CRITERIA FOR THE DESIGN OF

THE MAIN CONTROL ROOM

AND OTHER

OPERATING STATIONS

FOR

SYSTEM 80+

ABB COMBUSTION ENGINEERING NUCLEAR SYSTEMS

July, 1992

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

The Code of Federal Regulations (CFR) includes Nuclear Regulatory Commission (NRC) regulations governing the design, review, and certification of nuclear power plants. Human Factors Engineering (HFE) for standard design certification must satisfy the contents of 10 CFR 50 (Domestic Licensing of Production and Utilization Facilities) and 10 CFR 52, Subpart B, (Standard Design Certifications).

In particular, 10 CFR 50.34(f)(2)(iii) is the key regulation that mandates HFE in the design, as follows:

> "Provide, for Commission review, a control room design that reflects state-of-the-art human factors principles prior to committing to fabrication or revision of fabricated control room panels and layouts. (I.D.1)"

The parenthetical I.D.1 is a reference to the post-TMI action plans for a Control Room Design Review (CRDR) process outlined in NUREG-0660. The purpose of a CRDR was to "identify and correct design deficiencies," as part of the effort to improve the information provided to operators and, thereby, upgrade their accident prevention and mitigation abilities.

Subsequent guidance supporting the implementation and review of the CRDR process in existing plants has been provided by NUREG-0737, Supplement 1, NUREG-0700, NUREG-0800, and NUREG-0801. Although I.D.1 is aimed at remedial actions for existing plant control rooms, 10 CFR 50.34(f)(2)(iii) is clear in its applicability to both existing and future designs. Thus, the aforementioned supporting guidance is instructive in determining what types of activities, analyses, and technical guidance must be incorporated in a design to satisfy 10 CFR 50.34(f)(2)(iii), and has been an important input to the review methodology presented in this document.

One issue to emerge from the control room design review process for design certification is that fully detailed Man-Machine Interface (MMI) design information may not be available for review prior to certification. Thus, certification must be based in part on pre-certification approval of acceptance criteria for 1) the MMI design process and 2) MMI design product. Since a design process review has not been conducted previously by the NRC as part of reactor licensing, and is not addressed in the current guidance (i.e., Chapter 18 of NUREG-0800, the Standard Review Plan), a regulatory precedent and basis for such a review is not available. However, a satisfactory design <u>process</u> must include a sufficient set of analyses, requirements, and acceptance criteria to lead to a valid and certifiable design <u>product</u>.

The intent of this document is to provide a sufficient set of review criteria, irrespective of when they may be applied (i.e., prior to certification, as uAC or as ITAAC) for review of the System 80+ man-machine interface design process and design product. These criteria are a set of objective tests which will allow verification that the process or product is acceptable with minimum subjectivity

and without further evaluation of the process or product. That is, the criteria are intended to be specific enough to define sufficiency of the product and process prior to certification. Therefore, as product and process details are available (either prior to or post certification), their acceptability can be objectively determined (i.e., pass/fail) by comparison to the acceptance criteria in this document.

Part I of this document identifies a sufficient set of design process review criteria derived from a comprehensive review of 10 CFR and related guidance and developed specifically for an evolutionary PWR design. Goals, requirements and acceptance criteria are identified for each of a set of eight design process elements which correspond to those previously established by the NRC preliminary acceptance criteria.

Part II of this document defines acceptance criteria for the design of an advanced light water reactor main control room and other operating stations based on existing industry sources. These criteria are grouped according to functional elements which comprise an advanced control complex.

Definitions

Acceptance Criteria - Practical and reasonably objective pass/fail tests that operationalize the Requirements. Criteria may be qualitative or quantitative, and define sufficiency, not optimality.

Availability - Verification of task performance capability such that the necessary indications and controls to accomplish a defined set of tasks (e.g., emergency operating procedures) are afforded in a specified work area (e.g., a control room), per Section 3.2.2 and 3.7.2 of NUREG-0700.

Bypassed and Inoperable Status of Safety Systems - Per Reg. Guide 1.47.

Calendar-referenced - Use of specific quantitative dates; compare Schedule-referenced.

Control Room Design Review (CRDR) - A practical, validated methodology for evaluating existing control room designs for possible human engineering deficiencies (e.g., as described and supported by NUREG-0700).

Design Process Elements - The eight functional components in which the present Review Plan is organized.

Employ - To utilize in a responsible capacity.

Goal - Goals are the idealized functions of the Design Process Elements.

HFE Design Guidance - Guidelines for equipment and system design (e.g., Chapter 6 of NUREG-0700) formulated to incorporate State-of-the-Art Human Factors Principles, as defined.

HFE Specialists - Individuals with credentials in the area of Human Factors Engineering equivalent to 1) at least two years of successful graduate-level study of applicable subjects, plus a year of related design experience; or 2) five years of related design experience; 3) or any evenly proportioned combination of 1) and 2).

Human Factors Engineering (HFE) - The application of Human Factors Principles and methods to practical engineering and design problems; as distinguished from research and theoretical development.

Human Factors Principles - General principles of human perception, cognition, action, etc. that have practical implications for adequate (i.e., usable) design.

Indication and Control Features - General denotation for information output (i.e., from plant systems to human operator) and action input (i.e., from human operator to plant systems) features of the MMI systems, respectively, without regard for specific implementation.

Interdisciplinary - A philosophy which seeks to incorporate multiple technical viewpoints by specialty, with the aim of achieving a more well-rounded result. For example, four disciplines (HFE, Operations, I&C, and Nuclear Systems) have typically been specified for a CRDR. In the present context, in which I&C and systems design activity is a given, the concern is that HFE Specialists and Operations Experts be involved in those activities along with the I&C and systems engineers. Use of the term "Interdisciplinary" in this document thus presumes the participation of relevant I&C and systems engineers, and specifies only the additional requirement for the participation of HFE Specialists and/or Operations Experts.

Man-Machine Interface (MMI) - Organization, informational form, and human performance-related constraints of indication & control functional implementations.

Operations Experts - Currently or formerly licensed reactor operators with actual operating experience on similar units.

Post-Accident Monitoring Indications - Per Reg. Guide 1.97.

Requirements - The constituents that pragmatically define the Design Process Elements, based on consideration of specific, applicable regulations from 10 CFR.

Responsible Management Structure - The organizational and management structure responsible for the direction and integration of HFE in the design of the proposed plant.

Review Plan (RP) - The present document and its contents.

Safety-Related Design Basis Events (SRDBEs) - Unplanned occurrences that are analyzed for and accommodated in the design of the plant, and mitigated by a combination of automatic actuation of reactor protective systems and engineering safety features, and manual operator actions.

Safety-related operator's role - Operator's design basis role in protecting the health and safety of the public as defined by correct performance of operator actions in applicable emergency operating procedures, including credited operator actions in Safety-Related Design Basis Events.

Schedule-referenced - The use of a qualitative date, reflecting relative order information among scheduled items, e.g., among milestones. Compare Calendar-referenced.

State-of-the-Art - Interpreting a key reference from 10 CFR 50.34(f)(2)(iii), State-of-the-Art (i.e., Human Factors Principles) is defined as a criterion of acceptability referring to that which is grounded, practical, and valid. Grounded denotes a basis justified by the available (or lacking) content of the technical and scientific HFE literature. Practical denotes applied rather than abstract or theoretical; therefore with consideration of pragmatic design tradeoffs and constraints. Valid denotes adequate in terms of actual demonstrations of effective use.

Suitability - Verification of task performance capability such that the MMI design items are individually acceptable (i.e., are Usable, or suitable for their intended use) in terms of applicable HFE Design Guidance, per Section 3.2.2 and 3.7.2 of NUREG-0700.

Task Analysis - A formalized analytic method of decomposing human job and task activities into constituent elements such that their information inputs and action outputs can be identified.

Technical Resources - Technical expertise (e.g., HFE Specialists, Operations Experts) for which Employment by the program is required.

Usable - Operable, maintainable, testable, inspectable, efficient, effective, etc.; i.e., sufficient to support the operator's specified tasks.

Verification - Evaluation of Availability and Suitability; part of process (along with Validation) by which the HFE sufficiency of the MMI design is confirmed (per Section 3.7 of NUREG-0700).

Validation - Evaluation of the dynamic operating ensemble demonstrating trained operators' ability to successfully perform their anticipated (i.e., procedural) role in the afforded task environment (i.e., the control room design) under anticipated operating conditions (the Validation scenarios). Part of process (along with Verification) by which the HFE sufficiency of the MMI design is confirmed (per NUREG 0700, Section 3.8).

ACRONYMS

CFR	Code of Federal Regulations
CRDR	Control Room Design Review
DAC	Design Acceptance Criteria
GSI	Generic Safety Issues
HFE	Human Factors Engineering
ITAAC	Inspections Tests Analyses and Acceptance Criteria
MCR	Main Control Room
MMI	Man Machine Interface
NRC	Nuclear Regulatory Commission
O&M	Operations and Maintenance
P&ID	Piping and Instrumentation Diagram
PAMI	Post Accident Monitoring Instrumentation
PWR	Pressurized Water Reactor
RP	Review Plan
SOAC	Significant Operator Action Condition
SRDBE	Safety Related Design Basis Event
TA	Task Analysis
TSC	Technical Support Center
USI	Unresolved Safety Issues
VDU	Video Display Unit

PART I

DESIGN PROCESS REQUIREMENTS

Objectives

Part I of this document provides an approach for conducting HFE review of a design process, particularly in the context of evolutionary, pressurized-water reactor facilities. The specific objectives of this effort are:

1. To develop a practical and sound HFE program review framework to serve as the basis for NRC review of the HFE design process.

2. To identify a set of design process elements that are sufficient and practical requisites to the design of usable MMIs.

3. To specify the requirements and acceptance criteria by which the submitted design process will be evaluated.

4. To specify the relationship between the design process requirements and the NRC regulations.

Scope

The scope of the present approach to the review has been delimited, with justification, as follows.

PWR - The present approach is specified for Pressurized Water Reactor (PWR) design programs, to limit inclusion of regulations from 10 CFR 50 to those that are applicable to such designs (this affects only the Availability Verification element, I-2.6.)

Control Room - The present approach is focussed on the process of MMI development for control rooms (i.e., the main control room and remote shutdown area) per 10 CFR 50.34(f)(2)(iii) and GDC 19 of Part 50 Appendix A.

Design and Construction Phase - The present approach is limited to design processes occurring during design and construction phases of the facility. Operations issues that follow completed design are out of the scope of design process, and are managed through regulations on, and programs of, the licensee.

Separate and Distinct Responsibilities - The present approach excludes management or review of responsibilities that belong to other regulatory or programmatic scopes. Thus, while interaction with the following areas through design activities is expected, the following areas are not the particular responsibility of HFE design process planning, management, or review: Procedure development, training development, licensing examinations, reliability analysis, quality assurance, OSHA, ALARA, fire protection, security, or emergency planning.

Method

The CRDR process that was developed in response to NUREG-0660 and successfully implemented in existing plant evaluations embodies what has been termed a "systems approach" to evaluating HFE in design. This is a formalized approach, developed for the military, that provides a useful general model for organizing activities such as training program or hardware systems development. The NRC guidance on the CRDR process, various HFE texts treating the topic of systems development (e.g., DeGreene, 1970; Van Cott & Kinkade, 1972; Meister, 1985; Booher, 1990), and the military HFE requirements such as MIL-H-46855B (1979) all tend to reiterate a number of features that typify this general systems approach. These features are summarized as follows:

- Program formality
- Interaction of design disciplines
- Systematic incorporation of experience
- Functional evaluation of system operation
- Analysis/specification of task requirements
- Provision/application of MMI design guidance
- Verify necessary indication and control availability
- Validate sufficient operating ensemble

Review of the literature thus suggests that a satisfactory process for incorporating HFE in design should incorporate these features (this is, by extension of the previous discussion under **Objectives**, a more elaborate, but also more tentative, interpretation of 10 CFR 50.34(f)(2)(iii).) In turn, the requirements and criteria for design process review should verify proper incorporation of such features.

In determining what is proper, it is important to note that one of the strengths of the systems approach lies in its generality and flexibility. In keeping with these strengths, as well as its own philosophies, such a review of the design process should take place at a "functional" level (i.e., what purpose is to be accomplished) rather than a "structural" level (i.e., what mechanism has been employed to accomplish it). A functional approach to review accommodates a greater variety of approaches to design, judging them on their success, rather than their conformity.

Taking such an approach, questions of functional adequacy for a particular design process can be regarded as falling into two general categories. One is "necessary content": Have the required functions been performed? The other is "sufficient output": Are the products of the design process acceptable?

The sufficiency of output is regarded as evaluation of the design product. Ultimately this leads, through the various design activities, to verification and validation of the design. Technical questions arise and are resolved in the course of the design process, but adequacy of their resolution remains an evaluation of the design itself (i.e., the design product). Requirements and criteria for evaluating the design product are provided in Part II of this document.

Evaluation of the design process is thus considered primarily an issue of ensuring the inclusion of necessary functional content. To establish what is necessary, 10 CFR was reviewed for its applicability to the general systems approach features identified previously. With slight reorganization of the identified features into more concrete and unitary functional elements, the applicable 10 CFR regulations then serve as the core for the contents of this document's requirements. The Design Process Elements are identified in I-1.1; their contents (goals, requirements, and acceptance criteria) are detailed in I-2.

References

Booher, H. R. (Ed.) (1990). MANPRINT: An Approach to Systems Integration. New York, NY: Van Nostrand Reinhold.

DeGreene, K. B. (Ed.) (1970). Systems Psychology. New York, NY: McGraw Hill.

Department of Defense (1979). Human Engineering Requirements for Military Systems, Equipment, and Facilities (MIL-H-46855B).

Meister, D. (1985). Behavioral Measurement Methods. New York, NY: Wiley-Interscience.

Office of the Federal Register (1992). Code of Federal Regulations, Title 10, Chapter I - Nuclear Regulatory Commission (10 CFR Parts 0-199).

U.S. Nuclear Regulatory Commission (1973). Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Reg Guide 1.47).

U.S. Nuclear Regulatory Commission (1980). NRC Action Plan Developed as a Result of the TMI-2 Accident (NUREG-0660).

U.S. Nuclear Regulatory Commission (1980). Clarification of TMI Action Plan Requirements (NUREG-0737).

U.S. Nuclear Regulatory Commission (1981). Guidelines for Control Room Design Reviews (NUREG-0700).

U.S. Nuclear Regulatory Commission (1981). Evaluation Criteria for Detailed Control Room Design Review (NUREG-0801).

U.S. Nuclear Regulatory Commission (1982). Requirements for Emergency Response Capability (NUREG-0737, Supplement 1).

U.S. Nuclear Regulatory Commission (1983). Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident (Reg Guide 1.97).

U.S. Nuclear Regulatory Commission (1987). Standard Review Plan (NUREG-0800).

U.S. Nuclear Regulatory Commission (1992). HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors (Draft).

Van Cott, H. P. & [illegible]ade, R. G. (Ed.s) (1972). Human Engineering Guide to Equipment Design. Washington, DC: U.S. Government Printing Office.

I-1 Framework Description

I-1.1 Design Process Elements

A review of 10 CFR was conducted to identify regulations that apply to the general systems approach features identified previously under Method. Following this review, the features were reorganized slightly into more concrete and unitary functional elements, within which detailed design process requirements and acceptance criteria have been organized and detailed. The resulting Design Process Elements, which are detailed in I-2, are as follows:

1. HFE Program Management
2. Incorporation of Industry Experience
3. Evaluation and Allocation of System Functions
4. Task Analysis
5. Man-Machine Interface Design
6. Availability Verification
7. Suitability Verification
8. Validation of Ensemble

I-1.2 Element Structure

A generic structure consisting of goals, requirements, and criteria, is framework within which the Design Process Elements are specified. The elements are not intended to serve, necessarily, as structural objects to be located or isolated within the design organization. Rather, they define functions for which a variety of structural alternatives may meet the acceptance criteria.

I-1.2.1 Goals

The goal statement expresses the idealized function of the Design Process Element, with the assumption that goals may be constructively pursued without necessarily being possible to completely achieve. This specification is necessary because HFE goals cannot be effectively pursued unless operationalized, and this is not always practical within the State-of-the-Art (as defined in the Introduction).

Thus, goals are rendered distinct from requirements (the specific constituents that pragmatically define the element) and from criteria (the objective pass/fail tests that operationalize the requirements). Goals clarify the intentions of the Element, but also focus the questions of defining practical constituents and operationalizing their tests. This helps avoid confusion between intentions and capabilities.

I-1.2.2 Requirements

Requirements are the specific constituents that pragmatically define the Design Process Element. Requirements are based on consideration of specific, applicable regulations from 10 CFR (as cited under the individual Elements in I-2) and supporting NRC guidance. Requirements have been developed in consideration of the State-of-the-Art, and of their need for practical and objective acceptance criteria. Requirements that cannot be operationalized in this fashion will be, at best, ineffectual; at worst, a likely obstruction to the evaluative process. Such requirements (or their acceptance criteria) should be revised or removed.

Note that, since these are functional rather than structural Design Process Elements, certain provisions of the overall design program may meet the acceptance criteria and thus satisfy the HFE design review process requirements. A unique HFE mechanism is not necessarily required.

I-1.2.3 Acceptance Criteria

Acceptance criteria are the practical and reasonably objective tests that operationalize the requirements. A criterion is a pass/fail test that can be applied with a minimum of subjectivity and inter-rater variability. Criteria may be qualitative or quantitative, and by definition should define sufficiency, not optimality.

The framework of this approach is such that criteria do not serve, as may have been expected, to detail the requirements. Where further evaluation of the functional effectiveness of a Design Process Element function is desired, attention should instead be turned to evaluation of the design <u>product</u>, to see if problems (e.g., unsuitabilities) have resulted in the MMI. The product review portion of the design review process is covered by Part II of this document.

I-2 Element Descriptions

I-2.1 HFE Program Management[1]

I-2.1.1 Goals

A formal HFE Program is an important component of design team activities to reasonably ensure that 1) HFE input and operations experience is incorporated in system design and development activities to afford usable MMIs to plant operators, that 2) the final MMI design allows operators to sufficiently perform their normal and safety-related operating roles, and that 3) regulatory requirements pertinent to each of the HFE design process elements are satisfied.[2]

I-2.1.2 Requirements

I-2.1.2.1 Program Plan

Per the constraints previously defined under **Scope**, a description of the program management plan for HFE activities, herein referred to as the HFE Program Plan, shall be provided prior to certification that includes the following[3]:

I-2.1.2.1.1 **Responsible Management Structure** - The management and organization structure singularly responsible for the direction and integration of HFE in the design and construction of the proposed plant.

---

[1] This Design Process Element corresponds to Element 1 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[2] A formal HFE program is recommended as a useful step towards satisfying the requirements of 10 CFR 50.34(f)(2)(iii) to provide a control room whose design reflects state-of-the-art human factors principles.

[3] These requirements contribute to satisfying the requirements of 10 CFR 50.34(f)(3)(vii) to provide management plans for design and construction activities.

I-2.1.2.1.2 **Technical Resources** - The technical resources (i.e., HFE Specialists, Operations Experts) employed by the applicant to address usability issues in the design.

I-2.1.2.1.3 **Method of Interdisciplinary Interaction** - The manner by which the applicant ensures integration of HFE input and operations experience with I&C and systems design and construction. This shall include, for all incomplete and to-be-performed activities, the details of the methods of interdisciplinary interaction of the design and construction team members, including mechanisms of design tradeoff resolution and design review utilized under I-2.5, Man-Machine Interface Design.

I-2.1.2.1.4 **Method of Design Control** - The details of the method by which design control is exercised among team members.

I-2.1.2.1.5 **Design Process Elements** - Implementation of the following technical HFE elements in the design process:

a) Incorporation of Industry Experience
b) Evaluation and Allocation of System Functions
c) Task Analysis
d) Man-Machine Interface Design
e) Availability Verification
f) Suitability Verification
g) Validation of Ensemble

Goals and requirements for these elements are provided in remaining subsections of Section I-2. However, it is not required that program plans be organized in terms of this, or any other, particular set of process elements.

I-2.1.2.2 Responsibility

I-2.1.2.2.1 **Management Structure** - The responsible Management Structure shall be responsible for a) the implementation of the HFE Program Plan, b) the conformance of the design and construction process and products of all team participants to the requirements of the RP, and c) the resolution of all issues entered in the HFE Tracking System.

I-2.1.2.2.2 **HFE Specialists** - HFE Specialists (as defined in the Introduction) shall be employed by the Responsible Management Structure; the responsibilities of the HFE Specialists shall include the origination of all technical HFE products specified in the HFE Program Plan.

I-2.1.2.2.3 **Operations Experts** - Operations Experts (as defined in the Introduction) shall be employed by the Responsible Management Structure; the responsibilities of the Operations Experts shall include the review of all official milestone MMI design products for usability concerns.

I-2.1.2.2.4 **Interdisciplinary Interaction and Design Control** - All design activities are subject to, and shall utilize the mechanisms and meet applicable requirements, of the overall design team quality assurance (QA) program[4]. However, such compliance shall be the responsibility of the overall design team quality assurance program management structure, and is therefore not governed by the HFE Program Plan.

I-2.1.2.3 Scheduling

For those HFE aspects of the design whose adequacy must be analytically or empirically confirmed to satisfy Verification or Validation requirements, a schedule shall be provided showing that such evaluations will be complete and resulting questions will be resolved at or before the latest date stated in the application for completion of construction of the facility[5].

I-2.1.2.4 Tracking

I-2.1.2.4.1 **Tracking System** - A Tracking-of-Open-Issues (TOI) function shall be provided to ensure the proper disposition of HFE issues formally raised in design and construction analysis and evaluation activities.

---

[4] As implemented per the requirements of 10 CFR 50.34(a)(7), and 10 CFR 50.34(f)(3)(iii) for QA programs.

[5] These RP requirements are in keeping with the requirements of 10 CFR 50.34(a)(8).

I-2.1.2.4.2 **System Entries** - TOI entries shall include the source and a description of the issue, including its expected impact on overall system performance; a Calendar-referenced commitment date for resolution; and a deadline for implementation.

I-2.1.2.4.3 **Resolution of Entries** - Resolution of TOI entries shall include a description of the resolution, including the locus of its implementation; signatures of pertinent interdisciplinary discussants indicating their acceptance of the resolution; and a Calendar-referenced commitment date for implementation.

I-2.1.2.4.4 **Implementation of Resolutions** - Closeout of TOI entries shall include a description of the final implementation, and a signature indicating verification of the properly completed implementation by a representative of the Responsible Management Structure.

I-2.1.2.4.5 **Unmet Commitments** - Unmet commitment dates shall be responded to with reentry and, if appropriate, an update of the issue/resolution, along with a new commitment date. This process shall be referred to herein as "updating" the entry. The updated issue/resolution shall supersede (equivalent to closing out) the preceding issue/resolution.

I-2.1.3 Acceptance Criteria

I-2.1.3.1 Program Plan

I-2.1.3.1.1 **Effective Date** - A formal HFE Program Plan as described in I-2.1.2.1 is in effect.

I-2.1.3.1.2 **Responsible Management Structure** - The Responsible Management Structure presented in the HFE Program Plan a) shows an unambiguous (e.g., hierarchical) chain of HFE accountability from the level of technical origination to a solely responsible representative of top-level program management, b) is specified by organizational position and primary responsibilities, and c) is supported on request by an official letter or memorandum

identifying the particular individual in each identified position.

I-2.1.3.1.3 **Technical Resources** - Resumes of all HFE Specialists and Operations Experts that have been employed by the program and for which the program takes credit (e.g., for acceptable origination of HFE products) are retained and presented in the HFE Program Plan; their qualifications meet the stated definitions and requirements.

I-2.1.3.1.4 **Method of Interdisciplinary Interaction** - The HFE Program Plan provides an explanation of the interdisciplinary design process as described in I-2.1.2.3.

I-2.1.3.1.5 **Method of Design Control** - The HFE Program Plan details or references overall design program procedures for applicable design control methods including a) Quality Assurance procedures, and b) review and sign-off of documents.

I-2.1.3.1.6 **Design Process Elements** - Criteria for the various Design Process Elements are provided within individual sections of the RP. Satisfaction of the RP requirements is determined by evaluating the overall design program, its processes, and/or resulting products against the associated RP criteria.

I-2.1.3.2 Responsibility

I-2.1.3.2.1 **Management Structure** - The Responsible Project Office Manager and appropriate discipline managers have reviewed and approved a) the current HFE Program Plan, b) the design and construction products of all team participants for conformance to the requirements of the RP and as indicated by their sign-off per I-2.1.3.5, and c) resolution and implementation of all TOI items.

I-2.1.3.2.2 **HFE Specialists**

a) HFE Specialists (as defined in the Introduction) are Employed by the Responsible Management Structure;

b) HFE Specialists have originated all technical HFE products specified in the HFE Program Plan.

I-2.1.3.2.3 **Operations Experts**

a) Operations Experts (as defined in the Introduction) are Employed by the Responsible Management Structure;

b) Operation Experts have reviewed all milestone MMI design products as documented by official memoranda.

I-2.1.3.3 Scheduling

Verification and validation activities, including resolution of all resulting issues, are scheduled in an official project document for completion prior to the latest date stated in the application for completion of construction of the facility. (Schedule-referencing may be utilized, but the completion-of-construction milestone must be explicit.)

I-2.1.3.4 Tracking

I-2.1.3.4.1 **System Provision** - A TOI is defined that accommodates the information specified in I-2.1.2.4., and is in place upon acceptance of the HFE Program Plan.

I-2.1.3.4.2 **System Implementation** - Selective audit of the TOI system indicates that it is being implemented as specified by the requirements of I-2.1.2.4, including that all commitments have been met, or their entries suitably updated.

I-2.2 Incorporation of Industry Experience[6]

I-2.2.1 Goals

Many valuable lessons from industry experience in design, construction, operation, incidents, and accidents have been developed and documented. Such material should be considered during the design process, to avoid or mitigate the occurrence of similar problems, and to contribute to producing a more effective final design product.

I-2.2.2 Requirements

I-2.2.2.1 Administrative Procedures

Prior to certification, administrative procedures shall be available and be implemented for evaluating operating, design, and construction experience, and for ensuring that applicable important industry experiences will be provided in a timely manner to those designing and constructing the plant, per 10 CFR 50.34(f)(3)(i). A record of resulting transmittals from such provisions shall be maintained to verify implementation.

I-2.2.2.2 References and Studies

Prior to certification, a list of externally developed industry and regulatory references (e.g., NRC, EPRI, INPO, NUMARC, etc.) shall be developed to serve as input to be considered by design, and to provide a basis for the development of additional, specific Verification and Validation criteria.

I-2.2.2.3 Formal Treatment of Safety Issues

I-2.2.2.3.1 All Generic Safety Issues (GSIs) and Unresolved Safety Issues (USIs) shall be evaluated by, and the applicable issues disseminated throughout and receive formal disposition by, the Responsible Management Structure.

---

[6] This Design Process Element corresponds to Element 2 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

I-2.2.2.3.2 GSI and USI processing shall be controlled by formal procedures implemented prior to certification.

I-2.2.3 Acceptance Criteria

I-2.2.3.1 Administrative Procedures

Administrative procedures for evaluating and disseminating operating, design, and construction experience as described in I-2.2.2.1 is provided in an official project document. Audit of transmittal records verifies that the procedures have been actively implemented.

I-2.2.3.2 References and Studies

The list of references identified in I-2.2.2.2 is provided in an official project document. For each reference, a summary (e.g., one paragraph) description of how it contributed to the design is provided.

I-2.2.3.3 Formal Treatment of Safety Issues

Selective audit of the appropriate records indicates that GSIs and USIs have been evaluated, and are being tracked and dispositioned as required. Controlling procedures appear in official project documents or memoranda.

I-2.3 Evaluation and Allocation of System Functions[7]

I-2.3.1 Goals

The ensemble of facility systems must ensure the provision of certain operating functions to maintain successful performance, particularly in the area of the health and safety of the public. The human and machine elements within the ensemble should play complementary roles that make the successful accomplishment of these functions highly likely. To pursue this goal, the allocation of functions to the human and machine elements (particularly automated information processing and control) should consider how the facility is to be operated, how plant safety functions are accomplished, and the needs, capabilities, and limitations of the human operator (and the proposed machines.)

I-2.3.2 Requirements

I-2.3.2.1 Mandated Allocations

Prior to certification, the design shall incorporate these Federally mandated allocations of function:

a) Automatic indication of the Bypassed and Inoperable Status of Safety Systems; 10 CFR 50.34(f)(2)(v).

b) Automatic and manual initiation of auxiliary (and/or emergency) feedwater systems; 10 CFR 50.34(f)(2)(xii) and 50.62(c).

c) Automatic actuation of containment isolation systems, including all non-essential systems, on high containment pressure; 10 CFR 50.34(f)(2)(xiv)

d) No automatic reopening of automatically isolated containment valves on reset of automatic containment isolation signals; 10 CFR 50.34(f)(2)(xiv)(c).

---

[7] This Design Process Element corresponds to Elements 3 and 4 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

e) Automatic isolation of containment system paths to environs on high radiation; 10 CFR 50.34(f)(2)(xiv)(E).

f) Automatic initiation of protective systems including reactivity control (i.e., reactor trip) systems; 10 CFR 50, Appendix A, GDC 20(1).

g) Automatic initiation of systems and components important to safety (i.e., Engineered Safety Features); 10 CFR 50, Appendix A, GDC 20(2).

h) Automatic initiation of turbine trip; 10 CFR 50.62(c).

I-2.3.2.2 Critical Safety Functions

Prior to certification, a description of the plant Critical Safety Functions and the design basis for their implementation shall be documented sufficient to permit understanding of the operator's safety-related role a) as allocated as an integral part of the overall system design, b) as incorporated by the design basis evaluations (which shall be referenced) performed to establish the adequacy of the plant Critical Safety Functions, and c) as evaluated by Task Analysis, Verification, and Validation activities[8].

This may be "in the form of a discussion, with specific references, of similarities to and differences from, facilities of similar design for which applications have been previously filed with the commission"[9]. Alternately, or if no predecessor system is extant, a formal systems analysis may be provided.

I-2.3.2.3 HFE Evaluation of Allocations

The Task Analysis (Section I-2.4), Availability Verification (Section I-2.6), Suitability Verification

---

[8] This requirement is felt to be consistent with the general regulations of 10 CFR 50.34(b)(2) for "A description ... of the facility ... sufficient to permit understanding of the system designs and their relationship to safety evaluations."

[9] Per 10 CFR 50.34(a), footnote 5.

(Section I-2.7), and Validation (Section I-2.8) activities shall be sources of feedback on allocation issues. Performance problems thus identified in the design product shall be resolved using TOI system mechanisms per the Requirements of I-2.1.2.4.

I-2.3.3 Acceptance Criteria

I-2.3.3.1 Mandated Allocations

Mandated allocations, as stated in I-2.3.2.1, have been verified through review of the appropriate systems designs, and documented in official project documents or memoranda.

I-2.3.3.2 Critical Safety Functions

A official project document or memorandum exists which includes a description of the plant Critical Safety Functions and the design basis for their implementation as described in I-2.3.2.2.

I-2.4 Task Analysis[10]

I-2.4.1 Goals

Task Analysis should identify the human operator's detailed input and output requirements for a representative set of control room and remote shutdown area tasks. Task Analysis (TA) should also evaluate operator loading, to provide assurance that human performance capacities are not grossly or chronically exceeded by anticipated task demands. Task Analysis data can support the development/evaluation of the control room design, operating procedures, and operator training. Satisfactory TA results contribute to the basis for concluding that qualified operators are reasonably able to perform their required tasks, particularly those related to safety[11].

I-2.4.2 Requirements

I-2.4.2.1 Operational Basis

Task Analysis shall be based on operational input that provides a reasonable "best estimate" of how the plant will be operated. Source material should include a) operating procedures or procedure guidelines for similar existing facilities, b) analyzed operating sequences for proposed new facilities, and c) the input of Operations Experts. The balance of a) and b) utilized should reflect the degree to which the facility is similar to existing designs.

---

[10] This Design Process Element corresponds to Element 5 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[11] The application of task analysis is a basic component of the Control Room Design Review (CRDR) process specified by Section I.D.1 of NUREG-0660. Section I.D.1 is the related post-TMI action plan item referenced (per Footnote 8, "for information only") by 10 CFR 50.34(f)(2)(iii); performance of task analysis may thus contribute to providing "a control room design that reflects state-of-the-art human factors principles."

I-2.4.2.2 Design Basis Task Inventory

The inventory of control room and remote shutdown area tasks subject to TA shall include the contents of the emergency operating procedures, as well as a representative selection of normal operations and anticipated operating occurrences including startup, design basis load transients, shutdown, and uncomplicated reactor trip. "Worst case" justifications may be used to establish bounding cases and delimit the scope of analysis.

I-2.4.2.3 Level of Detail

The level of detail at which task elements are identified, and task element inputs and outputs are described, shall meet or exceed that embodied in the plant operating procedure steps

I-2.4.2.4 Methodology

Prior to certification, a task analysis methodology shall be documented and demonstrated capable of producing the following required results.

I-2.4.2.4.1 **Inputs and Outputs** - The TA data shall provide task element input and output characteristics in a manner sufficient to support the Verification of Availability as described in Section I-2.6.2.3.2.

I-2.4.2.4.2 **Workload Evaluation** - The TA shall incorporate a criterion-referenced method to evaluate operator loading. Analyzed conditions resulting in exceeding the loading criterion shall be entered for tracking as TOI issues per the Requirements of I-2.1.2.4.

I-2.4.2.5 Staffing Assumptions

The Task Analysis shall identify the relationship between the design basis for staffing and the staffing assumptions that are incorporated in the analysis, and shall verify (within the limits of the TA methodology) the acceptability of operator loading in terms of the design basis minimum staffing (as appropriate for the specified scenario).

I-2.4.2.6 Reporting of Results

Task Analysis reports shall provide a) an explanation of the methodology, assumptions, and criteria employed, b) citation of the inputs, bases, and references used, c) the resulting task element specification data, and d) a summary evaluation of the results, including identification of any specific concerns (e.g., cases of excessive loading).

I-2.4.2.7 Analysis of Human Error

Systematic error analysis is not required as part of the TA effort. While PRA activities may include HRA studies (and thus incorporate some Task Analysis activities) this shall be the responsibility of the PRA program and its associated management structure, and is therefore not governed by the HFE Program Plan or the present Process Element.

I-2.4.2.8 Role in Availability

The TA results, specifically the inventory of task elements and their data, shall serve as input to the Verification of Availability effort in I-2.6.

I-2.4.3 Acceptance Criteria

I-2.4.3.1 Operational Basis

I-2.4.3.1.1 Task Analysis Report(s) have been produced based on referenced procedural sources as described in I-2.4.2.1.

I-2.4.3.1.2 Task Analysis Report(s) have been co-originated by at least one Operations Expert, in addition to a Human Factors Specialist.

I-2.4.3.2 Design Basis Task Inventory

I-2.4.3.2.1 The Task Analysis Report(s) describes analyses which include all emergency operating procedure tasks, and an additional selection of normal and abnormal operating procedures, including startup, design basis load transients, shutdown, and uncomplicated reactor trip.

I-2.4.3.2.2 The Task Analysis Report(s) describes the basis for identifying the set of evaluated tasks as representative of all tasks required by anticipated operating occurrences.

I-2.4.3.3 Level of Detail

The level of task element detail of the TA is verified in the Task Analysis Report(s) to be not less than the level of detail provided by the plant operating procedure input.

I-2.4.3.4 Methodology

I-2.4.3.4.1 The TA method is demonstrated by example to provide the data required by Section I-2.6.2.3.2.

I-2.4.3.4.2 The TA method provides a criterion, basis, and evaluation of operator loading.

I-2.4.3.5 Staffing Assumptions

I-2.4.3.5.1 The design basis staffing and staffing assumptions incorporated in the analysis have been identified in the TA Report(s).

I-2.4.3.5.2 Operator loadings have been evaluated in the TA Report(s) for the design basis minimum staffing.

I-2.4.3.6 Reporting of Results

Reports at a minimum include the information required by Section I-2.4.2.6. All cases of results in which analyzed conditions exceeded the loading criterion of I-2.4.2.4.2 have been entered as TOI issues.

I-2.5 Man-Machine Interface Design[12]

I-2.5.1 Goals

The goal of Man-Machine Interface (MMI) design is to ensure that the final facility provides a thoroughly sufficient MMI, and a control room that reflects the State-of-the-Art in HFE. Stated differently, the aim is for the MMI designer's products to support the MMI user's needs. This is also the overall goal of HFE efforts; the specific efforts identified under MMI Design (the Process Element) focus on the provision and implementation of HFE Design Guidance, to provide criteria for and ensure the Suitability of the components comprising the MMI (e.g., labelling, layout, etc.)[13]

I-2.5.2 Requirements

I-2.5.2.1 HFE Design Guidance

I-2.5.2.1.1 **Provision** - Prior to certification, a collection of pertinent Human Factors Principles, as defined in the Introduction, shall be assembled by the design team to be applied to the MMI design as HFE Design Guidance.

I-2.5.2.1.2 **Applicability** - The HFE Design Guidance shall be applicable to the MMIs in all engineering control centers, including the main control room, the remote shutdown area, and local control stations.

---

[12] This Design Process Element corresponds to Element 6 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[13] As noted under I.3.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for Task Analysis, HFE design guidelines are a central component of CRDR; presuming sound bases for such guidelines, they may be construed as the required "principles" themselves. Incorporation of sound HFE Design Guidance in the design process thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

I-2.5.2.1.3 **Basis** - A technical basis for the HFE Design Guidance shall be provided. This shall include the scientific and/or technical references, studies, or rationale that supports the HFE Design Guidance provided. Justification in terms of juried scientific and technical publications shall be an acceptable basis for HFE Design Guidance; however, this shall not preclude the use of a priori reasoning.

I-2.5.2.1.4 **Content** - The HFE Design Guidance shall include coverage of the following topics:

a) Annunciator Warning Systems
b) Visual and Auditory Indications
c) Controls
d) Process Computers
e) Display-control Integration
f) Panel Layout and Organization
g) Labeling and Locator Aids
h) Workspace Layout and Environment
i) Communications
j) Anthropometry
k) Maintainability

This organization of topics is provided for information only, and is not required.

I-2.5.2.1.5 **Promulgation** - The HFE Design Guidance shall be formally promulgated by the Responsible Management Structure to the design team for implementation in the design.

I-2.5.2.1.6 **Control** - The HFE Design Guidance document(s) shall be subject to program design document control measures as applicable under I-2.1.2.2.4.

I-2.5.2.1.7 **Role in Suitability** - The HFE Design Guidance shall provide the criteria for the Verification of Suitability specified in I-2.7.

I-2.5.2.2 HFE Design Assumptions

I-2.5.2.2.1 **Workspace Conditions** - The MMI design and the corresponding HFE Design Guidance shall accommodate working conditions imposed within applicable workspaces as assumed in the analysis of SRDBEs, as defined in the Introduction.

I-2.5.2.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the MMI design or HFE Design Guidance shall not preclude the ability of the design to satisfy the requirements of 10 CFR 50.54(m)(2)(i) for minimum staffing.

I-2.5.2.3 Reference Design

I-2.5.2.3.1 **Documentation** - The Reference Design for main control room and remote shutdown area MMI systems and equipment shall be detailed within official program documents.

I-2.5.2.3.2 **Interdisciplinary Review** - Reference Design documents shall receive a documented interdisciplinary review, including participation of an HFE Specialist and an Operations Expert.

I-2.5.2.3.3 **Mockup Development** - The Reference Design documentation of I-2.5.2.3.1 shall be the basis for corresponding MMI mockups constructed for use in Suitability Verification.

I-2.5.2.3.4 **Product Review** - The Reference Design shall be the object of the product review of Part II of the RP.

I-2.5.3 Acceptance Criteria

I-2.5.3.1 HFE Design Guidance

I-2.5.3.1.1 **Provision** - A body of HFE Design Guidance has been assembled by the design team. Original guidance therein has been developed by HFE Specialists.

I-2.5.3.1.2 **Applicability** - The HFE Design Guidance, either through its contents or promulgation, formally indicates its applicability as specified under I-2.5.2.1.2.

I-2.5.3.1.3 **Basis** - A technical basis for the HFE Design Guidance has been provided as specified under I-2.5.2.1.3. If original, it has been explained by an HFE Specialist.

I-2.5.3.1.4 **Content** - The HFE Design Guidance includes coverage of the topics specified under I-2.5.2.1.4.

I-2.5.3.1.5 **Promulgation** - The HFE Design Guidance is verified by document distribution forms to have been formally promulgated by the Responsible Management Structure to the design team for implementation in the design.

I-2.5.3.2 HFE Design Assumptions

I-2.5.3.2.1 **Workspace Conditions** - The MMI design and the corresponding HFE Design Guidance shall accommodate working conditions imposed within applicable workspaces as assumed in the analysis of Safety-Related Design Basis Events, as defined in the Introduction.

I-2.5.3.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the MMI design or HFE Design Guidance shall not preclude the ability of the design to satisfy the requirements of 10 CFR 50.54(m)(2)(i) for minimum staffing.

I-2.5.3.3 Reference Design

I-2.5.3.3.1 The Reference Design for MMI systems and equipment documented and reviewed per the Requirements of I-2.5.2.3.

I-2.5.3.3.2 Corresponding mockups are verified to have been constructed for the Reference Design MMI.

I-2.6 Availability Verification[14]

I-2.6.1 Goals

The goal of Availability Verification is to ensure and document the presence, range, accuracy, etc. of the Indication and Control Features (as defined in the Introduction) required for operators to perform all necessary operating task elements in the main control room and remote shutdown area, per GDC 13 and 19 of 10 CFR 50, Appendix A.[15]

I-2.6.2 Requirements

I-2.6.2.1 Mandated Availability - The design shall make Available the following Federally mandated Indication and Control Features:

a) Integrated display of safety parameter indications; 10 CFR 50.34(f)(2)(iv).

b) Indication of the Bypassed and Inoperable Status of Safety Systems; 10 CFR 50.34(f)(2)(v).

c) Indication of relief and safety valve position; 10 CFR 50.34 (f)(2)(xi).

d) Indication of auxiliary feedwater system flow; 10 CFR 50.34 (f)(2)(xii).

e) Control of auxiliary feedwater system initiation; 10 CFR 50.34 (f)(2)(xii).

---

[14] This Design Process Element, along with Suitability Verification and Validation, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[15] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for Task Analysis (and as an explicit and objective use of the Task Analysis results), Availability Verification is a central component of CRDR. Verification of Availability thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

f) Indication of containment pressure; 10 CFR 50.34(f)(2)(xvii).

g) Indication of containment water level; 10 CFR 50.34(f)(2)(xvii).

h) Indication of containment hydrogen concentration; 10 CFR 50.34(f)(2)(xvii).

i) Indication of containment (high level) radiation intensity; 10 CFR 50.34(f)(2)(xvii).

j) Indication of noble gas effluents at potential accident release points; 10 CFR 50.34(f)(2)(xvii).

k) Indication of inadequate core cooling; 10 CFR 50.34(f)(2)(xviii).

l) Post-Accident Monitoring Indications; 10 CFR 50.34(f)(2)(xix).

m) Indication of inplant radiation and airborne activity; 10 CFR 50.34(f)(2)(xxvii).

I-2.6.2.2 I&C Inventory

I-2.6.2.2.1 **Database** - An I&C Inventory database shall be provided:

a) that allows the elements of the Task Inventory identified in I-2.4.2.2 (i.e their inputs and outputs) to be indexed and tracked against it the entries of I&C Inventory, and vice-versa;

b) whose data entries shall include device type, units, and required range, scale precision, and accuracy.

I-2.6.2.2.2 **Control** - The I&C Inventory shall be subject to program design control measures to maintain it current with the design configuration as applicable under I-2.1.2.2.4.

I-2.6.2.3 Formal Analysis

Prior to the combined operating license, a formal Availability Analysis will be performed to create the

I&C Inventory and test/verify its content against the TA Task Inventory.

I-2.6.2.4 Methodology

Prior to certification, an example of the methodology to be used in the formal Availability analysis shall be demonstrated.

I-2.6.2.5 Analysis Report

A report, explaining the methodology and summarizing the results of the formal Availability Analysis, including all discrepancies between required and actual I&C availability, shall be provided.

I-2.6.2.6 Discrepancies

Discrepancies between required and actual I&C availability specified by I-2.6.2.1 or I-2.6.2.2 shall be entered as TOI issues per the Requirements of I-2.1.2.4.

I-2.6.3 Acceptance Criteria

I-2.6.3.1 Mandated Availability

The design makes Available the Federally mandated indication and control features identified in I-2.6.2.1, or provides a technical justification for why they are no longer functionally required for plant operation. This is verified in an official project document.

I-2.6.3.2 I&C Inventory Database

An I&C Inventory database has been provided in the Availability Analysis Report that meets the requirements of I-2.6.2.3.

I-2.6.3.3 Formal Analysis

A formal Availability Verification analysis has been performed as stated in I-2.6.2.3.3.

I-2.6.3.4 Methodology

The methodology to be used in the formal Availability analysis has been demonstrated as stated in I-2.6.2.3.4.

I-2.6.3.5 Analysis Report

A report as specified in I-2.6.2.4.2 has been produced.

I-2.6.3.6 Discrepancies

The TOI database contents indicate that all discrepancies identified in the Availability Analysis Report have been entered as TOI issues.

I-2.7 Suitability Verification[16]

I-2.7.1 Goals

The goal of Suitability Verification is to ensure that the MMI's various Indication and Control Features (as defined in the Introduction) afforded by the main control room and the remote shutdown area are Usable designs that will support the operator's successful task accomplishment per the applicable HFE Design Guidance.[17]

I-2.7.2 Requirements

I-2.7.2.1 Formal Analysis

A formal Suitability Analysis shall be performed by an HFE Specialist to evaluate the Usability of the MMI Indication and Control Features of the main control room, and the remote shutdown area in terms of the HFE Design Guidance of I-2.5.

I-2.7.2.2 Relationship to HFE Design Guidance

Because of the necessarily generic and context-free nature of HFE Design Guidance, and the context-dependent nature of design tradeoffs, conformance to HFE Design Guidance is not itself a requirement. However, HFE Design Guidance shall provide the primary reference against which Suitability is evaluated.

---

[16] This Design Process Element, along with Availability Verification and Validation, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[17] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for HFE Design Guidance (and as an explicit application of that Guidance), Suitability Verification is a central component of CRDR. Verification of Suitability thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

I-2.7.2.3 Fidelity

Suitability Analysis shall utilize mockups or other representations of the completed design that manifest fidelity of the design characteristics being evaluated by the HFE Design Guidance. This may include evaluation of the completed design itself (e.g., a survey of installed lighting levels.)

I-2.7.2.4 Methodology

Prior to certification, an example of the methodology to be used in the Suitability analysis shall be demonstrated.

I-2.7.2.5 Analysis Report

Suitability Analysis report(s), explaining the methodology and summarizing the results of Suitability Analysis, including all discrepancies identified between the HFE Design Guidance and the actual design, shall be provided.

I-2.7.2.6 Discrepancies and Concerns

Discrepancies between the design and the HFE Design Guidance, and other concerns identified in Suitability Analysis reports, shall be entered as TOI issues per the Requirements of I.2.1.2.4.

I-2.7.3 Acceptance Criteria

I-2.7.3.1 Formal Analysis

Suitability has been formally Verified for the MMIs in all engineering control centers as specified in I-2.7.2.1 and documented in I-2.7.3.4.

I-2.7.3.2 Relationship to HFE Design Guidance

The Suitability Analysis Report indicates that the designs have been evaluated against the HFE Design Guidance Document of I-2.5.

I-2.7.3.3 Fidelity

Mockups and any other design representations used to

verify Suitability embody the evaluated characteristics specified in I-2.7.2.3, as recorded in an official project document.

I-2.7.3.4 Methodology

The methodology to be used in the Suitability analysis has been demonstrated as stated in I-2.7.2.3.4.

I-2.7.3.5 Analysis Report

Report(s) as specified in I-2.7.2.4 have been provided.

I-2.7.3.6 Discrepancies and Concerns

The TOI database indicates that discrepancies and concerns identified in Suitability Analysis reports have been entered as TOI issues.

I-2.8 Validation of Ensemble[18]

I-2.8.1 Goals

The goal of Validation is to ensure that the sum of the various MMI features afforded by both the main control room and the remote shutdown area provides a Usable operating ensemble that supports the successful accomplishment of the operator's functional role (i.e., as specified by training and procedures) under dynamic, real-time conditions.[19]

I-2.8.2 Requirements

I-2.8.2.1 Formal Evaluation

Prior to the combined operating license, formal Validation exercises for the main control room and the remote shutdown area shall be observed and documented by a team including HFE Specialist(s) and Operations Expert(s).

I-2.8.2.2 Relationship to Design Basis

Prior to certification, the set of Validation scenarios to be performed shall be specified, along with the applicable operating, tech spec, and safety function limits that will serve as acceptance criteria. The scenarios shall include normal operations (startup, design basis load transients, shutdown, and uncomplicated reactor trip), emergency operating procedures, and all SRDBEs (as defined in the

---

[18] This Design Process Element, along with Availability Verification and Suitability Verification, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[19] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for the Availability and Suitability aspects of Verification, Validation is a central (and the final) component of CRDR. Conduct of Validation exercises thus contribute directly to satisfying 10 CFR 50.34(f)(2)(iii).

Introduction) which credit operator actions in their analysis.[20]

I-2.8.2.3 Fidelity

Validation exercises shall utilize dynamic, stimulated, full-scope mockups, simulators, or other high fidelity facilities permitting real-time evaluation of the completed control room ensemble.

I-2.8.2.4 Evaluation Report

Validation report(s), describing the methodology and scenarios, the applicable criteria, and the summary results of the Validation exercises, shall be originated jointly by an observing HFE Specialist, an observing Operations Expert, and an SRDBE Safety Analyst. Validation report(s) shall include any failure to meet the detailed acceptance criteria of the exercises, including any case in which prior SRDBE analysis that has taken credit for operator action was not limiting in comparison to the corresponding Validation exercise.

I-2.8.2.5 Discrepancies and Concerns

Failures to meet Validation criteria, and other evaluator concerns identified in the Validation Reports, shall be entered as TOI issues per the Requirements of I-2.1.2.4.

I-2.8.3 Acceptance Criteria

I-2.8.3.1 Formal Evaluation

Validation for the main control room and the remote shutdown area has been performed and documented as described in I-2.8.2.1.

---

[20] This scope for Validation, one that includes both the intended methods of dealing with emergencies (i.e., the Emergency Operating Procedures) and the design basis emergencies themselves, is felt to provide a reasonable basis in the area of HFE, consistent with the extent and content of actual design basis safety analyses, for reaching "a final conclusion on ... safety questions associated with the design" per 10 CFR 52.47(a)(2).

I-2.8.3.2 Relationship to Design Basis

Official program documentation has indicated the scenarios to be performed, and criteria to be applied, as specified in I-2.8.2.2.

I-2.8.3.3 Fidelity

Facilities as specified in I-2.8.2.3 have been utilized for the validation exercises.

I-2.8.3.4 Evaluation Report

Validation report(s), as specified in I-2.8.2.3, have been originated jointly by an observing HFE Specialist, an observing Operations Expert, and an SRDBE Safety Analyst.

I-2.8.3.5 Discrepancies and Concerns

Failures to meet the Validation criteria, and other evaluator concerns identified in the Validation Reports, have been entered as TOI issues for resolution.

PART II

DESIGN PRODUCT REQUIREMENTS

OBJECTIVE

Part II of this document presents criteria for use in the design certification review of the main control room and other operating stations for an advanced light water reactor such as System 80+. It is intended that these criteria address NRC requirements such that subsequent review of the design shall be, principally, restricted to confirmation that the criteria have been met.

SCOPE

To facilitate implementation in a design review the criteria are grouped according to the functional elements which comprise an ALWR control room. Each section of Part II presents the criteria related to one of these groups, as shown in the Table of Contents.

METHOD

These criteria were derived from a review of documents (References through 27) which provide guidance for implementation of digital technology and application of human factors engineering in the evolutionary design of a nuclear power plant control complex.

REFERENCES

(1) ANSI/HFS 100-198 - American National Standard for Human Factors Engineering of Visual Display Terminal Workstations, Santa Monica, CA; Human Factors Society (1988).

(2) MIL-HDBK-761A - Human Engineering Guidelines for Management Information Systems; Washington, DC; Department of Defense (1989).

(3) MIL-STD-1472D - Human Engineering Design Criteria for Military Systems, Equipment, and Facilities; Washington, DC; Department of Defense (1981).

(4) NASA-STD-3000 - Man-Systems Integration Standards; Houston, TX; National Aeronautics and Space Administration (1989).

(5) NP-4350 - Human Engineering Design Guidelines for Maintainability; Palo Alto, CA; Electric Power Research Institute (1985).

(6) NPX80-IC-SD-791-01 - System Description for Control Complex Information System for Nuplex 80+, Rev. 01; Windsor, CT; ABB Combustion Engineering (1991).

(7) NUREG-0700 - Guidelines for Control Room Design Reviews; Washington, DC; US Nuclear Regulatory Commission (1981).

(8) NUREG-0899 - Guidelines for the Preparation of Emergency Operating Procedures; Washington, DC; US Nuclear Regulatory Commission (1982).

(9) NUREG/CR-3517 - Recommendations to the NRC on Human Engineering Guidelines for Nuclear Power Plant Maintainability; Washington, DC; US Nuclear Regulatory Commission (1985).

(10) UCRL-15673 - Human Factors Design Guidelines for Maintainability of Department of Energy Nuclear Facilities; Washington, DC; Department of Energy (1985).

(11) USE-1000 - Space Station Freedom Program Human Computer Interface Guide; Houston, TX; National Aeronautics and Space Administration (1988).

(12) 10 CFR 29 - Code of Federal Regulations, Occupational Health and Safety Administration; Washington, DC; Office of Federal Register (1990).

(13) Bailey, R. W. (1982) - Human Performance Engineering: A Guide for System Designers; Englewood Cliffs, NJ; Prentice Hall.

(14) Boff, K. R., and Lincoln, J. E. (1988) - Engineering Data Compendium: Human Perception and Performance; Wright-Patterson AFB, OH; Armstrong Aerospace Medical Research Laboratory.

(15) Ehrenreich, (1985); Computer Abbreviations: Evidence and a Synthesis. Human Factors, 27, 2, 143-156.

(16) Gilmore, W. E., Gertmann, D. I., and Blackman, H.S. (1989); User-Computer Interface in Process Control: A Human Factors Engineering Handbook; Idaho Falls, ID; Idaho National Engineering Laboratory.

(17) Helander, M. (Ed.); Handbook of Human-Computer Interaction; New York, NY; North-Holland (1988).

(18) Kiger, J. I. (1984). The Depth/Breadth Tradeoff in the Design of Menu-driven User Interfaces; International Journal of Man-Machine Studies, 20, 201-213.

(19) Ledgard, H. P. (1989) - The Case Against User Interface Consistency; Communications of the ACM, 32, 10, 1164-1173.

(20) Rasmussen, J. (1985) - The Role of Hierarchical Knowledge Representation in Decision Making and System Management; IEEE Transactions on Systems, Man, and Cybernetics, SMC-15, 2, 234-243.

(21) Rodgers, S. H. (Ed.) - Ergonomic Design for People at Work; Rochester, NY; Eastman Kodak Company (1983).

(22) Salvendy, G. (Ed.) - Handbook of Human Factors; New York, NY; Wiley (1982).

(23) Sanders, M. S., and McCormick, E. J. (1987) - Human Factors in Engineering and Design; New York, NY; McGraw-Hill.

(24) Tufte, E. R. (1983) - The Visual Display of Quantitative Information; Chesire, CT; Graphics Press.

(25) Van Cott, H. P., and Kinkade, R. G. (Ed.s) - Human Engineering Guide to Equipment Design; Washington, DC; Department of Defense (1972).

(26) Weiman, N., Beaton, R. J., Knox, S. T., and Glasser, P. C. (1985) - Effects of Key Layout, Visual Feedback, and Encoding Algorithm on Menu Selection with LED-based Touch Panels (Tech Report HFL-604-02); Beaverton, OR; Tektronix.

(27) Advanced Light water Reactor Utility Requirements Document, Volume II, ALWR Evolutionary Plant, Chapter 10, Man-Machine Interface Systems, Rev. 1, Electric Power Research Institute, August 31, 1990.

II-1 CRITERIA FOR ALARMS

1.1 Alarm Processing

1.1.1 The selection of conditions to be alarmed shall include the following:

a) Conditions related to exceeding safety limits, operating limits or manufacturer's limits on equipment shall be included.

b) Alarm conditions shall only represent infrequent, unexpected and/or undesired variable states, as a measure to reduce nuisance alarms.

c) Selection of alarm variables and setpoints shall be done with consideration that the alarm should allow the operator sufficient time and information to effectively and deliberately respond to the out-of-tolerance condition.

d) Alarm setpoints and logic shall be consistent with the Emergency Operating Procedures.

e) Data related to status information shall not be displayed as an alarm.

1.1.2 Methods of data validation shall be applied consistently to alarmed parameters and displayed parameters, such that the alarm condition is accurately represented in the relationship of the displayed parameter and the alarm setpoint. If validation is performed on an alarmed parameter, the validation shall be performed prior to processing the alarm.

1.1.3 Processing To Support Reduction Of Alarm Displays.

1.1.3.1 As a measure to reduce the potential for sensory overload, the total number of spatially dedicated alarm displays shall be limited. Redundant alarms, such as those representing separate channels of the same parameter, shall be represented by a single spatially dedicated alarm display, and alarms not related to the current operating mode shall be eliminated.

Additional acceptable methods for reducing the number of alarm displays:

a) Use of cross channel comparison to represent several channels of a single parameter with a single alarm.

b) Use of alarm logic and setpoints which are plant mode or equipment status dependent.

c) Combination of related alarms, such as those which require the same operator response, into a single display and use of alarm messages to indicate the specific condition in alarm. For example, if several alarms are associated with loss of cooling to a reactor coolant pump, these may be represented under a single alarm tile. This method of alarm grouping can be applied to both dedicated and selectable alarm displays, including: tiles, Video Display Unit (VDU) display directories and system level VDU displays.

d) Use of a multi-priority display scheme to combine alarms, such as low and low-low alarms, into a single alarm tile.

1.1.3.2 Where multi-input alarms are used, the capability to individually display the status of each alarm shall be provided.

1.1.4 Processing To Support Alarm Prioritization.

1.1.4.1 An alarm prioritization scheme shall be used, such that alarms requiring a quicker operator response will be identified as having a higher priority.

1.1.4.2 The number of priority categories shall be small (i.e., 2 to 4).

1.1.4.3 An acceptable basis for division of alarm priority is the proximity of an alarm setpoint to a Significant Operator Action Condition (SOAC), which is defined as one of the following undesirable plant conditions:

1) a critical function violation (safety or power production),

2) a success path violation (availability or performance),

3) major damage to equipment,

4) a personnel hazard.

1.1.4.4 An acceptable method of division of alarm priority is:

Priority 1 - Immediate Action (i.e., last warning prior to reaching an SOAC).

Priority 2 - Prompt Action (i.e., second to last warning prior to reaching an SOAC).

Priority 3 - Caution (i.e., any warning prior to the second to last warning prior to reaching an SOAC, and also for all non-SOAC alarms).

1.1.5 Integrated Alarms

1.1.6 Alarm List

1.1.6.1 Each alarm shall be tagged with its time of occurrence. The resolution shall be within 2 seconds for all alarms. For all exceptions, justification shall be provided that a coarser time resolution is adequate.

1.1.6.2 The operators shall be provided the capability to access at any time, via an on-line display and in printed form, the time sequence of alarms that have occurred. The capability to access the alarm list shall be provided at all (Main Control Room (MCR) workstations and in the technical support center.

1.1.6.3 The time period covered by the alarm list shall be predetermined and at least 4 hours.

1.1.6.4 Documentation shall be provided which demonstrates that the alarm system hardware and software have sufficient computational speed and capacity, and buffer capacity to assure that no alarm information would be lost from the alarm list historical record for the worst case upset or emergency that the plant may suffer.

1.1.6.5 The time sequence of alarms shall be recorded via non-volatile media.

1.2 Alarm Displays

1.2.1 The alarms shall be displayed in a manner such that the operator can discern the highest priority without first identifying them. The method of displaying alarm priority shall include these attributes:

a) Distinct visual cues to differentiate alarms of different priority; the cue for the higher priority alarms are the most salient.

b) The visual cues of alarm priority are applied consistently on different display media (e.g., on alarm tiles and VDU screens, overview displays, and in the redundant and diverse systems).

1.2.2 Visual display of alarms requiring immediate or prompt operator action shall be provided immediately, automatically (i.e., without operator action), and in a manner that enhances immediate recognition that an alarmed condition exists. Spatial dedication of such alarms, in a location directly viewable from the operator's normal working position, is an acceptable method.

1.2.3 Where alarms are grouped in a single display, lower priority alarms shall not mask higher priority alarms. Acceptable methods include:

a) Use of different color hues or flash rates to indicate the priority of the highest priority alarm represented by an annunciator.

b) Use of flash suppression to temporarily reduce emphasis of lower priority alarms in order to enhance emphasis of higher priority alarms.

1.2.4 Display techniques shall be utilized to correlate an alarm to related critical functions or success paths. The following techniques are acceptable:

a) Physical grouping of alarms for parameters, components or systems which share a common function.

b) Physical grouping of spatially dedicated alarms which have related safety functions to take advantage of pattern recognition.

c) Automatic indication of critical functions and success paths affected by actuated alarms.

1.2.5 Access to information supporting evaluation of the alarm condition shall be direct and prompt. Acceptable methods include:

a) Automatic display of messages related to the alarmed condition upon alarm acknowledgement.

b) Automatic display of an index or other prompt which identifies reference pages for further diagnostic information or a display which supports initiation of corrective actions.

1.2.6 The alarm display shall provide visual and audible indication of cleared alarm conditions.

1.2.7 Distinct visual cues differentiate alarm states (e.g., new, existing(acknowledged), cleared, reset(acknowledged)).

The visual cues for new, cleared and existing alarms shall not mask each other.

An acceptable scheme for visual differentiation:

Alarm State	Visual Cues
New	Fast Flash, Bright yellow.
Cleared	Slow Flash, Dark Yellow.
Existing	No Flash, Dull Yellow.
No Alarm or Reset	Normal Display with No Yellow Highlighting.

1.2.8 Visual display of the existence of an alarmed condition shall be provided at all times that any alarm condition requiring prompt or immediate operator action exists. That is, visual indication that an alarmed condition exists shall not require operator action, (e.g., activation of an appropriate display page shall not be necessary), and shall not be removed by automatic or operator action (e.g., due to selection of alternate display pages).

1.2.9 Spatial dedication of alarm displays shall be based on an evaluation of the significance of an operator response to the alarm, which includes consideration of the following factors: system impact, technical specification criteria, importance or severity of consequences, and time available to respond.

1.2.10 Where alarms are unacknowledged or deferred, they shall be stored in an ordered buffer and messages related to these alarms should be stored for ready access when the alarm is

acknowledged.

1.2.11 Overview Alarm Displays

1.2.11.1 The overview panel shall provide for the display of high level derive alarms such as would provide indication of plant mode or state, and availability of safety systems or functions. Indication of the following is required:

a) Alarms indicating failure of a critical safety function.

b) Alarms indicating poor performance or unavailability of success paths supporting critical safety functions.

c) Alarm mode, to indicate the state of the alarm system (for plant mode dependent alarm logic and setpoints).

1.2.11.2 Spatial dedication shall be provided on the overview display for certain key alarms. An acceptable approach is to provide dedicated display of the critical safety function alarms on the overview display.

1.3 Acknowledgement

1.3.1 Alarm acknowledgement techniques which facilitate acknowledgement of alarms without perceiving them, such as "global acknowledge", shall not be used.

1.3.2 A common acknowledge for redundant alarm systems shall be implemented such that the operator can acknowledge any alarmed condition on both systems with a single action.

1.3.3 Methods shall be implemented for reducing the burden associated with alarm acknowledgement. The following techniques are acceptable:

a) Provision of the capability to acknowledge alarms in small functionally related groups as well as individually.

b) Physical grouping of functionally related alarm displays.

c) Provision to display alarm messages convenient to the operator's position while performing other tasks.

d) Provision to defer acknowledgement of lower priority alarms such that distraction is reduced but notification is not lost. Such features may include: use of periodic rather than continuous audible alarms (e.g., momentary audible tones and reminder tones), and flash suppression (e.g., stop flash and resume flash).

1.4 Reliability

1.4.1 Alarms shall be provided by redundant means in all elements of power supply, processing and display to ensure that failures of normally replaceable parts do not result in loss of function.

1.4.2 For alarms related to critical safety function violations or prompting operator safety related mitigation actions for which there is no automatic action, the redundancy design shall meet separation and independence criteria similar to that provided for the redundant channels of the protection system. Exceptions to this criteria would be acceptable in areas where total separation would compromise the human factors aspects of the design (e.g., common acknowledgement vs separate acknowledgement, periodic data correlation). For these alarms, redundant elements shall be diverse to protect against common mode failure, and shall be seismically qualified.

1.4.3 Performance of the redundant systems should be monitored automatically via methods which detect deviations between the two systems and immediately report any indication of degraded performance to the operator.

1.4.4 Display of an alarmed condition shall occur within 5 seconds of reaching the associated setpoint.

1.5 Audible Tones

Implementation of audible tones shall comply with the following:

1.5.1 Audible tones shall be used to alert the operator to the presence of a new alarm condition and to the occurrence of cleared alarm conditions.

1.5.2 The location from which an audible tone is generated in the MCR shall be selected to enhance recognition of the physical location in the control room where the spatially dedicated display of the alarm resides.

1.5.3 Tones for new alarms are separate and distinct from tones used to signify clearing alarms.

1.5.4 The scheme for implementing audible annunciators shall limit the distraction and stress associated with audible alarms. The following are included as acceptable practices:

a) Use of momentary or self-silencing tones for new and cleared alarms.

b) Use of periodic, momentary reminder tones for unacknowledged alarms.

II-2 OPERATOR AIDS

2.1 Indication of the following shall be provided to the operator via visual cues that are distinct from the alarm displays.

2.1.1 Indication of the change of state of an interlock which allows manual action by the operator to take effect if certain conditions are met, and defeats the operator action if the conditions are not met.

2.1.2 Indication of automatic actuation that is appropriate for the plant state.

II-3 CRITERIA FOR PARAMETER INDICATIONS

3.1 Selection of Parameter Display Modes

3.1.1 Dedicated Displays

3.1.1.1 Dedicated display device(s) shall provide a continuous display of all Regulatory Guide 1.97 Category 1 variables as follows:

a) All Regulatory Guide 1.97 Category 1 variables shall be provided in a validated list.

b) Access to the individual channel parameter values shall be provided for all Regulatory Guide 1.97 variables.

3.1.1.2 Display device(s) shall be dedicated to access of the following key parameters. Multiple display pages can be used to accommodate display of this information.

a) Key parameters used to assess critical function status for safety and power production.

b) Key parameters indicative of success path performance for both safety and power production.

c) For composed parameters which are determined by an algorithm which uses sensor input from multiple parameters (e.g., determines average coolant temperatures from multiple hot leg and cold leg sensors), operator access to the individual sensor channels shall be provided.

3.1.2 Selectable Parameter Displays

3.1.2.1 Selectable displays shall provide all the plant parameters that are required for operation, but do not necessarily need to be displayed continuously.

3.1.2.2 Selectable parameter displays of like nature shall employ a consistent selection scheme throughout the control room.

3.2 Parameter Processing

3.2.1 Validation

3.2.1.1 Where multiple sensors or channels provide data for the same parameter to the control room, a validation scheme shall be implemented in determining a representative value to be displayed to the operator.

3.2.1.2 The operator shall be afforded a mechanism to access and view all sensor readings used in the validation scheme.

3.2.1.3 Indication shall be provided of data identified as suspect by a validation program. Use of a unique symbol, indicating suspect status, displayed adjacent to the displayed parameter value is an acceptable method.

3.2.2 Historical Recording

3.2.2.1 Facilities shall be provided so that operators can obtain past histories of particular parameters either through a VDU interface or on paper.

3.2.2.2 The capability to call up a pre-defined trend shall be provided for those parameters specified in the task analysis.

3.2.2.3 A trend shall be provided automatically in the display of certain parameters as identified in the task analysis.

3.2.3 Parameter values shall be adjusted through processing to provide the most applicable information possible with current plant instrumentation (e.g., compensated for density effects). This must be indicated to the operator by means of a label or coding scheme.

3.3 Features of Parameter Display

3.3.1 The rationale for selecting the manner in which parameter indications are presented to the operator (for characteristics range, display accuracy, response time, character size and time period for trends) shall be based on either task analysis, expert operator judgement, or predecessor designs, and documented. For example, the units of pressurizer pressure shall be the same on the display as it is described in the procedures and the procedure guidelines.

3.3.2 An alphanumeric designator or label shall identify parameter indications.

3.3.3 If two or more parameters are to be routinely compared then the difference, summation, average, etc. (as required) shall be displayed as a parameter in its own right.

3.3.4 When parameter information is displayed using bar graphs, all graphs shall be oriented consistently. To facilitate comparison and correlation among like parameters, scales shall also be consistent. Exceptions to this must be justified with respect to criteria 3.3.1.

3.3.5 When a bar graph is used to indicate a parameter, the operator shall be allowed access, either continuously or via some menuing mechanism, to the digital value of the parameter.

3.3.6 Scales shall conform to accepted HFE guidelines and these shall be applied consistently throughout the control room. The following are acceptable:

a) Grid lines on bar graphs shall be unobtrusive and shall not obscure data elements.

b) When parameters are to be displayed on a bar graph, the x-axis shall be time and the y-axis shall be the monitored parameter.

c) On the scale, the major and minor graduations shall have different sizes. Different lengths may be more legible for connotative point readings; different widths may be more visible if only quantitative check readings are required.

d) Graduation intervals shall be of one, two or five units, or multiples thereof by powers of ten.

e) Between the numbered graduations, the unnumbered

graduations shall not exceed nine in number.

f) When percentage scales are used, 0% of the scale shall correspond to the low end of the parameter, e.g.,minimum level, flow, power; similarly, 100% of scale shall correspond to the high end of the parameter range

g) The individual numerals on any scale should be vertically oriented with respect to the operator.

3.3.7 Display devices shall have sufficient scale range to accommodate all anticipated normal and abnormal operating conditions.

3.3.8 Instruments shall provide ranges such that nominal scale readings fall between 20% and 90% of full scale during normal operations.

3.3.9 If a display device incorporates the capability to automatically change the displayed range of a bar graph, then the operator shall automatically be informed before this occurs. Operator acknowledgement can be implemented to assure cognizance of the change.

3.3.10 Time history displays utilized in the control room shall have a consistent position for the origin.

3.4 Reliability

3.4.1 Parameter displays shall be provided by redundant means in all elements of power supply, processing and display to ensure that failure of normally replaceable parts do not result in loss of function.

3.4.2 Parameter displays shall be provided via redundant and diverse means, such that the processing and display of the following indications will be maintained even if a complete failure or common mode failure occurs in a system supporting those functions:

a) Information for Technical Specification monitoring with surveillance times less than 24 hours.

b) Information required to assess major equipment damage or personnel hazard alarms.

c) Regulatory Guide 1.97 Category 1 and 2 parameters (Types A-C) (not already on single parameter displays).

3.4.3 The devices used to display the Post Accident Monitoring Instrumentation (PAMI) parameters shall meet the applicable qualification criteria of Regulatory Guide 1.97.

3.4.4 If the device that displays the parameter indication fails then this shall be immediately apparent to the operator.

II-4 CRITERIA FOR INTEGRATED DISPLAYS

Integrated displays are those which combine parameter indications, alarms and component status indications to provide a higher level indication of system functional status. Piping and Instrumentation Diagram (P&ID) representations may be used in such displays.

4.1 Hierarchy of Displays

4.1.1 Integrated displays shall be organized in a hierarchical relationship that reflects the way that the operators will utilize them and the hierarchical scheme shall be documented. The hierarchy can be organized by sequence of use in particular tasks, by system or by function. Incorporation of the following features is acceptable:

a) Organization of the display hierarchy in such a way as to facilitate learning by the operator, including application of basic principles of the psychology of memory such as the limits of short term memory, chunking, etc.

b) Use of critical functions and success path monitoring as a basis in the design of the overview display, so that in training this basis can be used to guide the use of the overview display.

4.1.2 There shall be an overview display that provides the operator with information in a format so that high level "states" of the plant can be ascertained in minimum time.

4.1.3 A display of the overview shall be available at all normal operator working positions. Implementation of CRT displays at each working position or a big board panel in a location viewable from all such positions is acceptable.

4.2 Navigation

4.2.1 Integrated displays on CRTs shall afford the operator the ability to move from one display to another with a maximum of two torches. A design in which the first stroke accesses the pertinent detailed menu and the second stroke makes the specific item selection is acceptable.

4.2.2 Access to integrated display pages shall be afforded the perator by a system that makes use of "the human's natural inclination to point".

4.2.3 In order for the operator to select displays, the choices shall be displayed. An acceptable method is use of menus.

4.2.4 Elements of a menu shall belong to a logical group. Acceptable groupings of menu elements include:

a) Plant Sector
b) System
c) Function

4.2.5 The menu formats shall be consistent witnin particular display and control systems.

4.2.6 The ability to restore the display to the previous display page shall be provided to the operator.

4.2.7 Navigation through displays and through the hierarchy shall be facilitated by labeling and title schemes that reflect the commonly used terms for the elements displayed. Examples of this are: Labelling the part of a display that shows the safety injection system with "SIS", labeling a display page that contains an overview of the primary system with "PRI", etc.

4.2.8 When a single display, e.g., an alarm list, requires more screen area than is available, then the information shall be partitioned and some technique for the operator to move within and between partitioned groups shall be afforded. Direct access to the first page of such a display shall be provided on each page of the partitioned set.

4.3 Physical and Functional Features

4.3.1 Consistent coding of information shall be used throughout the integrated displays. A common metaphor, such as P&IDs, should be used consistently among the displays to the extent possible. Exceptions, and the basis for their use, shall be documented.

4.3.2 All integrated displays shall have the current time and date to facilitate date stamping activities as required for certain tasks. The format of this chronological indication shall be consistent across all displays.

4.3.3 Each integrated display shall provide a title by which it can be referred from a procedure or other document.

4.3.4 Coding schemes used on integrated displays shall conform to those specified by the parameter indications section and the component control section.

4.3.5 Screen loading or information density shall not exceed 50% of the total screen area (not including demarcation lines).

4.3.6 Empty screen area, lines and spaces should be the primary means of organizing and separating data.

4.3.7 Data presented to the user shall be in a readily usable and readable form, such that the user does not have to transpose, compute, interpolate or translate into other units, number bases or meaningful language.

4.3.8 Data fields that appear in multiple locations within a system shall have consistent names, and should have consistent relative position within similar displays.

4.3.9 The integrated displays shall duplicate and verify the information provided in a spatially dedicated manner.

4.3.10 Integrated displays shall provide quick direct access to supporting information for alarm conditions.

II-5 CRITERIA FOR DISCRETE COMPONENT CONTROL (ON/OFF)

5.1 Control Strategy

5.1.1 The current status (on/off, open/close) of a discrete state component shall be visible whenever the control mechanism for that component is available for use. The intent is to prevent blind operation of equipment.

5.1.2 Identification of locally controlled components for which status indication will be provided in the control room (e.g., containment latch door position) shall be determined by a documented task analysis, expert operator opinion or predecessor design. Status of such components shall be provided in the control room either by instrumentation or administrative procedure.

5.1.3 Consistent component status coding shall be used throughout the control room. For example, red status indicators for on or open; and green status indicators for off or closed.

5.1.4 The human factor attributes of *packaged* control devices shall be consistent, to the extent practical, with the human factors engineering standards set for the man-machine-interface.

5.1.5 The design shall provide mechanisms to restrict usage of component control devices (e.g., administrative control, automatic interlocks, alarms, two action controls, etc.).

5.1.6 Electrical current flow (amperage) indication shall be available for motor operated components rated at 100 h.p. (75 kw) and greater. This indication may be provided via soft-interface VDU, or continuous display hardware.

5.2 Auto/Manual Mode Changes

5.2.1 Automatic control shall be provided where manual control is not suitable due to response time requirements, the complexity of the control function, or the need to free the operator for other control room tasks.

This criteria is not intended to exclude the operator from the control loop. In general, the operator shall always have the ability to disable automatic control action and/or take manual control. This does not apply to automatic interlocks or actuation signals which are designed to keep the plant or equipment within the bounds of the technical specifications and plant operating procedures.

5.2.2 Control schemes with multiple modes (auto, manual, etc.) shall permit a "bumpless" transfer between any two control modes.

5.3 Auto Sequential Operations

5.3.1 Where two or more redundant components have a sequential auto start feature (e.g., at setpoint #1 start *A*, at setpoint #2 start *B*), the operator shall have the option to assign the in-service or first to start component, and the succeeding start sequence of the remaining redundant components if applicable. The intent is to give the operator the ability to establish a known sequence of events.

5.3.2 Where two or more redundant components have a standby feature (e.g., if *A* fails to start or trips, start *B*), the operator shall have the option to assign the first to start component, and the succeeding start sequence of the remaining redundant components if applicable. The intent is to give the operator the ability to establish a known sequence of events.

5.4 Common Coding Features

5 4.1 Spatially dedicated controls shall be provided for components that makeup the main flow path of normal and emergency success paths for all critical functions. *Spatially dedicated controls* shall meet the following criteria:

1. The controlling device shall operate the subject component and no others. It shall not share control function with other components.
2. The controlling device and its control state shall be continuously visible and available for use.
3. The controlling device shall occupy a fixed location on the control panel in an orientation that has a functional relationship to its adjacent controls.
4. Control action can be initiated directly (with no prior screen selection) or with minimal screen selection (i.e. one or two). Where selection is required it is only to access specific control options in a set of functionally related controls.

5.4.2 Control loops that require little or infrequent operator intervention may be accessed through selectable soft-interface VDU displays.

5.4.3 Failures in a component control loop that result in loss of control, or a control discrepancy shall be indicated at by a unique visual code or label. For example, use of a blinking switch position is an acceptable means of indicating that the demand state is different from the actual state of a controlled component.

5.5 Reliability

5.5.1 Component controls shall be redundant to the extent that a failure in the man-machine-interface device will not prevent further control action. The intent is to provide a backup means of inputting component control commands.

II-6 CRITERIA FOR MODULATING COMPONENT CONTROL

6.1 Controller Strategy

6.1.1 Control loops that have a cascade or nested relationship (e.g., master/subloop) shall be hierarchically arranged to clearly indicate their functional interaction.

6.1.2 Control systems with multiple input sources for the controlled variable shall indicate which input source is being used as the controlling variable. For example, if a control system can accept inputs from channel X, or channel Y, or the average of channels X and Y, then the control system must indicate which of the three options is being used and provide controls to change the input source.

6.1.3 Control systems with multiple setpoint sources (e.g., auto/operator) shall indicate the actual setpoint source at the control station. For example, if a control system can accept a setpoint from either the operator or some other source, an indication shall be provided to indicate which of the two possible setpoint sources the system is using and provide controls to change.

6.1.4 Control systems with a variable setpoint shall indicate the current value of the setpoint at the control station.

6.1.5 Control systems with auto/manual output modes shall indicate whether the source of the output signal is from the automatic or manual system.

6.1.6 Control systems with a variable output signal shall indicate the value (or relative analog) of the actual output signal.

6.1.7 Failures in a component control loop that result in loss of control or a control discrepancy shall be indicated by a unique visual code or label at the man-machine-interface. For example, use of a blinking switch position is an acceptable means of indicating that the demand state is different from the actual state of a controlled component.

6.2 Throttling Components

6.2.1 Components whose primary function is to provide throttling action (flow control) shall have real time throttle position feedback visible from the control station. The intent is to provide positive primary indication of component performance and not rely on secondary means (i.e., flow indication alone) for control action performance monitoring.

6.3 Reliability

6.3.1 Component controls shall be redundant to the extent that failure of a man-machine-interface device will not prevent further control action. The intent is to provide a backup means for inputting component control commands.

II-7 CRITERIA FOR SPECIAL CONTROLS

7.1 System Actuations

The following criteria apply to reactor trip, main turbine and generator trip, and engineered safety features actuation signals.

7.1.1 Control devices for manual reactor trip, main turbine and generator trip, and ESF system actuation shall be amenable to rapid actuation by one operator.

7.1.2 Control devices for manual trip and system actuation shall incorporate design techniques to reduce the potential for inadvertent actuation.

7.1.3 The current state (actuated/reset) of system actuation and trip shall be visible from the actuation control station.

7.2 Operating Stations

7.2.1 Spatially dedicated operator modules, related indications, and other control devices shall be grouped by function such that the control function can be accomplished without the need to rove. This should not be interpreted to preclude the use of multiple operating stations. Only that each operating station must have the necessary information and controls available within the immediate area. The intent is to prevent the need to rove from the operating station to perform related control actions or acquire information important to control.

7.2.2 There shall be spatially dedicated operating stations for the following systems and operational functions:

1) Reactor Coolant System: pressure, temperature, and inventory control
2) Reactor Control Rods
3) Main Feed System
4) Emergency Feed System
5) Main Turbine and Generator
6) Engineered Safety Features Systems
7) Heat Rejection Control Systems: atmospheric steam dump, steam bypass to main condenser, and long term decay heat cooling

7.2.3 The human factor attributes of *packaged* control devices shall be consistent with the human factors engineering standards set for the man-machine-interface.

7.3 Process Controls

7.3.1 Process control devices shall be separate from "indicate only" displays. The intent is to provide a clear distinction between indication only and active process control devices.

7.3.2 Process controllers shall provide continuous display of all parameters being controlled. As a minimum, process controllers shall have continuous display of the following:

- Mode of control (auto, manual, etc.)
- Setpoint and real time process value
- Process value identification tag

7.3.3 Response Time

Process controllers shall indicate the relative magnitude of the actual output signal being sent to the component in *real time* without the use of anticipatory simulation or other enhancement techniques. The intent is to keep the operator informed of the actual state of the control loop and thus prevent false expectations.

7.4 Engineered Safety Features Component Control and Monitoring

7.4.1 Operator Override

Operator override capability shall be provided on a component basis for all ESF actuated components. The logic shall be such that the override may be executed only after the ESF actuation signal.

7.4.2 When the ESF signal clears, the override logic shall also clear such that subsequent ESF actuation signals are not blocked.

7.4.3 Once the ESF actuation signal is cleared, repositioning of the component will occur only by a subsequent operator command or by an automatic control signal.

7.4.4 Inoperable Component Status Monitoring

ESF component inoperable conditions which may result from bypassed or inoperable conditions shall be continuously displayed to the operator per requirements in NRC Regulatory Guide 1.47. The intent is to identify ESF system availability prior to its actual need.

In addition to component inoperable conditions, the monitoring system shall also consider component misalignments.

In general, inoperable status monitoring should apply to all active components but are required for ESF components.

7.4.5 ESF Actuation Status Monitoring

ESF component status monitoring shall be provided such that upon the initiation of an ESF actuation signal the operator is able to determine if all components in the ESF trains have responded properly.

7.5 Auto Mode Selection With Multiple Components

This section addresses control designs that require multiple components to be controlled by the same automatic control signal.

7.5.1 There shall be one switch for each component if each component is being controlled individually.

7.5.2 There shall be one auto mode switch (not one for each component) if all components are controlled as a group. This switch shall be located and labeled to indicate its group orientation.

7.6 Features of Display

7.6.1 Process flow lines shall be included in all layouts of controls and dedicted indicators where the physical relationship of plant components is the basis for the layout.

7.6.2 Labels shall be provided in mimics such that all flow lines lead to or from a specified component, a source label or a destination label.

7.6.3 Demarcation lines and mimic flow lines on control panels shall be wide enough to provide the appropriate demarcation without adding visual clutter to the control boards. Use of lines at least 3/16 of an inch wide are acceptable.

7.6.4 Demarcation lines and mimic flow lines shall be consistently sized throughout the control room.

7.7 Overview Display

7.7.1 Component indications found on the overview display shall utilize the same coding conventions established in the control room.

7.7.2 When component indications are composite, that is, reflect the aggregate effect on flow path or the component, this shall be apparent to the operator by the indications used in the display.

II-8 CRITERIA FOR CONTROL ROOM MONITORING AND CONTROL FUNCTION LOCATION

8.1 Main Control Room Criteria for Control and/or Monitoring

The following criteria shall be considered when making control and instrumentation assignments in the MCR (potential exceptions to these general criteria will be on a case by case basis, with documentation of the rationale):

8.1.1 Controls and indication used for critical safety and production functions and their success paths (e.g., Emergency Cooling, Emergency Diesel Generators, Post Accident Monitoring) shall be directly or indirectly (e.g., verify that there is no leakage by monitoring a tank level) instrumented and displayed in the MCR;

8.1.2 Indication an associated controls for systems that require frequent (more than two times every eight hours) or expedited operation (two hours or less) should be located in the MCR;

8.1.3 The primary location for normal controls that can cause a reactor trip shall be the MCR (e.g., Reactor Coolant Pump controls, Circulating Water System Pump controls, etc.); Note: this does not preclude controls required for hot shutdown from being located in the Remote Shutdown Room (RSR) as well as the MCR, nor local controls for large circuit breakers or protective features;

8.1.4 The primary location for normal controls and indication used for critical safety and power production functions and their success paths shall be the MCR (e.g., Reactivity Control, Inventory Control, Pressure Control, Core Heat Removal, Emergency Diesel Generators, Post Accident Monitoring Indication, etc.). A method of backup control outside the MCR shall be provided at local control stations (e.g. Local Diesel Generator Control Panel for long term cold shutdown) or the RSP.

8.2 Criteria for Local Safety Related Control and/or Monitoring

8.2.1 Systems important to safety and that make use of local control stations (e.g., Local Diesel Generator Control Panel) shall have a Man-Machine Interface (MMI) that will avoid incompatibilities and encourage a high degree of positive transfer of training when compared to similar MMI in the MCR.

8.2.2 In addition to controls in the Main Control Room, local control shall be provided for all systems and components needed to achieve and maintain cold shutdown of the reactor (e.g., local Diesel Generator Control Panel) for which controls are not provided for in the Remote Shutdown Room;

8.2.3 Safety and non-safety related controls used primarily for initial system startup (e.g., pump suction isolation valves, instrument isolation valves, transformer cooling fans, lube oil systems, and fully automated support systems (i.e., oil systems, seal water)) may be locally controlled and not controlled from the MCR. Locating these controls locally will not significantly increase operator workload because these support systems are infrequently operated (e.g., after a refueling outage, after maintenance);

8.2.4 Local controls shall be provided for:

a. Where local manual control actions and/or surveillance must be accessed frequently or performed in close proximity to the equipment (e.g., cycling a valve during maintenance);

b. Where testing and surveillance would unnecessarily burden the MCR operators and not effect power production or safety;

c. Local disconnects for electrical components greater than 120 volts to provide personnel protection;

d. For cases in which safety, and power production support and/or auxiliary system processes are controlled locally (e.g., filling a diesel generator day tank, etc.), administrative controls (e.g., surveillance, test or operating procedures), physical barriers (e.g., key locks, locked doors) or alarms shall be provided to ensure that MCR operators are cognizant of all activities that could effect power production and safety.

8.3 Remote Shutdown Room Criteria for Control and/or Monitoring

8.3.1 The Remote Shutdown Room shall provide an alternate control station which can be used in the unlikely event that the MCR becomes uninhabitable or damaged. In the event that evacuation of the MCR becomes necessary, the operators shall be provided with the means to transfer control to the Remote Shutdown Room.

8.3.2 The RSR shall contain the controls and indication required to:

a) Achieve prompt hot shutdown of the reactor, subsequently referred to as hot standby per standard technical specifications (reactor subcritical at operating pressure and temperature);

b) Maintain the unit in a safe condition during hot standby;

c) Achieve and maintain cold shutdown per standard technical specifications.

8.3.3 Specifically, the RSR shall meet General Design Criteria (GDC) 19 of 10CFR50, Appendix A and Appendix R.

8.4 Surveillance, Maintenance and Testing Control and/or monitoring Criteria

8.4.1 The MCR operators shall be provided with all indication and controls needed to support any surveillance or testing that must be conducted by licensed operators. All systems should provide the operational status/readiness (bypassed, in test, disabled, etc.) for display in the MCR.

8.5 Access, Egress and Security Control and/or Monitoring Criteria

8.5.1 The MCR shall be given the ability to override security and provide permissive to allow access to all vital areas at the discretion of the Shift Supervisor or his designated representative. However, MCR operators should not be required to control or provide a permissive to access vital areas as a part of their routine duties. In addition, the MCR personnel shall be automatically alerted to security alerts or changes in plant security status, and whenever any vital I&C equipment door is opened since these may have a direct impact on plant operation and/or safety.

II-9 CRITERIA FOR MAIN CONTROL ROOM (MCR) CONFIGURATION

9.1 Overall MCR Configuration

9.1.1 The Main Control Room (MCR) shall contain areas to accommodate the following:

a) Controlling Work Space with workstations containing plant controls, displays and alarms.
b) Offices for the plant shift supervisor, control room supervisor and remaining operating staff.
c) Reference material and emergency equipment storage.

9.1.2 The controlling work space shall allow operation by a single operator between hot standby and full power. Adequate workspace shall be provided to accommodate up to two supervisors and up to four operators continuously.

9.1.3 Techniques shall be used in the MCR configuration design which limit the required access to the controlling work space for non-operating staff during both normal and emergency operation. This is intended to prevent unnecessary distractions to plant operators at the controls.

9.1.4 The MCR configuration shall provide a work station for a control room supervisor within the controlling work space to allow direct coordination of controlling workspace activities and support his/her tasks.

9.1.5 The control room configuration shall allow visibility of a "big board" overview display from all locations within the MCR controlling work space, and from control room offices.

9.1.6 The Technical Support Center (TSC) shall be provided with systems and/or features to ensure effective communication with personnel in the MCR including viewing of MCR activities. Acceptable systems and/or facilities include Telephones, Viewing Window, Television Display.

9.1.7 The capability shall be provided outside the MCR for plant technical staff to access the same real time plant performance data as in the MCR. Video display devices are an acceptable means to accomplish this.

9.1.8 Accessibility of Instrumentation and Controls - The operators shall not have to leave the controlling workspace to attend to control room instrumentation on back panels or elsewhere during operations.

9.1.9 Operator Freedom of Movement - Operators should be able to get to any point in the control room without having to overcome obstacles such as filing cabinets, storage racks, or maintenance equipment. Adequate space shall be available for the operator to freely access console operating positions.

9.1.10 Communications - The arrangement of consoles and desks in the controlling workspace shall facilitate direct communication between operators at any combination of workstations.

9.1.11 Legibility - All labels and indications shall be legible at defined reading distances.

9.2 Panel Arrangements

9.2.1 The MCR controlling work space shall provide dedicated main operational areas for normal, frequently performed operations and infrequent auxiliary or safety operations. The normal operating area shall be designed for seated and occasional standing operation. The auxiliary and safety operations workstations may be designed for seated or standing operation.

9.2.2 The normal operator workstation shall provide all controls and indicators to perform the following tasks:

a) Perform all monitoring and control tasks associated with maneuvering the plant from hot shutdown to full power operation and return to hot shutdown
b) Monitor all major automatic controls (e.g., pressurizer automatic pressure and level controls) to maintain plant availability
c) Perform standard post trip actions following a reactor trip
d) Monitor Critical Function Processes during plant emergencies

9.2.3 The normal operator workstation panels that contain functions performed most frequently shall be placed toward the center of the console.

9.2.4 Controls for safety related systems shall be located on panels such that they can be managed independently from power production and auxiliary systems and so that they are clearly distinguished from non-safety controls.

9.2.5 Controls for non-safety related systems and functions not required to be assessed frequently for normal power production shall be located on panels such that they can be managed independently from power production and safety systems.

II-10 CRITERIA FOR INDIVIDUAL CONTROL PANELS

10.1 Panel Section Arrangement

10.1.1 Instrumentation and controls on individual panel sections shall be laid out based on operator functions as the primary design criteria, and not on functions of equipment or systems.

10.2 Panel Dimensions

10.2.1 Standardized panel profiles shall be used for sit-down panels (that accommodate both seated and standing viewing) and panels that accommodate standing operation only. These panels shall be designed to meet a project specific set of Human Factors Engineering anthropometric guidelines. These panels shall be designed to accommodate the 5th percentile female through the 95th percentile male.

10.3 Panel Layout

10.3.1 FUNCTIONAL LAYOUT

10.3.1.1 Separate functional groups of components should be spaced apart so that the functional group boundary is obvious.

10.3.1.2 Demarcation shall separate functional groups of components, particularly where ample space between functional groups of components is not available.

10.3.1.3 Functional groups within a panel shall be identified by the use of name tags and demarcations.

10.3.1.4 Spatially dedicated alarm tiles shall be placed in the upper most section of a control panel to accommodate viewing when not directly in front of a panel.

10.3.1.5 Display only devices (e.g. VDUs and discrete indicators) shall be placed in the vertical section of a control panel to accommodate viewing from locations not directly in front of a panel.

10.3.1.6 Control devices (e.g. process controllers, on/off switches) shall be placed in the apron section of panels, below their functionally related display and alarm devices to provide a distinctive break from monitoring functions.

10.3.1.7 Devices within panel sections shall be arranged to promote easy understanding of the relationships between the devices and the system. Acceptable relationships for use in determining panel arrangements include the following: sequence of operation, related function and system flow path.

10.3.1.8 Arrangement of Physically Similar Components

a. Consistent Layout - The layout of similar control and display sets shall be consistent at all locations.

b. Orientation - Horizontal rows rather than vertical columns should be used.

c. Parsing Rows of Components - Large groups of similar components shall not be laid out in an unbroken row or column (e.g., no more than 5 similar components shall be laid in an unbroken row or column).

d. Mirror Images - Plant relationships may show bilateral (i.e. left-right) symmetry, and this may be an effective organizing framework for displays and controls. However, arbitrary reversal of component layout relationships (mirror-imaging) that does not denote a meaningful attribute of the system shall be avoided.

e. Large Matrices

Matrices of similar components shall have labeled coordinate axes for identification of any single component within the grid. The left and top sides of the matrix shall be used for labeling. Large (more than 5 by 5 element) matrices shall be broken up using physical spacing or demarcation.

10.3.1.9 Paired Controls & Displays

Controls and related displays shall be closely placed so that the two items are readily associated and can be used conveniently with one another. The control shall be placed so that the display is not obscured by the operator during control operation.

10.3.1.10 Paper Surfaces

Sit down panels should be provided with open surfaces for required operator paperwork (e.g. operating procedures, logs, alarm response procedures, etc.). If sit down panels are not provided with open surfaces, such areas shall be provided within the controlling work space with full visibility to the controlling work space panels.

10.3.2 Component Spacing

10.3.2.1 Separation between control devices should be sufficient such that access to one device cannot be impeded by adjacent devices, and that erroneous activation of components can be reasonably avoided.

10.3.2.2 Where simultaneous actuation of devices is necessary anthropometric guidance shall be provided to ensure that all operators can accomplish all required control uctions (e.g., the devices should not be separated by more than 40 inches).

10.3.3 Display Position

Displays and controls shall be positioned on panels considering all project specific ergonomic criteria. These criteria shall include:

visual field
display height/vertical angle
horizontal display plane angle
display distance.

Display position shall accommodate the 5th percentile female through the 95 percentile male to provide indications within the nominal field of vision, controls within the nominal reach and to avoid excessive movement.

II-11 CRITERIA FOR WORK SPACE ENVIRONMENT

11.1 Lighting & Illumination

The level of control room illumination (in foot candles) shall be high enough to adequately perform all anticipated duties without being so high as to cause undue problems with glare and reflectance. Because some tasks, such as VDU viewing, will require relatively low levels while others, such as paperwork or maintenance may require high levels, control room lighting shall be adjustable and non-uniform.

11.1.1 Task lighting

I umination levels should be uniform at each work station.

11.1.2 Emergency lighting

a) Loss of lighting AC power shall activate emergency lighting, which shall be independent of non-emergency power supplies.

b) Under emergency conditions where off site power, or any AC power is available, lighting levels shall be kept the same as during normal conditions.

c) Battery packs (for emergency lights) shall be mounted as unobtrusively as possible but still be accessible for testing. Bulb change in regular fixtures must be able to be carried out in a speedy manner which does not impair plant operations.

11.1.3 Task area luminance ratios

Extreme differences or sudden transitions between the luminance of a task and its surrounds (e.g., ratios in excess of 100:1 or 1:100) shall be avoided.

11.1.4 Reducing glare and reflectance

Techniques shall be taken to limit problems with glare and undesirable reflectance. Acceptable methods include:

a) maintaining low task area luminance ratios,
b) low reflectance flooring and wall covering,
c) anti-glare screens

11.2 Noise

11.2.1 Noise levels in control room & work spaces

The acoustic design of the control room shall ensure that 1) verbal communications between operators are unimpaired; 2) auditory signals are readily detected; and 3) techniques are used to minimize auditory distraction, irritation, and fatigue of operators.

11.2.2 Noise levels in equipment spaces

It is recognized that due to flow, operating equipment, etc., the balance of plant will contain many areas that are noisier than the Main Control Complex. Nonetheless, noise levels in equipment spaces should be minimized, where reasonable possible, particularly for excessive noise from isolated sources. Project specific maximum noise levels shall be established.

11.3 Air Quality and Temperature

11.3.1 Temperature and humidity

The climate control system shall be capable of continuously maintaining temperature and humidity within the project specific comfort zone for an approved heating, ventilation and air conditioning guideline (e.g., Ashrae Comfort Standard 55-74).

11.3.2 Ventilation

The ventilation system should be capable of introducing outdoor air into the control room.

11.4 Architectural Features

11.4.1 Operator comfort

Design features shall be employed to assure operator comfort. Towards that end, the following architectural and design features shall be incorporated:

a. Adequate seating shall be provided in all work spaces, sufficient to support intended staffing.

b. Personal storage space for each on-duty operator shall be provided within or adjacent to the control room (but outside the controlling work space).

c. Work space environmental controls such as temperature and humidity shall provide work space staff with a suitable range of adjustment to maintain comfort and compensate for changes in plant and ambient environmental conditions.

d. Accessories and work equipment (logs, chart paper, office supplies, etc.) shall have appropriate and convenient storage within or adjacent to the control room (but outside the controlling work space)

11.4.2 Bathrooms, kitchens and other facilities

11.4.2.1 Bathrooms

Separate men's and women's lavatories shall be provided within 100 feet of the main control room.

11.4.2.2 Kitchen

A kitchen or food storage and preparation area shall be provided within 100 feet of the main control room, including an eating area, sink, microwave, and refrigerator.

11.4.2.3 Other facilities

A clothes change and coat storage area (which could double as an air-pack, hard hat, flashlight, etc. area) shall be provided within 100 feet of the main control room.

11.4.2.4 Flooring

Flooring should be non-slip, non-glare, and minimize foot fatigue. Flooring should aid in dust control. Inside the control room, carpeting shall be used.

In the event carpeting is not allowed for fire or other technical concerns, rubberized mats or similar devices to reduce operator foot fatigue shall be used.

11.4.2.5 Wall covering

Wall covering should be low-glare and sound-absorbent, and durable aesthetically (easy to clean, able to withstand rubbing and scrapping).

Communication links between the office and the main operating area shall be provided.

11.4.3 Storage

11.4.3.1 Document storage

Storage space shall be provided so that procedures, logs, and drawings needed for routine job performance at operator work stations are conveniently available for the operator. Document storage shall permit individual documents to be easily located and extracted.

11.4.3.2 Emergency equipment storage

Emergency equipment shall all be stored so as to be readily accessible, and kept in an immediately useable state.

Equipment such as air packs, protective clothing, flashlights, etc. shall be located such that operators do not have to traverse 'hostile' environment to reach it.

11.5 Desks and Chairs

11.5.1 Desks

Desks shall provide for flat laydown of the maximum size drawing used in the MCR.

11.5.2 Chairs

Chairs used at desks and seated work stations should have back rests, arm rests, cushions, breathable covering, adjustable seat height, be able to rotate and have mobility.

II-12 CRITERIA FOR PRINT & TEXT FORMAT CONVENTIONS

12.1 Abbreviations and Acronyms

12.1.1 Acronyms and abbreviations shall be combined and maintained on a single list, known as the Approved Abbreviations List.

12.1.2 Management of the approved abbreviations list

The Approved Abbreviations List shall support consistent development of meaningful materials for use by operators, maintainers, designers, engineers, technicians, and other Operations and Maintenance (O&M) technical staff. This list will be controlled and updated as necessary to incorporate new terms. This list of abbreviated O&M terms shall not incorporate organizational or administrative terms unless these will be used in labeling, procedures, test specs, etc.

12.1.3 Guidance for generating abbreviations and acronyms shall be provided. Acceptable means of guidance include things such as an algorithm made available to all personnel who have a need to generate an abbreviation or acronym.

12.2 Alphanumeric Characters for Labels & Text

Human factors standards and guidance shall be developed and documented for alphanumeric characters for labels and text, based on accepted industry guidance. These shall be applied throughout the design or mechanisms shall be in place to detect non-compliance during subsequent design phases. The guidance shall address the following basic issues: font style, use of cases, character size and viewing distance, character width, stroke width and spacing.

12.3 Other Concerns

12.3.1 Warning Labels - Titles on warning labels (e.g., Caution Warning, radioactivity, etc.) should be 3 times the minimum specification for legible character size at the specified reading distance. Text beneath the title should use the standard size of characters based on the viewing distance.

12.3.2 VDU Resolution - The minimum font matrix size should be 7 by 9 dots or pixels per character (12 raster lines per text line).

II-13 CRITERIA FOR OTHER CONTROL PANELS

13.1 Remote Shutdown Panel

13.1.1 The Remote Shutdown Panel shall conform to Main Control Room anthropometric guidelines and panel profiles.

13.1.2 System/device layouts on the panel shall use the same layout/format, where possible, as those same features are laid-out on the Main Control Room Panels.

13.1.3 The criteria for print and text format, equipment labels, demarcations, color coding, lighting, noise, and air quality and temperature used in the Main Control Room shall also apply to the Remote Shutdown Panel.

13.2 Local Panels

Local panels containing safety related equipment (e.g., Diesel Generator Control Panel) shall provide a Man-Machine Interface (MMI) to operators that will avoid incompatibilities and encourage a high degree of positive transfer of training when compared to similar MMI interfaces in the Main Control Room.

Acceptable methods of accomplishing this are use of the same Human factors Standards and Guidelines and use of standard MMI devices.

II-14 CRITERIA FOR MAINTAINABILITY

Maintainability human factors standards and guidelines shall be developed and documented. These shall be applied throughout the design or mechanisms shall be in place to detect non-compliance during subsequent design process elements. The guidance shall address the following maintainability issues: general HFE principles, standard materials, removal and replacement fool proof features (e.g., alignment aids or interlocks), In-situ maintenance, (e.g., accessibility modular construction), facility arrangements and installation (e.g., laydown space), and documentation of maintenance task data and requirements, and software maintainability.