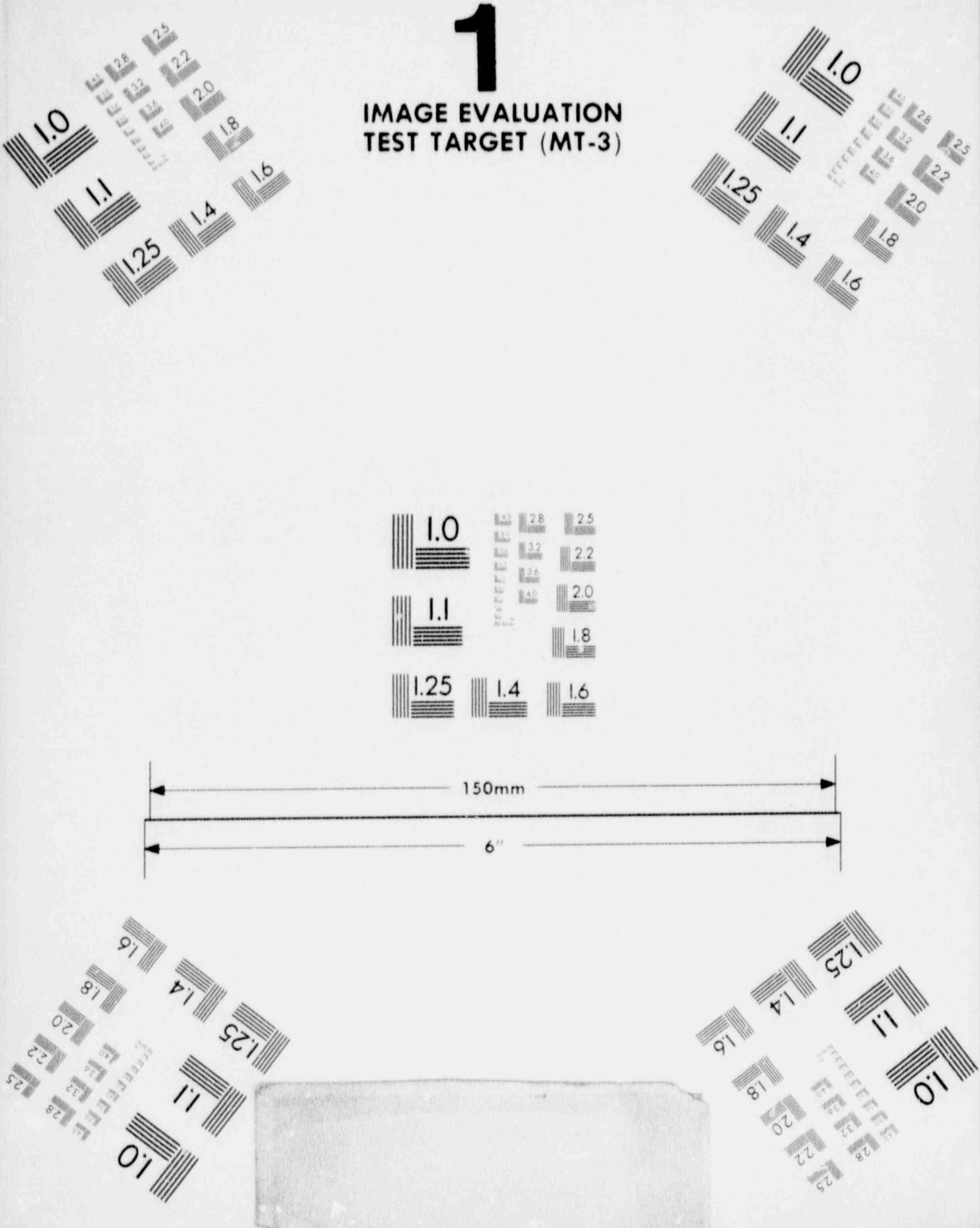
Paragraph No.	Requirement	Rationale	Rev
6.2.11.3	**Instrumentation Cables**	**Instrumentation Cables**	0
	Instrumentation (signal) cable consisting of two or more twisted conductors shall require individual twisted conductor shielding and overall shielding with a drain wire (attached to shielding).	This is to provide a method of reducing or eliminating electrostatically induced noise in low level electronic type signal circuits.	0
6.2.11.4	**Fiber Optics**	**Fiber Optics**	0
	Cable supports, raceways and penetrations which accommodate fiber optic cables shall consider the minimum bend radius for the fiber optic cable.	Fiber optic cable specification requires a minimum turn radius to prevent the breaking of the brittle fiber optic cable.	0
6.2.12	**Field Termination and Splices**	**Field Termination and Splices**	0
6.2.12.1	The method of field wire termination and splices shall have the following characteristics:		0
	• Have a positive securing feature to withstand the design basis seismic event and plant equipment vibrations without inadvertently disconnecting.	• There is a tradeoff of assuring security which ring lugs provide; however, ring lugs have the disadvantage of time-consuming field wire termination labor and added space. This requirement permits the Plant Designer other methods of termination.	0
	• Permit work space for improved maintainability.	• This is a cabinet requirement; however, it is worth specifying because consideration for maintainability has been an issue on previous plant designs. Different field wire termination methods could have improved the maintainability.	0
	• Be easy to disconnect for service, maintenance, and replacement.	• The requirement reduces the labor cost.	0
	• Include provisions for terminal identification.	• Self-explanatory.	0

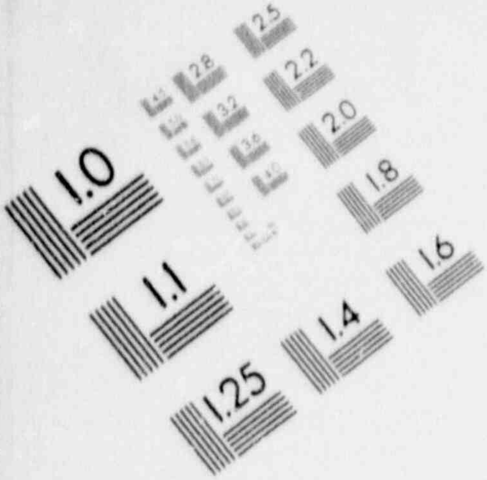
Paragraph No.	Requirement	Rationale	Rev
	• Incorporate material that is compatible with the environmental conditions so that the signal is not degraded.	• Environmental conditions can cause degradation of materials, thereby leading to degradation of signals. Material compatibility can also degrade the signals.	0
	• Incorporate a straightforward and simple field termination and splicing procedure for use by utility personnel that does not require excessive or frequent training or specially designed tools.	• Major cause of field termination failures has been improper installation due to lack of training, poor training, or using the wrong tools to perform work. Special tools are often expensive and require long lead times to obtain.	0

Paragraph No.	Requirement	Rev.
6.3	COMMON CONTROL SYSTEM REQUIREMENTS	0
6.3.1	**Definition**	0
6.3.1.1	**Purpose**	0
	The purpose of this subsection is to define common requirements for the design, selection, and installation of a specific M-MIS control system. This subsection does not repeat any requirements specified in Sections 7 through 11 of this Chapter.	0
6.3.1.2	**Scope**	0
	The common requirements in this section cover all control systems required for operation and maintenance of the plant. The requirements have been organized as follows:	0
	• Design Requirements;	0
	• Performance Requirements;	0
	• Availability/Operability;	0
	• Testability and Qualification;	0
	• Maintainability and Serviceability.	0

1

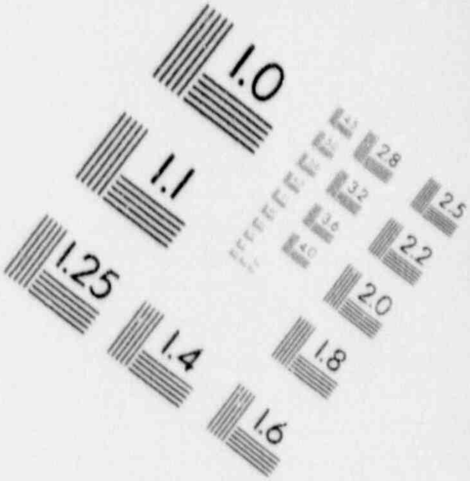
IMAGE EVALUATION TEST TARGET (MT-3)

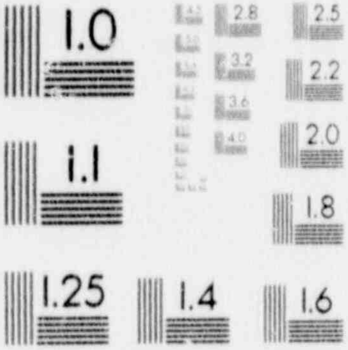


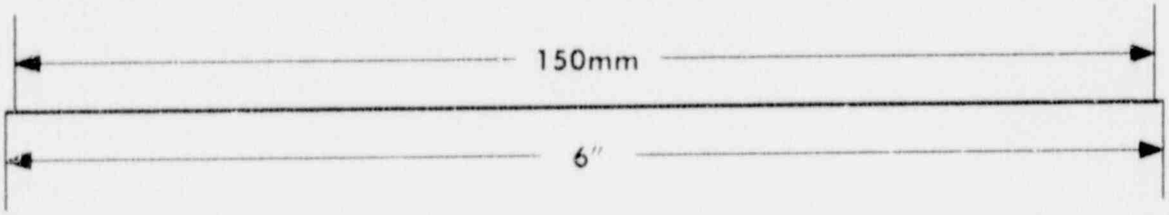


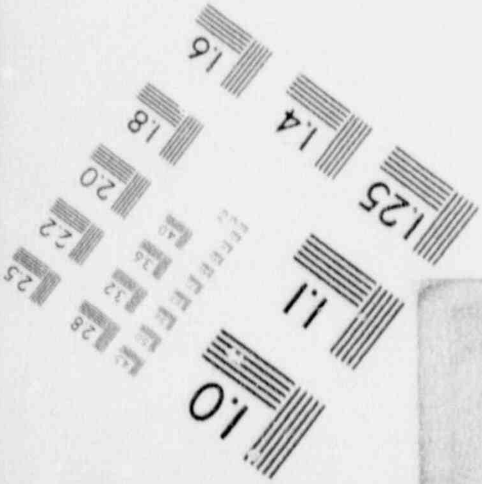
1

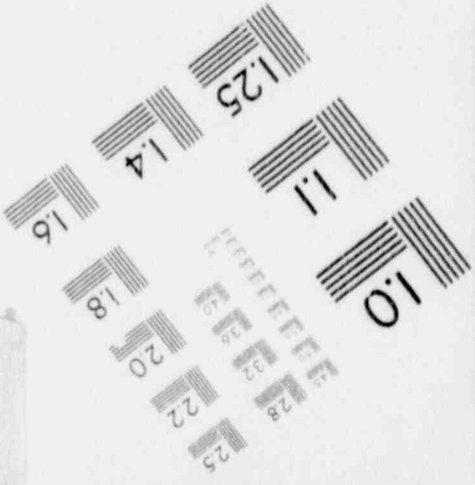
IMAGE EVALUATION TEST TARGET (MT-3)





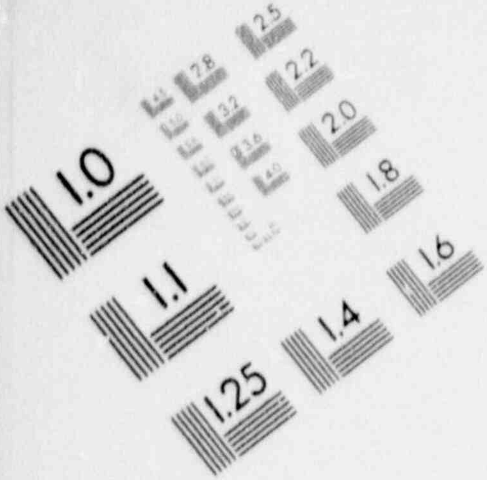


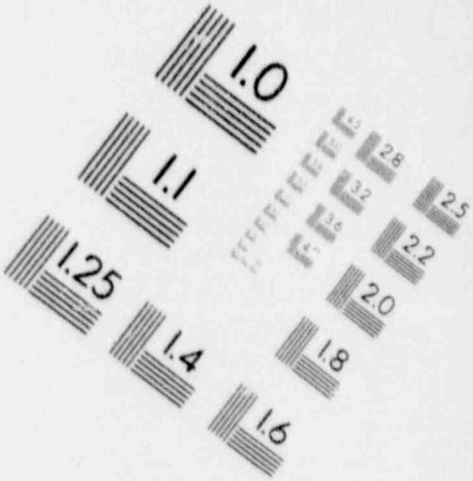


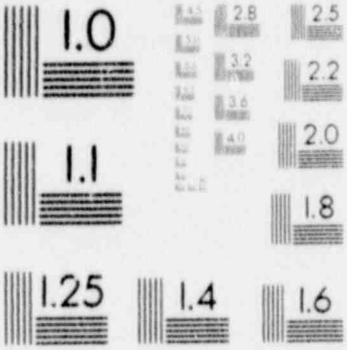


1

IMAGE EVALUATION TEST TARGET (MT-3)

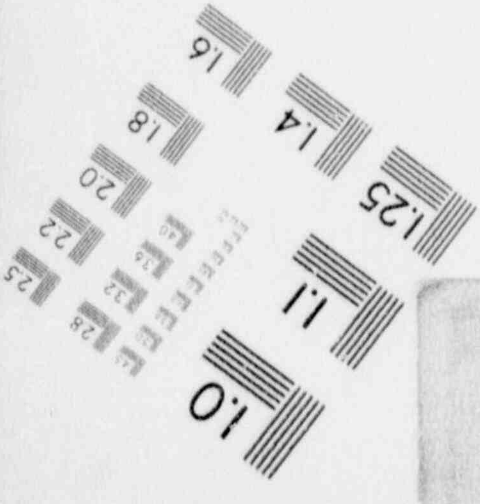


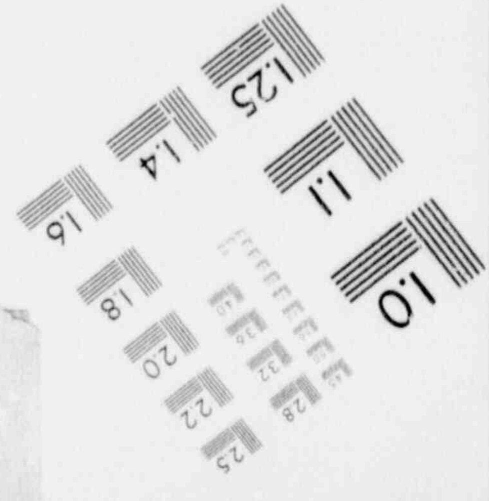




150mm

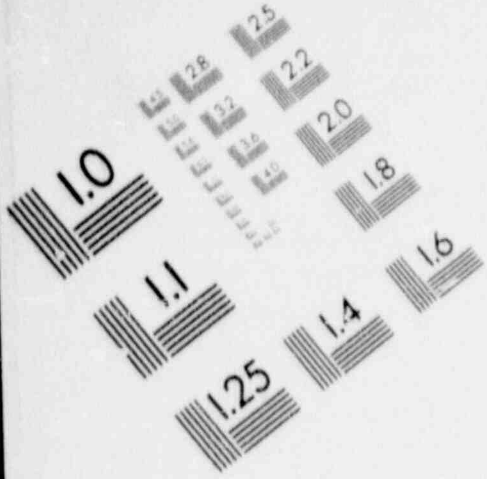
6″

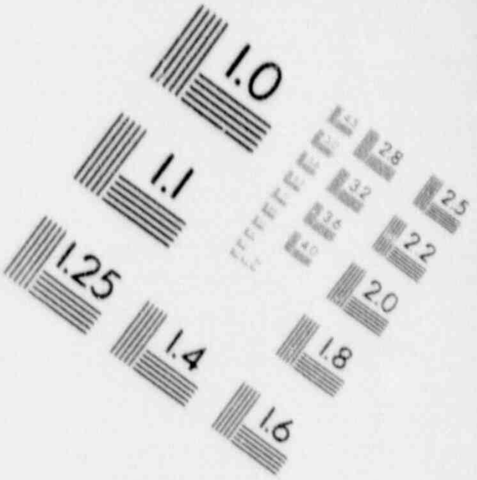


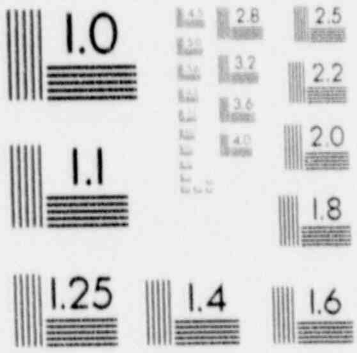


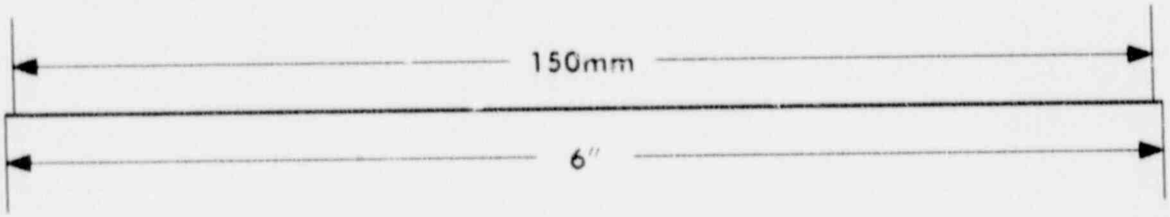
1

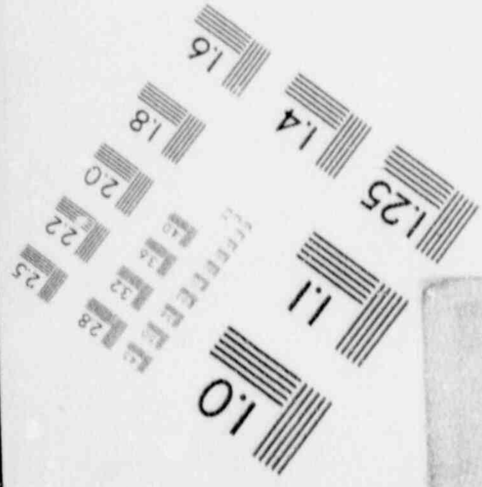
IMAGE EVALUATION TEST TARGET (MT-3)

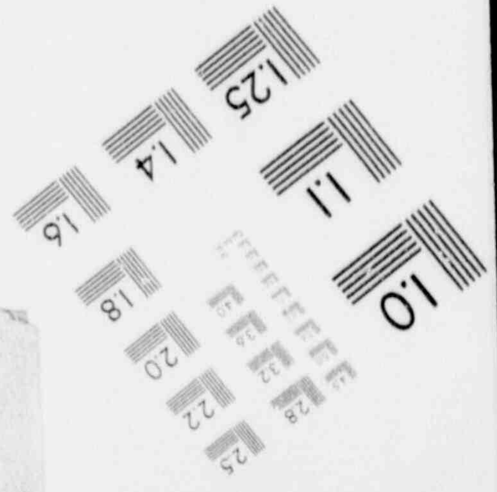






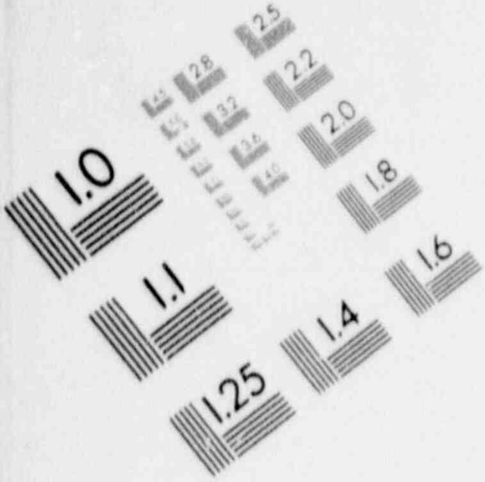


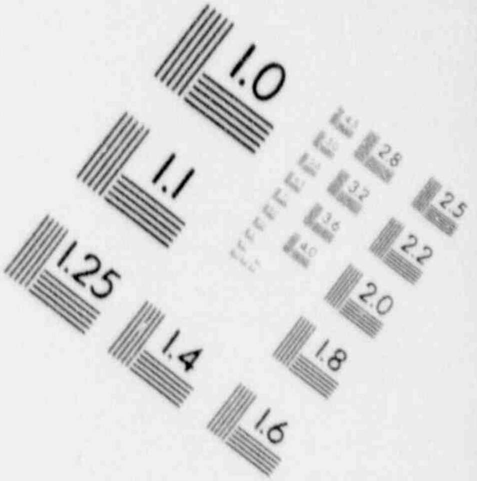


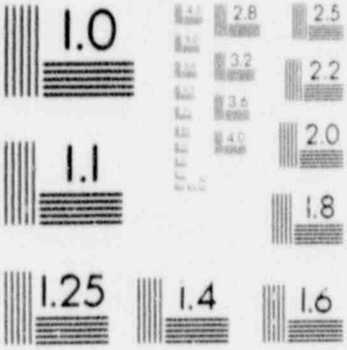


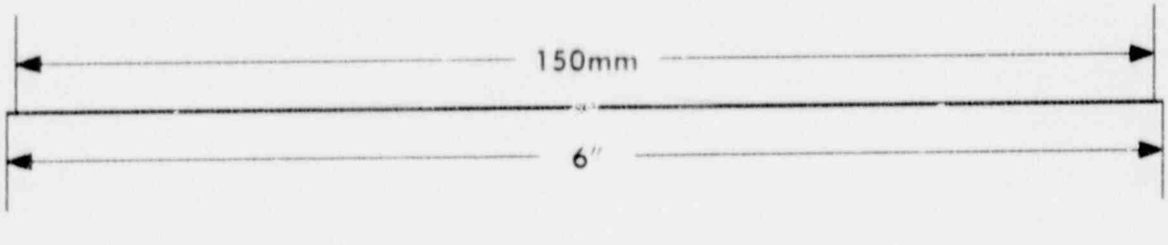
1

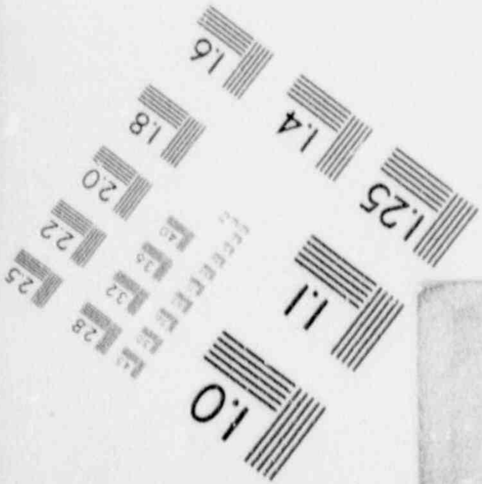
IMAGE EVALUATION TEST TARGET (MT-3)

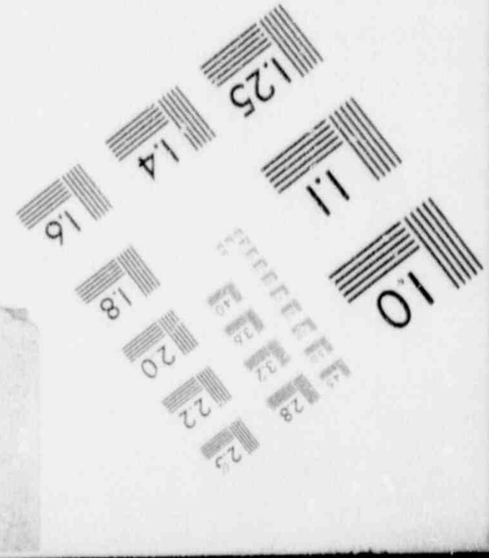












Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.3.2	**Design Requirements**	**Design Requirements**	0
6.3.2.1	All safety-related control system software shall be retained on power interrupts. Storage of programs on PROMs (Programmable Read Only Memory) is the preferred method of meeting this requirement. If battery-backed Read Only Memory (ROM) is used, the Designer shall demonstrate that there is sufficient battery capacity that the probability of loss of program is low enough to consider it an improbable event.	The loss of control system software would not inhibit the automatic startup of the control system. The reloading of the programs may increase the downtime of the system or require special skills to perform the reload operation.	0
6.3.2.2	Software interface of a safety-related system with a non-safety-related system is discouraged. If the designer chooses to do so, the designer shall demonstrate that isolation is provided to preclude the propagation of errors from a non-safety-related system to a safety-related system.	Hardware and software separation and isolation criteria are not identical although the intent may be the same (e.g., six-inch separation and use of barriers make little sense for software).	0
6.3.2.3	When evaluating stability and response rates, the Plant Designer shall consider the following:		0
	• Plant and equipment non-linearities. The characteristics of the turbine valves, feedwater valves, plant processes, etc. change with the operating point. The control systems must compensate for these non-linearities to provide the required response and stability for all expected combinations of operating points.	• Typical characteristics that affect closed loop system response and stability.	0
	• Time delays caused by backlash, wind-up, dead times, transport delays, etc. in plant equipment and processes.		0
	• The effect of sample rate and resolution when sampled data systems are used. The potential effect on limit cycles as well as transient response and stability shall be considered.	• To assure adequate consideration of the characteristics caused by sampled data systems that can degrade system performance.	0

Paragraph No.	Requirement	Rationale	Rev.
	• Potential effects of sensing subsystem components (e.g., sensors, instrument lines, snubbers) on system performance.	• Components in the sensing subsystem can affect fast response control loops.	0
	• Potential effects of environmental extremes and process conditions on control equipment and sensing subsystem components.	• The effect of environment and process conditions on sensing subsystem components is of particular importance. For example, the effect of environment on level sensing reference legs and the effect of process conditions on fluid densities can have a significant impact on system accuracy.	0
6.3.2.4	Set points, calibration constants, sensor limits, and any other required process constants shall be maintained in non-volatile memory to prevent their loss on a power interruption.	Having the current values such as set points and calibration constants stored in non-volatile memory enables the M-MIS to maintain this information during and after a power failure. Otherwise it would be necessary for the operator to re-enter this information upon restart, which is a time-consuming process that is prone to error. Furthermore, automating the restart of the M-MIS upon restoration of power is necessary for all portions of a distributed M-MIS to start in a coordinated fashion.	0
6.3.2.5	The Plant Designer shall define and design plant systems and component controls that will remain in the known safe state following restoration of power (control or motive) from a loss of power event.	Industry experience has shown that previous plant designs have exhibited uncontrolled restoration of control or motive power which have driven the system away from the known safe state.	0

Paragraph No.	Requirement	Rationale	Rev.
6.3.3	**Performance Requirements**	**Performance Requirements**	0
6.3.3.1	Control algorithms which use reset action shall provide an anti-windup feature. The anti-windup shall operate so that the absolute value of the integrator is equal to the proportional part subtracted from the limit value.	Anti-windup is required for a well behaved control system. It is usually implemented in analog controllers, but it also must be used for digital control algorithms.	0
6.3.3.2	Transfers between manual and automatic control shall be bumpless.	To prevent undesired transients.	0
6.3.3.3	The settings of all control parameters (proportional band, reset rate, limits, etc.) shall provide a resolution and accuracy of 1 percent or better of the full-scale adjustment range specified for the parameter.	Setability of control parameters should be consistent with the specified range to ease pre-op and startup testing.	0
6.3.3.4	If sampled data is used in the control systems, then:	Digital control introduces sampled data concerns.	0
	• Analog data acquisition modules shall provide filtering so that noise aliased into the signal frequency band contributes less than one tenth of the allowable signal error.	• To address aliasing problem for sampled data systems.	0
	• If digitized input signals are used at a lower rate than provided by the interfacing system, the data rate shall be digitally filtered to the same requirements as above.	• Aliasing can also occur when resampling a previously digitized signal.	0
	• The designer shall establish the signal reconstruction requirements for the control system. The signal reconstruction shall be zero order hold type. As a minimum, the requirements for droop between refresh, output glitches in amplitude, frequency of occurrence, and distortion shall be specified.	• Signal reconstruction hardware (i.e., digital to analog convertors) can introduce noise and other errors. [EPRI Contractor should review or establish satisfactory requirements for signal reconstruction. Zero order hold should be used because most available modules use it. Different classes of reconstruction may be provided if appropriate.]	0
6.3.3.5	Interrupts shall not be used in the main functional processors which have direct protection or control function.	The protection or control function should be the top priority activity. Interruptions to its functions should not be permitted.	0

Paragraph No.	Requirement	Rationale	Rev.
6.3.3.6	The protection function shall be the highest priority followed by the control function. The lowest priority is the monitoring function. Therefore, if a protection or control function is encountered, it shall interrupt the monitoring function.	Self-explanatory.	0
6.3.3.7	The design of the control and instrumentation systems shall include pre-operational considerations of initial plant startup test requirements. The systems shall be designed to minimize the need for special sensors, interconnections, etc. for startup test data calibration.	Requirements for special startup test instrumentation increases expense and time for startup testing.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
6.3.4	**Availability/Operability**	**Availability/Operability**	0
6.3.4.1	For non-Class 1E systems, availability shall be achieved to the extent practical by the use of inherently reliable components. The use of redundancy to achieve hign availability shall be minimized.	Minimum use of redundancy is required to minimize plant equipment. Implementing control algorithms in software, the use of distributed control, and a data transmission system that provides wide accessibility of process signals may be used to enhance availability without providing system unique redundant equipment.	0
6.3.4.2	Where possible, signals from other systems shall be used in the control systems to enhance availability. (For example, the use of wide range level sensors for checking the validity of the narrow range level sensors for feedwater control. The wide range sensors could also be used to temporarily control feedwater if repairs to the narrow range sensor could be achieved in a short time.)	Self-explanatory.	0
6.3.4.3	Where feasible, redistribution of control tasks among control computers on detection of failures shall be used to enhance reliability.	There may be cases where operating computers can assume some or all of the tasks of a failed computer. This provides partial redundancy for functions that do not have redundancy designed into them.	0
6.3.4.4	The control and instrumentation system shall be a distributed system. Local control shall be performed. Only monitoring data shall be transmitted to a central host.	A distributive control system reduces the field wiring cost as well as reducing the potential for common mode failures inherent in central control system.	0
		The loss of the communication link would only affect the monitoring data that is being transmitted through the communication link.	0

Paragraph No.	Requirement	Rationale	Rev.
6.3.5	**Testability and Qualification**	**Testability and Qualification**	0
	For redundant systems, the designer shall establish the criteria for determining system disagreements and the methodology to be used for selection of the correct control systems.	Disagreements in redundant systems must be resolved, especially for distributive, redundant systems.	0
6.3.6	**Maintainability/Serviceability**	**Maintainability/Serviceability**	0
6.3.6.1	The maintenance interface shall provide the capability to access the diagnostic, calibration, and other maintenance aids. Design consideration shall meet the following requirements:		0
	• Hardware or software control shall be provided to control access to critical system parameters.	• Aids in preventing unauthorized access to the systems.	0
	• The maintenance interface functions shall not be placed in any location that interferes with plant operations.	• This requirement is to prevent interference between maintenance and operations personnel.	0
	• System connection shall be via electrically isolated test points and/or a suitably isolated data link.	• To prevent disturbance to the signals being measured so that plant operation is not disturbed and measured signal level correctly indicates the state of the parameter.	0
6.3.6.2	Design provision shall be available to access all of the system inputs and outputs. Additional capability shall be provided as required for the various systems.	Minimum required for any maintenance activity. Additional access helps to pinpoint problems.	0
6.3.6.3	Control system design shall provide an indication in the main control room that maintenance activities are in progress.	Self-explanatory.	0

7 OVERALL PLANT, REACTOR, AND REACTOR COOLANT SYSTEMS M-MIS REQUIREMENTS 0

7.1 PURPOSE AND SCOPE 0

The reactor and reactor coolant group of systems includes those which are covered by Chapters 3 and 4 of this ALWR Requirements Document. In addition to those individual systems, this section covers the requirements for the M-MIS which monitors and controls the overall power production of the plant. This includes requirements for directly associated control and instrumentation equipment, e.g., sensors, indicators, control devices, data transmission and processing equipment, and alarms. Only requirements which relate to use in overall plant control or in the reactor and reactor coolant group of plant systems are covered; general requirements on the use of these types of equipment are addressed in other sections of Chapter 10. The mechanical and electrical components which make up the individual systems, e.g., pumps, motors, tanks, piping, valves, power cables, and switch-gear, are covered in other chapters of the ALWR Requirements Document. 0

This section of Chapter 10 covers only a portion of the M-MIS requirements for these systems. Many of the requirements on the plant systems in other chapters, particularly Chapters 1, 3, and 4, are directly applicable to the M-MIS for this group of systems; however these will not generally be repeated unless they need to be expanded to clarify their applicability to the M-MIS or need special emphasis. In particular, this section provides requirements which cover: 0

- The allocation of the functions of the M-MIS for this group of systems among the individual plant systems; 0
- The identification of the physical boundaries and interfaces of the M-MIS for the purpose of defining the scope of requirements for this group of systems; 0
- The strategies for control and monitoring (for example, manual or automatic and local or remote) which shall be followed for various operating modes of the individual plant systems, e.g., startup, normal operation, shutdown or reconfiguration, and testing; 0
- The integration of the M-MIS for the individual systems and overall plant M-MIS with the M-MIS of other plant systems and the coordination of their operation. 0

Paragraph No. *Requirement* *Rev.*

7.2 GENERAL REQUIREMENTS FOR OVERALL PLANT, REACTOR, AND REACTOR COOLANT SYSTEMS GROUP M-MIS 0

7.2.1 Functions 0

The M-MIS for the overall plant and this group of individual systems shall provide the monitoring and control necessary to carry out their required functions. These plant and system functions are defined in Chapters 1, 3 and 4. 0

The M-MIS Designer shall allocate the various M-MIS functions among the overall plant power control M-MIS and the individual plant systems M-MIS such that the required functions and tasks as determined in the design process (Section 3.1.3.3) can be satisfactorily accomplished. This section provides an initial allocation of these M-MIS functions; however, it is a primary responsibility of the M-MIS Designer to integrate and coordinate the operation of all M-MIS so that all functions are adequately performed. Figure 10.7-1 illustrates how the major functions of the systems in this group have been allocated to the individual plant systems for the purposes of this Requirements Document. Other allocations of the functions may be used if they can be shown to improve significantly the plant's operability, simplicity, or reliability and if they are fully in accordance with the M-MIS design process requirements in Section 3, particularly the requirements for a functional design approach (3.1.1.1) and the analysis of functions and tasks (3.1.3.3). 0

7.2.1.1 Overall Energy Production, Transport, and Conversion 0

The M-MIS shall provide for the monitoring and control of the overall process of producing energy in the reactor core and eventually delivering some part of it to the utility power grid and rejection of the remainder to the heat sink and environment. This overall M-MIS function is accomplished by the integration and coordination of individual plant systems M-MIS. 0

7.2.1.2 Reactor Energy Production 0

The M-MIS shall provide for the monitoring and control of reactor core energy production. This function shall be accomplished by monitoring the neutron flux and by adjusting the reactivity to maintain a proper magnitude and distribution of fission energy production. For PWRs, the monitoring also includes reactor core outlet temperatures. This function is accomplished largely by the control rods, soluble boron in the coolant (normally PWRs only), and the reactor coolant temperatures and flow rate (BWRs). 0

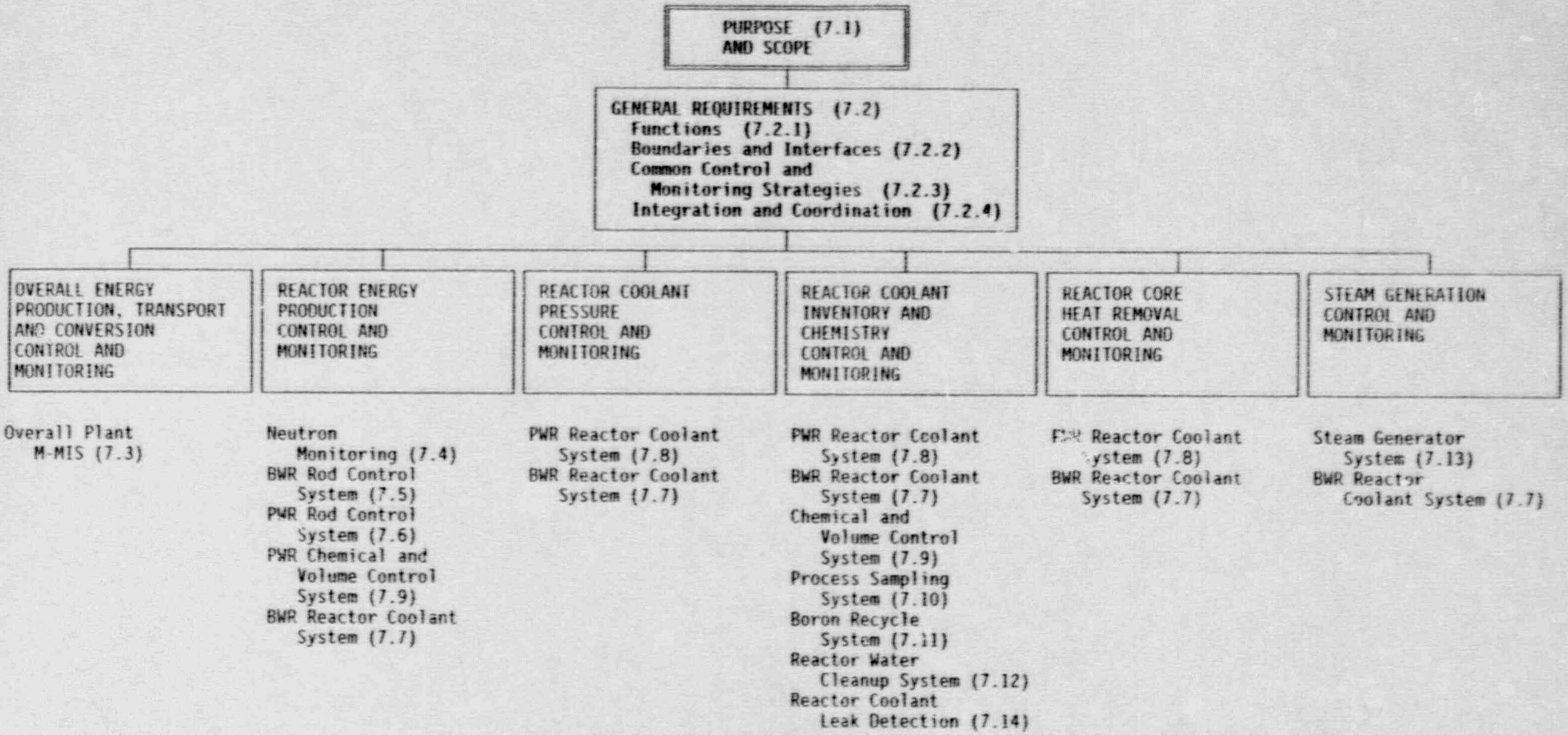

PURPOSE (7.1)
AND SCOPE
GENERAL REQUIREMENTS (7.2)
Functions (7.2.1)
Boundaries and Interfaces (7.2.2)
Common Control and
Monitoring Strategies (7.2.3)
Integration and Coordination (7.2.4)
OVERALL ENERGY PRODUCTION, TRANSPORT AND CONVERSION CONTROL AND MONITORING
REACTOR ENERGY PRODUCTION CONTROL AND MONITORING
REACTOR COOLANT PRESSURE CONTROL AND MONITORING
REACTOR COOLANT INVENTORY AND CHEMISTRY CONTROL AND MONITORING
REACTOR CORE HEAT REMOVAL CONTROL AND MONITORING
STEAM GENERATION CONTROL AND MONITORING
Overall Plant M-MIS (7.3)
Neutron Monitoring (7.4)
BWR Rod Control System (7.5)
PWR Rod Control System (7.6)
PWR Chemical and Volume Control System (7.9)
BWR Reactor Coolant System (7.7)
PWR Reactor Coolant System (7.8)
BWR Reactor Coolant System (7.7)
PWR Reactor Coolant System (7.8)
BWR Reactor Coolant System (7.7)
Chemical and Volume Control System (7.9)
Process Sampling System (7.10)
Boron Recycle System (7.11)
Reactor Water Cleanup System (7.12)
Reactor Coolant Leak Detection (7.14)
PWR Reactor Coolant System (7.8)
BWR Reactor Coolant System (7.7)
Steam Generator System (7.13)
BWR Reactor Coolant System (7.7)

FIGURE 10.7-1

ALWR M-MIS FOR OVERALL PLANT, REACTOR, AND REACTOR COOLANT SYSTEMS

Paragraph No.	Requirement	Rev.
7.2.1.3	**Reactor Coolant Pressure**	0
	The M-MIS shall provide the control and monitoring required to maintain the Reactor Coolant System pressure within the proper range for operation and with the design limits. This function is accomplished largely by the M-MIS for the Reactor Coolant System, particularly the pressure relief valves and, in PWRs, the pressurizer heaters and sprays.	0
7.2.1.4	**Reactor Coolant Inventory and Chemistry**	0
	The M-MIS shall provide the control and monitoring required to maintain an adequate inventory of coolant in the Reactor Coolant System and, in addition, assure that the coolant chemistry is within an acceptable range. This function is accomplished largely by the Reactor Coolant System M-MIS in conjunction with the Chemical and Volume Control System (PWRs) and the Reactor Water Cleanup System (BWRs). The monitoring of the chemistry is largely accomplished by the Process Sampling System M-MIS. The monitoring of reactor coolant leakage is accomplished by the Reactor Coolant Leak Detection M-MIS.	0
7.2.1.5	**Reactor Core Heat Removal**	0
	The M-MIS shall provide the control and monitoring required to remove the energy produced in the reactor core. In the case of a BWR, this includes the generation of steam and providing it at the proper conditions to the main and extraction steam system and returning feedwater to reactor. In the case of a PWR, this includes the delivery of heated reactor coolant to the steam generator and the return of the cooled reactor coolant to the reactor. This function is accomplished largely by the Reactor Coolant System.	0
7.2.1.6	**Steam Generation**	0
	The M-MIS shall provide for the monitoring and control of the process of generating steam in the reactor vessel in a BWR and steam generators in a PWR. This includes maintaining an adequate water level in the reactor vessel or steam generators and ensuring that the reactor vessel or steam generators are not overfilled. This function is accomplished largely by the M-MIS for the BWR Reactor Coolant System and the PWR Steam Generator System.	0

Paragraph No.	Requirement	Rev.
7.2.2	**Boundaries and Interfaces**	0
	The physical boundaries of the individual systems which make up the reactor and reactor coolant group of systems are defined in the appropriate sections of Chapters 3 and 4. The boundaries of the M-MIS for the group of systems shall be consistent with those physical boundaries of the plant systems; however, they shall also encompass the M-MIS hardware, which includes:	0
	• Instrument sensors;	0
	• Data transmission equipment;	0
	• Data processing equipment;	0
	• Controllers and logic devices;	0
	• Operator interface hardware (e.g., controls, indicators);	0
	• Software to support M-MIS hardware.	0
	The interfaces of the individual systems which make up the reactor and reactor coolant group of systems are defined in the appropriate sections of Chapteis 3 and 4. The interfaces of the M-MIS for the group of systems shall be consistent with those plant system interfaces. The M-MIS interfaces shall be formally defined and controlled in accordance with the M-MIS Design Plan (Section 3.1.2.4). The M-MIS Designer shall define and control other interfaces among the various M-MISs and other plant systems as may be necessary to integrate and coordinate the operation of the plant systems even though these interfaces are not defined as physical interfaces in Chapters 3 and 4.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.2.3	**Common Control and Monitoring Strategies for the Overall Plant, Reactor, and Reactor Coolant Systems**	**Common Control and Monitoring Strategies for the Overall Plant, Reactor, and Reactor Coolant Systems**	0
	The M-MIS Designer shall use a consistent control and monitoring strategy for all the parts of the M-MIS for the overall plant and this group of systems except as modified by individual systems M-MIS requirements. This common control strategy shall also be consistent with that used for the remainder of the M-MIS.	A consistent control strategy supports the overall objective of a high level of standardization for the ALWR. It also tends to simplify training of operators and maintenance technicians. For example, consistent control strategies tend to lead to similar controls, displays, and control stations.	0
7.2.3.1	**Startup and Shutdown Operations**	**Startup and Shutdown Operations**	0
	The M-MIS for this group of systems shall normally provide for the monitoring and control necessary to startup or shutdown a system to be done by the operators, i.e., the control shall be manual. Specific tasks involved may be automated if analyses of functions and tasks (Section 3.1.3.3) show manual operation is a significant burden or distraction for the operators. As required by 3.4.4 and 4.9.1.2, the main control room operators shall be responsible for these operations only to the extent that analysis of functions and tasks shows that local operations are not compatible with operability requirements.	The startup and shutdown of this group of systems is largely paced by the operators and may involve a very large number of individual operations, particularly local operations such as the repositioning of valves. Automation of these operations would significantly increase the complexity of the plant and is not desirable. There may be portions of the startup or shutdown which could be automated and thereby reduce the time to startup or the risk of errors.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.2.3.2	**Normal Operations**	**Normal Operations**	0
	The M-MIS for this group of systems shall normally provide for automatic or unattended operation for continuous or often repeated tasks when the plant is in nominally steady operation above a low power level. This low power level shall be established by the M-MIS Designer based on a specific tradeoff evaluation which considers the functions and tasks required at low power levels, the potential frequency and duration of low power operation, and the relevant equipment and system constraints on low power operation. This tradeoff evaluation shall be documented and reviewed in the design process. The evaluation to select a power level shall be combined with the similar tradeoff evaluation required by 9.2.3.2.	The automatic, unattended operation of this group of systems is intended to be consistent with the main control room staffing in Section 4.2.4. That requirement cannot be expected to be met if an operator is occupied most of the time by the need to control a system in this group. It is also current practice for these systems to operate without constant operator attention. Tasks that are done manually, at relatively long intervals, for example, refilling a tank or reconfiguring a system to equalize service time, probably do not need to be automated.	0
7.2.3.3	**Reconfiguration Operations**	**Reconfiguration Operations**	0
7.2.3.3.1	The M-MIS shall provide for automatic reconfiguration (e.g. shutdown) of a system when necessary to avoid personnel hazard, major equipment damage, or to support actions by other parts of the plant M-MIS, for example, when the reactor is automatically shutdown by the Reactor Protection System or a safety system is actuated.	Some reconfiguration actions cannot depend on the operators because of timing constraints or the risk or error. In addition, it has been the practice to automate such tasks.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.2.3.3.2	The return of a system to its initial configuration after an automatic reconfiguration shall normally be by operator action, i.e., not automatic. Return to the initial configuration may be automatic if the M-MIS Designer establishes that such automatic action would significantly:		0
	• Reduce the challenges to protection and safety systems;		0
	• Reduce hazards to personnel;		0
	• Improve the plant availability; or		0
	• Reduce the risk of damage to major plant equipment.		0
7.2.3.3.3	The operators shall be notified of any such automatic return to the original configuration.		0
7.2.3.4	**Testing Operations**	**Testing Operations**	0
	The M-MIS for this group of systems shall normally provide for on-line testing only at the direction of the operator. The testing itself should be automated and assisted as required in Section 3.6 so that operator actions are simple and have little risk of causing a plant upset.	The testing of these systems often must be done while the systems are in operation. Mistakes in the testing have often resulted in a loss of generation or serious upsets and plant trips. Section 3.6 contains a number of specific requirements to enhance the testability of the ALWR. The testing strategy for these systems is intended to be consistent with those requirements.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.2.4	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS designs for the systems in this group shall be integrated and coordinated so that the overall plant performance and functional requirements as well as those of individual systems are met. Those requirements are found in Chapter 1 and in other chapters of the ALWR Requirements Document, particularly Chapters 3 and 4. In addition, the M-MIS Designer shall coordinate the design features with other parts of the M-MIS, especially those portions of the M-MIS which control the energy transfer and electrical generation (e.g., Section 9 of Chapter 10).	Although the requirements for the individual systems define the functions and interfaces, it is the basic responsibility of the M-MIS Designer to connect the various systems and their requirements in a sensible and efficient manner. The specific methods used to connect the operation of the various systems and the logic are to be selected by the M-MIS Designer. The ALWR Requirements Document has specifically avoided defining how this is to be accomplished. It is intended that the M-MIS Designer not be constrained to current practice and be encouraged to develop strategies for control and monitoring which consider the many interactions among the various systems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.3	**OVERALL PLANT M-MIS**	**OVERALL PLANT M-MIS**	0
7.3.1	**Functions**	**Functions**	0
	The function of the overall plant M-MIS is to ensure that all parts of the main energy transport process operate in an efficient and effective manner and deliver the required energy to the external electric grid.	This function is consistent with the goal to make the ALWR an active part of the utility electric supply grid.	0
7.3.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	Above the power level specified in Chapter 1, the M-MIS shall provide for the adjustment of plant power level directly by the utility load dispatcher. Under these conditions the M-MIS shall ensure that rates and magnitudes are limited to those acceptable to the plant. If all systems are operating normally, the load dispatcher shall not be able to take any action - accidental or deliberate - which will cause the plant to trip or challenge the protection and safety systems.	Although operation of the ALWR as part of a utility grid is a fundamental requirement, the load dispatcher can never have the knowledge about the actual plant conditions which is available to the main control room operators. They must have the ability to quickly intercede if they detect unusual conditions.	0
	In addition, the M-MIS Designer shall provide the capability to adjust the limits on the remote maneuvering to account for systems or components out of service or to lock out power level control by the dispatcher. All power changes required by the load dispatcher shall be immediately identified to the operators in the main control room without any action on their part. Furthermore, controls shall be provided for the control room operators to immediately and simply take the plant control away from the load dispatcher. The communication between the operators and the utility dispatcher shall be explicitly included in the analyses of function and tasks.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.3.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the overall plant shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	The major part of the Overall Plant M-MIS design is the integration and coordination of other plant systems.	0
	• The energy production in the reactor;		0
	• The conversion of energy in the steam to electricity in the main turbine-generator.		0
7.3.4	**Performance Monitoring**	**Performance Monitoring**	0
	The Overall Plant M-MIS shall provide the capability for the operator to call up a monitoring display which provides a heat balance of the plant and which shows whether all major components are operating efficiently and effectively. This operator aid shall provide the operator with the capability to test whether other equipment alignments, set points, etc. (within technical specification limits) would provide more efficient operation or to determine the penalty for an alternate alignment.	This operator aid would allow the selection of optimum operating conditions and allow the operators to assess the effect of maintenance operations. It could potentially provide a warning for conditions which would lead to technical specification violations.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.4	**NEUTRON MONITORING SYSTEM M-MIS**	**NEUTRON MONITORING SYSTEM M-MIS**	0
7.4.1	**Functions**	**Functions**	0
	The Neutron Monitoring M-MIS shall provide the monitoring required to determine whether the amount, rate of change, and distribution of fission energy production in the core is within acceptable values.	This function allocation is consistent with current practice.	0
7.4.2	**Monitoring Strategy**	**Monitoring Strategy**	0
	The M-MIS Designer shall establish by analysis the functions and tasks which involve knowledge of the neutron level or distribution and thereby establish:	Although the Neutron Monitoring M-MIS does not involve indirect actuations, it will be the source of signals for automatic actions in other systems and will be the source of information on which the operators will take action.	0
	• The monitoring which must be done automatically and that which can be done in response to operator demand;		0
	• The data which must be presented to the operators, including special processing or reduction of the individual readings, so that the information is immediately useful to the operators;		0
	• The conditions which need to be alarmed or otherwise brought to the operators' attention.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.4.3	**Integration and Coordination**	**Integration and Coordination**	0
	The Neutron Monitoring M-MIS shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	These other plant systems all take action based on the Neutron Monitoring System.	0
	• The operation of the control rods;		0
	• The operation of the Reactor Coolant System (BWR) which affects reactivity;		0
	• The operation of the Chemical and Volume Control System (PWR);		0
	• The operation of the Reactor Protection System;		0
	• The monitoring of core outlet temperatures (PWR).		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.5	**BWR ROD CONTROL SYSTEM M-MIS**	**BWR ROD CONTROL SYSTEM M-MIS**	0
7.5.1	**Functions**	**Functions**	0
	The M-MIS for the BWR Rod Control System shall provide the monitoring and control necessary to position the control rods so that the magnitude and distribution of the fission energy production in the core is within acceptable limits for the time in core life and the plant conditions.	This is consistent with current practice.	0
7.5.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
7.5.2.1	**Shutdown or Startup**	**Shutdown or Startup**	0
	Normal shutdown or startup shall be under direct manual control; however, the M-MIS Designer shall evaluate the automation of portions of the operations which the analysis of the functions and tasks shows will require continuous operator attention for significant periods.	Reactor shutdown or startup also involves substantial activities throughout the plant. The loss of the services of a control room operator because of operation of the control rods may not be consistent with efficient utilization of the plant staff and may impact availability.	0
7.5.2.2	**Testing Operations**	**Testing Operations**	0
	The design process for the BWR Rod Control system M-MIS shall include an analysis of the functions and tasks involved in the periodic testing of scram time. Special provisions to assure this testing can be accomplished accurately, reliably, and expeditiously shall be provided including automation of some parts of the control action and automatic data collection and reduction.	Scram time testing provides information to identify system performance degradation; however, it can be time consuming.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.5.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the BWR Rod Control System shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	These systems provide the major inputs to determine rod control automatic action.	0
	• The operation of the Reactor Protection System;		0
	• The information from the Neutron Monitoring System.		0

Paragraph No.	Requirement	Rationale	Rev.
7.6	**PWR ROD CONTROL SYSTEM M-MIS**	**PWR ROD CONTROL SYSTEM M-MIS**	0
7.6.1	**Functions**	**Functions**	0
	The M-MIS for the PWR Rod Control System shall provide the monitoring and control necessary to position the control rods so that the magnitude and distribution of the fission energy production in the core is within acceptable limits for the time in core life and the plant conditions.	This is consistent with current practice.	0
7.6.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	Normal Shutdown and startup shall be under direct manual control; however, the M-MIS Designer shall evaluate the automation of portions of the operations which analysis of the functions and tasks shows will require continuous operator attention for significant periods.	Reactor shutdown and startup also involves substantial activities throughout the plant. The loss of the services of an operator because of operation of the Rod Control System may not be consistent with efficient and effective utilization of the plant staff and may impact availability.	0
7.6.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the PWR Rod Control System shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	These systems provide the major inputs to determine rod control automatic action.	0
	• The operation of the Reactor Protection System;		0
	• The operation of the Chemical and Volume Control System;		0
	• The information from the Neutron Monitoring System.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.7	**BWR REACTOR COOLANT SYSTEM M-MIS**	**BWR REACTOR COOLANT SYSTEM M-MIS**	0
7.7.1	**Functions**	**Functions**	0
	The M-MIS for the BWR Reactor Coolant System shall provide the monitoring and control necessary:	This allocation of functions is consistent with current practice.	0
	• To adjust the reactivity effect of boiling in the core so that reactor power level and distribution are within limits;		0
	• To maintain the pressure in the Reactor Coolant System within limits;		0
	• To maintain the reactor coolant inventory in the Reactor Coolant System within appropriate limits;		0
	• To remove energy produced in the reactor core both during normal power operation and when the reactor is shutdown;		0
	• To produce adequate quantities of steam at the proper pressure and moisture content and to provide it to the main steam lines.		0
	• To avoid operation at conditions of flow and power which may be unstable.		0
	• To avoid overfilling the reactor vessel.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.7.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS for the BWR Reactor Coolant System shall provide for the necessary functions to be accomplished without direct operator attention. However, adequate monitoring means and controls shall be provided so that it is practical for the operators to manually control the functions if problems develop in the automatic control.	It is inconsistent with the staffing of the main control room to have an operator normally devoted to the BWR Reactor Coolant System operation. Practical manual backup is needed to assure a minimum impact on availability of automatic control system problems.	0
7.7.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the BWR Reactor Coolant System shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	The Reactor Coolant System forms a major link in the energy transport process. Its operation must be fully integrated so that a mismatch of energy flow and a serious plant upset does not result.	0
	• The operation of the Rod Control system;		0
	• The operation of the Main and Extraction Steam System;		0
	• The operation of the Feedwater and Condensate System;		0
	• The operation of the Main Turbine.		0

Paragraph No.	Requirement	Rationale	Rev.
7.8	**PWR REACTOR COOLANT SYSTEM M-MIS**	**PWR REACTOR COOLANT SYSTEM M-MIS**	0
7.8.1	**Functions**	**Functions**	0
	The M-MIS for the PWR Reactor Coolant System shall provide the monitoring and control necessary:	This allocation of functions is consistent with current practice. These functions include specialized monitoring such as PWR reactor pressure vessel instruments (Chapter 4, Section 6) and PWR core outlet instrumentation (Chapter 4, Section 7).	0
	• To maintain the pressure in the Reactor Coolant System within appropriate limits;		0
	• To maintain an adequate inventory of reactor coolant in the Reactor Coolant System;		0
	• To remove the heat produced in the reactor core without exceeding appropriate limits, including operation at power and when shutdown.		0
7.8.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS for the PWR Reactor Coolant System shall provide for the necessary functions to be accomplished without direct operator attention. However, adequate monitoring means and controls shall be provided so that it is practical for the operators to manually control the functions if problems develop in the automatic control.	It is inconsistent with the staffing of the main control room to have an operator normally devoted to the PWR Reactor Coolant System operation. Practical manual backup is needed to assure a minimum impact on availability of automatic control problems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.8.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the PWR Reactor Coolant system shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	The Reactor Coolant System forms a major link in the energy transport process. Its operation must be fully integrated so that a mismatch of energy flow and a serious plant upset does not result.	0
	• The operation of the Rod Control System;		0
	• The operation of the Chemical and Volume Control System;		0
	• The operation of the Steam Generator System.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.9	**PWR CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS) M-MIS**	**PWR CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS) M-MIS**	0
7.9.1	**Functions**	**Functions**	0
	The M-MIS for the CVCS shall provide the monitoring and control necessary:	This allocation of functions is consistent with current practice.	0
	• To maintain the boron concentration in the reactor coolant at the value necessary to ensure that the core reactivity and, consequently, its energy production, can be adequately controlled;		0
	• To maintain an adequate inventory of reactor coolant in the Reactor Coolant System;		0
	• To maintain the chemistry of the reactor coolant within an acceptable range.		0
7.9.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The CVCS M-MIS shall specifically provide for the detailed requirements on operating modes for the volume control tank (VCT) and pressurizer level controls in Section 6.5 of Chapter 3. This includes:	The specific requirements unique to the control and monitoring for the CVCS are covered in Chapter 3 and need not be repeated in Chapter 10.	0
	• Automatic VCT level control in normal operation;		0
	• Semi-automatic boronation and dilution on operator initiation;		0
	• Manual backup capability;		0
	• Automatic realignment of charging pump suction on low VCT level;		0
	• Automatic letdown and charging flow control in normal operation.		0

Paragraph No.	Requirement	Rationale	Rev.
7.9.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the CVCS shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	The CVCS provides a major link between the Reactor Coolant System and a number of other major plant systems. The integration and coordination of its M-MIS with those of other systems is an important part of the M-MIS Designer's responsibility.	0
	• The control of reactor power level by the control rods;		0
	• The control of the Reactor Coolant System pressure including operation of relief valves;		0
	• The control of the Boron Recycle System;		0
	• The monitoring provided by the Process Sampling System.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.10	**PROCESS SAMPLING SYSTEM M-MIS**	**PROCESS SAMPLING SYSTEM M-MIS**	0
7.10.1	**Functions**	**Functions**	0
	The M-MIS for the Process Sampling System shall provide the control and monitoring necessary:	This function allocation is consistent with Chapter 3, Section 7.	0
	• To remove representative samples from various selected plant fluid and gas systems;		0
	• To determine the conditions in the process streams from various selected plant fluid and gas systems.		0
7.10.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
7.10.2.1	**Sampling**	**Sampling**	0
	Sampling from systems shall be manually initiated locally; however, to facilitate regular or periodic monitoring, an operator aid shall be provided to ensure that times and periodicity of the samples are met. Suitable interlocks shall be provided or automatic sequencing of sampling activity shall be provided to ensure that operator errors in taking samples do not result in loss of availability.	Many samples must be performed on a regular basis, omission of samples or irregularity can reduce the quality and timeliness of the information. Sampling is a service function, it would be inconsistent with the overall availability goals of the ALWR to permit sampling errors to lead directly to a loss of plant output.	0
7.10.2.2	**Process Stream Monitoring**	**Process Stream Monitoring**	0
	The continuous or highly repetitive monitoring of process streams shall not require operator initiation or actions. The data shall be made available in a form which is immediately usable to the operators or plant staff, i.e., manual data reduction shall not be required if the operators are expected to act on the information in the short term. When a process sampling result requires automatic action which results in the shutdown or reconfiguration of a system, this shall be annunciated to the operators.	It would be inconsistent with the manning to be provided for the main control room, to require operator action to carry out the continuous or highly repetitive monitoring of process streams. However, process streams which do not meet requirements must be brought to the operators' attention, particularly if an automatic action has, or should have resulted.	0

Paragraph No.	Requirement	Rationale	Rev.
7.10.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Process Sampling System shall be integrated and coordinated with the M-MIS for the systems in which the process streams are monitored and those systems from which samples are obtained as required in 7.2.4	Although the process Sampling System services most of the plant systems, direct integration would be intended to be limited to those which lead to an automatic action. In most other cases the integration and coordination would be largely affected by deliberate operator action.	0
7.11	**PWR BORON RECYCLE SYSTEM M-MIS**	**PWR BORON RECYCLE SYSTEM M-MIS**	0
7.11.1	**Functions**	**Functions**	0
	The M-MIS shall provide the monitoring and control necessary to process liquid from the reactor coolant and provide recycle recycled makeup water and boric acid of adequate chemistry for reuse in the Reactor Coolant System.	This M-MIS function is consistent with Chapter 3.	0
7.11.2	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Boron Recycle System shall be integrated and coordinated with the M-MIS for other plant systems as required in 7.2.4. This shall include particular consideration of:	Although the Boron Recycle System fulfills a service function, i.e., it is not part of the main energy transport process, it must be integrated to the extent necessary to support the other systems. The direct integration with other plant systems should be a minimum.	0
	• The operation of the Chemical and Volume Control System to control Reactor Coolant System inventory.		0
	• The operation of the Radioactive Waste System.		0
	• The operation of the auxiliary steam system and component cooling water system for the operation of degasifiers and evaporators.		0

Paragraph No.	Requirement	Rationale	Rev.
7.12	**BWR REACTOR WATER CLEAN UP (RWCU) SYSTEM M-MIS**	**BWR REACTOR WATER CLEAN UP (RWCU) SYSTEM M-MIS**	0
7.12.1	**Functions**	**Functions**	0
	The M-MIS for the RWCU System shall provide the monitoring and control necessary:	The M-MIS functions are consistent with Chapter 3 and current practice.	0
	• To remove reactor coolant and thereby maintain the proper inventory in the reactor vessel primarily during startup and shutdown;		0
	• To maintain the chemistry of the reactor coolant within an acceptable range.		0
7.12.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
7.12.2.1	**Startup and Shutdown**	**Startup and Shutdown**	0
	The RWCU System M-MIS shall provide for the startup and shutdown of the system from the main control room. Operations associated with the filter/demineralizers shall be from a local station outside the main control room.	This is consistent with Section 9 of Chapter 3.	0
7.12.2.2	**Normal Operations**	**Normal Operations**	0
	When the plant and the RWCU System are operating normally, the main control room operators shall be able to monitor the proper operation of the RWCU; however, their continuous attention shall not be required. The operation of the RWCU System filter/demineralizers shall normally be from a local control station. Precoating and resin discharge operations shall be automated to the degree necessary to provide adequate water chemistry control. Other system operation shall be from the main control room. Controls necessary in the main control room for the RWCU M-MIS shall be determined by the analysis required in Section 3.1.3.3.	The RWCU System is used for discharge of reactor coolant to the condenser hotwell or to radwaste during normal plant startup and shutdown. These operations are reactor vessel level control functions and, hence, must be performed by the reactor operator from the main control room, not from a local control station. During accident conditions, the RWCU system can be used to supplement reactor pressure control and level control. Significant effort by the operator is not required during normal plant operation. Automation of some operations has been found to improve water chemistry control.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.12.2.3	**Reconfiguration**	**Reconfiguration**	0
	The isolation of the system shall be automatically effected by the M-MIS in the event of containment isolation if automatic monitoring detects a significant leak in the RWCU System piping or if the Standby Liquid Control System (8.7) is initiated.. Operations associated with the filter/demineralizers, such as changing of resin, precoating, isolation, etc., shall only be accomplished from the local control station.	Automation of the isolation is needed to avoid large discharges of reactor coolant outside the containment and to avoid negating the effect of the Standby Liquid Control System.	0
7.12.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the RWCU System shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This shall include particular consideration of:	Although the RWCU System fulfills a service function, i.e., it is not part of the main energy transport process, it must be integrated to the extent necessary to support the other systems. The direct integration with other plant systems should be a minimum.	0
	• The control of inventory in the reactor by the Feedwater and Condensate System,		0
	• The monitoring provided by the Process Sampling System;		0
	• The monitoring for leaks by the Reactor Coolant Leak Detection System.		0
	• The operation of the Standby Liquid Control System.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.13	**PWR STEAM GENERATOR SYSTEM M-MIS**	**PWR STEAM GENERATOR SYSTEM M-MIS**	0
7.13.1	**Functions**	**Functions**	0
	The M-MIS for the Steam Generator System shall provide the monitoring and control necessary:	The steam generator in a PWR forms a major part of the process chain which transports the core energy. This function allocation is consistent with current practice.	0
	• To generate adequate quantities of steam to support the transfer of the energy produced in the reactor core to the Main Steam and Turbine-Generator Systems. In particular, this involves maintaining an adequate inventory (and level) in the steam generator so that the heat is removed from the reactor coolant, so that steam of the proper conditions (pressure and moisture) can be provided to the main turbine-generator, and so that overfilling a steam generator can be prevented.		0
	• To remove reactor decay heat under some shutdown conditions. In this instance steam will be generated as for power operation; however, the quantity will be much less and it will not be used in the main turbine. Under these conditions the major function of the M-MIS shall be to ensure that reactor core decay heat is adequately transported to a heat sink, i.e., the condenser or to the atmosphere.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
7.13.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
7.13.2.1	**Startup Operation**	**Startup Operation**	0
	The Steam Generator System M-MIS shall provide for manual operation largely from the main control room for the early stages of plant startup; however, as soon as sufficient steam is being generated to require substantial operator attention to maintain an adequate inventory (level) in the steam generator, level control shall be automatic. This shall apply to operation on both startup feed pumps or the main feed pumps.	Manual maintenance of proper steam generator level at low power levels has been a burden on plant operators. It takes their attention from other startup operations which cannot be practically automated. Operator errors from this source have occurred.	0
7.13.2.2	**Normal Operation**	**Normal Operation**	0
	When the plant is operating normally at power the Steam Generator System M-MIS shall provide for automatic operation of the inventory (level) control. However, the M-MIS shall also provide adequate monitoring information and control stations so that manual operation from the main control room is also practical.	The control of steam generator inventory (level) manually at power would require essentially full time attention of an operator. This would not be consistent with the staffing for the main control room. The backup of manual control would be used to avoid unnecessary plant shutdown and loss of availability if there were problems in the automatic system.	0
7.13.2.3	**Shutdown or Reconfiguration**	**Shutdown or Reconfiguration**	0
	Normal shutdown of the steam generators both planned and unplanned, e.g., from a reactor and turbine trip, inventory (level) shall be automatic in the sense that at no time shall it be required that a main control room operator devote continuous attention to steam generator control. Adequate monitoring shall be provided for the operator to be aware of the progress of the shutdown and it shall be ensured that the operator has adequate information and controls to take over the manual control of inventory if the automatic control is not adequately maintaining the steam generator conditions.	Many of the other responsibilities of the control room operators during a shutdown, particularly if unplanned, cannot be practically automated. Unless level control is automated at least one operator would have to devote full time and attention to the level control. This would not be compatible with the control room staffing and would impair the operators' ability to cope with problems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
7.13.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Steam Generator System shall be integrated and coordinated with the M-MIS for other plant systems as required in 7.2.4. This shall include particular consideration of:	As an essential part of the main energy transport process, both at power and when shutdown, the steam generator control has a significant effect on other major systems. A major part of the success of the M-MIS design depends on how well the steam generator control is integrated and coordinated with the other plant systems.	0
	• The operation of the Emergency Feed System;		0
	• The operation of the Feed and Condensate System;		0
	• The operation of the Reactor and the Reactor Coolant System;		0
	• The operation of the Main and Extraction Steam System.		0
7.14	**REACTOR COOLANT SYSTEM LEAK DETECTION M-MIS**	**REACTOR COOLANT SYSTEM LEAK DETECTION M-MIS**	0
7.14.1	**Functions**	**Functions**	0
	The M-MIS for Reactor Coolant Leak Detection shall provide the monitoring necessary to assure that the Reactor Coolant System leakage is within acceptable limits.	The detection of Reactor Coolant System Leakage is essential to the justification of "leak-before-break."	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.14.2	**Monitoring Strategies**	**Monitoring Strategies**	0
	The Reactor Coolant Leak Detection M-MIS shall monitor the quantities and parameters necessary to determine the magnitude and, to the degree practical, the location of reactor coolant leakage, including steam generator leakage. This monitoring shall be automatic and the data sorted as a permanent record. The M-MIS shall provide for the reduction of these data and the presentation to operators on essentially a continuous basis using an operator aid (display) which summarizes the current estimated leak rate and other indications which indicate possible reactor coolant leakage, for example:	Leakage from the reactor coolant system which cannot be located and proved to not be through cracks in the reactor coolant boundary will require shutdown even though the leakage is well within the makeup ability. It is intended that the M-MIS Designer provide a comprehensive system which has adequate discrimination to detect real leaks but still avoid unnecessary loss of plant availability.	0
	• Reactor coolant inventory balance results (including such related quantities as makeup flow and volume control tank levels);		0
	• Results of radiation monitoring or process streams and areas;		0
	• Flow to sumps and drain tanks;		0
	• Containment cooler condensate flows;		0
	• Safety/Relief valve leakage indications;		0
	• Indications of leakage into other system (e.g., high surge tank levels in cooling water systems);		0
	• Acoustic monitoring.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
7.14.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for Reactor Coolant Leak Detection shall be integrated and coordinated with the M-MIS of other plant systems as required in 7.2.4. This integration and coordination shall be such that the leakage results presented to the operators are appropriately corrected for plant events so that there is little potential for misleading results being provided to the operators, e.g., the impact of plant and system transients on inventories must be properly considered in the M-MIS design.	The detection of leakage from the Reactor Coolant System is a serious concern and can lead to shutdown of the plant. To avoid the impact of false indications on plant availability, the M-MIS for leak detection must provide highly reliable information to the operators.	0

8 REACTOR PROTECTION AND SAFETY SYSTEMS M-MIS REQUIREMENTS 0

8.1 PURPOSE AND SCOPE 0

The reactor protection and safety group of systems includes the safety systems which are covered by Chapter 5 of the ALWR Requirements Document. In addition to the M-MIS for those individual systems, this section covers the requirements for the M-MIS which provides reactor protection. This section includes requirements for directly associated control and instrumentation equipment, e.g., sensors, indicators, control devices, data transmission and processing equipment, and alarms. Only requirements which relate to use in the reactor protection and safety systems are covered, general requirements on the use of these types of equipment are addressed in other sections of Chapter 10. The mechanical and electrical components which make up the individual systems, e.g., pumps, motors, tanks, piping, valves, power cables, and switch-gear, are covered in other chapters of the ALWR Requirements Document. 0

This section of Chapter 10 covers only a portion of the M-MIS requirements for these systems. Many of the requirements on the plant systems in other chapters, particularly Chapters 1 and 5, are directly applicable to the M-MIS for this group of systems; however, these will not generally be repeated unless they need to be expanded to clarify their applicability to the M-MIS or need special emphasis. In particular, this section provides requirements which cover: 0

- The allocation of the M-MIS functions for this group of systems among the M-MIS for the individual plant systems; 0
- The identification of the physical boundaries and interfaces of the M-MIS for the purpose of defining the scope of requirements for this group of systems; 0
- The strategies for control and monitoring (for example, manual or automatic and local or remote) which shall be followed for various operating modes of the individual plant systems, e.g., system startup, normal operation, shutdown or reconfiguration, and testing; 0
- The integration of the M-MIS for the individual systems and overall plant M-MIS with the M-MIS of other plant systems and the coordination of their operation. 0

8.2 GENERAL REQUIREMENTS FOR REACTOR PROTECTION AND SAFETY SYSTEMS GROUP M-MIS 0

8.2.1 Functions 0

The M-MIS for the reactor protection and safety group of systems shall provide the monitoring and control necessary to carry out the required plant and system functions defined in Chapters 1 and 5. 0

The M-MIS Designer shall allocate the various M-MIS functions among the Reactor Protection System and the individual safety systems M-MIS such that the required functions and tasks as determined in the design process (sections 3.1.3.3) can be satisfactorily accomplished. This section provides an initial allocation of these M-MIS functions; however, it is a primary responsibility of the M-MIS Designer to integrate and coordinate the operation of all M-MIS so that all functions are adequately performed. Figure 10.8-1 illustrates how the major functions of the systems in this group have been allocated to the individual plant systems for the purposes of this Requirements Document. Other allocations of the functions may be used, if they can be shown to improve significantly the plant's operability, simplicity, or reliability and if they are fully in accordance with the M-MIS design process requirements in Section 3, particularly the requirements for a functional design approach (3.1.1.1) and the analysis of functions and tasks (3.1.3.3). 0

The M-MIS functions for the reactor protection and safety systems are divided into two major categories (see Chapter 5): 0

- Functions related to preventing core damage; 0
- Functions related to mitigating the effects if core damage were to occur. 0

Events may occur which result in some core damage despite the prevention functions being accomplished and as a result the mitigation functions will be implemented. For such events the M-MIS shall still address the damage-prevention functions to the maximum practical degree to limit the amount of core damage. 0

8.2.1.1 Control and Monitoring to Limit Reactor Power Level 0

As part of the general function to prevent core damage, the M-MIS design shall provide the control and monitoring necessary to limit the reactor energy production to a rate which does not result in core damage. This function is accomplished largely by the Reactor Protection System which monitors the power level and other plant parameters and initiates rod motion (e.g., trip) to reduce the core reactivity. For very long term conditions, means are provided to introduce soluble poisons into the reactor to reduce the reactivity and the energy production. 0

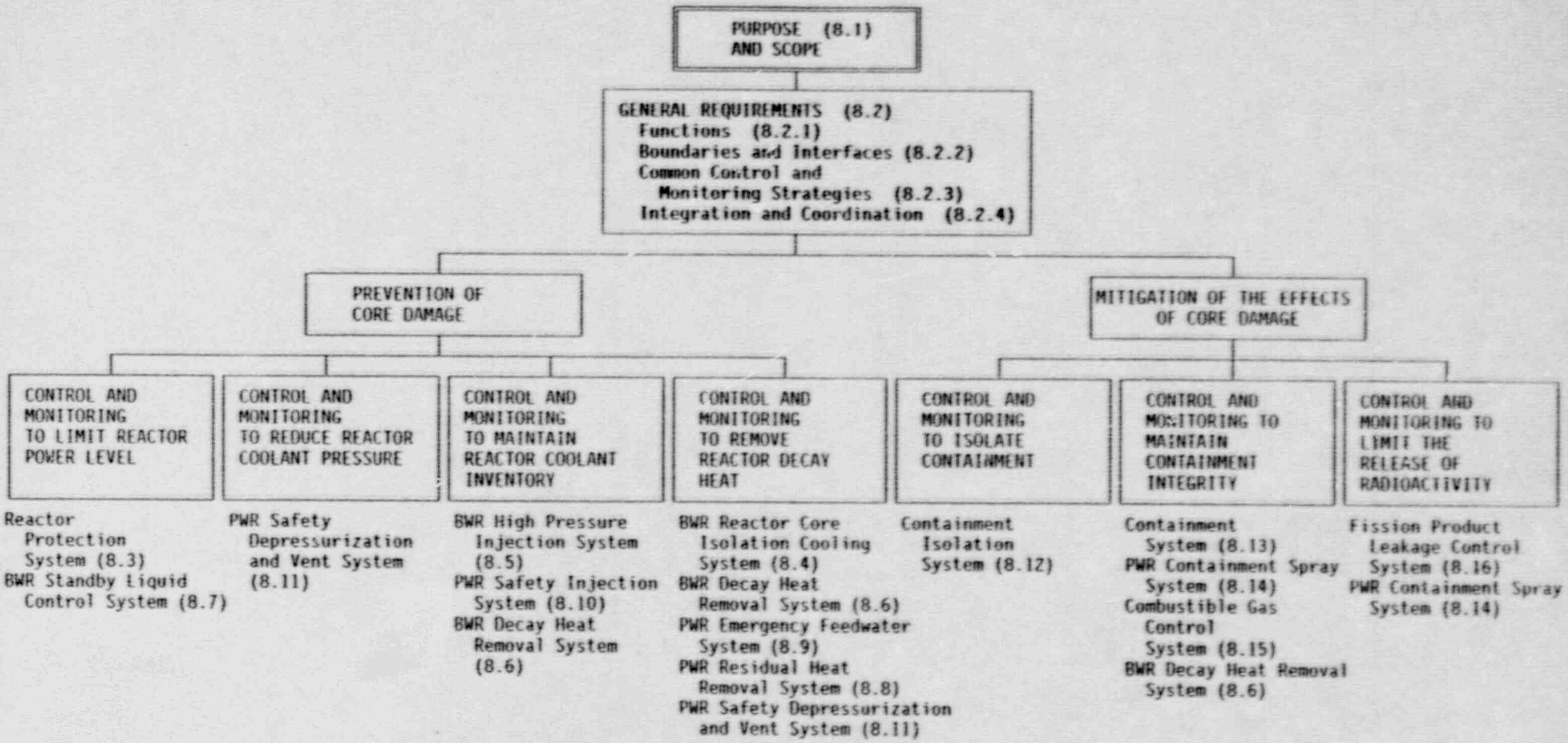

PURPOSE (8.1) AND SCOPE
GENERAL REQUIREMENTS (8.2)
Functions (8.2.1)
Boundaries and Interfaces (8.2.2)
Common Control and Monitoring Strategies (8.2.3)
Integration and Coordination (8.2.4)
PREVENTION OF CORE DAMAGE
MITIGATION OF THE EFFECTS OF CORE DAMAGE
CONTROL AND MONITORING TO LIMIT REACTOR POWER LEVEL
CONTROL AND MONITORING TO REDUCE REACTOR COOLANT PRESSURE
CONTROL AND MONITORING TO MAINTAIN REACTOR COOLANT INVENTORY
CONTROL AND MONITORING TO REMOVE REACTOR DECAY HEAT
CONTROL AND MONITORING TO ISOLATE CONTAINMENT
CONTROL AND MONITORING TO MAINTAIN CONTAINMENT INTEGRITY
CONTROL AND MONITORING TO LIMIT THE RELEASE OF RADIOACTIVITY
Reactor Protection System (8.3)
BWR Standby Liquid Control System (8.7)
PWR Safety Depressurization and Vent System (8.11)
BWR High Pressure Injection System (8.5)
PWR Safety Injection System (8.10)
BWR Decay Heat Removal System (8.6)
BWR Reactor Core Isolation Cooling System (8.4)
BWR Decay Heat Removal System (8.6)
PWR Emergency Feedwater System (8.9)
PWR Residual Heat Removal System (8.8)
PWR Safety Depressurization and Vent System (8.11)
Containment Isolation System (8.12)
Containment System (8.13)
PWR Containment Spray System (8.14)
Combustible Gas Control System (8.15)
BWR Decay Heat Removal System (8.6)
Fission Product Leakage Control System (8.16)
PWR Containment Spray System (8.14)

FIGURE 10.8-1

ALWR M-MIS FOR REACTOR PROTECTION AND SAFETY SYSTEMS

Paragraph No.	*Requirement*	*Rev.*
8.2.1.2	**Reactor Coolant Pressure Reduction**	0
	As part of the general function to prevent core damage, the M-MIS design shall provide the control and monitoring necessary to reduce the pressure in the Reactor (and Reactor Coolant System) to a value appropriate for the plant conditions. For most conditions, pressure control and monitoring is provided by the Reactor Coolant System M-MIS (see Section 7). For the safety-related function of appropriately reducing the Reactor Coolant System pressure, an M-MIS shall be provided which is independent of the Reactor Coolant System M-MIS.	0
8.2.1.3	**Maintain Reactor Coolant Inventory**	0
	As part of the general function to prevent core damage, the M-MIS shall provide the control and monitoring necessary to maintain an adequate inventory of reactor coolant in the Reactor and Reactor Coolant System. For most conditions, the reactor coolant inventory shall be controlled and monitored by the Reactor Coolant System M-MIS and the Reactor Coolant System Leak Detection M-MIS. For the safety-related function of maintaining reactor coolant inventory, a separate M-MIS shall be provided to assure that the separate safety features and systems included to maintain inventory will function satisfactorily.	0
8.2.1.4	**Remove Reactor Decay Heat**	0
	As part of the general function to prevent core damage, the M-MIS shall provide the control and monitoring to assure that the decay heat produced in the reactor core is removed without exceeding temperatures at which core damage would occur. This function can be accomplished by several diverse, independent systems; the M-MIS shall maintain the independence of these systems by appropriate segmentation and separation.	0
8.2.1.5	**Isolate Containment**	0
	As part of the general function to mitigate the effects of core damage, the M-MIS design shall provide the monitoring necessary to establish that containment isolation should be initiated, provide the control to accomplish the isolation, and provide the monitoring to confirm the completion and maintenance of the isolation.	0

8.2.1.6 Maintain Containment Integrity 0

As part of the general function to mitigate the effects of core damage, the M-MIS shall provide the control and monitoring necessary to maintain the integrity of the boundary of the containment. This includes providing cooling of the containment and preventing excessive pressures which would fail the structure or increase the leakage. The M-MIS shall also provide a means to monitor parameters which affect the integrity of the containment, e.g., suppression pool level and temperature, when no core damage has occurred so that the containment could perform its safety function if it were called upon. 0

8.2.1.7 Limit the Release of Radioactivity 0

As part of the general function to mitigate the effects of core damage, the M-MIS design shall provide the monitoring necessary to identify the potential for release of radioactivity and the control necessary to limit the release to an acceptably small amount. 0

8.2.2 Boundaries and Interfaces 0

The physical boundaries of the individual systems which make up the safety systems are defined in the appropriate sections of Chapter 5. The boundaries of the M-MIS for the group of systems shall be consistent with those physical boundaries of the plant systems; however, they shall also encompass the M-MIS hardware, which includes: 0

- Instrument sensors; 0
- Data transmission equipment; 0
- Data processing equipment; 0
- Controllers and logic devices; 0
- Operator interface hardware (e.g., controls, indicators); 0
- Software to support M-MIS hardware. 0

The interfaces of the individual systems which make up the safety systems are defined in the appropriate sections of Chapter 5. The interfaces of the M-MIS for the group of systems shall be consistent with those plant system interfaces. The M-MIS interfaces shall be formally defined and controlled in accordance with the M-MIS Design Plan (Section 2.1.2.4). The M-MIS Designer shall define and control other interfaces among the various M-MISs and other plant systems as may be necessary to integrate and coordinate the operation of the plant systems even though these interfaces are not defined as physical interfaces in Chapter 5. 0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.2.3	**Common Control and Monitoring Strategies for Reactor Protection and Safety Systems**	**Common Control and Monitoring Strategies for Reactor Protection and Safety Systems**	0
	The M-MIS Designer shall use a consistent control and monitoring strategy for all the parts of the M-MIS for this group of systems except as modified by individual system M-MIS requirements. This common control strategy shall also be consistent with that used for the remainder of the M-MIS.	A consistent control strategy supports the overall objective of a high level of standardization for the ALWR. It also tends to simplify training of operators and maintenance technicians. For example, consistent control strategies tend to lead to similar controls, displays, and control stations.	0
8.2.3.1	**Startup and Actuation Operation**	**Startup and Actuation Operation**	0
	The M-MIS for the protection and safety systems shall normally provide for automatic startup or actuation. That is, the condition which requires the protection or safety action shall initiate the appropriate system action without operator action. The operators, however, shall also be able to manually initiate the system action. The initiation of a protection or safety system shall be alarmed in the main control room and the main control room operators shall be provided with adequate information to confirm that: • The actuation was necessary, i.e., was in response to an actual plant need; • The actuation resulted in the expected system action, e.g., pumps started, valves opened, etc.	The protection and safety systems will not be called upon to function unless the normal plant systems are no longer capable of carrying out their functions. This may be a result of equipment failure or human error. Under these conditions, it is inconsistent to rely on the operators to provide the actuation. There are, however, a number of systems for which deliberate, operator directed initiation is completely adequate. In those cases automatic actuation would increase plant complexity and raises the potential of inadvertent actuation and the disruption of plant operation. The automatic actuation of one of these safety systems is a major change in plant conditions and the operators must be made fully aware of the action. In these cases, the operators provide a valuable backup to the automatic initiation. The operators also need the capability to initiate the safety systems when they detect a need for such action, i.e., they should not have to wait for the automatic initiation. It is expected that operator aids (see Section 3.4.5) will be provided to facilitate the operator's confirmation tasks.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
8.2.3.2	**Normal Operation**	**Normal Operation**	0
	The M-MIS for the protection and safety systems shall normally provide for the system to continue to operate automatically after actuation for at least 20 minutes. After that time some manual actions may be permitted; however, essentially continuous manning to carry out a protection or safety function for extended periods of time, e.g., hours or days, shall not be required.	The time before manual action can be assumed is based on Chapter 1 and Chapter 5. It is the intent of this requirement that the operators not be occupied full time running the safety systems after an actuation so that they will have time to adequately assess the overall situation and cope with the inevitable complicating features which almost always accompany a real event.	0
8.2.3.3	**Shutdown or Reconfiguration Operation**	**Shutdown or Reconfiguration Operation**	0
	The M-MIS for these protective and safety systems shall normally provide for the shutdown (or return to standby) to be accomplished manually by the operators. The M-MIS shall provide the minimum interlocks necessary to assure that the manual shutdown or reconfiguration of protection or safety systems takes place only when essential to prevent increasing the seriousness of an event. Automatic shutdown or reconfiguration of systems to prevent equipment damage should be minimized, i.e., priority shall be given to maintaining the safety function.	The shutdown or reconfiguration (return to standby or reset) of a protective system is a deliberate action which should be under operator control. Interlocks are required; however, if overdone, they can prevent sensible actions and make recovery very difficult. The design philosophy applied to normal plant systems often results in equipment shutdown on a conservative basis which emphasizes equipment damage. However, for safety systems, damage to components must be secondary to maintaining the safety function. For example, operation of a pump with some cavitation may well be preferable to tripping the pump and losing all flow.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
8.2.3.4	**Testing Operation**	**Testing Operation**	0
	The M-MIS for the protection and safety systems shall normally provide for testing to be initiated at the direction of the operator, but the testing itself to be largely automatic. For portions of the M-MIS of these systems which can be tested without activation of system components, the incorporation of automatic testing shall be evaluated by the M-MIS Designer. Where automatic testing is impractical, the M-MIS Designer shall provide operator aids or other features to minimize the potential for operator errors. In no case shall the testing impair the ability to carry out the protection or safety function. Where practical, the system shall automatically realign itself when its action is called for while on test.	The testing of these systems often must be done with the plant at power. Errors in testing can have effects on plant operation and loss of availability. Early detection of problems in these systems is also essential to maintaining the plant in operation. Section 3.6 contains a number of specific requirements to enhance the testability of the ALWR. It is particularly important that the testing of the protective and safety systems is consistent with those test requirements. It is intended that advanced, self-testing M-MIS designs be used to reduce the need for manual testing operations and allow enhanced readiness of these systems to be achieved without burdening the operators or increasing the risk of operator error.	0
8.2.4	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS designs for the systems in this group shall be integrated and coordinated so that the overall plant performance and functional requirements as well as those of individual systems are met. Those requirements are found in Chapter 1 and in other chapters of the ALWR Requirements document, particularly Chapter 5. In addition, the M-MIS Designer shall coordinate the design features with other parts of the M-MIS, especially those portions of the M-MIS which control the energy production (e.g., Section 7 of Chapter 10). The M-MIS Designer shall explicitly coordinate the M-MIS for the protection and safety systems with the M-MIS for the electric power supply systems (Chapter 11) so that electric power supply appropriate to the importance of the functions is assured, particularly where systems such as the RCIC and EFW Systems are required to perform functions without ac power.	Although the requirements for the individual systems define the functions and interfaces, it is the basic responsibility of the M-MIS Designer to connect the various systems and their requirements in a sensible and efficient manner. The specific methods used to connect the operation of the various systems and the logic are to be selected by the M-MIS Designer. The ALWR Requirements Document has specifically avoided defining how this is to be accomplished. It is intended that the M-MIS Designer not be constrained to current practice and be encouraged to develop strategies for control which consider the many interactions among the various systems.	0

Paragraph No.	Requirement	Rev.
8.3	**REACTOR PROTECTION SYSTEM (RPS)**	0
8.3.1	**System Definition**	0
8.3.1.1	**Scope**	0
	This section, together with the other applicable sections of this chapter, provides the requirements for the RPS for the ALWR plant.	0
	The RPS includes the following control and instrumentation equipment:	0
	• The sensors which generate the signals used by the RPS;	0
	• The processing equipment for the signals used by the RPS;	0
	• The data transmission equipment for the signals used by the RPS;	0
	• The equipment (and software) used to effect the protection logic and generate the signals necessary to carry out the protection action;	0
	• The equipment including cables, trip breakers, and relays used to produce the protective action;	0
	• The test or diagnostic equipment needed to maintain the RPS in a state of readiness, confirm its operational status, or determine the type and location of faults.	0
	The mechanical and electrical components which effect the protective action, primarily the motion of control rods, are covered in Chapter 4 of the ALWR Requirements Document.	0
	The RPS is an integral part of the systems provided to prevent core damage. The other systems specified in Chapter 5 for prevention of core damage depend heavily on the RPS to shutdown the reactor and thereby reduce the amount of heat produced to more manageable levels.	0
8.3.1.2	**Functions**	0
	The RPS shall monitor key plant parameters and, based on those parameters, determine whether the reactor must be shutdown to prevent core damage. If the RPS determines the reactor must be shutdown, the RPS shall provide control signals to the reactor Rod Control Drive System to reduce the reactivity (and power production) by inserting control rods.	0
	These functions are all safety-grade.	0

Paragraph No.	*Requirement*	*Rev.*
8.3.1.3	**Interfaces**	0
	The RPS interfaces with the following systems:	0
	• The Neutron Monitoring System provides information on the magnitude and distribution of neutron power in the reactor core which is used as input to the RPS logic and used to confirm its effectiveness, if it acts.	0
	• The Reactor and Reactor Coolant System provides for sensors which generate the signals used as input to the RPS logic.	0
	• The Main Steam, the Main Turbine-Generator Systems, and other plant systems may provide for sensors which generate the signals used as input to the RPS logic.	0
	• The Control Rod Drive System provides control rod motion in response to the commands generated by the RPS logic and provides signals to confirm its effectiveness, if it acts.	0
	• The Electric Power Distribution System provides the electric power necessary to operate the RPS from suitably vital, redundant, and diverse sources.	0
	• The Heating, Ventilating, and Air Conditioning System provides environmental control for the RPS equipment.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.3.2	**Performance**	**Performance**	0
8.3.2.1	**Initiation Signals**	**Initiation Signals**	0
	The M-MIS Designer shall select the minimum set of plant process variables necessary to provide adequate protection of the reactor core from damage. That is, variables should not be used in the RPS logic to provide anticipatory or diverse trips beyond those needed by the requirements for reliability of the RPS.	The use of a large number of trip signals has been found to increase the number of false trips without materially increasing the protection provided. The intent of this requirement is that the M-MIS Designer justify the set of RPS signals chosen.	0
8.3.2.2	**Completion of Action**	**Completion of Action**	0
	Once the RPS logic initiates action to shutdown the reactor, that action shall proceed to completion.	This is to assure a defined endpoint and is consistent with the practice for protection systems.	0
8.3.2.3	**Reset**	**Reset**	0
	Once the RPS action has resulted in reactor shutdown, manual action with suitable provisions for administrative control shall be required to reset the RPS logic and permit control rod withdrawal.	A reactor trip by the RPS is always an indication of some abnormal condition and investigation of the cause must be completed before rods can be withdrawn.	0
8.3.2.4	**Effect of Failures in RPS on Protection Action**	**Effect of Failures in RPS on Protection Action**	0
	No single failure in the RPS shall prevent or cause the initiation of protection action. A second failure in the RPS shall not prevent the protection action; however, it may result in reactor shutdown. The scope of this double failure requirement is limited to the sensors and actuation portion of the RPS and does not include the reactor trip devices. Furthermore, the applicability of the double failure requirement is limited to the non-test condition of the RPS.	The protection action needs to have priority; however, plant shutdown for a single RPS failure would not be consistent with the ALWR reliability goals. Extension of the double failure requiremant to the reactor trip devices would require additional electro-mechanical equipment. Limiting the applicability of the double failure requirement to the non-test conditions recognizes that additional redundancy is not justified to provide the RPS with double failure capability during brief periods that the actuation logic is undergoing test.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
8.3.2.5	**Coincidence of Signals**	**Coincidence of Signals**	0
	The logic for RPS shall be such that it requires coincidence of two or more channels of the same variable or the same combination of variables to initiate protection action. That is, the coincidence of different variables shall not result in protection action.	This requirement reduces the potential for false actions, and with adequate redundancy of channels for a single variable it should not affect the ability to protect the plant when there is an actual need.	0
8.3.2.6	**Independence of Manual and Automatic Initiation**	**Independence of Manual and Automatic Initiation**	0
	The manual initiation of the protection action shall be independent of the automatic initiation equipment or its protection logic. The scope of this requirement does not include the reactor trip devices.	Since manual initiation of protection is inherently a backup to the automatic protection, manual initiation should not depend on the functioning of the automatic initiation equipment or its logic, since they may not be functional.	0
8.3.2.7	**BWR Backup RPS Action**	**BWR Backup RPS Action**	0
	For BWRs, part of the RPS shall provide the control signals for electric motors which can drive the control rods into the reactor core if the primary scram is not effective. This function shall be provided by a portion of the BWR RPS separate from the portion of the RPS which initiates normal reactor scram. This backup portion of the system shall not use the same sensors as the normal RPS. The backup system need not meet the single failure criterion (8.3.2.4).	This backup scram system is currently required for BWRs because of ATWS concerns (10CFR50.62).	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.3.2.8	**PWR Backup RPS Action**	**PWR Backup RPS Action**	0
	For PWRs, the M-MIS shall provide a diverse, backup reactor trip system which is independent of the normal reactor trip system (from the sensor output to the interruption of power to the control rod drive mechanisms). In lieu of a backup reactor trip system for PWRs, the Plant and M-MIS Designers may provide design margins and design features, such as diversity and redundancy of the normal RPS, so that no backup reactor trip function is required. Irrespective of the approach adopted by the Plant Designer, the basis for this selection shall be documented and reviewed in the design process. This review shall specifically evaluate the impact on reliability and availability of an additional system compared to the potentially increased complexity of alternative designs which do not require a backup reactor trip system.	Backup reactor trip systems are currently required by regulations (10CFR50.62) on only some PWRs. If such backup trip systems increase the complexity of the plant, they may increase the potential for false trips and adversely impact availability; however, a backup reactor trip system may be a better approach if it avoids complicating other plant systems.	0
8.3.2.9	**Testing**	**Testing**	0
	The RPS shall provide for automatic self-testing of as much of the system as is practical. That is, the RPS shall require initiation of testing by the operators only where automatic testing is not practical.	It is particularly important that the RPS be kept in a high state of readiness and that conditions which reduce its resistance to false trips are promptly identified and corrected.	0
8.3.2.10	**Environmental Effects on Equipment**	**Environmental Effects on Equipment**	0
	The RPS shall perform its safety function at the extremes of environmental conditions which may be encountered, including:	The RPS protection functions cannot be compromised. If any of the environment conditions were to jeopardize the RPS functions it could lead to plant outages.	0
	• Normal operation;		0
	• Maintenance;		0
	• Postulated accidents, e.g., LOCA and design basis accidents;		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
	• Losses of electric power, both ac and dc;		0
	• Operation of fire suppression systems such as water sprinklers, Halon, or carbon dioxide systems (this excludes operation with a direct spray of high or low pressure manual fire hoses on RPS equipment).		0
8.3.3	**Configuration**	**Configuration**	0
8.3.3.1	**Location**	**Location**	0
	The RPS equipment shall be located such that local events, e.g., sabotage, would not be able to prevent the RPS from carrying out its protection function. The RPS shall be located entirely within the protected area. Where practical, the segments of the system shall be located so that no more than one segment can be affected by a single event.	The RPS is essential to plant safety, and access by unauthorized personnel should be prevented. Separation of the segments makes it more difficult to disable the system rapidly and without detection.	0
8.3.3.2	**Confirmation of RPS action and Status**	**Confirmation of RPS action and Status**	0
	The main control room operators shall be provided with operator aids (displays) which provide the capability to determine rapidly and unambiguously that: • The RPS action has been initiated; • The RPS action has been completed and, if not complete, what action remains to be accomplished; • The RPS action was based on actual conditions, i.e., it was not a false trip; • The RPS is in a condition of reduced resistance to false actuation.	Although the RPS normally operates without operator attention, its actuation needs the backup of the operator. However, RPS actuation and reactor shutdown will involve a number of duties for the operators. The operator's concern with the condition of the RPS cannot be eliminated, but it should have a minimum impact on the operator who must also be concerned with the other aspects of the shutdown. That is, it should not require a significant time for the operator to assess the RPS status.	0

Paragraph No.	Requirement	Rationale	Rev.
8.3.3.3	**Changes in Set points**	**Changes in Set points**	0
	The system configuration shall provide safeguards against both inadvertent and unauthorized changes in RPS set points. This shall include features to assure that a set point change has proper approval and cannot be made without generating adequate records of the change.	Improper set point adjustment can render the RPS ineffective in providing protection against core damage or can result in false trips even if all the equipment and logic is flawless.	0
8.3.4	**Equipment Requirements**	**Equipment Requirements**	0
	The equipment used in the RPS shall generally be the same as that used in safety systems and other systems which require highly reliable components. Requirements for these components are specified in Section 6 and below.		0
8.3.4.1	**Reactor Trip Breakers**	**Reactor Trip Breakers**	0
8.3.4.1.1	**Review of Experience**	**Review of Experience**	0
	As part of the Review of Experience required in Section 3.1.3.1, the M-MIS Designer shall identify problems associated with the design, operation, maintenance, and testing of existing reactor trip breakers. The M-MIS Designer shall establish functional and design requirements, manufacturing specifications, and a factory testing plan for the ALWR reactor trip devices which specifically address the problems associated with existing reactor trip breakers.	Metal-clad air circuit breakers used as reactor trip devices in existing LWRs have experienced a number of problems, including deficiencies in undervoltage trip attachments, lubricants, manufacturing tolerances, etc. A specific review of these problems should assure that they are not repeated in the ALWR.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.3.4.1.2	**Operating Duty Cycle**	**Operating Duty Cycle**	0
	The M-MIS Designer shall select a reactor trip device which is specifically designed to withstand without degradation the expected number of operations associated with maintenance and testing, as well as actual trips, over the life of the plant.	The metal-clad air circuit breakers used as reactor trip devices in existing LWRs were designed primarily as fault interrupters and not as switching devices. Reactor trip devices are subject to a large number of operations due to the stringent maintenance and testing requirements placed on these safety-related components throughout their installed life. In order to meet the functional and service requirements, the M-MIS Designer may need to supply switching devices for reactor trip which are capable of withstanding a large number of operations and which are separate from the interrupting devices for protection from circuit faults.	0
8.3.4.2	**Manual Reactor Trip Controls**	**Manual Reactor Trip Controls**	0
	Manual controls to initiate the reactor trip shall meet the following requirements: • They shall be readily accessible to the operators and shall be capable of operation by a single operator. • They shall be protected against inadvertent actuation; however, key-locked controls or controls which require an active system or special devices to actuate shall not be used.	The manual trip controls provide the backup to the RPS automatic functions. If these controls are ever used, the situation will be highly stressful and simplicity of operation is essential. Although accidental trips need to be precluded, the operator must not be prevented from effecting a trip when it is needed. These requirements may preclude the use of some types of so-called "soft" controls for manual reactor trip.	0
	• Although multiple controls may be provided to maintain separation and segmentation, an operator shall be able to initiate an effective reactor trip by a simple control action, e.g., a trip shall not require more than a few simple manual actions; it shall not require these manual actions to be done in a complicated sequence or combination; and special training shall not be necessary.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
	• The controls shall be located so that the operator is provided with immediate feedback that he has been successful in initiating the reactor trip.		0
8.4	**BWR REACTOR CORE ISOLATION COOLING (RCIC) SYSTEM M-MIS**	**BWR REACTOR CORE ISOLATION COOLING (RCIC) SYSTEM M-MIS**	0
8.4.1	**Functions**	**Functions**	0
	The M-MIS for the RCIC System shall provide the monitoring and control necessary to assure that the inventory of reactor coolant in the reactor vessel is maintained at a safe level even though normal feedwater is not available. The M-MIS shall support the performance of this function with a complete loss of ac power.	This function allocation is consistent with Section 4.3 of Chapter 5.	0
8.4.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	After automatic initiation, the main control room operators shall be provided with control and monitoring necessary to manually adjust the RCIC flow rate to match decay heat generation.	This is consistent with Section 4.3 of Chapter 5. It provides a capability which experience shows is desirable.	0
8.4.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the RCIC System shall be integrated and coordinated with the M-MIS of other plant systems as required in 8.2.4. This shall include particular consideration of: • The signals for initiation and control from the Reactor Coolant System; • The emergency electric power systems (for the conditions of complete loss of ac power).	It is intended that the signals from other M-MIS to initiate and control the RCIC System be kept to a minimum to enhance the separation of the RCIC System operation from problems in other systems. The RCIC system is designed so that it does not depend on ac power and the M-MIS must be consistent with that requirement.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.5	**BWR HIGH PRESSURE INJECTION (HPI) SYSTEM M-MIS**	**BWR HIGH PRESSURE INJECTION (HPI) SYSTEM M-MIS**	0
8.5.1	**Functions**	**Functions**	0
	The M-MIS for the HPI System shall provide the monitoring and control necessary to inject water into the reactor to maintain the inventory of reactor coolant even though normal feedwater is not available and the RCIC has not been effective in maintaining the inventory.	This allocation of functions is consistent with Section 4.4 of Chapter 5.	0
8.5.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	After the automatic initiation of the HPI System, the M-MIS shall provide automatic, unattended operation to maintain the level in the reactor vessel between predetermined high and low levels.	This is consistent with Section 4.4 of Chapter 5. Since the actuation of the HPI will likely be a result of problems with other systems, it is not prudent to tie up an operator for a level control task.	0
8.5.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the HPI System shall be integrated and coordinated with the M-MIS of other plant systems as required in 8.2.4. This shall include particular coordination of:	It is expected that other requirements for separation and segmentation will result in very little direct connection between the HPI System M-MIS and the M-MIS for other plant systems.	0
	• The signals for initiation and control from the Reactor Coolant System;		0
	• The signals for initiation from the Containment System.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.6	**BWR DECAY HEAT REMOVAL (DHR) SYSTEM**	**BWR DECAY HEAT REMOVAL (DHR) SYSTEM**	0
8.6.1	**Functions**	**Functions**	0
	The M-MIS for the DHR System shall provide the monitoring and control necessary to:	These functions are consistent with Section 4.5 of Chapter 5.	0
	• Remove decay and sensible heat from the reactor after shutdown, and after the reactor has been cooled to 135 psig saturated conditions by other systems;		0
	• Maintain the inventory of reactor coolant in the reactor vessel if other inventory maintenance systems are not available;		0
	• Remove heat from the suppression pool to control the temperature and pressure in the containment;		0
	• Remove heat from containment by diverting water from the DHR System through the heat exchanger to spray headers in the wet well and dry well;		0
	• Remove heat from the fuel pool, if supplemental cooling is required.		0
8.6.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The inventory maintenance function shall be automatically initiated. The other functions shall be initiated and controlled by the operators; however, the M-MIS Designer shall specifically evaluate the need for automatic initiation of the suppression pool cooling function. The M-MIS Designer shall specifically evaluate the degree of automation necessary for long term activities of the system to avoid unnecessarily burdening the operators with maintaining control over reactor or pool temperatures.	When the plant is shutdown, particularly if it were forced to shutdown, it may not be consistent with proper utilization of the staff to occupy one of them with routine and repetitive operations needed to control the DHR System and maintain control over reactor or pool temperatures.	0

Paragraph No.	Requirement	Rationale	Rev.
8.6.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the DHR System shall be integrated and coordinated with the M-MIS for other plant systems as required in 8.2.4. This shall include particular coordination of:	It is expected that other requirements on separation and segmentation will result in very little direct connection between the DHR M-MIS and other plant M-MIS.	0
	• The signals for initiation and control from the Reactor Coolant System;		0
	• The signals for initiation and control from the Containment System.		0

Paragraph No.	Requirement	Rationale	Rev.
8.7	**BWR STANDBY LIQUID CONTROL (SLC) SYSTEM**	**BWR STANDBY LIQUID CONTROL (SLC) SYSTEM**	0
8.7.1	**Functions**	**Functions**	0
	The M-MIS for the SLC System shall provide the monitoring and control necessary to inject a solution containing a neutron absorber into the reactor coolant so that there is sufficient negative reactivity to bring the reactor to a cold subcritical condition without the control rods.	This allocation of functions is consistent with Section 4.6 of Chapter 5.	0
8.7.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The SLC system shall be initiated only by direct operator action in the main control room. This operator action shall involve protective features which effectively preclude inadvertent actuation and assure that the Shift Supervisor concurs in the system actuation.	This is consistent with Section 4.6 of Chapter 5. The inadvertent injection into the system would require substantial cleanup effort.	0
8.7.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS shall be integrated with the M-MIS design of other plant systems only as necessary to assure that adequate information is available from the Neutron Monitoring and Rod Control Systems for the operator to decide to use the SLC System and to isolate the RWCU System to ensure it does not remove the neutron absorber from the reactor coolant.	It is expected that there will be no direct connection between the SLC System M-MIS and other plant M-MIS except for the RWCU System M-MIS.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.8	**PWR RESIDUAL HEAT REMOVAL (RHR) SYSTEM**	**PWR RESIDUAL HEAT REMOVAL (RHR) SYSTEM**	0
8.8.1	**Functions**	**Functions**	0
	The M-MIS for the RHR System shall provide the monitoring and control necessary to remove core decay heat and sensible heat when the Reactor Coolant System is at a reduced pressure. This includes normal cooldown and safe cold shutdown by directly cooling the reactor coolant and indirectly by cooling the in-containment refueling water storage tank during feed and bleed cooling. It also includes use of a core spray pump as a backup to an RHR pump during RHR system operation.	This allocation of functions is consistent with Section 5.2. of Chapter 5.	0
8.8.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The RHR System shall be manually initiated from the main control room. When in normal operation, e.g., maintaining a steady cold shutdown, the RHR M-MIS shall not require continuous operator attention.	Shutdown periods and use of the RHR System may extend over long periods. It would be inconsistent with the staffing and other demands on the operators to require them to devote constant attention to the removal of decay heat.	0
8.8.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the RHR System shall be integrated and coordinated with the M-MIS for other plant systems as required in 8.2.4. This includes particular consideration of:	This is consistent with current practice and Chapter 5.	0
	• The operation of the Reactor Coolant System;		0
	• The operation of the Containment Spray System;		0
	• The operation of the CVCS, which provides reactor coolant purification when the Reactor Coolant System is at low pressure.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.9	**PWR EMERGENCY FEEDWATER (EFW) SYSTEM M-MIS**	**PWR EMERGENCY FEEDWATER (EFW) SYSTEM M-MIS**	0
8.9.1	**Functions**	**Functions**	0
	The M-MIS for the EFW System shall provide the monitoring and control necessary to remove reactor decay heat through the steam generators when the main and startup feedwater systems are not available.	This allocation of functions is consistent with Section 5.2 of Chapter 5.	0
8.9.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS shall provide adequate monitoring capability (e.g., alarms) so that the EFW System can be manually initiated by the operators for most events which involve the loss of main or startup feedwater before the automatic initiation takes place.	This strategy is consistent with Chapter 5, Section 5.2.	0
8.9.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the EFW System shall be integrated and coordinated with the M-MIS of other plant systems as required in 8.2.4. This shall include particular consideration of: • The signals for initiation and control from the Steam generator System, the Main Feedwater System, and the Reactor Coolant System; • The emergency electric power systems (for the conditions of a complete loss of ac power).	It is intended that the signals from other M-MIS to initiate and control the EFW System be kept to a minimum to enhance the separation of EFW System operation from problems in other systems. The EFW System is designed so that it does not depend on ac power and the M-MIS must be consistent with that requirement.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.10	**PWR SAFETY INJECTION (SI) SYSTEM M-MIS**	**PWR SAFETY INJECTION (SI) SYSTEM M-MIS**	0
8.10.1	**Functions**	**Functions**	0
	The M-MIS for the SI System shall provide the monitoring and control necessary to:	This allocation of function is consistent with Chapter 5, Section 5.4.	0
	• Maintain the inventory in the Reactor Coolant System;		0
	• Control excess reactivity of the reactor core by the injection of water with a high concentration of neutron absorber;		0
	• Remove reactor decay heat by feeding cool water from the in-containment refueling water storage tank and bleeding high temperature water from the Reactor Coolant System using the Safety Depressurization and Vent System.		0
8.10.2	**Control and Monitoring Strategy**	**Control and Monitoring Strategy**	0
	After the automatic initiation of the SI System and the action has restored inventory to a safe level, the M-MIS for the SI System shall provide the ability to control the injection flow rate manually from the main control room. The M-MIS for SI System shall provide for manual initiation and operation feed-and-bleed cooling.	This is consistent with Section 5.4 of Chapter 5.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.10.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the SI System shall be integrated and coordinated with the M-MIS for other plant systems as required in 8.2.4. This shall include particular consideration of:	It is intended that direct connections among these systems will be minimized by the requirements on separation and segmentation.	0
	• The signals for initiation and control from the Reactor Coolant System, the Chemical and Volume Control System, and the Containment System;		0
	• The operation of the Safety Depressurization and Vent System during feed-and-bleed cooling.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.11	**PWR SAFETY DEPRESSURIZATION AND VENT (SDV) SYSTEM M-MIS**	**PWR SAFETY DEPRESSURIZATION AND VENT (SDV) SYSTEM M-MIS**	0
8.11.1	**Functions**	**Functions**	0
	The M-MIS for the SDV System shall provide the monitoring and control necessary to:	This allocation of functions is consistent with Section 5.5 of Chapter 5.	0
	• Achieve and keep the Reactor Coolant System pressure at a value which permits the proper operation of other systems when normal means to reduce pressure are unavailable;		0
	• Vent non-condensible gases from high points in the Reactor Coolant System;		0
	• Bleed reactor coolant from the Reactor Coolant System as part of a feed-and-bleed method to remove core decay heat.		0
8.11.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS for the SDV System shall provide for direct manual control by the operators. The system shall not initiate automatically and, in addition, the M-MIS Designer shall provide effective protection against inadvertent actuation by an operator error.	This is consistent with Chapter 5. Inadvertent actuation of this system would, in effect, be a loss of coolant accident and would challenge other safety systems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
8.11.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the SDV System shall be integrated and coordinated with the M-MIS for other plant systems as required by 8.2.4. In particular, this includes consideration of:	It is expected that other requirements on separation and segmentation will result in very few direct connections between the SDV System M-MIS and other plant M-MIS.	0
	• The conditions in the Reactor Coolant System;		0
	• The status of other safety system which may be unavailable.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.12	**CONTAINMENT ISOLATION M-MIS**	**CONTAINMENT ISOLATION M-MIS**	0
8.12.1	**Functions**	**Functions**	0
	The Containment Isolation M-MIS provides the control and monitoring necessary to isolate the containment to minimize the release of radioactivity to the environment.	This allocation of functions is consistent with Section 6.2 of Chapter 5.	0
8.12.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
8.12.2.1	**Confirmation of Isolation Action**	**Confirmation of Isolation Action**	0
	The containment isolation shall be initiated and accomplished without operator action. The operators shall be provided with a comprehensive operator aid (display) and appropriate controls which will allow them expeditiously and efficiently to:	Although the isolation is automatic the operator provides valuable backup. There are, however, many components involved in an isolation. Unless special steps are taken to aid the operator, they will not provide an effective backup.	0
	• Confirm that the required isolation has been completed and to take manual action, if necessary, to complete the isolation;		0
	• Confirm that the initiation of the isolation was based on valid information;		0
	• Take manual control to return isolated systems to service when conditions permit.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.12.2.2	**Protection Against Inadvertent Isolation**	**Protection Against Inadvertent Isolation**	0
	The Containment Isolation M-MIS shall provide effective protection against inadvertent manual or automatic initiation of containment isolation.	The system transients involved in an inadvertent containment isolation are severe, and loss of generation would undoubtedly result. An inadvertent containment isolation is not consistent with ALWR goals for availability.	0
8.12.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for Containment Isolation shall be integrated and coordinated with the M-MIS for other plant systems as required in 8.2.4. This includes particular consideration of:	The containment isolation involves a large number of plant systems and therefore extensive direct connections among the various M-MIS. Integration and coordination will be a major part of the M-MIS Design for Containment Isolation.	0
	• The systems which provide the signals which are the basis for the initiation of isolation;		0
	• The systems which have components which are automatically controlled as part of the containment isolation.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.13	**CONTAINMENT SYSTEM M-MIS**	**CONTAINMENT SYSTEM M-MIS**	0
8.13.1	**Functions**	**Functions**	0
	The M-MIS for the Containment system provides the monitoring and control necessary to contain potentially radioactive materials in the containment vessel.	This function allocation is consistent with Sections 7 and 8 of Chapter 5.	0
8.13.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The monitoring of conditions in the containment shall not require direct operator action. The main control room operators shall be provided with aids (displays) which concisely show: • The state of readiness of the containment system; • The status of the containment in the course of an accident, including appropriate algorithms to process the data, such as compensating level indications for actual temperatures of the sensing lines.	The containment must be kept in a state of readiness to permit operation of the plant. Violations of Technical Specifications and plant shutdowns can result. In the stress of an accident situation, the large amount of data from the containment has the potential to overwhelm the operators unless assistance is provided in its interpretation.	0
8.13.3	**Integration and Coordination**	**Integration and Coordination**	0
	The Containment system M-MIS should not require significant integration and coordination with other plant M-MIS.	The containment system operates without active control; however, some coordination of the monitoring will be needed to support the status displays for the operators.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.14	**PWR CONTAINMENT SPRAY SYSTEM M-MIS**	**PWR CONTAINMENT SPRAY SYSTEM M-MIS**	0
8.14.1	**Functions**	**Functions**	0
	The M-MIS for the Containment Spray System shall provide the control and monitoring necessary to:	This allocation of functions is consistent with Section 8.2. of Chapter 5.	0
	• Remove heat from the containment atmosphere after an accident to control the temperature and pressure in the containment and thereby maintain the structural integrity of the containment;		0
	• Reduce the concentration of fission products within the containment atmosphere after an accident;		0
	• Remove reactor decay heat which is transferred to the in-containment refueling water storage tank during post-LOCA operation.		0
8.14.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
8.14.2.1	The initiation of the containment spray system shall be automatic with manual actuation on a system and component level as a backup. The M-MIS Designer shall incorporate features which assure that inadvertent automatic or manual initiation and actual spraying of the containment (e.g., by improper test operations) is extremely unlikely.	This is consistent with Chapter 5, Section 8.2. Special emphasis is placed on avoiding inadvertent actuation of the system because of the severe impact on plant availability which would probably result from such an event.	0
8.14.2.2	The operations necessary to realign the systems to use an RHR pump for core spray or to use a core spray pump in the RHR system shall be manual; however, once that is completed, the system operation shall be equivalent to before the pump realignment.	It is intended that the decision and action to interconnect the systems be made directly by the operators, but once a pump is allocated to a different system, then that system should operate in essentially the same manner as before the substitution.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.14.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Containment Spray System shall be integrated and coordinated with other plant M-MIS as required by 8.2.4. In particular this shall include consideration of:	These requirements are consistent with Section 8.2 of Chapter 5.	0
	• The information on containment conditions from the Containment System;		0
	• The backup use of an RHR pump to provide the spray function, and the backup use of a containment spray pump in the RHR System.		0
8.15	**COMBUSTIBLE GAS CONTROL SYSTEM M-MIS**	**COMBUSTIBLE GAS CONTROL SYSTEM M-MIS**	0
8.15.1	**Functions**	**Functions**	0
	The M-MIS for the Combustible Gas M-MIS shall provide the monitoring and control necessary to maintain the integrity of the containment even though combustible gas has been released in an accident.	This allocation of functions is consistent with Section 6.5 of Chapter 5.	0
8.15.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS shall provide monitoring of the combustible gas content of the containment atmosphere including local areas and appropriate annunciation of conditions without direct operator action. Actuation of system components shall be manual.	The production of combustible gas would be the result of serious failures in other safety systems, consequently, the overall plant conditions at the time combustion gas control is needed are relatively unpredictable and automatic operation may not be practical. By the time this system is needed, direct operator control is not expected to be a burden.	0
8.15.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS Designer shall minimize the need for integration and coordination of the Combustible Gas M-MIS with other plant M-MIS.	The Combustible Gas Control System is only a factor after other serious failures. Because the nature of the problem is unpredictable, it is prudent to keep the system as separate as possible from other plant M-MIS.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
8.16	**FISSION PRODUCT LEAKAGE CONTROL (FPLC) SYSTEM M-MIS**	**FISSION PRODUCT LEAKAGE CONTROL (FPLC) SYSTEM M-MIS**	0
8.16.1	**Functions**	**Functions**	0
	The M-MIS for the FPLC System shall provide the control and monitoring necessary to limit potentially radioactive leakage to the environment.	This function allocation is consistent with Section 6.4 of Chapter 5.	0
8.16.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
	The M-MIS for the FPLC System shall provide for the automatic monitoring of any potentially radioactive effluents and shall provide automatic interlocks which prevent inadvertent release to the environment which exceed allowable values.	The presence of radioactive material in an effluent stream in excess of requirements is not a normal condition. It would not be prudent to count on the operators to prevent release under these conditions.	0
8.16.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the FPLC System shall be integrated and coordinated with the M-MIS for other plant systems as required by 8.2.4. In particular, this shall include consideration of:	A major part of the M-MIS design for the FPLC will be the integration and coordination with other plant M-MIS.	0
	• The monitoring of radiation levels by the Environmental Monitoring System;		0
	• The operation of the Containment Isolation M-MIS;		0
	• The Heating, Ventilating, and Air Conditioning System.		0

9 POWER GENERATION AND MAIN TURBINE-GENERATOR SYSTEMS M-MIS REQUIREMENTS 0

9.1 PURPOSE AND SCOPE 0

The power generation and main turbine-generator group of plant systems includes those individual plant systems which are covered by Chapters 2 and 13 of the ALWR Requirements Document. The requirements of this section are limited to those which relate to the M-MIS for the power generation and main turbine-generator systems group including its directly associated control and instrumentation equipment, e.g., sensors, indicators, control devices, data transmission and processing equipment, and alarms. Only requirements which relate to use in the systems group are covered, general requirements on the use of this type of equipment are addressed in other sections of Chapter 10. The mechanical and electrical components which make up the individual systems, e.g., pumps, motors, tanks, piping, valves, power cables, and switch-gear, are covered in other chapters of the ALWR Requirements Document. 0

This section of Chapter 10 covers only a portion of the M-MIS requirements for these systems. Many of the requirements on the plant systems in other ALWR chapters, particularly Chapters 2 and 13 are directly applicable to the M-MIS for this group of systems; however, these will not generally be repeated unless they need to be expanded to clarify their applicability to the M-MIS or need special emphasis. In particular, this section provides requirements which cover the following: 0

- The allocation of the functions of the M-MIS for the power generation and main turbine-generator systems group among the individual plant systems; 0
- The identification of physical boundaries and interfaces of the M-MIS for the purpose of defining the scope of requirements for the M-MIS of the power generation and main turbine-generator systems group; 0
- The strategies for control and monitoring (for example, automatic or manual and local or remote) which shall be followed for various normal and abnormal operating modes and transients of the individual plant systems, e.g., startup, normal operation, shutdown, and testing; 0
- The integration of the M-MIS for the individual plant system with other plant M-MIS and the coordination of their operation. 0

9.2 GENERAL REQUIREMENTS FOR POWER GENERATION AND MAIN TURBINE-GENERATOR SYSTEMS GROUP M-MIS 0

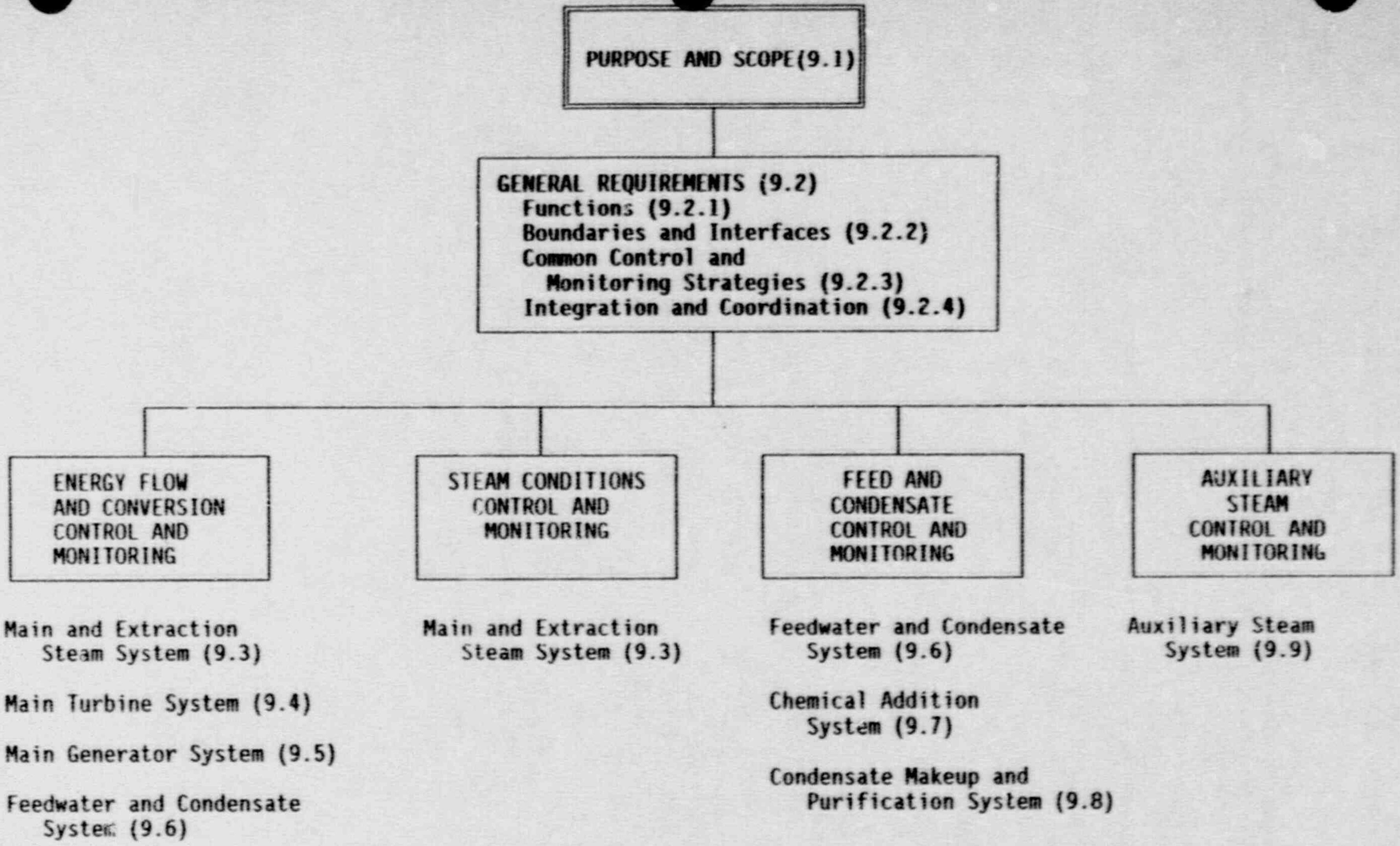
9.2.1 Functions 0

The M-MIS for this systems group shall provide the monitoring and control necessary for the individual power generation and main turbine-generator systems to carry out their required functions. These plant system functions are defined in Chapters 2 and 13. 0

The M-MIS Designer shall allocate the various M-MIS functions among the individual plant systems M-MIS such that the required functions and tasks as determined in the design process (Section 3.1.3.3) can be satisfactorily accomplished. This section provides an initial allocation of these M-MIS functions, however, it is a primary responsibility of the M-MIS Designer to integrate and coordinate the operation of all plant M-MIS so that all functions are adequately performed. Figure 10.9-1 illustrates how the major functions of this group of systems have been allocated to the individual plant systems for the purposes of this Requirements Document. Other allocations of the functions may be used if they can be shown to improve significantly the plant's operability, simplicity, or reliability and if they are fully in accordance with the M-MIS design process requirements in Section 3, particularly the requirements for a functional design approach (3.1.1.1) and the analysis of functions and tasks (3.1.3.3). 0

9.2.1.1 Energy Flow and Conversion 0

The power generation and main turbine-generator systems group M-MIS shall monitor and control the transport of energy as steam from the steam generator (PWR) or reactor vessel (BWR) to the main turbine. This energy transport function will be accomplished largely by the main and extraction steam systems. The conversion of the energy in the steam to electrical energy will be accomplished by the main turbine and generator systems. The M-MIS Designer shall integrate the operation of these systems as well as coordinate their operation with the M-MIS for the reactor coolant system and electrical distribution system. The M-MIS shall also control and monitor the operation of steam bypass or relief devices to provide for the flow of energy when the conversion in the main turbine-generator is limited or out-of-balance with the energy production. 0



PURPOSE AND SCOPE(9.1)

GENERAL REQUIREMENTS (9.2)
Functions (9.2.1)
Boundaries and Interfaces (9.2.2)
Common Control and
Monitoring Strategies (9.2.3)
Integration and Coordination (9.2.4)

ENERGY FLOW AND CONVERSION CONTROL AND MONITORING

Main and Extraction Steam System (9.3)

Main Turbine System (9.4)

Main Generator System (9.5)

Feedwater and Condensate System (9.6)

STEAM CONDITIONS CONTROL AND MONITORING

Main and Extraction Steam System (9.3)

FEED AND CONDENSATE CONTROL AND MONITORING

Feedwater and Condensate System (9.6)

Chemical Addition System (9.7)

Condensate Makeup and Purification System (9.8)

AUXILIARY STEAM CONTROL AND MONITORING

Auxiliary Steam System (9.9)

FIGURE 10.9-1

ALWR M-MIS FOR POWER GENERATION AND MAIN TURBINE-GENERATOR SYSTEMS

Paragraph No.	Requirement	Rev.
9.2.1.2	**Steam Conditions**	0
	The power generation and main turbine-generator systems group M-MIS shall maintain the steam conditions, e.g., its properties of pressure or moisture content, within acceptable ranges. The M-MIS shall monitor and control these conditions largely by the operation of the main and extraction steam system. This function requires the M-MIS Designer to integrate main and extraction steam system's operation with the control of energy flow since the control of energy flow will directly impact the steam conditions.	0
9.2.1.3	**Feed and Condensate Supply**	0
	The M-MIS for the power generation and main turbine-generator systems group shall monitor and control the feed and condensate system operation so that feedwater at the proper conditions, e.g., temperature and pressure, is available for the plant systems which control the inventory in the steam generator (PWR) or reactor vessel (BWR). The M-MIS for the feed and condensate system shall coordinate its operation with the M-MIS for the level control as well as integrate its operation with the M-MIS for main steam and turbine-generator systems. In addition to the control and monitoring of the conditions of pressure and temperature, the M-MIS for this group of systems shall also monitor and control the chemical conditions of the feedwater. This function shall be largely accomplished by the operation of chemical addition and the condensate makeup purification systems and the M-MIS for those plant systems.	0
9.2.1.4	**Auxiliary Steam Supply**	0
	The M-MIS for the power generation and main turbine-generator systems group shall monitor and control the conditions of the auxiliary steam so that the systems which use the steam can perform their functions. This monitoring and control of the auxiliary steam shall be carried out by the auxiliary steam system; however, its M-MIS shall be coordinated with the M-MIS of the user systems and integrated with the main and extraction steam M-MIS when main steam is the source of auxiliary steam.	0

9.2.2 Boundaries and Interfaces 0

The physical boundaries of the individual systems which make up the power generation and main turbine-generator group of systems are defined in the appropriate sections of Chapters 2 and 13. The boundaries of the M-MIS for this group of systems shall be consistent with those physical boundaries of the plant systems; however, they shall also encompass the M-MIS hardware, which includes: 0

- Instrument sensors; 0
- Data transmission equipment; 0
- Data processing equipment; 0
- Controllers and logic devices; 0
- Operator interface hardware (e.g., controls, indicators); 0
- Software to support M-MIS hardware. 0

The interfaces of the individual systems which make up the power generation and main turbine-generator group of systems are defined in the appropriate sections of Chapters 2 and 13. The interfaces of the M-MIS for the group of systems shall be consistent with those plant system interfaces. The M-MIS interfaces shall be formally defined and controlled in accordance with the M-MIS Design Plan (Section 3.1.2.4). The M-MIS Designer shall define and control other interfaces among the various M-MISs and other plant systems as may be necessary to integrate and coordinate the operation of the plant systems even though these interfaces are not defined as physical interfaces in Chapter 2 and 13. 0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.2.3	**Common Control and Monitoring Strategies**	**Common Control and Monitoring Strategies**	0
	The M-MIS Designer shall use a consistent control and monitoring strategy for all the parts of the M-MIS for this group of systems except as modified by individual system M-MIS requirements. This common control strategy shall also be consistent with that used for the remainder of the M-MIS.	A consistent control strategy supports the overall objective of a high level of standardization for the ALWR. It also tends to simplify training of operators and maintenance technicians. For example, consistent control strategies tend to lead to similar controls, displays, and control stations.	0
9.2.3.1	**Startup and Shutdown Operations**	**Startup and Shutdown Operations**	0
	The M-MIS for this group of systems shall normally provide for the monitoring and control necessary to startup or shutdown a system to be done by the operators, i.e., the startup shall be manual. Specific tasks involved in the startup or shutdown may be automated if analyses of functions and tasks (Section 3.1.3.3) show manual operation is a significant burden or distraction for the operators.	The startup and shutdown of this group of systems is largely paced by the operators and may involve a very large number of individual operations, particularly local operations such as the repositioning of valves. Automation of these operations would significantly increase the complexity of the plant and is not desirable. There may be portions of the startup and shutdown which could be automated and thereby reduce the time to startup or the risk or errors.	0
9.2.3.2	**Normal Operations**	**Normal Operations**	0
	The M-MIS for this group of systems shall normally provide for automatic or unattended operation for continuous or often repeated tasks when the plant is in nominally steady operation above a low power level. This low power level shall be established by the M-MIS Designer based on a specific tradeoff evaluation which considers the functions and tasks required at low power levels, the potential frequency and duration of low power operation, and the relevant equipment and system constraints on low power operation. This tradeoff evaluation shall be documented and reviewed in the design process. The evaluation to select a power level shall be combined with the similar tradeoff evaluation required by 7.2.3.2.	The automatic, unattended operation of this group of systems is intended to be consistent with the main control room staffing in Section 4.2.4. That requirement cannot be expected to be met if an operator is occupied most of the time by the need to control a system in this group. It is also current practice for these systems to operate without constant operator attention. Tasks that are done manually, at relatively long intervals, for example, refilling a tank or reconfiguring a system to equalize service time, probably do not need to be automated.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.2.3.3	**Reconfiguration Operations**	**Reconfiguration Operations**	0
9.2.3.3.1	The M-MIS design shall provide for reconfiguration or automatic shutdown of a system when necessary to avoid personnel hazard, major equipment damage, or to support actions by other parts of the plant M-MIS, for example, when the reactor is automatically shutdown or a safety system is actuated.	The reconfiguration of the system may involve a large number of individual operations in the long term. It is not practical to completely automate some of them without adding extensive complexity. However, some reconfiguration actions cannot depend on the operators because of timing constraints or the risk of error. In addition, it has been the practice to automate such tasks.	0
9.2.3.3.2	The return of a system to its initial configuration after an automatic reconfiguration shall normally be by operator action, i.e., not automatic. Return to the initial configuration may be automatic if the M-MIS Designer establishes that such automatic action would significantly:		0
	• Reduce the challenges to protection and safety systems;		0
	• Reduce hazards to personnel;		0
	• Improve the plant availability; or		0
	• Reduce the risk of damage to major plant equipment.		0
9.2.3.3.3	The operators shall be notified of any such automatic return to the original configuration.		0
9.2.3.4	**Testing Operations**	**Testing Operations**	0
	The M-MIS for this group of systems shall normally provide for on-line testing only at the direction of the operator. The testing itself should be automated and assisted as required in Section 3.6 so that operator actions are simple and have little risk of causing a plant upset.	The testing of these systems often must be done while the systems are in operation. Mistakes in the testing have often resulted in a loss of generation or serious upsets and plant trips. Section 3.6 contains a number of specific requirements to enhance the testability of the ALWR. The testing strategy for these systems is intended to be consistent with those requirements.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.2.4	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS designs for the systems in this group shall be integrated and coordinated so that the overall plant performance and functional requirements as well as those of individual systems are met. Those requirements are found in Chapter 1 and in other chapters of the ALWR Requirements Document, particularly Chapter 2 and Chapter 13. In addition, the M-MIS Designer shall coordinate the design features with other parts of the M-MIS, especially those portions of the M-MIS which control the energy production (e.g., Section 7 of Chapter 10).	Although the requirements for the individual systems define the functions and interfaces, it is the basic responsibility of the M-MIS Designer to connect the various systems and their requirements in a sensible and efficient manner. The specific methods used to connect the operation of the various systems and the logic are to be selected by the M-MIS Designer. The ALWR Requirements Document has specifically avoided defining how this is to be accomplished. It is intended that the M-MIS Designer not be constrained to current practice and be encouraged to develop strategies for control which consider the many interactions among the various systems.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.3	**MAIN AND EXTRACTION STEAM SYSTEM M-MIS**	**MAIN AND EXTRACTION STEAM SYSTEM M-MIS**	0
9.3.1	**Functions**	**Functions**	0
	The M-MIS for the main and extraction steam system shall provide the monitoring and control necessary to assure that:	The M-MIS Designer has the responsibility (Section 9.2.1) to allocate the functions among the individual portions of the total M-MIS. This allocation of functions is consistent with current practice.	0
	• The energy received from the rector (BWR) or steam generator (PWR) is transported effectively and efficiently to the main turbine;		0
	• The conditions of the steam provided to the main turbine (e.g., its pressure or moisture) are within the acceptable ranges for the power output;		0
	• Design conditions are not exceeded (e.g., pressure or rate of temperature change) in the system or in connected systems (e.g., the steam generator or main turbine).		0
9.3.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
9.3.2.1	**Transfer Between Manual and Automatic Control**	**Transfer Between Manual and Automatic Control**	0
	The M-MIS Designer shall ensure that systems which are in automatic control when the plant is operating normally, but are under manual control for other common conditions (e.g., startup or shutdown) can be transferred between automatic and manual control smoothly and at an appropriate and convenient time in the plant evolution.	There have been some problems in existing plants with making the transfers between automatic and manual control at a low enough power level.	0

Paragraph No.	Requirement	Rationale	Rev
9.3.2.2	**Maneuvering and Load Follow**	**Maneuvering and Load Follow**	0
	The M-MIS shall specifically provide for the maneuvering and load follow events defined in Chapter 1, Table 3-6 to be accommodated without any short term operator action to readjust or reconfigure the system.	In order for the requirements on the number of operators in the main control room required for normal operation to be met (Section 4.2.4) it is necessary for the majority of the maneuvering and load follow evolutions not to require the operators attention to the main and extraction steam system since his attention will be needed to monitor and control the reactor and turbine-generator.	0
9.3.2.3	**Automatic Reconfiguration**	**Automatic Reconfiguration**	0
	The M-MIS actions shall be compatible with any concurrent operations of the reactor and safety systems (whether manual or automatic) and, in particular, automatically maintaining energy flow in the main steam system to remove energy from the reactor when the turbine-generator or the main condenser is not available and limiting the pressure in the system.	Reconfiguration of the main and extraction steam system, like start-up, would become complex if it were totally automated. There are, however, tasks to shutdown portions of the system or reconfigure it in response to protection or safety systems which are under too stringent a time constraint to count on operator action. These tasks will have to be automatic. This strategy is consistent with current practice.	0
9.3.2.4	**On-line Testing**	**On-line Testing**	0
	The M-MIS control strategy shall be compatible with the effects of on-line testing of turbine intercept valves and other major components which can perturb the main steam conditions.	Because of the close relation between the conditions in main steam system and the large energy flow through it, perturbations from testing both in the system and in other systems can have serious disruptive effects in relatively short times. Accommodating testing is a particularly important part of the M-MIS design for the main and extraction steam system.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.3.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the main and extraction steam system shall be integrated and coordinated with the M-MIS of other plant systems as required in 9.2.4. This shall include particular consideration of: • The control of the reactor power production; • The control of the main turbine and generator;	The main steam system is the major physical link between the reactor and the production of electricity. Its control affects directly or indirectly a very large number of plant systems. Integration and coordination of the main steam system operation with the rest of the plant systems is a major effort for the M-MIS Designer.	0
	• The control of reactor vessel conditions and inventory (BWR);		0
	• The control of the steam generator conditions and inventory (PWR);		0
	• The control of bypass and relief valves;		0
	• The control of main steam isolation valves.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.4	**MAIN TURBINE SYSTEM M-MIS**	**MAIN TURBINE SYSTEM M-MIS**	0
9.4.1	**Functions**	**Functions**	0
	The M-MIS for the main turbine shall provide the monitoring and control necessary to convert the steam provided by the main steam system into mechanical energy which drives the main generator.	Main turbine M-MIS has typically been designed as part of the turbine-generator control system. It is expected that this would be the practice for the ALWR; however, it is intended that the plant's M-MIS Designer be responsible to assure that the main turbine M-MIS is fully consistent and integrated with the remainder of the total M-MIS for the plant.	0
9.4.2	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the main turbine shall be integrated and coordinated with the M-MIS of other plant systems as required in 9.2.4. This shall include particular consideration of:	The M-MIS Designer will be expected to integrate the main turbine control system, which is normally provided as part of the main turbine, with the remainder of the plant M-MIS.	0
	• The control of steam flow to the main turbine in the main and extraction steam systems;		0
	• The control of the conditions in the main condenser, in the feed and condensate and in the circulating water systems;		0
	• The control of the main generator;		0
	• The control of the production of energy in the reactor and the generation of steam in the reactor (BWR) or steam generator (PWR).		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.5	**MAIN GENERATOR SYSTEM M-MIS**	**MAIN GENERATOR SYSTEM M-MIS**	0
9.5.1	**Functions**	**Functions**	0
	The M-MIS for the main generator shall provide the monitoring and control necessary to convert the mechanical energy produced by the main turbine to electrical energy.	The main generator M-MIS has typically been designed as part of the turbine-generator control system. It is expected that this will be the practice for the ALWR; however, it is intended that the plant's M-MIS Designer be responsible to assure that the main generator M-MIS is fully consistent and integrated into the remainder of the total M-MIS for the plant.	0
9.5.2	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the main generator shall be integrated and coordinated with the M-MIS for other plant systems as required by 9.2.4. This shall include particular consideration of:	It is expected that the integration of the control of the main generator with the main turbine will be provided largely by the turbine-generator vendor.	0
	• The control of the main turbine;		0
	• The control of the plant electrical systems.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.6	**FEEDWATER AND CONDENSATE SYSTEM M-MIS**	**FEEDWATER AND CONDENSATE SYSTEM M-MIS**	0
9.6.1	**Functions**	**Functions**	0
	The M-MIS for the Feedwater and Condensate System shall provide the monitoring and control necessary to assure that an adequate quantity of high quality feedwater is transported from the condenser hotwell to valves which control the introduction of feedwater into the BWR reactor vessel or a PWR steam generator.	The M-MIS Designer has the responsibility (Section 9.2.1) to allocate the functions among the individual portions of the total M-MIS. This allocation of functions is consistent with current practice.	0
9.6.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
9.6.2.1	**Startup and Shutdown**	**Startup and Shutdown**	0
	The M-MIS design shall provide features which ensure that: • Operation at low power levels does not require essentially continuous operator attention, e.g., as may be caused by control valve leakage; • Systems which will be under automatic control when the plant is operating normally can be transferred to automatic control smoothly and can be transferred at a convenient time in the startup.	The startup and shutdown of the feed and condensate system would result in excessive complexity if entirely automated. It is not the intent, however, to use manual operations when function and task analysis shows the potential for substantial gains in operability. This may include shifting some systems to automatic control earlier in the startup sequence or remaining on automatic control later in a shutdown. It may also include special features to accommodate unavoidable control valve leakage without constant operator attention.	0
9.6.2.2	**Normal Power Changes**	**Normal Power Changes**	0
	The M-MIS for the feed and condensate system shall provide for normal power changes without short-term operator action.	Although the operator will need to be alert to upsets in the feed and condensate system, it would not be consistent with the control room staffing (Section 4.2.4) if the operators were to have to man the controls on this system for normal power changes.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.6.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the feed and condensate system shall be integrated and coordinated with the M-MIS for other plant systems as required by 9.2.4. This shall include particular consideration of:	The feed and condensate is an integral part of the chain of systems which controls the flow of energy through the plant. As such, its upsets can have rapid and far reaching effects and it must respond rapidly and correctly to conditions in other systems.	0
	• The control of steam generator (PWR), or reactor water level (BWR);		0
	• The control of the removal of reactor decay heat;		0
	• The control of the main and extraction steam system;		0
	• The control of the main turbine.;		0
	• The control of condensate makeup purification and chemical addition systems.		0
9.7	**CHEMICAL ADDITION SYSTEM M-MIS**	**CHEMICAL ADDITION SYSTEM M-MIS**	0
9.7.1	**Functions**	**Functions**	0
	The M-MIS for the chemical addition system shall provide the control and monitoring necessary to assure that the condensate, feedwater, and offgas (BWR) chemistry is maintained within required limits.	The M-MIS Designer has the responsibility (Section 9.2.1) to allocate the functions among the individual portions of the total M-MIS. This allocation of functions is consistent with current practice.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.7.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
9.7.2.1	**Location of Operations**	**Location of Operations**	0
	The M-MIS Designer shall evaluate the degree to which the operations are done locally instead of in the main control room. In any case, the M-MIS shall provide specific capability for the control room operators to confirm that proper chemical addition has taken place and to be alerted to a need for chemical addition.	The chemical addition is a support function for the other plant systems and it is not directly in the power generation chain; however, improper chemistry can have serious effects on the operability of the plant. It would not be consistent with control room staffing (Section 4.2.4) for the control room operators to have to spend significant effort to attend the chemical addition system during normal operation; however, they must be aware of problems with the chemical addition.	0
9.7.2.2	**Impact of Automatic Shutdown or Reconfiguration Operations**	**Impact of Automatic Shutdown or Reconfiguration Operations**	0
	The M-MIS Designer shall ensure that automatic actions in the chemical addition system, whether from anticipated control actions or component failures, do not cause a shutdown of other plant systems.	Since the chemical addition is a support function, its problems should not routinely affect plant availability. This supports the overall ALWR availability goals.	0
9.7.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the chemical addition system shall be integrated and coordinated with the M-MIS for other plant systems as required in 9.2.4. This shall include particular consideration of the control of the Feed and Condensate System. It should be an objective to keep the M-MIS for the chemical addition system separate from the M-MIS for other plant systems.	As for the overall control strategy, the intent would be to keep the chemical addition system connections to the other systems simple and to minimize the control room operators' involvement in its operation.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.8	**CONDENSATE MAKEUP AND PURIFICATION SYSTEM M-MIS**	**CONDENSATE MAKEUP AND PURIFICATION SYSTEM M-MIS**	0
9.8.1	**Functions**	**Functions**	0
	The M-MIS for the Condensate Makeup and Purification System shall provide the monitoring and control necessary to assure that an adequate supply of makeup condensate of suitable quality is available for the M-MIS which controls the inventory of condensate.	The M-MIS Designer has the responsibility (Section 9.2.1) to allocate the functions among the individual portions of the total M-MIS. This allocation is consistent with current practice.	0
9.8.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
9.8.2.1	**Normal Operation**	**Normal Operation**	0
	The M-MIS shall provide for normal changes in power without short term operator action. The M-MIS shall also provide the capability for the operator to confirm that the Condensate Makeup and Purification System is operating normally and shall alert the operators appropriately.	The Condensate Makeup and Purification System performs a service function and is not directly in the energy transfer chain; therefore, it should be able to cope with normal power operation without attention by the operators. However, the maintenance of adequate condensate makeup is essential to the operability of the plant and immediate action may be needed if problems are detected.	0
9.8.2.2	**Shutdown or Reconfiguration**	**Shutdown or Reconfiguration**	0
	The M-MIS Designer shall ensure that automatic actions in the Condensate Makeup and Purification System, whether from anticipated control actions or component failures, do not cause a shutdown of other plant systems unless the shutdown is, in fact, necessary to prevent damage to other equipment or hazards to personnel.	It is important that upsets of the Condensate Makeup and Purification System do not propagate into those power generation systems which are directly involved in the energy transfer function. This will ensure that ALWR availability goals are met.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
9.8.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Condensate Makeup and Purification System shall be integrated and coordinated with the M-MIS for other plant systems as required by 9.2.4. This shall include particular consideration of the control of the Feed and Condensate System. It should be an objective to keep the M-MIS for the Condensate Makeup and Purification System separate from the M-MIS for other plant systems.	As for the overall control strategy, the Condensate Makeup and Purification System provides a support function and the intent would be to keep the connections to other plant systems simple and to minimize the control room operator's involvement in its operation.	0
9.9	**AUXILIARY STEAM SYSTEM**	**AUXILIARY STEAM SYSTEM**	0
9.9.1	**Functions**	**Functions**	0
	The M-MIS for the Auxiliary Steam System shall provide the monitoring and control necessary to assure that an adequate supply of auxiliary (low pressure) steam or proper chemistry and conditions (e.g., pressure) is provided to those plant systems which utilize auxiliary steam to perform their functions.	The M-MIS Designer has the responsibility (Section 9.2.1) to allocate the functions among the individual portions of the total M-MIS. This allocation is consistent with current practice.	0
9.9.2	**Control and Monitoring Strategies**	**Control and Monitoring Strategies**	0
9.9.2.1	**Location of Operations**	**Location of Operations**	0
	The M-MIS Designer shall not include any controls for this system in the main control room unless function and task analysis (3.1.3.3) shows them to be essential.	Even though the Auxiliary Steam System may provide a service function when other steam is unavailable, it is expected that the startup and operation of an auxiliary boiler from the control room will not be necessary, and, accordingly, the control room operators should not have to attend to it in the short term. That is, auxiliary boiler operation could be left to a local operator. It is expected that those local controls would be provided as part of the boiler package.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
9.9.2.2	**Impact of Automatic Shutdown or Reconfiguration Operations**	**Impact of Automatic Shutdown or Reconfiguration Operations**	0
	The M-MIS Designer shall ensure that automatic actions in the Auxiliary Steam System, whether from anticipated control actions or component failures, do not cause a shutdown of other plant systems.	Since the Auxiliary Steam System provides a support function, its problems should not routinely affect plant availability. This supports the overall ALWR availability goals.	0
9.9.3	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS for the Auxiliary Steam System shall be integrated and coordinated with the M-MIS for other plant systems as required by 9.2.4. Since the Auxiliary Steam System provides steam to a number of different systems (see Chapter 2, Section 7.1.B) its M-MIS design will have a close relation to a large number of systems and its integration and coordination are particularly important. It should be an objective to keep the M-MIS for the Auxiliary Steam System separate from the M-MIS for other plant systems.	Although some of the Auxiliary Steam System components, e.g., a boiler, will involve its own control system which will probably be provided as part of the boiler package, the M-MIS Designer will have to ensure that its control is properly integrated with the operation of the plant systems it services and that its design is consistent with the rest of the plant M-MIS. However, the M-MIS should minimize the operators' involvement in its operation.	0

10 AUXILIARY AND PLANT SUPPORT SERVICES SYSTEMS M-MIS REQUIREMENTS 0

10.1 PURPOSE AND SCOPE 0

The auxiliary group of systems includes the following systems covered by this ALWR Requirements Document: 0

- Chapter 8, Plant Cooling Water System; 0
- Chapter 9, Section 7, Compressed Air and Gas Systems; 0
- Chapter 9, Section 8, Heating, Ventilating and Air Conditioning System (HVAC); 0
- Chapter 11, Electric Power Systems. 0

The plant support services group of systems includes the following systems covered by this ALWR Requirements Document: 0

- Chapter 7, Fuel Handling Systems; 0
- Chapter 9, Section 3, Fire Protection; 0
- Chapter 9, Section 4, Environmental Monitoring; 0
- Chapter 9, Section 5, Site Security; 0
- Chapter 9, Section 6, Decontamination; 0
- Chapter 9, Section 9, Laboratories; 0
- Chapter 12, Radioactive Waste Processing. 0

This section covers the requirements for the M-MIS which control and monitor these systems. This includes requirements for directly associated control and instrumentation equipment for this group of systems, e.g., sensors, indicators, control devices, data transmission and processing equipment, and alarms. Only requirements which relate to use in the auxiliary group of plant systems are covered; general requirements on the use of these types of equipment are addressed in other sections of Chapter 10. The mechanical and electrical components which make up the individual systems, e.g., pumps, motors, tanks, piping, valves, power cables, and switch-gear, are covered in other chapters of the ALWR Requirements Document. 0

This section of Chapter 10 covers only a portion of the M-MIS requirements for these systems. Many of the requirements on the plant systems in other chapters, particularly Chapters 7, 8, 9, 11, and 12 are directly applicable to the M-MIS for the groups of systems; however, the requirements will not generally be repeated unless they need to be expanded to clarify their applicability to the M-MIS or need special emphasis. In particular, this section provides requirements which cover: 0

- The allocation of the functions of the M-MIS for this group of systems among the individual plant systems; 0
- The identification of the physical boundaries and interfaces of the M-MIS for the purpose of defining the scope of requirements for this group of systems; 0
- The strategies for control and monitoring (for example, manual or automatic and local or remote) which shall be followed for various normal and abnormal operating modes and transients of the individual plant systems, e.g., startup, normal operation, shutdown or reconfiguration, and testing; 0
- The integration of the M-MIS for the individual systems with the M-MIS of other plant systems and the coordination of their operation. 0

10.2 GENERAL REQUIREMENTS FOR AUXILIARY AND PLANT SUPPORT SERVICES SYSTEMS GROUPS M-MIS 0

10.2.1 Functions 0

The M-MIS for these systems groups shall provide the monitoring and control necessary for the individual systems to carry out their required functions. These plant system functions are defined in the individual system chapters (7, 8, 9, 11, and 12). 0

The M-MIS Designer shall allocate the various M-MIS functions among the individual plant systems M-MIS such that the required functions and tasks as determined in the design process (Section 3.1.3.3) can be satisfactorily accomplished. This section provides an initial allocation of these M-MIS functions; however, it is a primary responsibility of the M-MIS Designer to integrate and coordinate the operation of all plant M-MIS so that all functions are adequately performed. Figure 10.10-1 illustrates how the major functions of the auxiliary group of systems have been allocated to the individual plant systems for the purposes of this Requirements Document. Figure 10.10-2 illustrates the allocations for the plant support services group. Other allocations of the functions may be used if they can be shown to improve significantly the plant's operability, simplicity, or reliability and if they are fully in accordance with the M-MIS design process requirements in Section 3, particularly the requirements for a functional design approach (3.1.1.1) and the analysis of functions and tasks (3.1.3.3). 0

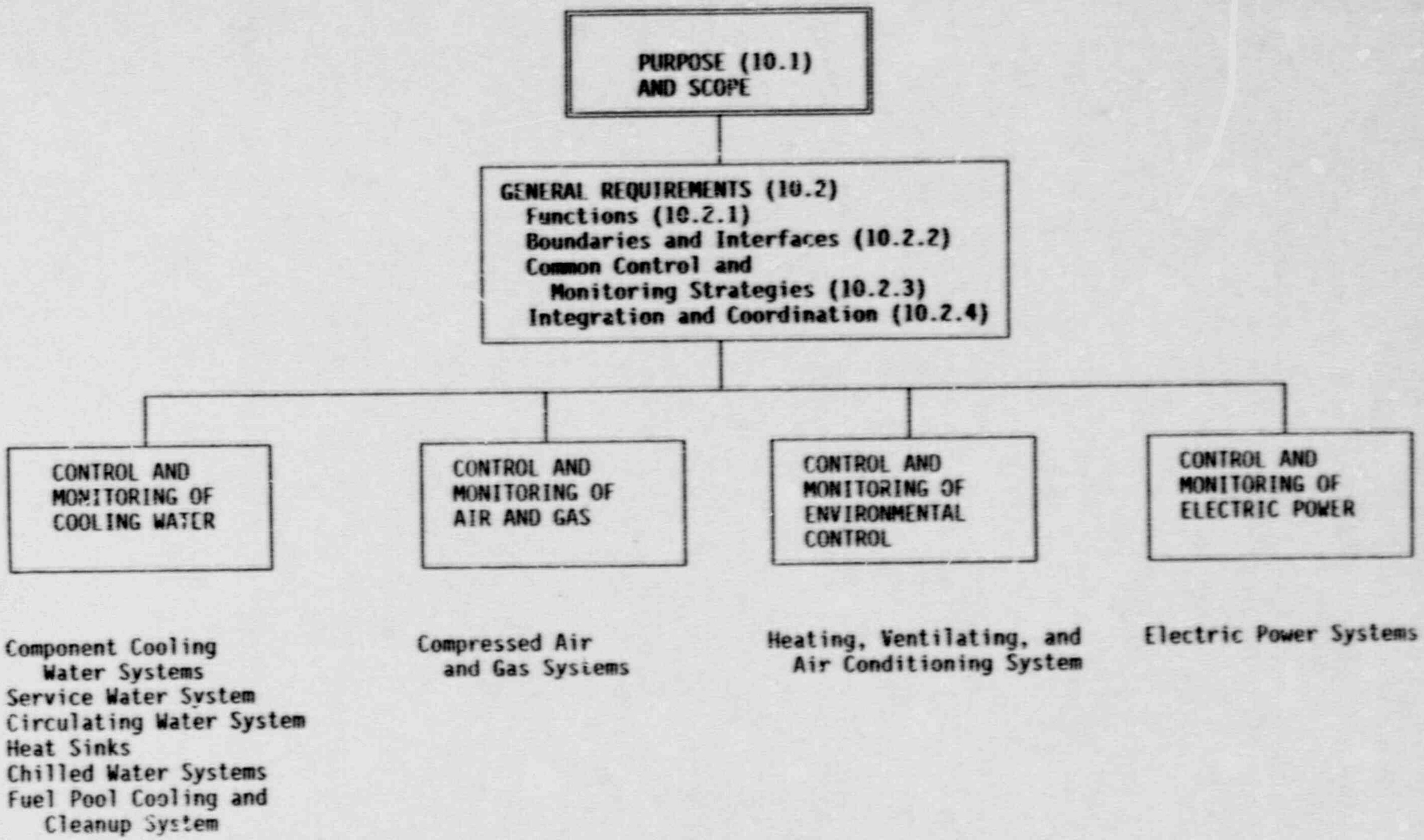

PURPOSE (10.1)
AND SCOPE
GENERAL REQUIREMENTS (10.2)
Functions (10.2.1)
Boundaries and Interfaces (10.2.2)
Common Control and
Monitoring Strategies (10.2.3)
Integration and Coordination (10.2.4)
CONTROL AND MONITORING OF COOLING WATER
CONTROL AND MONITORING OF AIR AND GAS
CONTROL AND MONITORING OF ENVIRONMENTAL CONTROL
CONTROL AND MONITORING OF ELECTRIC POWER
Component Cooling Water Systems
Service Water System
Circulating Water System
Heat Sinks
Chilled Water Systems
Fuel Pool Cooling and Cleanup System
Compressed Air and Gas Systems
Heating, Ventilating, and Air Conditioning System
Electric Power Systems

FIGURE 10.10-1

ALWR M-MIS FOR AUXILIARY SYSTEMS

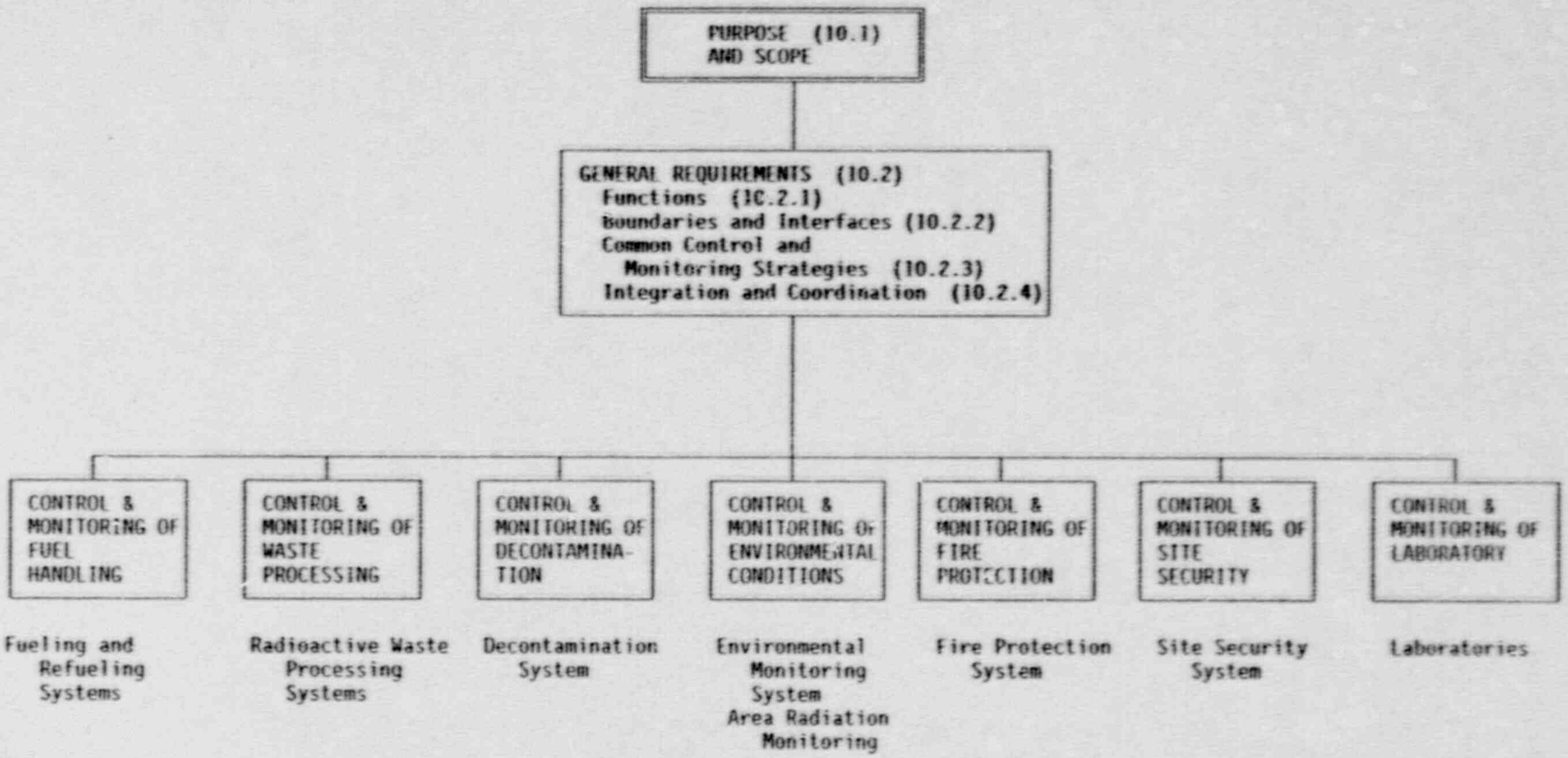

PURPOSE (10.1)
AND SCOPE
GENERAL REQUIREMENTS (10.2)
Functions (10.2.1)
Boundaries and Interfaces (10.2.2)
Common Control and
Monitoring Strategies (10.2.3)
Integration and Coordination (10.2.4)
CONTROL & MONITORING OF FUEL HANDLING
CONTROL & MONITORING OF WASTE PROCESSING
CONTROL & MONITORING OF DECONTAMINATION
CONTROL & MONITORING OF ENVIRONMENTAL CONDITIONS
CONTROL & MONITORING OF FIRE PROTECTION
CONTROL & MONITORING OF SITE SECURITY
CONTROL & MONITORING OF LABORATORY
Fueling and Refueling Systems
Radioactive Waste Processing Systems
Decontamination System
Environmental Monitoring System
Area Radiation Monitoring
Fire Protection System
Site Security System
Laboratories

FIGURE 10.10-2

ALWR M-MIS FOR PLANT SUPPORT SERVICES SYSTEMS

Paragraph No. *Requirement* *Rev.*

10.2.1.1 Cooling Water 0

The auxiliary systems group M-MIS shall monitor and control the removal of heat from plant systems, structures, and components and the transfer of those heat loads to the environment. This energy tranuport function is accomplished by the component cooling water system, service water systems, circulating water systems, plant heat sinks, chilled water systems, and the fuel pond cooling and cleanup systems. M-MIS shall provide monitoring and control during normal operation, transient, shutdown, and accident conditions. 0

10.2.1.2 Air and Gas 0

The auxiliary systems group of M-MIS shall monitor and control the supply and distribution of compressed air and gas. This air service function is accomplished by plant service air, instrument air and breathing air systems. The compressed gas service is provided in separate, isolated subsystems from high pressure cylinders. M-MIS for these systems shall be appropriate to the service and provide the control and monitoring during all plant conditions which require the air or gas service. 0

10.2.1.3 Environmental Control 0

The auxiliary systems group of M-MIS shall monitor and control the services which ensure the plant environment is suitable for the safety and comfort of plant personnel and operability of plant equipment during normal operating and anticipated operational occurrences. The auxiliary systems group of M-MIS also shall monitor and control collection, filtration and discharge of toxic or radioactive effluent resulting from maintaining the plant environment. The environmental control service functions are accomplished by the heating, ventilation and cooling system and related gas treatment, cleanup and purge sub-systems. 0

10.2.1.4 Electrical Power 0

The auxiliary systems group of M-MIS shall monitor and control the systems which supply electric power to the plant auxiliary and service loads, including instrumentation and control system loads. The electrical power service functions are provided by the off-site power supply systems, the on-site standby AC power supply system, the DC and vital instrumentation AC power supply systems and the lighting and electrical protective systems. M-MIS shall provide monitoring and control to the plant electrical power non-safety loads during normal plant operation, startup and normal shutdown; and to the engineered safety systems for accident initiation and safe shutdown. 0

Paragraph No.	*Requirement*	*Rev.*
10.2.1.5	**Fuel Handling**	0
	The plant support services group M-MIS shall monitor and control fuel handling activities. This fuel handling function is accomplished by the refueling machine and associated equipment. M-MIS shall provide monitoring and control during fuel handling operations, i.e., during other plant operating modes this system has no significant functions.	0
10.2.1.6	**Fire Protection**	0
	The plant support services group M-MIS shall monitor and control fire detection and suppression. M-MIS shall provide monitoring and control to the plant fire protection system during normal operation, shutdown and accident conditions.	0
10.2.1.7	**Environmental Monitoring**	0
	The plant support services group M-MIS shall monitor and control, and provide data management for the environmental monitoring systems. These systems provide data necessary to control plant releases and assess the impact of plant effluent released on the environment. Environmental monitoring is accomplished by the plant meteorological system, water quality monitoring, and monitoring for the solid waste processing system and radiation monitors at and beyond the site boundary. M-MIS shall provide monitoring, control, and data management during normal operation, shutdown, and accident conditions.	0
10.2.1.8	**Site Security**	0
	The plant support services group M-MIS shall monitor, control, and provide data management for site security systems which:	0
	• Prevent unauthorized access into vital or protected areas;	0
	• Detect attempts to gain unauthorized access or introduce unauthorized materials in such areas;	0
	• Facilitate authorized activities and conditions within protected and vital areas;	0
	• Provide for authorized access and assure detection of unauthorized penetration of protected or vital area boundaries.	0
	M-MIS shall provide monitoring, control, and data management during normal operation, shutdown, and accident conditions.	0

Paragraph No.	*Requirement*	*Rev.*
10.2.1.9	**Decontamination**	0
	The plant support services group M-MIS shall monitor and control decontamination systems and facilities which remove or reduce radioactive contaminants from plant equipment, protective clothing, and personnel. This decontamination function is accomplished by delivery system controllers, spray nozzle assemblies, chemical and/or abrasive supply systems, collection and storage tanks, high pressure pumps, filters, demineralizers, and piping connections to waste processors. M-MIS shall provide monitoring and control during normal operation, shutdown, and accident conditions.	0
10.2.1.10	**Laboratories**	0
	The plant support services group M-MIS shall monitor, control and provide data management for laboratories which analyze plant systems and environmental samples. The plant laboratories include an analytical chemistry laboratory and a radio chemistry laboratory. Also included is a computer based data management system capable of interfacing with the main plant data base computer system. M-MIS shall provide monitoring, control, and data management during normal operation, shutdown, and accident conditions.	0
10.2.1.11	**Radioactive Waste Processing**	0
	The plant support services group M-MIS shall monitor and control radioactive waste processing systems which collect, segregate, store, and process the wastes for safe monitored discharge or disposal. The radioactive waste processing functions are provided by gaseous, liquid, and solid radioactive waste processing systems. M-MIS shall provide monitoring and control during normal operation, shutdown, and accident condition.	0
10.2.1.12	**Area Radiation Monitoring**	0
	The plant support services group M-MIS shall monitor the radiation in those areas of the plant which may have radiation sources (Chapter 6, Section 4.2.8) and which may be occupied by personnel. This monitoring shall provide local and remote indication and alarming appropriate to the significance and use of the measured radiation levels. The M-MIS shall be integrated and coordinated with the M-MIS for the radiation monitoring of process streams (Chapter 3, Section 7, and Section 7.10 of this chapter) as necessary to support control of personnel exposures, provide indication of equipment malfunctions, and meet applicable regulations. The M-MIS shall provide monitoring during normal, shutdown, and accident conditions.	0

10.2.2 Boundaries and Interfaces 0

The physical boundaries of the individual systems which make up the auxiliary and plant support services systems groups are defined in the appropriate sections of Chapters 7, 8, 9, 11, and 12. The boundaries of the M-MIS for the group of systems shall be consistent with those physical boundaries of the plant systems; however, they shall also encompass the M-MIS hardware, which includes: 0

- Instrument sensors; 0
- Data transmission equipment; 0
- Data processing equipment; 0
- Controllers and logic devices; 0
- Operator interface hardware (e.g., controls, indicators); 0
- Software to support M-MIS hardware. 0

The interfaces of the individual systems which make up the auxiliary and plant support services systems group are defined in the appropriate sections of Chapters 7, 8, 9, 11, and 12. The interfaces of the M-MIS for the group of systems shall be consistent with those plant system interfaces. The M-MIS interfaces shall be formally defined and controlled in accordance with the M-MIS Design Plan (Section 3.1.2.4). The M-MIS Designer shall define and control other interfaces among the various M-MISs and other plant systems as may be necessary to integrate and coordinate the operation of the plant systems even though these interfaces are not defined as physical interfaces in Chapters 7, 8, 9, 11, and 12. 0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
10.2.3	**Control and Monitoring Strategies for Auxiliary and Support Systems**	**Control and Monitoring Strategies for Auxiliary and Support Systems**	0
	The M-MIS Designer shall use a consistent control and monitoring strategy for all the parts of the M-MIS for this group of systems, except as modified by specific requirements in other chapters. This common control strategy shall also be consistent with that used for the remainder of the M-MIS. This control and monitoring shall not take place in the main control room or involve those operators unless analyses of the functions and tasks shows their involvement to be necessary to the function.	A consistent control strategy supports the overall objective of a high level of standardization for the ALWR. It also tends to simplify training of operators and maintenance technicians. For example, consistent control strategies tend to lead to similar controls, displays, and control stations. These systems differ from those in Sections 7, 8, and 9, in that the main control room operators are not necessarily involved directly. The control and monitoring strategy needs to recognize this fundamental difference. It is intended that requirements 4.9.1.1 be strictly adhered to, i.e., that functions and tasks involved in the operation of these auxiliary and support systems not be assigned to the main control room operators if personnel outside the main control room can adequately and effectively handle them.	0
10.2.3.1	**Startup and Snutdown Operations**	**Startup and Shutdown Operations**	0
	The M-MIS for this group of systems shall provide for the monitoring and control necessary for a normal startup or shutdown of a system to be done locally by the operators or other qualified members of the plant staff, i.e., the control and monitoring shall be manual and shall not be in the main control room. Specific tasks involved may be automated or performed in the main control room if analyses of functions and tasks (Section 3.1.3.3) show manual or local operations are a significant burden or distraction for the operators or may be unreliable.	The normal startup and shutdown of this group of systems is largely paced by the operators and may involve a very large number of individual operations, particularly local operations such as the repositioning of valves. Automation of these operations would significantly increase the complexity of the plant and is not desirable. However, there may be operations which should be automated and thereby reduce the time to startup or shutdown or lower the risk of errors.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev*
10.2.3.2	**Normal Operations**	**Normal Operations**	0
	The M-MIS for this group of systems shall normally provide for automatic or unattended operation when the plant is in nominally steady operation, including normal power changes. This applies to continuous or often repeated tasks while the plant is operating normally.	The automatic, unattended operation of this group of systems is intended to be consistent with the main control room staffing in Section 4.2.4. That requirement cannot be expected to be met if an operator is occupied most of the time by the need to control a system in this group. It is also current practice for these systems to operate without constant operator attention. Tasks that are done manually at relatively long intervals, for example, reconfiguring a system to equalize service time, probably do not need to be automated.	0
10.2.3.3	**Reconfiguration Operations**	**Reconfiguration Operations**	0
	The M-MIS shall provide for automatic reconfiguration (e.g., shutdown) or a system when necessary to avoid personnel hazard, major equipment damage, or to support actions by other parts of the plant M-MIS, for example, when the reactor is automatically shut down or a safety system is actuated. For other changes in configuration and the operations to restore the system's normal status, the necessary control and monitoring shall normally be accomplished manually outside the main control room. Return to the initial configuration may be automatic if the M-MIS Designer establishes that such automatic action would significantly:	Some reconfiguration actions cannot depend on the operators because of timing constraints or the risk of error. In addition, it has been the practice to automate such tasks.	0
	• Reduce the challenges to protection and safety systems;		0
	• Reduce hazards to personnel;		0
	• Improve the plant availability; or		0
	• Reduce the risk of damage to major plant equipment.		0
	The operators shall be notified of any such automatic return to the original configuration.		0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
10.2.3.4	**Testing Operations**	**Testing Operations**	0
	The M-MIS for this group of systems shall normally provide for on-line testing only at the direction of the operator or other qualified member of the plant staff. The testing itself should be automated and assisted as required in Section 3.6 so that operator actions are simple and have little risk of causing a plant upset. As for other operations of these systems, the testing shall normally be accomplished manually outside the main control room.	The testing of these systems often must be done while the systems are in operation. Mistakes in the testing have resulted in a loss of availability of the system, serious upsets, and even plant trips. Section 3.6 contains a number of specific requirements to enhance the testability of the ALWR. The testing strategy for these systems is intended to be consistent with those requirements.	0
10.2.4	**Integration and Coordination**	**Integration and Coordination**	0
	The M-MIS designs for the systems in this group shall be integrated and coordinated so that the overall plant performance and functional requirements as well as those of individual systems are met. Those requirements are found in Chapter 1 and in other chapters of the ALWR Requirements Document. In addition, the M-MIS Designer shall coordinate the design features with other parts of the M-MIS.	Although the requirements for the individual systems define the functions and interfaces, it is the basic responsibility of the M-MIS Designer to connect the various systems and their requirements in a sensible and efficient manner. The specific methods used to connect the operation of the various systems and the logic are to be selected by the M-MIS Designer. The ALWR Requirements Document has specifically avoided defining how this is to be accomplished. It is intended that the M-MIS Designer not be constrained to current practice and be encouraged to develop strategies for control which consider the many interactions among the various systems.	0
10.2.5	**Independence and Redundancy Requirements**	**Independence and Redundancy Requirements**	0
	The M-MIS design shall meet the requirements for independence and redundancy which are contained in the individual system chapters for the auxiliary group. In particular, failures in the M-MIS for these systems shall not contribute to plant availability or result in challenge to reactor protection or safety systems.	The requirement for integration and coordination of the overall M-MIS must not compromise the individual system requirements for independence and redundancy. The overall availability goals require that the auxiliary and support systems be very reliable. The M-MIS for these systems must also meet very high standards of reliability.	0

Paragraph No.	*Requirement*	*Rationale*	*Rev.*
10.2.6	**Fire Protection and Security**	**Fire Protection and Security**	0
	The M-MIS design shall enhance the plant capability for fire protection and security. In particular, the M-MIS for these auxiliary systems shall provide alternate control, monitoring strategies and design features so that fires and fire suppression sprinkling which would not require plant shutdown do not result in shutdown because of M-MIS equipment unavailability. The M-MIS design also shall minimize those features which would allow a security breach to disable a total system, cause plant shutdown, or disable a portion of a system needed to perform a safety function.	The requirements for active fire protection and security are contained in Chapter 9 and the requirements for passive fire protection are contained in Chapter 6. The M-MIS design needs to minimize concerns about fire and security as well as facilitate design of these protective systems.	0

Paragraph No.			*Rev.*
A.1	**DEFINITIONS OF ACRONYMS (CONTINUED)**		0
	I/O	Input/Output	0
	IPCEA	Insulated Power Cable Engineers Association	0
	LOCA	Loss of Coolant Accident	0
	LCO	Limiting Condition of Operation	0
	MCR	Main Control Room	0
	MSIV	Main Steam Isolation Valve	0
	MTBF	Mean Time Between Failures	0
	NEMA	National Electrical Manufacturers Association	0
	NSSS	Nuclear Steam Supply System	0
	P&ID	Piping and Instrument Drawing	0
	PROM	Programmable Read Only Memory	0
	PRA	Probabilistic Risk Assessment	0
	PWR	Pressurized Water Reactor	0
	QA	Quality Assurance	0
	RAM	Random Access Memory	0
	RCIC	Reactor Core Isolation Cooling	0
	RFI	Radio Frequency Interference	0
	RHR	Residual Heat Removal	0
	RO	Reactor Operator	0
	ROM	Read Only Memory	0
	RPS	Reactor Protection System	0
	RTD	Resistance Temperature Device	0
	RWCU	Reactor Water Cleanup	0
	SCA	Sneak Circuit Analysis	0
	SDV	Safety Depressurization and Vent	0
	SLC	Standby Liquid Control	0
	SQAP	Software Quality Assurance Program	0
	SRO	Senior Reactor Operator	0

Paragraph No.			*Rev.*
A.1	**DEFINITIONS OF ACRONYMS (CONTINUED)**		0
	STA	Shift Technical Advisor	0
	SVVP	Software Verification and Validation Plan	0
	TSC	Technical Support Center	0
	V&V	Verification and Validation	0
	VCT	Volume Control Tank	0
A.2	**DEFINITIONS OF TERMS**		0
	Diversity: Accomplishing an objective with two or more means which are distinctly different. Diversity can refer to functional diversity or hardware and software diversity.		0
	Redundancy: Parallel repetition of hardware and software to provide continued operation in the presence of a failure.		0
	Segmentation: Use of functional and physical separation to prevent failure in one control system or function from propagating to another and thereby reducing the chances of complex plant transients.		0
	Separation: Refers to the physical separation (by distance or barrier) of equipment to prevent coincidental failure due to local external events.		0
	Software: Any program or series of programs designed to aid in the execution of a problem program; the supervisory control programs of an operating system; a program designed to perform special functional operations for any other program that requires those services.		0

APPENDIX B GENERIC SAFETY AND LICENSING ISSUES 0

B.1 CONTROL SYSTEM FAILURES 0

B.1.1 RELATED ISSUE 0

A-47 Safety Implications of Control Systems 0

76 Instrumentation and Control Power Interactions 0

B.1.2 ISSUE SUMMARY 0

This issue concerns the potential for accidents or transients being made more severe as a result of control system failures, including control and instrumentation power supply faults. These failures or malfunctions may occur independently or as a result of an accident or transient and would be in addition to any control system failure that may have initiated the event. Although it is generally believed that control system failures are not likely to result in loss of safety functions which could lead to serious events or result in conditions that safety systems are not able to cope with, in-depth studies have not been performed. The purpose is to define generic criteria that may be used for plant specific reviews. 0

B.1.3 DISCUSSION AND REGULATORY STATUS 0

During the plant licensing process, the NRC staff performs an audit review of the non-safety grade control systems on a case-by-case basis to assure that an adequate degree of separation and independence is provided between these non-safety grade systems and the safety systems. Additionally, the audit review assures that effects of the operation or failure of these systems are bounded by the accident analysis in Chapter 15 of the plant's Safety Analysis Report. On this basis, it is generally believed that control system failures are not likely to result in loss of safety functions that could lead to serious events or result in conditions that the safety systems are not able to mitigate. In-depth studies for all the non-safety grade systems have not been performed, however, and there exists some potential for accidents or transients being made more severe than previously analyzed as a result of some of these control system failures or malfunctions. 0

To resolve this issue, an in-depth evaluation of the control systems that are typically used during normal plant operation was performed by the NRC. Upon completion, the NRC issued NUREGS which either verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to non-safety grade control system failures. 0

The NRC has completed part of this evaluation for typical PWRs and BWPs, and published the results in NUREGs CR-3958, CR-4385, CR-4386, and CR-4387. Based on these results, the NRC has indicated the following changes may be required or are desirable for future plant designs. 0

(1) Reduce the potential for steam generator (SG) overfill in PWRs by including an automatic high water level trip for the main (MFW) and emergency feedwater (EFW) systems. This reduces the potential for spillover by the MFW or by the EFW after a normal trip. Though not required, the NRC feels the automatic trip should be safety grade for future plants. At a minimum, it should be part of the technical specifications and independent of potential event initiators such as power supply failure. 0

(2) Provide a safety grade high water level trip of feedwater for BWRs. This would reduce potential for spillover into the main steam lines causing a main steam line break (MSLB). 0

(3) Include the automatic actuation of PORV block valves to protect against inadvertent PORV lifts. The automatic logic would close the upstream block valves if inadvertent opening or leakage is sensed, thereby decreasing the probability of a small break LOCA. 0

(4) Provide increased injection capability for the SIS to protect against small break LOCAs. 0

Additionally, the NRC has concerns regarding dc power systems. The main concerns include: (1) a control and instrumentation power supply fault can cause a critical challenge to standby engineered safety features; (2) the same control and instrumentation power supply fault could defeat some of the engineered safety features called upon to mitigate the initiating event; (3) the same control and instrumentation power supply fault could blind or partially blind the operators to the status of the plant. However, these concerns have not as yet been evaluated by the NRC. 0

These and other ALWR requirements concerning this issue are addressed in the ALWR Requirements Document as follows. 0

B.1.4 ELEMENTS OF RESOLUTION 0

B.1.4.1 Introduction 0

The design philosophy of the ALWR is to provide highly reliable safety grade control systems that are required to satisfy all of the current regulatory requirements intended to prevent or mitigate transient and accident events. These include requirements concerning criteria for single failure, separation, independence, redundancy, diversity, and physical protection. It is the ALWR position that all of these requirements together assure that an ALWR plant will not pose an unacceptable risk due to non-safety grade control system failures, including C&I power supply failures. The key requirements that address the issues are provided below. 0

B.1.4.2 Requirements for All ALWRs 0

- Section 2.2.F.7 of Chapter 1 requires the spatial separation of systems and equipment to prevent adverse interaction of non-safety grade equipment with safety-grade equipment. The Plant Designer must review design documentation based on operating experience to identify potential system interactions to be avoided. 0
- Section 2.2.8 of Chapter 5 requires that each division of the engineered safety systems requiring electric power be provided with an independent emergency on-site source of ac and/or dc power. If one division is defeated by C&I power supply fault, there is a separate, independently powered division to perform the safety functions. 0
- Section 2.2.9 of Chapter 5 requires that at least two separate and independent connections for off-site ac power sources capable of starting and running all Class 1E loads required for safe shutdown be provided. This prevents a C&I power supply fault from leading to a loss of off-site power. 0
- Section 2.3.1 of Chapter 5 requires that the specified functions of engineered safety systems be met by use of redundant divisions. The redundancy is necessary to meet the single failure criterion, viz., the most limiting single failure in addition to those failures which, by assumption, constitute the accident. 0
- Section 2.3.2 of Chapter 5 requires each division of engineered safety systems be totally independent and separated both mechanically and electrically except for areas in which it is physically impractical or less safe. Divisional independence and separation reduce the potential for failure propagation from one division to another. 0
- Section 2.3.4 of Chapter 5 requires the capability to depressurize and cool down the primary system using safety grade equipment, assuming a single active component failure. This eliminates the need for or use of non-safety grade control systems. 0

- Section 2.4.1.2 of Chapter 5 requires that active systems used for the containment function be single failure proof and safety grade. 0
- Section 3.2.1 of Chapter 5 requires that the core coolant inventory systems provide for redundant, safety grade means to supply injection water to the reactor vessel. 0
- Section 3.3.1 of Chapter 5 requires the decay heat removal system to be redundant and safety grade. 0
- Section 3.5 of Chapter 5 requires the ALWR diverse reactivity control system to satisfy GDC 26. 0
- Section 2.1.4 of Chapter 10 states that an objective of the ALWR design is to achieve very high reliability. It requires that the M-MIS be designed so that failures or problems in one function are incapable of propagating into other functions so that the extent of the upset is minimized and the operator burden is not increased. 0
- Section 2.2.3 of Chapter 10 states the policy that the M-MIS design should possess sufficient segmentation and independence that a failure or upset in one plant control function cannot propagate to other plant control functions and thereby overburden the operators due to complex transient events. 0
- Section 2.3.9 of Chapter 10 states that, as part of the policy for designing automatic controls, the effect of failures of automatic control systems must also be addressed as part of the process of selecting automated or manual controls. Automatic control systems should employ, wherever possible, fail safe features. 0
- Section 3.1.3.4 of Chapter 10 requires that the M-MIS design process explicitly consider the potential for and the consequences of failures of plant and M-MIS system components. 0
- Section 3.5.1.1 of Chapter 10 requires the M-MIS Designer, together with the Plant Designer, to select the appropriate failure state of the plant equipment upon loss of motive power on a case-by-case basis. The M-MIS Designer is also required to ensure that the M-MIS does not change the state of control components and is initialized in the manual mode upon restoration of power to the control systems. 0
- Section 3.5.1.2 of Chapter 10 requires that no single failure of any M-MIS equipment or its supporting equipment (e.g., HVAC, power supplies) will cause a forced plant outage. 0

Paragraph No. *Rev.*

- Section 3.5.3.1 of Chapter 10 requires that no single failure of any M-MIS equipment or its supporting equipment (e.g., HVAC, power supplies) will cause a forced plant outage. Section 3.5.3.1 of Chapter 10 requires that the functional and physical designs of the M-MIS control and monitoring systems is to be segmented to protect against failures degrading the performance of more than one major control or monitoring function. In those cases where strict segmentation of the major control functions is not practical, the designer is to identify alternative design approaches which will achieve the same functional requirement, e.g., a combina'ion of redundancy and diversity. 0

- Section 3.5.3.1.1 of Chapter 10 requires that each segmented function of the M-MIS control and monitoring systems use different sets of sensors and transmitters, and data communication paths from sensors and transmitters to data processing equipment whenever practical. This requirement minimizes use of common sensing instrumentation for more than one major control function, reducing the possibility of a single problem causing a large-scale upset that would be difficult for the operators to handle or causing multiple indications to the operator of problems in segmented functions which are confusing to the operator. 0

- Secuon 3.5.3.1.2 of Chapter 10 requires that each segmented function use different processors and power supplies (but not necessarily different power feeds or sources) whenever practical even if redundancy is employed. That is, to the degree practical, functions of one segment shall not be combined with functions of another segment in a single processor or set of processors, or power supply. This requirement minimizes the use of common processor or power supplies for more than one major control function reducing the possibility that a single problem will cause a large scale upset that would be difficult for the operaiors to handle or causing multiple indications to the operator of problems in segmented functions which are confusing to the operator. 0

- Section 3.5.3.1.3 of Chapter 10 requires that data processing and data communication electronic equipment for the different segments be housed in separate enclosures whenever practical. Equipment for segmented functions may share a common room or cubicle and be subject to a common ambient environment. The data communication links for segments are not to share a conduit or other communication pathway enclosure even if there are redundant pathways also carrying these functions. 0

- Section 3.5.3.1.4 of Chapter 10 requires that for the different segmented functions, signal communication paths, multiplexers and demultiplex units for transmitting information to the main control room displays and alarms, and for transmitting control commands from the control room to the data processing or output processing equipment, have separate power supplies and be housed in separate enclosures outside the control room to the maximum degree practical. This requirement is to prevent propagation of failures originating in the data communication paths between the control room and data processing equipment or originating in the multiplex/demultiplex equipment at either end. 0

- Section 3.5.3.1.5 of Chapter 10 requires that, to the maximum degree practical, segmentation within major functions of the M-MIS are to mimic the segmentation within the mechanical systems being monitored and controlled. This requirement is intended to prevent single failures of problems in the M-MIS which can result in a loss of control or monitoring of the infra-function segments provided by the mechanical portion of the system. An example would be a single failure within the pressure control function of the M-MIS which would result in a loss of control of all banks of pressurizer heaters. 0

- Section 6.2.6.1 of Chapter 10 requires that the engineered safety signal isolation devices provide Class 1E to non-Class 1E digital and analog signal isolation while maintaining Class 1E integrity in accordance with Regulatory Guide 1.75. 0

- Section 6.3.2.2 of Chapter 10 requires that software interface of a safety-related system with a non-safety-related system is discouraged. If the designer chooses to do so, the designer is to demonstrate that isolation is provided to preclude the propagation of errors from a non-safety-related system to a safety-related system. 0

B.1.4.3 Additional Requirements for BWRs 0

- Section 4.2.2.1 of Chapter 5 requires three independent divisions for the CCIC and DHR systems. 0

- Section 4.2.3.1.11 of Chapter 5 requires separation of the divisions for the CCIC and DHR systems to protect each division against damage resulting from failure of another division. 0

- Section 4.2.7.1 of Chapter 5 requires that each division of the CCIC and DHR systems have its own independent emergency ac and dc power source. 0

B.1.4.4 Additional Requirements for PWRs 0

- Section 3.3.2 of Chapter 3 requires that the pressurizer size and spray capacity be sufficiently large that automatically actuated PORVs are not required to mitigate overpressure transients. With no PORV, the concern for inadvertent opening of the PORV is eliminated. 0

- Section 3.3.4 of Chapter 3 requires that a leak detection system be provided for each pressurizer safety valve. 0

- Section 4.2.3.4 of Chapter 3 requires the emergency feedwater control system to have a safety grade actuation feature. 0

- Section 5.1.2.1 of Chapter 5 requires two independent divisions for the CCIC and DHR functions. 0

- Section 5.2.3.1.1 of Chapter 5 requires two independent divisions of RHR. 0

- Sections 5.3 and B.4 of Chapter 5 describe the emergency feedwater system (EFW). The EFW is required to be a dedicated safety grade system and to be automatically initiated, when main feedwater pumps are lost, on low SG level by a safety grade actuation system. 0

- Section 5.4 of Chapter 5 describes the safety injection system (SIS). The SIS is required to have sufficient decay heat removal capability to satisfy performance requirements for feed-and-bleed operation. This provides the small break LOCA coverage desired in NRC's recommendation number discussed in B.1.3 above. 0

- Section 5.5.4 of Chapter 5 requires the safety depressurization and vent system (SDVS) to have two valves in series for each train such that vent flow can be terminated, assuming a single failure. Additionally, indication of downstream temperature will be available providing leak detection capability. This requirement, along with the elimination of the PORV, precludes the need for NRC's recommendation number discussed in B.1.3 above. 0

Paragraph No. | *Rev.*

B.1.4.5 Resolution Summary 0

Resolution of this issue has been achieved by a design that exceeds current requirements concerning reliability, separation, redundancy, diversity, independence, and physical protection and provides design improvements which meet or exceed NRC recommendations for future plants. Together, these design requirements and design improvements assure that an ALWR plant will not pose an unacceptable risk due to non-safety grade control system failures, including C&I power supply failures. However, it is an ALWR requirement that the ALWR design will satisfy NRC requirements and, thus, any additional criteria resulting from this issue will also be met by the ALWR design. Based on these requirements, this issue should be considered resolved for the ALWR. 0

B.2 EQUIPMENT PROTECTIVE DEVICES ON ENGINEERED SAFETY FEATURES 0

B.2.1 RELATED ISSUE 0

2 Failure of Protective Devices on Essential Equipment 0

110 Equipment Protective Devices on Engineered Safety Features 0

B.2.2 ISSUE SUMMARY 0

There have been a large number of failures or incapacitation of essential equipment as a result of either the failure or the intentional bypass, by ESF actuation signals, of protective devices intended to trip active ESFs for indications of equipment faults. The systems affected exist throughout the plant and include the plant control system, the plant protection system, and the engineered safety features. Particularly vulnerable are actuators that require power in order to drive motors and operate valves. The failures are not limited to overcurrent protectors but occur in equipment such as torque limiters, overspeed protectors, and other interlocks and may be caused by improper applications or adjustments as well as component failures. In cases where the protective devices are intentionally bypassed, the rationale has been that, in a genuine demand, it is better to risk self-destruction of the engineered safety feature than to tolerate spurious trips when the equipment is required. However, probabilistic risk assessments are showing that there is often sufficient time periods to diagnose the fault and override the protective trip if necessary. Thus, it appears plausible that it may be safer to trip the equipment to enable evaluation, repair, and restart without potential equipment damage. 0

B.2.3 DISCUSSION AND REGULATORY STATUS 0

This issue was identified by the ACRS in NUREG-0572. The NRC is concerned that the reliability estimates for essential equipment may not account properly for failure of the protective devices. Because of some reports of the loss of redundant devices through failures of circuits intended to be independent, there is an increased probability of common mode failure of redundant vital services. 0

The NRC intends to study this issue further to determine if there is an increase in failure rate estimates for essential equipment and if essential equipment could be made significantly more reliable by improving reliability of protective devices. 0

Paragraph No. *Rev.*

B.2.4 ELEMENTS OF RESOLUTION 0

B.2.4.1 Introduction 0

The ALWR approach to the problem presented in this issue is to design engineered safety feature equipment and protective devices that have a high reliability. Both spurious trips from the equipment protective devices and actual ESF equipment faults will be minimized. In addition, the ESF equipment will be more robust and able to survive actuations when faults are present. The requirements in the ALWR Requirements Document which achieve this are as follows. 0

B.2.4.2 Requirements for All ALWRs 0

- Section 2.2.7 of Chapter 5 requires ALWR plant systems to embody sufficient robustness of design to tolerate a conservative number of spurious or inadverter [illegible] 'eered safety system actuations without the need for follow-up t [illegible] inspections to verify systems' integrity or operability. This would also give the engineered safety feature equipment a higher probability of tolerating actuations when equipment faults are indicated by protective devices. 0
- Section 2.3.2 of Chapter 5 of the ALWR Requirements Document requires each division of engineered safety systems to be totally independent electrically except for areas in which it is physically impractical or less safe. Divisional independence and separation reduce the potential for propagation from one division to another. This requirement is intended to reduce the use of cross-connections. This will minimize the potential for common mode failures in vital services. 0
- Section 2.2.3 of Chapter 10 specifies the ALWR policy, concerning instrumentation, control, and protection systems, that robust system design, including segmentation of major functions, separation of redundant equipment within a segment, and fault tolerant equipment, will be used to achieve high reliability and protection against the propagation of failures. 0
- Section 2.2.4 of Chapter 10 specifies the ALWR policy regarding in-service testing of the M-MIS. Chapter 10 requires the M-MIS equipment to be designed and configured to readily support in-service testing by providing built-in test features, incorporating good human factors principles, and avoiding the use of undesirable features such as test jumpers or lifting of leads. 0

- Section 3.1.3.4 of Chapter 10 requires that the Man-Machine Interface Systems (M-MIS) design process explicitly consider the potential for and the consequences of failures of plant and M-MIS system components. That is, functions and tasks which result from the opera:or coping with equipment failures are to be identified as part of the M-MIS design bases. The analysis and validation testing of the M-MIS is to include the postulated failures and recovery from them. 0

- Section 3.6.1 of Chapter 10 requires that the capability for continuous on-line self-testing of hardware integrity be provided for as much of the M-MIS as is practical. This testing is not to affect the system functionality and is to be performed on the module, as opposed to the system basis. 0

- Section 3.6.4 of Chapter 10 requires that, upon detection of a failure in the M-MIS, a system be designed so that it can be placed in a configuration such that an additional single failure will not prevent system-level protection or safety action. This reconfiguration is to be automatic in the case of continuous on-line self-testing with notification of the new reconfiguration given to the operator. 0

- Section 3.7.4 of Chapter 10 requires that the mean time to detect and repair failures down to the lowest replaceable module, averaged across all types of M-MIS equipment for the entire design life, is to be less than four hours. The maximum time to detect and repair failures of any M-MIS module is to be less than eight hours. This time is to include the time to detect the failure, gain access to the faulty equipment, determine the necessary repair, obtain necessary replacements or spares, make the repair or replacement, and verify that the repair has been successfully accomplished. This requirement applies to all M-MIS equipment with self-test capability. 0

- Section 8.3.2.4 of Chapter 10 requires that no single failure in the RPS prevent or cause the initiation of protection action. A second failure in the RPS is not to prevent the protective action. 0

B.2.4.3 Resolution Summary 0

The ALWR approach is to design the engineered safety feature (ESF) equipment and protective devices to be highly reliable. The ALWR ESF equipment will be designed to experience fewer equipment faults and spurious trips by protective devices, and it also will be more robust and likely to operate when faults are present. Therefore, this issue should be considered resolved for the ALWR. 0

B.3 DESIGN FOR ATWS EVENT 0

B.3.1 RELATED ISSUE 0

75 Generic Implications of ATWS Events at Salem Nuclear Plant 0

B.3.2 ISSUE SUMMARY 0

On two occasions, Salem Unit 1 failed to scram automatically due to failure of both reactor trip breakers to open on receipt of an actuation signal. In both cases the unit was successfully tripped by manual action. The failure of the breakers has been attributed to excessive wear due to improper maintenance of the undervoltage relays which receive the trip signal from the protection system and cause mechanical action to open the breakers. Failure to scram (also commonly referred to as anticipated transient without scram) could result in unacceptable consequences. 0

B.3.3 DISCUSSION AND REGULATORY STATUS 0

The NRC investigated the two Salem events and reported the results in NUREG-0977. An NRC task force was formed to study the overall generic implications of these events and the results were reported in NUREG-1000. Subsequently, the task force outlined the proposed actions for licensees, applicants, and the NRC staff in SECY 83-248. This lead to the NRC issuing the required actions for licensees and applicants in Generic Letter 83-28. 0

Additionally, AEOD reviewed the Salem events and published a report which focused on two issues: (1) the adequacy of NRC's reporting requirements and (2) the potential for trends and patterns analyses to predict such events before they occur. From the conclusions of this report, AEOD plans a number of actions and endorsed other planned actions. 0

The NRC considers that the actions resulting from the NRC task force and AEOD reports can be categorized as either licensee actions or staff actions. The licensee actions are those published for licensees and applicants in Generic Letter 83-28 and are considered resolved with issuance of the generic letter. Of the staff actions, all but two were either prioritized as licensing issues, as not applicable, or as being covered by the ATWS rule amendment (USI A-9) or the Human Factors Program. The remaining two staff actions may result in requirement changes under this issue. 0

The licensee actions from Generic Letter 83-28 are summarized as follows: 0

1. Post-trip Review - This action addresses the program, procedures and data collection capability to assure that the causes for unscheduled reactor shutdowns, as well as the response of safety-related equipment, are fully understood prior to plant restart. 0

2. Equipment Classification and Vendor Interface - This action addresses the programs for assuring that all components necessary for accomplishing required safety-related functions are properly identified in documents, procedures, and information handling systems that are used to contrc' safety-related plant activities. In addition, this action addresses the establishment and maintenance of a program to ensure that vendor information for safety-related components is complete. 0

3. Post-maintenance Testing - This action addresses post-maintenance operability testing of safety-related components. 0

4. Reactor Trip System Reliability Improvements - This action is aimed at assuring that vendor-recommended reactor trip breaker modifications and associated reactor protection system changes are completed in PWRs, that a comprehensive program of preventive maintenance and surveillance testing is implemented for the reactor trip breakers in PWRs, that the shunt trip attachment activates automatically in all PWRs that use circuit breakers in their reactor trip system, and to ensure that on-line functional testing of the reactor trip system is performed on all LWRs. 0

The two staff actions which may result in requirements are summarized as follows: 0

1. Quality Assurance (operations) - The staff plans to issue Revision 3 to Regulatory Guide 1.33, *Quality Assurance Program Requirements (Operation)* which will contain detailed procedures and more stringent criteria for operational Quality Assurance Programs. 0

2. General Operating Criteria - The staff proposes to draft a set of general operating criteria, analogous to the currently used general design criteria, which would codify good operating practices. The areas to be addressed in the general operating criteria would include the following: 0

   - Management philosophy and policies; 0
   - Management oversight and review responsibility; 0
   - Organization and communication; 0
   - Operating and emergency procedures; 0
   - Staffing, qualifications, and training; 0
   - Assurance of quality in operations; 0
   - Preventive and corrective maintenance; 0
   - Data collection, use, retention and reporting; 0
   - Operating experience evaluation; 0
   - Replacement of equipment; 0

- Planning and scheduling of safety-related work; 0
- Post-maintenance and periodic inspection and testing. 0

B.3.4 ELEMENTS OF RESOLUTION 0

B.3.4.1 Introduction 0

Some of the major elements discussed under this issue are being addressed for resolution elsewhere. An important example is the ATWS rule amendment (10CFR50.62) which was resolved under USI A-9. The impact of the ATWS rule amendment and other ATWS related requirements, resulting from other issues, on the ALWR design are not covered under this issue. Additionally, some of the staff actions which were prioritized as licensing issues or as not applicable, do not directly affect plant design and so will not be addressed here. Finally, this leaves the four licensee actions in Generic Letter 83-28 and the two remaining staff actions from NUREG-1000 as the actions from this issue which may impact the ALWR design. 0

The two staff actions (operations quality assurance and general operating criteria) concern the operation of nuclear power plants and are not within the scope of the ALWR Requirements Document; however, there are requirements on the ALWR design which will impact how operations in these areas are carried out. The four licensee actions (post-trip review, equipment classification and vendor interface, post-maintenance testing, and reactor trip system reliability improvements) generally concern programmatic efforts by an operating plant and, as such, are not totally within the scope of the ALWR Requirements Document; however, there are requirements on the ALWR design which will impact how these operations are carried out. 0

The requirements in the ALWR Requirements Document which have major impact on the two staff actions and the four licensee actions are summarized below. Note that these do not include the requirements which deal with meeting the ATWS rule, e.g., Sections 8.3.2.7 and 8.3.2.8 of Chapter 10 which deal with backup reactor trip systems, or the requirements on protection features directly mandated by 10CFR50.62. 0

B.3.4.2 Requirements for All ALWRs 0

Requirements which impact operational quality assurance include: 0

- Section 6.1.2 of Chapter 10 defines quality assurance requirements for the increased software which is expected to be used in the ALWR M-MIS. The M-MIS Designer is required to consider the entire software life cycle not just the initial preparation. 0

Requirements which have special impact on operating criteria include: 0

- Section 4.6 of Chapter 10 defines requirements for plant voice communication systems. 0
- Section 2.2.10 of Chapter 10 establishes the policy that operating and emergency procedures, including alarm response procedures, will be directly displayed to operators at the main control room work stations. 0
- Section 4.1.6.4 of Chapter 10 requires that the M-MIS Designer prepare generic operating procedures for all work stations and to validate them using mockups and active simulation. 0
- Sections 2.2.7 and 4.2 of Chapter 10 state the policy for operator staffing and define the staffing basis to be used in the design of M-MIS work stations. 0
- Section 5 of Chapter 10 defines the requirements for the plant data gathering, transmission, and processing systems. These systems will provide enhanced capability to collect and process plant data compared to existing plants as well as provide aids for the operator to track various plant activities, such as maintenance and testing, and help the operators in the decision-making process. 0
- Section 3.7 of Chapter 10 requires the M-MIS to simplify and reduce the amount of difficulty of maintenance required over the lifetime of the plant. This includes requirements on maintenance burden, planning for replacement, and other specific requirements aimed at simplifying the operating practices in the maintenance area. 0

Requirements which impact the capability to perform post trip reviews include: 0

- Section 5 of Chapter 10 defines the requirements for plant data collecting including data time tagging (5.4.1) which is essential for adequate post-trip review. 0
- Section 4.3.4.8 of Chapter 10 defines the requirements on maintaining the time sequence of alarms for post-event analysis. 0

Requirements which impact equipment classification are addressed by the requirements of Chapter 1 which define the configuration management system for the ALWR plant. 0

Requirements which impact post-maintenance testing include: 0

- Section 2.2.4 of Chapter 10 states the policy that the ALWR design provide a high degree of testability of the M-MIS, particularly self-testing, and Section 3.5 of Chapter 10 provides requirements to carry out this policy. The high degree of testability which will be required of the M-MIS will facilitate performing post-maintenance testing. The self-test features will reduce the number of special post-maintenance tests which are needed. 0
- Section 3.1.3.6.1 of Chapter 10 requires that test plans be prepared for all systems and components and specifically requires that these plans include the tests required to verify the operability of systems or components after maintenance. 0
- Section 3.7.7.1 of Chapter 10 requires that the M-MIS Designer identify the tasks required to maintain the M-MIS, including any testing required as part of the maintenance. Section 3.7.7.2 of Chapter 10 requires these maintenance tasks be evaluated to assure they can be accomplished. 0

Requirements which impact reactor trip reliability include: 0

- Section 3.5 which requires detailed, systematic analysis of the reliability of the M-MIS and, therefore, the reliability of reactor trip. 0
- Section 8.3.4.1.1 of Chapter 10 requires that the M-MIS Designer identify problems associated with the design, operation, maintenance, and testing of existing reactor trip breakers. The M-MIS Designer is to establish functional and design requirements, manufacturing specifications, and a factory testing plan for the ALWR reactor trip devices which specifically address the problems associated with existing reactor trip breakers. A specific review of these problems should assure that they are not repeated in the ALWR. 0
- Section 8.3.4.1.2 of Chapter 10 requires that the M-MIS Designer select a reactor trip device which is specifically designed to withstand without degradation the expected number of operations associated with maintenance and testing, as well as actual trips, over the life of the plant. 0

B.3.4.3 Resolution Summary 0

The requirements in the ALWR Utility Requirements Document concerning M-MIS testability, data gathering, transmission and processing, RPS redundancy and diversity, and the selection and maintenance of the reactor trip breakers will greatly aid the operating ALWR in meeting future requirements resulting from this issue. And, although the total resolution of this issue is not within the scope of the ALWR Requirements Document, the requirements of this issue, including the requirements of the ATWS rule in 10CFR50.62, will be met by the ALWR design. Therefore, this issue is considered resolved for the ALWR. 0

Paragraph No.		Rev.
B.4	**DESIGN OF ABWR WATER LEVEL INSTRUMENTATION**	0
B.4.1	**RELATED ISSUE**	0
	101 Break Plus Single Failure in BWR Water Level Instrumentation	0
B.4.2	**ISSUE SUMMARY**	0
	An NRC concern has been identified for BWRs about a postulated break in an instrument line in conjunction with the worst single failure. The concern is that if one of two reference columns breaks, a single failure associated with the other reference column could completely defeat mitigation systems for the resulting transient.	0
B.4.3	**DISCUSSION AND REGULATORY STATUS**	0
	BWRs typically have two reference columns in their water level instrumentation. Water level is measured by means of differential pressure sensors connected between the reactor vessel and the reference columns which are full of water. If a reference column is broken, the water in it will flash to steam and the water level indication in all channels connected to the broken column will give a false "high" reading.	0
	The scenario, first identified by the AEOD, is that one of the reference columns breaks and a worst single failure causes the other one to indicate high water level. This could lead to the possibility of a low water level situation where the false high water signals would prevent mitigating systems, such as ECCS, from initiating. In some plants this may lead to core uncovery.	0
	However, since designs of water level instrumentation vary, the above worst case scenario is less severe in many BWRs and not applicable to some. Therefore, since there is no single scenario, the NRC does not recommend a generic solution or specific modifications at this time.	0

B.4.4 ELEMENTS OF RESOLUTION 0

Section 3.3.3.2.1 of Chapter 4 requires that a wide range set of reactor pressure vessel level instruments, consisting of four divisions with instrument taps located in each of four quadrants, shall provide signals for reactor protection and safety systems. These taps permit the use of two-out-of-four logic. In addition to this basic capability for multiple level instruments, Chapter 10 includes requirements on the design process and on reliability which should assure that the ALWR is not subject to the scenario identified in this issue. In particular, Section 3.1.3.1 of Chapter 10 requires the M-MIS to perform a review of existing LWR plant designs to identify problems and develop ALWR design solutions for the problems identified. The requirements for availability and reliability of Section 3.5.1 require that no single random failure of any M-MIS equipment will cause a forced outage. Additional requirements of Section 3.5.2 address multiple random failures of M-MIS equipment, and their effects are addressed in Section 3.5.4.3. This issue should be considered resolved for the ALWR. 0

B.5 ACCIDENT MANAGEMENT 0

B.5.1 RELATED ISSUE 0

116 Accident Management 0

B.5.2 ISSUE SUMMARY 0

The emergency procedure guidance has resulted in training operators in the avoidance of degraded cooling of reactor cores. It has not trained them in the diagnosis, prognosis, or management of accidents which go beyond a point of no return to core meltdown. Should a core meltdown accident occur, operators without procedures and untrained in core melt accident progression, phenomena, and consequences may very well (1) fail to take full advantage of opportunities to delay or minimize containment failure and the release of fission products and (2) they may give erroneous advice and guidance on the prognosis of the accident to emergency response personnel, leading to inappropriate emergency response actions. 0

B.5.3 DISCUSSION AND REGULATORY STATUS 0

The NRC has not completed its evaluation of this issue, but it is scheduled to be prioritized some time in 1989. 0

B.5.4 ELEMENTS OF RESOLUTION 0

B.5.4.1 Introduction 0

The subject of this issue, the training of plant operators in the diagnosis, prognosis and management of accidents, is not within the scope of the ALWR Requirements Document. As such, this issue cannot be totally resolved by the requirements of this document. However, as stated in Chapter 1 of the ALWR Requirements Document, one of the primary objectives of the ALWR design is to reduce, relative to previous plants, the probability and consequences of accidents that could endanger the safety of in-plant personnel or the general public, cause radioactive release, or damage plant equipment. To meet this objective, the ALWR will reduce dependence on active systems and components to achieve safety and increase dependence on characteristics such as natural circulation, low power density and increased coolant inventory. Also the ALWR design will improve operator performance by the simplification of systems and controls, by providing information in a direct easily understood form, and by the use of human engineering in the overall plant, including the main control room, remote shutdown panel, and local control stations. Some of the requirements in the ALWR Requirements Document that achieve these objectives are as follows. 0

Paragraph No. *Rev.*

B.5.4.2 Requirements for All ALWRs 0

- Section 2.3 of Chapter 1 provides overall plant design requirements for the ALWR to reduce the probability and consequences of accidents from those in current LWRs. These requirements concern preventing core damage for pipe breaks up to a certain size, increased operating margin, increased operator transient response time, less dependence on active systems and components, and more dependence on characteristics such as natural circulation, low power density, and increased coolant inventory. 0

- Section 2.2.3 of Chapter 5 requires that engineered safety systems be designed for simplification so as to make the operators' procedures less complex and interdependent, particularly for emergency conditions. 0

- Section 2.3.6 of Chapter 5 requires the operators to be provided with sufficient information to assess core cooling conditions and to perform the CCIC and DHR functions. Any information needed to perform these functions is to be determined by direct measurement. Unambiguous alarms are to alert the operator to the need for manual action to provide the CCIC or DHR function in abnormal situations. 0

- Section 2.4.2.8 of Chapter 5 requires the ALWR plant design to contain instrumentation sufficient to determine whether core damage has occurred. 0

- Section 3.2.2 of Chapter 5 requires the source of core coolant inventory makeup to be adequate for at least 36 hours without need for manually switching suction sources for non-LOCA events. This minimizes operator actions during reactor shutdown. 0

- Section 3.3.6 of Chapter 5 requires that the decay heat removal systems be designed to provide sufficient thermal and operational range envelope to preclude operational difficulties in transfer from normal to shutdown cooling. The operational difficulties includes taking into account instrument errors and operator response time for required operator action with some margins. 0

- Section 6.6.5.2 of Chapter 5 requires that instrumentation to indicate the presence of water inventory in the cavity or drywell prior to reactor vessel melt-through be provided to assist the plant operators in decision making. 0

- Section 7.3.3 of Chapter 5 requires that instrumentation be provided to monitor containment conditions during all plant operating and postulated accident conditions. 0

- Section 2.2 of Chapter 10 discusses the policy of the ALWR Utility Requirements Document concerning the control room, local control stations, and remote shutdown panel. The objectives are to take full advantage of overall plant simplification to reduce or eliminate the need for complex or complicated control systems or operator tasks; provide automatic controls where warranted, considering system response requirements, complexity of operation, plant conditions, impact of misoperation, and regulatory requirements; and to provide expert system capability to perform artificial intelligence where feasible. 0

- Section 2.2.10 of Chapter 10 describes the ALWR main control room concepts. Several of its key features will greatly aid the ALWR operator in accident management. Some of these features are: 0

  - Electronically displayed normal and emergency procedures. 0

  - Electronically displayed presentations of plant operational parameters and technical data based on operator tasks and event categories in graphical and diagrammatical format showing present values, trends over various operator selected intervals, acceptable ranges, set points, control bands, correlations, and other explanatory information. 0

  - Electronically displayed alarms, designed specifically (based on plant conditions) to minimize nuisance alarms. Alarm messages should be organized and coordinated with the overview displays as well as workstation displays and controls to support the decision-making approach. The workstation should provide alarm reflash capability and access to electronically displayed alarm data sheets to provide basic causal and recommended recovery action information. Diagnostic aids should be employed to help operators investigate problems and plan recovery actions. 0

  - Plant equipment and controls that are well coordinated with the decision-making approach, overview displays, and workstation presentations. 0

- Sections 3 and 4 of Chapter 10 provide requirements on design of the M-MIS and the ALWR control stations. These requirements implement the objectives and policy discussed in Sections 2. These ALWR requirements will help assure improved operator performance with less likelihood of inappropriate emergency response actions by providing human factored control stations that are better designed for diagnosis, prognosis, and accident management. 0

B.5.4.3 Additional Requirements for BWRs 0

- Section 4.2.6 of Chapter 5 requires that, for the CCIC and DHR systems, status indication be provided for any switched function and any bypassed or manual override, that instrumentation provided to monitor process conditions be sufficient to analyze performance of the system and to detect problems with the operation of equipment. 0

B.5.4.4 Additional Requirements for PWRs 0

- Section 5.2.3.12.4 of Chapter 5 requires that the capability be provided to permit control of RHR operation from the standby shutdown panels. This is to include providing the operators with sufficient information to permit such control to be readily accomplished. 0
- Section 5.2.3.13.1 of Chapter 5 requires that adequate information and warnings be provided to the plant operator for proper system operation and avoiding loss of RHR. 0
- Section 8.1.3.2 of Chapter 5 requires that instrumentation be provided to monitor conditions within containment following an accident. 0

B.5.4.5 Resolution Summary 0

Although the emergency procedure guidance and the training of operators are not within the scope of this document, the requirements in the ALWR Requirements Document are designed to minimize operator error and improve plant performance in preventing and mitigating accidents. This will be achieved by the use of simplification of systems and controls, improved instrumentation, good human engineering, and a shift of reliance on active systems and components for safety to characteristics such as natural circulation, low power density and increased coolant inventory. This will lead to improved, simpler emergency procedure guidance and operator training on the diagnosis, prognosis, or management of accidents. Because the ALWR will develop emergency procedure guidance and an operator training program based on the above described ALWR design and the requirements and/or recommendations resulting from this issue, this issue should be considered resolved for the ALWR. 0

B.6 SAFETY-RELATED OPERATOR ACTION 0

B.6.1 RELATED ISSUE 0

B-17 Criteria for Safety-related Operator Actions 0

B.6.2 ISSUE SUMMARY 0

This issue involves developing criteria for safety-related operator action (SROA) during the response to or recovery from transients and accidents. The criteria would include a determination of actions that are to be automated in lieu of operator action and the development of a time criterion for SROA. Specifically to be determined is whether or not to require an automatic switchover from the injection mode to the recirculation mode following a LOCA. 0

B.6.3 DISCUSSION AND REGULATORY STATUS 0

The development and implementation of criteria for SROA may result in automating some actions currently performed by the operator. The NRC expects that this would reduce the potential for operator error. Of particular concern to the NRC is the automation of the ECCS realignment following a LOCA, which is currently a manual operation in some PWRs. This is a concern because the ECCS realignment operations is dependent on break size and must be accomplished before the borate water storage tank is depleted. The SROA criteria would also include a time criterion, that is, a maximum time for the operator to take a specified safety-related action after the initiation of the event. Implementation of a new SROA criteria may result in changes and additions to the ALWR design for the ESF control systems, but the impact is expected to be minimal. 0

B.6.4 ELEMENTS OF RESOLUTION 0

B.6.4.1 Introduction 0

The ALWR plant design requires the automation of the initiation of protection and safety systems and, in addition, the automation of the operation of these systems for at least 20 minutes. The capability for manual initiation and operation is not precluded, and adequate information and control capabilities are required so that the operators can effectively provide back-up for the automated actions. 0

B.6.4.2 Requirement for All ALWRs 0

- Section 2.3.A.3 of Chapter 1 of the ALWR Requirements Document specifies the ALWR overall requirements for the time after an event is initiated in which the operator must act as not less than 20 minutes with a target of 30 minutes, assuming a single failure. This same time requirement is also specified for certain automated safety-related actions such as in Section 3.3.8 of Chapter 5 for automatic initiation of the PWR decay heat removal systems. 0

- Section 2.1.1 of Chapter 10 states the objective of the ALWR design shall be to take full advantage of operator capabilities, but not to challenge operator limitations. 0

- Section 2.2.9 of Chapter 10 states the policy for the design of the ALWR M-MIS which requires that each monitoring, control, and protection function be evaluated as part of the design process to determine the appropriate level of automation. Consideration is required of such factors as operator workload, system response, operation complexity, level and duration of the operator's attention, and failure of the automatic features. 0

- Section 3.4.3 of Chapter 10 requires that the design choice on automatic versus manual control or monitoring is to be based on evaluations which specifically include consideration of operator workload, operator capability, past experience with automatic or manual controls or monitoring in similar applications, operator vigilance and the need to keep the operator involved and knowledgeable as to the plant status, amount and complexity of M-MIS equipment (including software) and the resulting maintenance and testing burden, the consequences of and potential for malfunctions of the automatic equipment and for operating errors, and regulatory requirements. 0

- Section 8.2.3 of Chapter 10 defines the control and monitoring strategies which shall be used for protection and safety systems. This includes the requirement that startup or actuation of these systems shall be automatic but with an effective manual backup. It also requires that these systems operate automatically after actuation for at least 20 minutes and that manual operations be limited so that essentially continuous manning for extended periods of time, e.g., hours or days, is not required. 0

- The part of this issue concerning automatic versus manual ECCS realignment does not apply to the ALWR PWR. The PWR safety injection system (SIS) maintains inventory by pumping water from an in-containment refueling water storage tank (IRWST) to the reactor vessel. The IRWST provides a continuous source of water to the SIS pumps because water collects in the IRWST and thus eliminates the need for realignment of the SIS pumps for long-term post-LOCA recirculation. 0

B.6.4.3 Resolution Summary 0

The ALWR design will satisfy NRC requirements concerning automation of safety-related operator actions and operator response times. Since that part of the issue concerning automatic realignment of ECCS is nct applicable to the ALWR by design, this issue is considered resolved for the ALWR. 0

Paragraph No. *Rev.*

B.7 FEED-AND-BLEED COOLING 0

B.7.1 RELATED ISSUE 0

122.2 Initiating Feed-and-Bleed 0

B.7.2 ISSUE SUMMARY 0

During the loss of feedwater event at Davis-Besse, the operators were reluctant to initiate feed-and-bleed cooling. This issue deals with the adequacy of emergency procedures, operator training, and available plant monitoring systems for determining the need to initiate feed-and-bleed cooling following loss of the steam generator heat sink. 0

B.7.3 DISCUSSION AND REGULATORY STATUS 0

Feed-and-bleed cooling is a last resort method of core cooling following loss of feedwater at most PWRs. It must be manually initiated and is not currently required by the NRC. 0

During the loss of feedwater event at Davis-Besse, the steam generators became dry, meeting the criteria for the initiation of feed-and-bleed cooling. However, feed-and-bleed cooling was not initiated by the operators, possibly, for the following reasons: 0

- They believed restoration of the auxiliary feedwater was imminent. 0
- Feed-and-bleed cooling releases primary coolant to the containment, requiring extensive shutdown to decontaminate. 0
- The operators were unsure that the criteria to initial feed-and-bleed were met due to inadequate control room instrumentation and an unavailable SPDS. 0

The NRC is concerned that procedures and/or training may not be adequate to assure a high reliability of operators initiating feed-and-bleed cooling when it is necessary to avert core-melt. The NRC will investigate the need for additional regulatory guidance for emergency operating procedures, operator training and/or instrumentation for the manual initiation of feed-and-bleed cooling. The general technical aspects of feed-and-bleed decay heat removal are addressed under Unresolved Safety Issue A-45. 0

B.7.4 ELEMENTS OF RESOLUTION 0

This is generally an operating plant issue in that its resolution mainly involves operator training and the development of emergency operating procedures. Some of these issues are not within the scope of the ALWR design. However, other aspects of this issue related to operating procedures and control room instrumentation are addressed in Chapter 10. Section 3 of Chapter 10 requires the M-MIS Designer to perform a complete analysis of functions and tasks to be performed by the operator. The results of the function and task analysis will be used in the development of control room instrumentation and operating procedures. 0

The operators at Davis-Besse, because of inadequate control room instrumentation and an unavailable SPDS, were unsure if the criteria for initiating feed-and-bleed cooling was met. To address this problem in the ALWR, Chapter 10 of the ALWR Requirements Document requires that the ALWR include highly reliable control room instrumentation providing all information needed for operators to carry out their functions and tasks, including the ability to determine conditions in the steam generators. 0

The requirements on control room instrumentation reliability will ensure that the ALWR operators will be able to easily determine if conditions in the steam generator require the initiating of feed-and-bleed cooling. Therefore, this issue should be considered resolved for the ALWR. 0

Paragraph No. *Rev.*

B.8 SAFETY PARAMETER DISPLAY SYSTEM AVAILABILITY 0

B.8.1 RELATED ISSUE 0

125.I.3 Long-term Generic Actions as a Result of the Davis-Besse Event of 6/9/85 – SPDS Availability 0

B.8.2 ISSUE SUMMARY 0

During the Davis-Besse loss of feedwater event, the PORV stuck open and both steam generators (SG) became "dry". The operator was unaware of this, partly, because the SPDS was inoperable and therefore not available to supply information so that the operator could determine the PORV and SG status. This issue would determine if NRC requirements should be revised regarding SPDS availability. 0

B.8.3 DISCUSSION AND REGULATORY STATUS 0

At Davis-Besse the SPDS has the capability of displaying a full range of relevant plant parameters and trends on demand by the operator. Although the SPDS has two channels or trains, both were inoperable prior to the event. If the channels had been available, the operators could have used the SPDS in two ways to have alleviated the loss of feedwater event at Davis-Besse. These were: 0

(1) The PORV stuck open causing a rapid depressurization of the RCS thus aggravating recovery from the event. The operator believed the PORV was closed, based on the signal indicator and indicated pressurizer level. There was an acoustic monitor available to verify PORV closure which was not used. An available SPDS could have trended RCS pressure and temperature and OTSG pressure and level, providing information needed to determine PORV status. 0

(2) When both steam generators are dry, the operators are to initiate the "feed-and-bleed" method for decay heat removal. The instrumentation in the Davis-Besse control room was inadequate to determine with certainty if these conditions exist in a steam generator. The SPDS was intended to provide this information. The shift supervisor knew that the feed-and-bleed cooling may be required, but partly due to the lack of definitive information the SPDS would have supplied, he did not initiate it. 0

As in both of these cases, the SPDS is a secondary source of information to be used to verify status or operator analysis of the situation initially determined from other primary sources. Even though in NUREG 0696 the NRC gives an operational unavailability goal for Emergency Response Facilities of 0.01, which includes the SPDS among other systems, there are currently no requirements on operational availability of SPDS alone. 0

The NRC has prioritized this issue as "nearly-resolved" and is currently drafting a generic letter, licensing and inspection guidance, and a NUREG. 0

B.8.4 ELEMENTS OF RESOLUTION 0

The ALWR will provide highly reliable information processing and display systems that provide all information the operators require to carry out their functions and tasks, including maintaining an awareness of the status of all important safety parameters. Monitoring of safety parameters will be a part of the overall M-MIS design and will not be an "add-on" system (SPDS) as in existing plants. This will enhance the effectiveness of safety parameter monitoring. These requirements, along with the commitment to meet any availability requirements resulting from this issue, will assure reliable monitoring of safety status at ALWR plants. Therefore, this issue is considered resolved for the ALWR. 0

B.9 PLANT-SPECIFIC SIMULATOR 0

B.9.1 RELATED ISSUE 0

125.I.4 Long-term Generic Actions as a Result of the Davis-Besse Event of 6/9/85 – Plant-Specific Simulator 0

B.9.2 ISSUE SUMMARY 0

This issue concerns the need for a plant specific simulator. 0

B.9.3 DISCUSSION AND REGULATORY STATUS 0

This issue was assigned a priority of "Drop" by the NRC in February, 1987. 0

B.9.4 ELEMENTS OF RESOLUTION 0

Due to the "drop" priority assigned by the NRC, this issue has been dropped by EPRI for purposes of the ALWR design. However, it should be noted that the ALWR Requirements Document calls for the use of a plant simulator as a design tool for developing and verifying the ALWR plant design. Consequently, an accurate, plant-specific simulator will be available for the ALWR long before any need for operator training. 0

B.10 SAFETY SYSTEM TESTING 0

B.10.1 RELATED ISSUE 0

125.I.5 Long-term Generic Actions as a Result of the Davis-Besse Event of 6/9/85 – Safety Systems Tested in All Conditions Required by Design Basis Analysis 0

B.10.2 ISSUE SUMMARY 0

This issue concerns the adequacy of NRC requirements and guidance to assure that safety systems are tested in all conditions required by the design basis analysis. 0

B.10.3 DISCUSSION AND REGULATORY STATUS 0

The NRC investigated the loss of feedwater event at Davis-Besse and issued their findings in NUREG-1154. They concluded that the underlying cause of the event was the lack of attention to detail in the case of plant equipment. This included, among other things, the testing of equipment, and they reiterated the importance of thoroughness in testing systems under conditions for which they may have to perform. In addition to this conclusion the NRC noted the following specific findings: 0

- The causes of the auxiliary feedwater system containment isolation valve and pump malfunctions could have been detected and corrected prior to the event by straightforward tests. 0
- The reliable operation of the power operated relief valve had not been established by a suitable test program nor was its operational readiness verified by a periodic surveillance test. 0
- Thorough integrated system testing under various system configurations and plant conditions, as near as practicable to those for which the system is required to function during an accident, is essential for timely detection and correction of common mode design deficiencies. 0

This issue is currently being evaluated by the NRC and is scheduled to be prioritized soon. 0

B.10.4 ELEMENTS OF RESOLUTION 0

B.10.4.1 Introduction 0

The need for increased testing capability of plant systems and equipment while in operation is recognized in the ALWR design. In addition to the extensive testing performed in the preoperational testing process and the normal surveillance and functional tests performed on equipment, the ALWR design provides for full flow integrated testing capability of the safety systems while in operation. These and other testing requirements are provided in the ALWR Requirements Document as follows. 0

B.10.4.2 Requirements for All ALWRs 0

- Section 4.7 of Chapter 1 gives requirements on the testing of systems and equipment to insure that functional operability will be maintained under design conditions. 0
- Section 6.2.B of Chapter 1 gives system design requirements concerning testing of equipment. These include requirements that testing operations be explicitly included in the design of the system and equipment and that the principles of human factors be used to assure the equipment configurations and procedures are conducive to proper operations and will help prevent operator errors. 0
- Section 6.2.2.2 of Chapter 5 requires that the ALWR have the capability to accomplish valve testing, including operability testing, of containment isolation valves. 0
- Section 2.2.4 of Chapter 10 states, as a policy of the ALWR design of the instrumentation, control and protection systems, that built-in test features are to be provided to perform continuous self-diagnosis of digital hardware and communication paths and annunciate detected failures. Built-in test features will provide computer-aided, periodic functional testing capabilities that automatically verify system functionality once they are manually initiated, locate failures upon detection, and record test results. 0
- Section 3.1.3.6.1 of Chapter 10 requires that the M-MIS design process define the test requirements for both systems and components in formal test plans. All testing required to justify the M-MIS design, prepare the systems for operation, and the tests required after the systems are in service are to be included. 0

- Section 3.1.3.6.2 of Chapter 10 requires that the design process for the M-MIS include the explicit identification of all in-service surveillance testing of plant components and M-MIS components which is required to ensure satisfactory long-term operation of the equipment and to meet all applicable regulatory requirements. The functions and tasks to accomplish this testing are to be included in the design basis of the M-MIS and are to be fully accounted for in the design process, e.g., generic procedures for these tests are to be prepared and used in walkthroughs in control station mockups. 0

- Section 3.1.3.6.3 of Chapter 10 requires that the M-MIS design process include the preparation of test plans and generic procedures for the testing to be performed on the M-MIS components and systems after they are installed in the plant and the testing to be performed by the utility operating staff as part of the initial plant startup. 0

- Section 3.6.1 of Chapter 10 requires that the capability for continuous on-line self-testing of hardware integrity be provided for as much of the M-MIS as is practical. This testing is not to affect the system functionality and is to be performed on the module, as opposed to the system basis. These tests may include, but are not limited to, RAM and ROM failure checks, arithmetic processing unit failure checks, data link buffer checks, and CPU reset of watch-dog timers. 0

- Section 3.6.2 of Chapter 10 requires that the capability for periodic functional testing of the systems be provided. This periodic testing is to be manually initiated, but automatically performed once initiated, and shall meet the requirements of Regulatory Guides 1.22 and 1.118 and IEEE Standard 338. 0

- Section 3.6.8 of Chapter 10 requires that the safety-related systems, e.g., reactor protection and engineered safety features actuation systems, have automatic test features that are sufficient to meet the Technical Specification requirements for periodic surveillance of the system's functionability as defined by Regulatory Guides 1.22 and 1.118 and IEEE Standard 338. 0

B.10.4.3 Requirements for BWRs 0

- Section 4.2.8 of Chapter 5 gives requirements on the testing and testing provisions of the core coolant inventory control and decay heat removal systems. Full flow test capability, including valve testability from the control room, is specified to eliminate all uncertainty about the performance of pumps and valves after they are installed. All active components (including the control system) are required to be functionally testable during normal plant operation. 0

- Section 4.6.3.1 of Chapter 5 requires the SLCS to include provisions for functional testing. 0

B.10.4.4 Requirements for PWRs 0

- Section 5.2.3.8 of Chapter 5 requires periodic surveillance testing of the residual heat removal pumps and motor operated valves. A means is to be provided to test the pumps at full design flow with the reactor at power. The capability is to be provided to permit periodic valve tests during normal operation. 0
- Section 5.3.3.2.5 of Chapter 5 requires a means for periodic surveillance testing of emergency feedwater pumps and valves and functional testing of the integrated operation of the system. Full flow test capability with the plant in operation is also specified. 0
- Section 5.4.3.8 of Chapter 5 requires that a means be provided to permit periodic surveillance testing of SIS pumps and valves, and functional testing of the integrated operation of the system. Also, a means is to be provided to test the pumps at full design flow with the reactor at power. 0

B.10.4.5 Resolution Summary 0

The need for thorough testing of systems and equipment, both in the design process and while in operation, is recognized in the ALWR design requirements. A key element of these testing requirements are the provisions for testing capability of safety systems while in operation. This capability along with the requirements for extensive testing during the design process, surveillance testing, and other functional tests resolves this issue for the ALWR. 0

Paragraph No. *Rev.*

B.11 VALVE TORQUE LIMIT AND BYPASS SWITCH SETTINGS 0

B.11.1 RELATED ISSUE 0

125.I.6 Long-term Generic Actions as a Result of the Davis-Besse E'ent of 6/9/85 -- Valve Torque Limit and Bypass Switch Settings 0

B.11.2 ISSUE SUMMARY 0

This issue concerns the adequacy of the engineering basis for the specification of the adjustments for safety-related valves such as torque switch and torque switch bypass settings for all design basis events. 0

B.11.3 DISCUSSION AND REGULATORY STATUS 0

This issue was assigned a priority of "Drop" by the NRC. 0

B.11.4 ELEMENTS OF RESOLUTION 0

Due to the "drop" priority assigned by the NRC, this issue has been dropped by EPRI for purposes of the ALWR design. However, it should be noted that the general requirements on valves and valve operators in Section 12 of Chapter 1 specifically require that valves be operable under all design basis events. The settings of torque switches are an integral part of meeting this requirement. 0

B.12 MAN-MACHINE INTERFACE 0

B.12.1 RELATED ISSUES 0

125.II.13	Long-term Generic Actions as a Result of the Davis-Bosse Event of 6/9/85 – Operator Job Aids	0
HFO1.3.4a	Human Factors Program Plan - Man-Machine Interfaces - Local Control Stations	0
HFO1.3.4b	Human Factors Program Plan - Man-Machine Interfaces - Interface Annunciators	0
HFO1.3.4c	Human Factors Program Plan - Man-Machine Interfaces - Operational Aids	0
HFO1.3.4d	Human Factors Program Plan - Man-Machine Interfaces - Automation and Artificial Intelligence	0
HFO1.3.4e	Human Factors Program Plan - Man-Machine Interfaces - Computers and Computer Displays	0

B.12.2 ISSUE SUMMARY 0

The part operators play in preventing, mitigating, or increasing the severity of events at nuclear plants has been and will continue to be of major concern. One of the keys to assuring that nuclear plant operators take the appropriate actions is to provide nuclear plant controls which are designed to maximize operator efficiency and minimize operator error. Therefore, this issue concerns ensuring the adequacy of man-machine interface in all aspects of nuclear power plant operations to assure that nuclear power plants pose no undue risk to public health and safety. The aspects of man-machine interface addressed by this issue are: 0

- Apply human factors engineering techniques, similar to those used in control room design reviews, to local control stations; 0
- Use advanced computer-based technologies to improve annunciator systems and to cut down the number of annunciators; 0
- Evaluate the overall effectiveness and availability of the operational aid systems in improving operator performance and avoiding excessive number of alarms; 0
- Application of artificial intelligence to nuclear reactor operations in areas of acting as "consultant" to control room operators, automated procedures for specific plant conditions, and machine handling of alarms based on operator-provided guidance; 0

- Monitor advanced control room design activities and concepts, identify resulting changes in operator workload and identify performance requirements for functions allocated to computer-driven devices, and review function/task allocation between humans and computers. Also evaluate industry guidelines on human interface hardware for computer-driven displays and the methods proposed by industry to validate and display plant data. 0

B.12.3 DISCUSSION AND REGULATORY STATUS 0

The Man-Machine Interface (MMI) issue is one of seven elements in the NRC's Human Factors Program Plan (HFPP) described in NUREG-0985. The Plan was developed from the investigations which followed the accident at TMI-2 that identified the need to include human factors considerations into the regulatory process. The stated objective of the MMI issue is to ensure that MMI is adequate for safe operation and maintenance of nuclear power plants. The NRC will obtain this objective by developing (1) human factors engineering guidelines for correcting MMI problems and (2) regulatory guidance for integrating human factors engineering into new designs and into advanced technological improvements incorporated into existing designs. New guidelines and guidance concerning MMI can be expected to be in the form of revision to the SRP, new Regulatory Guides, and NUREG reports. 0

Note that Issue #125.II.13 has been dropped by the NRC as a separate issue. However, it is included here because its subject matter is also addressed as part of the HFPP described above. 0

B.12.4 ELEMENTS OF RESOLUTION 0

B.12.4.1 Introduction 0

The ALWR design philosophy is to include human factors considerations in all aspects of plant design. New and improved designs and systems, such as annunciator systems, computer systems and other operational aids, will be included in the ALWR plant design to improve man-machine interface where appropriate. The ALWR requirements are based on a total system approach to the design of nuclear plant instrumentation, controls and man-machine interfaces. 0

The requirements in the ALWR Requirements Document that achieve this are as follows. 0

Paragraph No. *Rev.*

B.12.4.2 Requirements for all ALWRs 0

- Section 1.4.B.11 of Chapter 1 states that "Human Factor considerations are to be included in all aspects of the plant design." 0
- Section 2.2 of Chapter 1 requires that the design process for an ALWR emphasize the human-machine interfaces and that an on-going analysis be conducted to assure that these requirements will be met. 0
- Section 2.2.F.4 of Chapter 1 requires the Plant Designer to provide a plant simulator/performance model which can be used as a design tool in studying human-engineering aspects of the plant controls and control room design. 0
- Section 2.2.G of Chapter 1 requires the Interdisciplinary Design Review Group to include at least one member knowledgeable in the principles of human factors. 0
- Section 8.2.B.4 of Chapter 1 requires human factors design principles to be consistently applied throughout the design process for each operation work space in the ALWR plant to reduce operation errors during all plant modes. Specific operation related human factors requirements are given for instrumentation and controls, control room design, control panels and cabinets, and operating area environment. 0
- Section 2.1.1 of Chapter 10 states that an objective of the M-MIS is to take full advantage of operator capabilities, but not to challenge operator limitations. This includes the explicit inclusion of the human component in the man-machine interface. 0
- Section 2.2.8 of Chapter 10 states the policy to apply human factor engineering principles as a formal part of the ALWR design process. Particular emphasis will be placed on: 0
  - Elimination of potential sources of human error; 0
  - Reduction in the probability of error; 0
  - Provision for the detection and recovery from human errors. 0
- Section 2.2.10 of Chapter 10 states the policy to apply advanced technology to the main control room to enhance the design compared to existing plants. It also describes many of the features which are expected to be included in the ALWR to improve the interface with the operators. 0

Other sections of Chapter 10 include specific requirements which are intended to assure that human factors are adequately addressed in the design process. Those sections which are especially pertinent to the five aspects of the man-machine interface identified in B.12.2 are as follows: 0

- Section 4 covers human factors requirements which are to be applied to all control stations, i.e., local control stations are to meet these requirements as well as the main control room. 0
- Section 4.3 covers requirements for annunciator (alarm) systems, and Section 4.3.3.4 addresses the need to reduce the number of annunciators in an upset. 0
- Sections 3.4.5 and 5.6 define the requirements for various systems to aid the operators in carrying out their assigned tasks including the monitoring of technical specification limits; the status of safety systems, and plant diagnostic, maintenance, and testing activities. 0
- Section 3 requires specific identification of functions and tasks and the systematic allocation of them among the operators and automatic systems, e.g., computers. This includes requirements to verify and validate these allocations by systematic processes involving mock-ups, simulation, and human factors reviews. 0
- Section 4.2.5.2 requires that the M-MIS Designer develop and verify human factor practices for advanced man-machine interface technology where there is limited published guidance. 0

B.12.4.3 Resolution Summary 0

Much of Chapter 10 of the ALWR Utility Requirements Document concerns improvements in the man-machine interface to reduce operator error and improve operability, which is a stated goal of the ALWR plant design. It is part of the ALWR overall requirements that not only will human factors be a consideration in all design aspects of the plant design but that human factors will be under continuous analysis and also be an on-going consideration in the operation of the ALWR plant. Based on these extensive requirements in man-machine interface design, particularly in Chapter 10, this issue should be considered resolved for the ALWR. 0

Paragraph No.		Rev.
B.13	**TESTING AND MAINTENANCE OF MANUAL VALVES IN SAFETY-RELATED SYSTEMS**	0
B.13.1	**RELATED ISSUE**	0
	127 Testing and Maintenance of Manual Valves in Safety-related Systems	0
B.13.2	**ISSUE SUMMARY**	0
	Following a loss of Integrated Control System power at Rancho Seco, an attempt was made to close the auxiliary feedwater manual isolation valve. The isolation valve could not be moved even when a valve wrench was used. The valve was seized from inadequate lubrication due to a lack of preventative maintenance over the 10 to 12-year operational life of the plant.	0
B.13.3	**DISCUSSION AND REGULATORY STATUS**	0
	This issue was assigned a "low" priority by the NRC in June 1987.	0
B.13.4	**ELEMENTS OF RESOLUTION**	0
	Due to the low priority assigned by the NRC, this issue is considered "dropped" by EPRI for purposes of the ALWR design. However, it should be noted that the ALWR will have an enhanced plant-wide data handling and computer capability compared to existing plants. This is expected to permit better tracking of preventive maintenance and thereby reduce the instances of omitted maintenance.	0

APPENDIX C ADVANCED CONTROL ROOM DESIGN 0

C.1 ALWR POSITION 0

The ALWR will have a computer-based control room with an integrated man-machine interface featuring electronic displays for monitoring, alarms, and controls. The monitoring and safety protection systems will be designed to satisfy the regulatory requirement for redundancy, separation, independence, seismic and environmental design, and the fail-safe and single failure criterion. Although the workstation controls are not dedicated and, therefore, will require a new interpretation of the single failure criterion, the automatic safety systems will meet existing single failure criterion requirements and will not be defeated by a single failure or erroneous signal from the workstation or elsewhere. 0

C.2 DISCUSSION 0

The ALWR control room will utilize a workstation design that is computer based and makes extensive use of electronic displays for monitoring, alarms, and controls. This control room is comprised of two or more identical workstations for operation, another workstation for monitoring only (shift supervisor use), and one large mimic-board which gives spatially dedicated plant overview status and trip level alarms. This presents an integrated man-machine interface which has the benefits of providing the operator with the information he needs quickly and in a format which is concise, uncluttered, and easy to interpret. 0

The workstation design allow operators to control the plant at a single workstation during normal operation. An operator will be able to locate needed alarms, displays, and controls quickly and can maintain an overview of the plant state through the workstation and the large mimic-board. At the same time, the capabilities and flexibility of modern computer driven displays will provide greater flexibility to the operator by permitting rapid access to plant variables and equipment status information at more than one location on the workstation. This will reduce the need for the operator to leave one station to obtain information from another or to assume an awkward position to maintain sight of a display while actuating or modulating a control. The superior graphics capabilities of computer generated displays will provide trending data with replay and operator selectable scaling. In addition, algorithms will provide the operators with more informative, more effective displays than those that are practical with the technologies used in existing LWRS. Finally, the workstation design will enable the operator to access electronically displayed normal, abnormal, and emergency operating procedures and Tech Spec limits without leaving his seat. The electronic procedures will include imbedded dynamic indication and alarm information and provide the means for flagging and logging actions taken by the operators which deviate from the set of recommended options, as determined by the software logic and plant state. 0

In addition to the reduction in the likelihood of operator error inherent in this design, the risk of system and component failures will also be minimized. First, the control room workstations will be required to be Class 1E, qualified both environmentally and seismically. Secondly, a combination of improved reactor design (i.e., evolutionary and passive plants), less active components, and increased automation will provide for less demand on the operator, more time for response, and, therefore, less chance of failures in the control systems. And thirdly, although the workstation displays and controls may not be dedicated to a single function, the design will provide protection and monitoring systems which satisfy the regulatory requirements for separation, independence, diversity, and the single failure and fail-safe criterion. This is achieved by providing each workstation with complete monitoring and control capability, separate and independent from each other, and by protection systems which are automatic centralized systems taking action through multi-train channels which are single failure proof. A single failure in or an erroneous signal from a non-dedicated control in the workstation will not override automatic safety signals generated by the protection systems. 0

Paragraph No.	*Requirement*	*Rev.*
APPENDIX C	**ADVANCED CONTROL ROOM DESIGN**	0
C.1	**ALWR POSITION**	0
	The ALWR will have a computer-based control room with an integrated man-machine interface featuring electronic displays for monitoring, alarms, and controls. The monitoring and safety protection systems will be designed to satisfy the regulatory requirement for redundancy, separation, independence, seismic and environmental design, and the fail-safe and single failure criterion. Although the workstation controls are not dedicated and, therefore, will require a new interpretation of the single failure criterion, the automatic safety systems will meet existing single failure criterion requirements and will not be defeated by a single failure or erroneous signal from the workstation or elsewhare.	0
C.2	**DISCUSSION**	0
	The ALWR control room will utilize a workstation design that is computer based and makes extensive use of electronic displays for monitoring, alarms, and controls. This control room is comprised of two or more identical workstations for operation, another workstation for monitoring only (shift supervisor use), and one large mimic-board which gives spatially dedicated plant overview status and trip level alarms. This presents an integrated man-machine interface which has the benefits of providing the operator with the information he needs quickly and in a format which is concise, uncluttered, and easy to interpret.	0

Paragraph No.	Requirement	Rev.
	The workstation design allow operators to control the plant at a single workstation during normal operation. An operator will be able to locate needed alarms, displays, and controls quickly and can maintain an overview of the plant state through the workstation and the large mimic-board. At the same time, the capabilities and flexibility of modern computer driven displays will provide greater flexibility to the operator by permitting rapid access to plant variables and equipment status information at more than one location on the workstation. This will reduce the need for the operator to leave one station to obtain information from another or to assume an awkward position to maintain sight of a display while actuating or modulating a control. The superior graphics capabilities of computer generated displays will provide trending data with replay and operator selectable scaling. In addition, algorithms will provide the operators with more informative, more effective displays than those that are practical with the technologies used in existing LWRS. Finally, the workstation design will enable the operator to access electronically displayed normal, abnormal, and emergency operating procedures and Tech Spec limits without leaving his seat. The electronic procedures will include imbedded dynamic indication and alarm information and provide the means for flagging and logging actions taken by the operators which deviate from the set of recommended options, as determined by the software logic and plant state.	0
	In addition to the reduction in the likelihood of operator error inherent in this design, the risk of system and component failures will also be minimized. First, the control room workstations will be required to be Class 1E, qualified both environmentally and seismically. Secondly, a combination of improved reactor design (i.e., evolutionary and passive plants), less active components, and increased automation will provide for less demand on the operator, more time for response, and, therefore, less chance of failures in the control systems. And thirdly, although the workstation displays and controls may not be dedicated to a single function, the design will provide protection and monitoring systems which satisfy the regulatory requirements for separation, independence, diversity, and the single failure and fail-safe criterion. This is achieved by providing each workstation with complete monitoring and control capability, separate and independent from each other, and by protection systems which are automatic centralized systems taking action through multi-train channels which are single failure proof. A single failure in or an erroneous signal from a non-dedicated control in the workstation will not override automatic safety signals generated by the protection systems.	0

Additionally, the workstations will be constructed of highly reliable, robust components, including robust software, to minimize the risk of failures. This will include the use of algorithms and improved versions of on-line software diagnostics to perform checks or verification functions, neither of which are available in current control rooms. There will be sufficient segmentation and independence so that a failure or upset in one plant control function cannot propagate to other plant control functions and thereby overburden the operators as a result of complex transient events. This will require multiple computers as well as extensive use of distributed microprocessors. 0

C.3 ASSESSMENT 0

The modern control room, to minimize failures and operator error, must combine the requirements for rugged and reliable control stations (i.e., environmentally and seismically qualified, designed for single failure, etc.), and the need for improved and integrated man-machine interface between the control stations and the operator. Failures are minimized by a design that combines rugged and reliable control stations and software that features algorithms and diagnostics that perform checks or verification. However, experience has shown that operator error due to incorrect, misunderstood, or badly presented information and awkward hard-to-use controls has been a significant contributor toward creating or degrading events. Because the risk of hardware failures in the control station panels is minimal, the design of the man-machine interface and improvement in operator performance is given priority. 0

The computer-based workstation will inherently minimize the risk of operator error. The operators will make extensive use of computer generated displays for indication and information (e.g., plant status, technical data, alarms, procedures, P&IDs), data base management, information processing and presentation techniques to provide decision-making support. The controls, information systems, and operator will be integrated in a compact, efficient workstation in which the operators will be able to make more timely, informative, and error-free decisions. 0