HUMAN FACTORS ENGINEERING

VERIFICATION AND VALIDATION PLAN

FOR

NUPLEX 80+

NPX80-IC-VP790-03
Revision 00

ABB COMBUSTION ENGINEERING, INC.
Nuclear Power
Windsor, Connecticut 06095-0500

Prepared by R.L. Rescorl, Man-Machine Interface Design Date 9/24/93

Prepared by R.B. Fuld, Lead Human Factors Engineer Date 9/24/93

Approved by D.L. Harmon, Supervisor, Man-Machine Interface Design Date 9/24/93

Approved by T.J. Rozek, Manager, I&C Monitoring Systems Engineering Date 9/24/93

Issue Date 9/24/93

RECORD OF REVISIONS

NO.	DATE	PAGES INVOLVED	PREPARED BY	APPROVALS
00	9/24/93	ALL	R.L. Rescorl R.B. Fuld	D.L. Harmon T.J. Rozek

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

ABB-CE	Asea Brown Boveri - Combustion Engineering
ATWS	Anticipated Transients Without Scram
CCS	Component Control System
CFR	Code of Federal Regulations
COL	Combined Operating License
CRT	Cathode Ray Tube
CSAS	Containment Spray Actuation Signal
DIAS	Discrete Indication & Alarm System
DPS	Data Processing System
EFAS	Emergency Feedwater Actuation Signal
EPG	Emergency Procedure Guidelines
ESDE	Excess Steam Demand Event
ESF-CCS	Engineered Safety Features Component Control System
FTA	Function & Task Analysis
HFE	Human Factors Engineering
HRA	Human Reliability Assessment
HSI	Human-Systems Interface
I&C	Instrumentation and Control
ICR	Instrumentation and Control Requirements
IPSO	Integrated Process Status Overview
OSIP	Operational Support Information Program
LOAF	Loss of all Feedwater
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MSIS	Main Steam Isolation Signal
OSIP	Operational Support Information Program
PPS	Plant Protection System
PRA	Probable Risk Assessment
PZR	Pressurizer
RCS	Reactor Coolant System
RSP	Remote Shutdown Panel
RSR	Remote Shutdown Room
SGTR	Steam Generator Tube Rupture
SIAS	Safety Injection Actuation Signal
TOI	Tracking-of-Open-Issues (database)
VAC	Volts Alternating Current
VDC	Volts Direct Current
V&V	Verification and Validation

1.0 PURPOSE

The Human Factors Engineering (HFE) Verification and Validation (V&V) Plan for Nuplex 80+ describes how the HFE V&V is managed, administered, and performed. Additionally, the V&V analysis criteria, methodology, required resources (e.g. Emergency Procedure Guidelines (EPGs), normal and abnormal operating sequences, I&C design requirements, HSI design validation facilities, schedule for activities, and milestones are provided. Specifically, the HFE V&V Plan meets the design process requirements and criteria for availability verification, suitability verification, and validation of the design as defined in Sections A-3.6, A-3.7, and A-3.7 of the Human Factors Program Plan for System 80+ (TM) Standard Plant Design (Reference 1).

The V&V Plan addresses the requirements of standard industry references for control room V&V activities (e.g., References 8, 9, and 10). It also addresses the requirements of Element 8, Human Factors Verification and Validation of the draft NRC Program Review Model (Reference 6). This plan satisfies the intent of the criteria defined in Element 8. It includes:

1) the design commitment of thoroughly evaluating the HSI as an integrated system using HFE evaluation procedures, guidelines, standards, and principles,
2) Inspection/Test/Analysis including the following: method for implementing HFE V&V, documentation of analyses and findings, and review by the Nuplex 80+ Design Team,
3) Design Acceptance Criteria including the following:
   a) General Criteria - criteria for availability verification, suitability verification, and validation, is described in Sections 6.1.5, 6.2.5, and 6.3.5,
   b) Implementation Plan - This plan will serve as an implementation plan when supplemented by Appendix B items to be addressed in more detail before initiation of the V&V activities,
   c) Analysis Results Report - the Availability Verification, Suitability Verification, and Validation Reports document all V&V analyses,
   d) Design Team Evaluation Report results - the ABB-CE document distribution, review, and comment process (Appendix A provides comments) ensure that the results of the HFE V&V activities are received, reviewed and commented on by the Nuplex 80+/System 80+ design team.

2.0 SCOPE

The HFE V&V Plan applies to all Human System Interfaces (HSI) and workspace environments in the Main Control Room (MCR), Remote Shutdown Room (RSR) and those local control stations specified in the EPGs. This V&V of the design precedes similar testing of final procedures, which is performed as the final step of procedure development by the Combined Operating License (COL) Applicant. The relationship of the HSI V&V to the procedures V&V is discussed in Reference 1, Sections 4.2 and 5.7.

HFE V&V is a three step process, 1) availability verification, 2) suitability verification, and 3) validation. Availability verification assures that the System I&C Inventory meets all requirements (e.g., Federally mandated indication and control requirements) and that the as-designed HSI is complete and only the needed information and controls are present. Suitability verification addresses the issue of whether the form and arrangement of HSI indications and controls and environment supports operator task accomplishment. Validation ensures that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EPGs provide usable work ensembles that support the successful accomplishment of the operator's required tasks.

3.0 REFERENCES

1. Human Factors Program Plan for the System 80+ (TM) Standard Plant Design, NPX80-IC-DP790-01, Rev 01, December 15, 1992.

2. Guidelines for Control Room Design Reviews, NUREG-0700, U.S. NRC, 1981.

3. Advanced Human-System Interface Design Review Guideline, NUREG/CR-5908, Draft, 1992.

4. Nuplex 80+ Verification Analysis Report, NPX80-TE-790-01, Rev 2, December 1989.

5. Simulator Performance Measures, Final Report, CE-NPSD-514, Task 572, Combustion Engineering, Inc., December, 1988.

6. Human Factors Engineering Standards, Guidelines, and Bases for System 80+, NPX80-IC-DR-791-02, (Draft).

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

8. Standard Review Plan, NUREG-0800, U.S. NRC, 1984.

9. IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generating Station Control Rooms and Other Peripheries, IEEE Std 845-1988, IEEE, 1988.

10. Design for Control Rooms of Nuclear Power Plants, IEC 964, Bureau Central de la Commission Electrotrotechnique Internationale, 1989.

11. A Status Report Regarding Industry Implementation of Safety Parameter Display Systems, NUREG-1342, U.S. NRC, April 1989.

12. Instrumentation for Light-water cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Regulatory Guide 1.97.

4.0 DEFINITIONS

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 (Reference 2).

Features - MCR console annunciators, displays and controls are implemented using Video Display Unit (VDU) devices and backlit component control switches on each control console panel. The following applications are standardized Human-System Interface (HSI) features that utilize common characteristics and conventions at Nuplex 80+ control panels:

DPS Display Hierarchy
DIAS Alarm Tile Displays
DIAS Dedicated Parameter Displays
DIAS Multiple Parameter Displays
CCS Process Controller Displays
CCS Switch Configurations

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-System Interface (HSI) - The operator's point of use of a controlled system in terms of indication and control; with particular emphasis on its organization, and the resulting human performance-related constraints.

Information and Control Requirements (ICR) - A summarization of the procedure-based parametric requirements for display and control variables identified by the FTA. Summaries are sorted from the FTA database for each variable. For example, characteristics for "pressurizer pressure" are summarized for each distinct gross function where pressurizer pressure is used. Characteristics include the following areas: device type, range, accuracy, and units.

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

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

Suitability - Verification of task performance capability such that the HSI 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 (Reference 2).

System I&C Inventory - This inventory includes instrumentation characteristics (requirements) (e.g. device type, range, accuracy, units, precision, etc.) for all displays, controls, and annunciators needed (from the system design engineers perspective). This inventory is generated by the system cognizant engineering organization.

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

Verification - Availability and Suitability analyses and inspection; part of the design process (along with Validation) by which HSI design sufficiency is confirmed (per Section 3.7 of Reference 2).

Validation - Evaluation of a dynamic operating ensemble demonstrating the capability of trained users 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). Verification and validation are the design evaluation processes by which the HSI design sufficiency is confirmed (per Section 3.8 of Reference 2).

5.0 MANAGEMENT OF V&V

The Responsible Management Structure of HFE V&V is integrated into the Human System Interface (HSI) design process as described in Reference 1. The responsible management structure will be responsible for the following:

1. the development of the HFE V&V Plan;
2. the implementation of the HFE V&V Plan;
3. the final disposition and resolution of all findings identified during the V&V activities.

5.1 V&V PLAN REVISIONS

Revisions to the HFE V&V Plan are administratively controlled.

5.2 EVALUATION OF V&V RESULTS

Findings and associated resolutions identified during the V&V tasks, as exemplified in Reference 4 will be itemized and documented in its associated V&V report. The V&V report will be sent to the Nuplex 80+ design team for review and comment. The Responsible Management Structure of HFE V&V will ensure that all comments are resolved.

5.3 V&V REPORT STRUCTURE AND CONTENT

V&V analysis reports will be structured in accordance with ABB-CE internal documentation format requirements. The HFE V&V analysis and inspection reports shall include sections or appendices containing the following information: purpose, scope, references, resources used during the analysis and inspection, analysis and inspection methodology, analysis and inspection criteria and metrics, completed analysis and inspection checklists or data sheets, recommendations, resolutions, and a list of discrepancies entered into the Tracking-of-Open-Issues (TOI) database.

5.4 DESIGN TEAM REVIEW

The ABB-CE document review and comment process and document distribution process ensure that the results of the HFE V&V activities are received, reviewed and commented on by the Nuplex 80+ design team. An internal procedure described in Reference 1 requires all human factors and man-machine interface documents for Nuplex 80+, including V&V documents, to be distributed in accordance ABB-CE internal distribution requirements.

6.0 V&V TASK METHODOLOGY AND CRITERIA

6.1 AVAILABILITY VERIFICATION

6.1.1 Purpose

Availability verification (see Figure 7.1) takes part in two phases, Phase 1 (availability analysis) and Phase 2 (availability inspection).

Phase 1 (Availability Analysis) assures the following:

1. That System I&C Inventory (as defined in section 4.0) meet the following requirements:

   a. Information & Control Requirements (ICR) (as defined in Section 4.0) specified in the Functional Task Analysis,

   b. Federally mandated indication and control requirements and,

   c. Fixed position MCR HSI for credited safety function success path tasks identified in the EPGs, and the PRA Critical Tasks.

   d. Each entry has a specified basis.

2. Unresolved TOI database issues are reviewed to identify any issues that should be considered during availability analysis.

After assuring the above requirements are met in the System I&C Inventory, a checklist of System I&C Requirements applicable to the MCR, RSR, and local control stations specified in the EPGs is developed. This will be used during the Phase 2 Inspection of the as-designed HSI.

Phase 2 (Availability Inspection) compares the as-designed HSI to the availability checklist produced by the Phase 1 analysis. This includes:

1. Verifying and documenting that all System I&C Inventory identified on the Availability checklist are available in the HSI design;

2. Identifying candidate HSI indications or controls for removal.

6.1.2 Scope

Phase 1 (Availability Analysis)

The System I&C Inventory for the panels in the Main Control Room (MCR), Remote Shutdown Room (RSR), and those local control stations specified in the EPGs are compared to the following:

1. Federally mandated indication and control requirements,

2. ICR (from FTA) and,

3. minimum set of fixed position MCR annunciators, controls, and displays needed to complete the credited safety function success path tasks identified in the in the EPGs and PRA critical tasks.

Phase 2 (Availability Verification) will be performed on the HSI for all of the control stations in the MCR, RSR and those local control stations specified in the EPGs, using the availability checklist developed in Phase 1.

6.1.3 Resources

The following resources will be available:

- individual panel design reports containing the MCR and RSR database inventory elements. The MCR inventory elements used for the verification shall include device type, range, accuracy, and units in a database;

- ICR from the FTA;

- minimum set of fixed position MCR annunciators, controls, and displays needed to complete the credited safety function success path tasks identified in the in the EPGs and PRA critical tasks.

- System I&C Inventory will come from a controlled System 80+ project document or database;

- HFE TOI database;

- a qualified HFE specialist available to direct and review the analysis.

6.1.4 Methodology

The following methodology is used for Availability Verification. Portions of this methodology have been exemplified in preliminary form in Reference 4.

6.1.4.1 Phase 1 Methodology (Availability Analysis)

The following activities are performed (see Figure 7.1):

1. Unresolved issues in the TOI database are reviewed to identify issues that should be considered during availability verification;

2. A list of all Federally mandated indication and control requirements in 10CRF50.34 will be compiled based on criteria in Section 6.1.5. Each indication and control from the compiled list will be confirmed to be in the System I&C Inventory;

3. A list of minimum fixed position MCR annunciators, controls, and displays needed to complete the credited safety function success path tasks identified in the EPGs and PRA critical tasks will be compiled. Each indication and control from the compiled list will be confirmed to be in the System I&C Inventory;

4. The FTA produces a list of ICR. This ICR will be confirmed to be in the System I&C Inventory;

Findings and resolutions (i.e. missing or unjustified entries in the System I&C Inventory) are reported and resolved in accordance with HFE V&V administrative procedures (See Section 8.1).

An availability inspection checklist is developed to be used in phase 2. This checklist includes all required I&C Inventory for the MCR, RSR, or local control stations specified in the EPGs. Included in this checklist are following two types of requirements:

1. HFE identified requirements (as verified in Phase 1) from the ICR, Federally mandated requirements, etc. (e.g., display, control or annunciator required, fixed position for a required display, method of display [e.g. analog, time history]),

2. System cognizant engineering organization requirements (e.g., displays, controls, or

annunciators required, along with their instrumentation characteristics). These requirements will also include I&C Inventory that were not identified as part of the HFE analyses (e.g., displays, controls and annunciators required for tasks not analyzed during the Functional Task Analysis) but needed for plant operation.

The requirements-to-inventory mapping, findings, explanations (if necessary), resolution, and availability inspection checklist will be documented in accordance with the HFE V&V Administrative Procedures (See Section 8.1).

6.1.4.2 Phase 2 Methodology (Availability Inspection)

The availability inspection checklist will be used to evaluate HSI in the MCR, RSR, and those local control stations specified in the EPGs for completeness. Discrepancies between the design HSI and the availability inspection checklist will be formally evaluated and resolved. This analysis will identify findings such as missing required panel HSI, and unnecessary panel HSI. The findings and a resolution will be documented in accordance with the HFE V&V Administrative Procedures (See Section 8.1).

6.1.5 Criteria

6.1.5.1 Phase 1 Availability Analysis Criteria

1. All of the required Federally mandated indication and control features listed below are included in the System I&C Inventory:

   a) Integrated display of safety parameter indications; 10 CFR 50.34(f)(2)(iv) (Reference 7) and in accordance with NUREG 1342 (Reference 11).

   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).

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) and in accordance with Reg Guide 1.97 (Reference 12; as specified in CESSAR-DC Section 7.5).

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

2. All of the fixed position MCR annunciators, controls, and displays needed to complete the credited safety function success path tasks identified in the EPGs and PRA critical tasks are included and identified in the System I&C Inventory.

3. All of the ICR identified in the FTA are included in the System I&C Inventory.

4. Each System I&C Inventory entry has a specified basis.

6.1.5.2 Phase 2 Availability Inspection Criteria

1. All System I&C Inventory items identified on the availability checklist (with appropriate characteristics) are found on HSI designs;

2. The following checklist specifications are satisfied for each as-built item: 1) Device type, 2) Range, 3) Units, 4) Accuracy, and 5) Precision.

6.2 SUITABILITY VERIFICATION

6.2.1 Purpose

Suitability verification addresses the issue of whether the form and arrangement of HSI indications and controls and environment supports operator task accomplishment. It roughly spans the gap between the questions of "is the needed information, and only the needed information, present?" (Availability) and "does the design, in terms of actual operators, using the full control room, the actual procedures, the real plant dynamics, etc. actually work together as a whole?" (Validation). Suitability therefore overlaps somewhat with both these areas of evaluative effort.

6.2.2 Scope

Suitability verification will be performed on indication and control features and environmental conditions in the MCR and RSR, and on the HSI features of local control stations specified in the EPGs. All HSI elements will be included in and reviewed as part of the verification of a group of elements (e.g., a particular control panel, a particular local control station, etc.).

6.2.3 Resources

The following resources will be available:

- sources for the individual panel I&C features from the individual panel reports as exemplified by the panel mockups or prototypes;
- prototypes of added HSI features;
- HFE Standards, Guidelines, and Bases for System 80+;
- suitability inspection criteria provided in the form of checklists (to be developed as part of the suitability verification process), as exemplified in Reference 4;
- HFE TOI database;
- a qualified HFE specialist and an operations expert to perform the analysis.

6.2.4 Methodology

Prior to the analysis, unresolved issues in the TOI database will be reviewed to identify issues that should be addressed. Then, as exemplified in Reference 4, a two part methodology will be applied. A "top-down" approach evaluates the appropriateness of the design selections in the context of the big picture. This is a knowledge-based review that considers the overall system design, the nature of real-world operator tasks, and the integration of the parts of the man-machine interface into a coherent and easily used whole. A "bottom-up" approach applies the guidelines found in Reference 6 as elemental HSI criteria. These are particularly useful for identifying individual item discrepancies, such as inadequate letter sizes or lighting levels, where genuine specifications exist. Substantial but incomplete overlap between the two approaches is expected, as they both are directed towards the same system and overall goals, but are more complete together than is either one alone.

6.2.4.1 Phase 1 (Suitability Analysis) Methodology

Suitability analysis will be performed to cover all indication and control features and environmental conditions in the MCR, the RSR, and local control stations specified in the EPGs. Groups of HSI features (e.g., a particular panel, local control station, etc.) will be subjected to Suitability analysis as they are readied by the design process. All HSI elements (e.g., annunciators, displays, controls, etc.) will be included in and reviewed as part of the verification of one or another such groups. New or non-standard features will require the most scrutiny, while standard features will be more familiar.

Using the top-down approach, the analyst will evaluate the various aspects of the prototype HSI for usability in terms of expected tasks. The analyst will seek to identify and document problems by considering the user's elemental tasks.

All documented problems and nonconformances will be documented in accordance with the HFE V&V Administrative Procedures (See Section 8.1)

6.2.4.2 Phase 2 (Suitability Inspection)

Using the bottom-up approach, the analyst will evaluate the various aspects of the prototype HSI for conformance

to applicable portions of Reference 6. Nonconformances to Reference 6 Standards must be documented.

An inspection checklist is generated based on input from the HFE Standards, Guidelines, and Bases for System 80+ (Reference 6), the results of the suitability analysis and the criteria identified in Section 6.2.5. The criteria will address suitability for all areas of the Nuplex 80+ HSI design, including, but not limited to the following:

- workspace environment,
- communications,
- annunciators,
- controls,
- visual displays,
- labels and location aids,
- process computers,
- panel layout, and
- control-display integration.

The checklist includes a place for comments.

The Suitability inspection, also using a bottom-up approach, evaluates panel HSI designs and the associated environment using the inspection checklist. The evaluation is performed on all as-built panels and HSI features, and actual workspace environments.

The process will be repeated until the HSI panel designs are suitable. The results of suitability inspection will be documented in accordance with the HFE V&V Administrative Procedures (See Section 8.1)

6.2.5 Criteria

The true analytic criteria are those of the bottom-up approach, and are detailed in Reference 6. Top-down suitability criteria depend on the knowledge-base and perceptions of the expert analyst, and are thus particular to the specification of a problem. While this is, at best, an undesirably fuzzy situation, it adds desirable flexibility to the analysis.

6.3 VALIDATION

6.3.1 Purpose

The purpose of validation is to ensure that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EPGs provide usable work ensembles that support the successful

accomplishment of the operator's required tasks (i.e., to validate performance of the integrated Man-Machine system for System 80+). Validation includes exercise of specified scenarios and plant operating sequences (per the Scope in 6.3.2). Validation tests the following objectives:

1. Ability to execute operator tasks required by procedure guidance, given the MCR configuration and staffing assumptions;

2. Confirmation of Task Analysis results;

3. Time response for credited operator actions based on the safety analysis;

4. Allocation of functions and operator situational awareness;

5. Operator communication and team interaction;

6. Operation with HSI and I&C equipment failures;

7. Alarm system effectiveness.

6.3.2 Scope

Validation activities will be performed for representative operating sequences (specified in Section 6.3.4.2) in the MCR, the RSR, and at local control stations where actions are specified in the EPGs.

6.3.3 Resources

The following resources are required for validation:

6.3.3.1 Facilities

The following test facilities are needed to perform the Validation activities for the Scope identified in 6.3.2:

1. An MCR validation facility that a) physically represents the MCR configuration, b) dynamically represents the operating characteristics and responses of the System 80+ plant, and c) meets applicable portions of the performance requirements in Sections 4.1 and 4.2 of ANSI 3.5.

2. An RSR validation facility that a) physically represents the RSR configuration, b) dynamically represents the shutdown operating characteristics and responses of the System 80+ plant, and c) meets

applicable portions of the performance requirements in Sections 4.1 and 4.2 of ANSI 3.5.

3. In-scope local control stations mockups (or as-built facilities) that physically represent the configuration and b) dynamically represent the operating characteristics and responses of the relevant System 80+ plant equipment.

These facilities shall conform to the following requirements:

1. Replicate the physical HSI characteristics of the corresponding as-built hardware (re: 3.2.1 and 3.2.2 of ANSI 3.5);

2. Replicate the informational (i.e., format and content) characteristics of the corresponding as-built HSI (re: 3.2.2 of ANSI 3.5);

3. Replicate corresponding as-built workspace environments with as much fidelity as practical (re: 3.2.3 of ANSI 3.5).

4. Meet additional requirements of Appendix B of this document.

6.3.3.2 Operating Sequences

The following System 80+ operating sequence information is needed to perform the Validation activities for the Scope of activities identified in 6.3.2, and must be prepared according to the requirements of Appendix B:

1. Technically complete procedure guidance;

2. Technically accurate test bed scenarios for normal, abnormal, and emergency events and operations based on safety and transient analyses.

6.3.3.3 Team Personnel

The validation team personnel shall include HFE Specialist(s) and Operations Experts. The validation team should include some members of the design team, but shall have independence from the design team. The validation team should be familiar with the validation facility, the actions required by the scenarios, and the evaluation methods and criteria prior to running the exercises. Specifications for team personnel must be prepared according to the requirements of Appendix B.

6.3.4 Methodology

6.3.4.1 General Description

Real-time exercises, supplemented by walk-throughs and talk-throughs, will be performed for each of the plant operating sequences listed in section 6.3.4.2. Design basis minimum staffing levels as specified in CESSAR-DC (Section 18.3.2) shall be used. Unresolved issues in the TOI database will be reviewed to identify issues that should be evaluated during validation.

Validation team personnel, including both observers and performers, will hold a pre-scenario briefing on the purpose and objectives of the exercises. The team will then participate in the planned real-time scenario. Afterwards, observers and performers will hold a post-exercise evaluation, to complete the subjective data and review the objective results. Walk-throughs or other analyses may be used to supplement these data.

The overall performance of the system shall be evaluated against both general and event-specific criteria. Failures to meet these criteria, and human errors identified in task performance, shall be documented as findings. Errors associated with Critical Tasks shall be identified as such and receive appropriate attention. Resolutions leading to design or other changes shall require the validation exercise to be repeated, unless this can be justified as unnecessary to complete validation.

Completed checklists, reviewers notes, findings, identified discrepancy forms, will be compiled and summarized will be documented in accordance with the HFE V&V Administrative Procedures (See Sectior 8.1).

6.3.4.2 Operating Sequences

The following sequences form a representative set of plant operations that will be incorporated in the scenarios used to perform HSI design validation.

A. Normal Operation (using Normal Operating Sequences)

1. Plant Heatup from Tech Spec Mode 5 (Cold Shutdown) to Hot Zero Power Conditions (Mode 3 Hot Standby)

2. Reactor/Plant Startup and Maneuvering (0% to 100% power), including Turbine Startup, Parallel, and Load Change

3. Uncomplicated Reactor Trip and Trip Recovery Using Reactor Trip Guideline

4. Plant and Reactor Shutdown (100% power to 0% power)

5. Plant Cooldown to Tech Spec Mode 5 (Cold Shutdown) using Shutdown Cooling, including mid-loop RCS level operations

B. Abnormal Operation (using Abnormal Operating Sequences)

1. Rod Drop from 100% power (Reactivity anomaly and power transient)

2. Inadvertent Emergency Feedwater Actuation Signal (EFAS) from at-power conditions

3. Plant Shutdown and Cooldown from the Remote Shutdown Panel (including transfer of control from the MCR, and startup of the Shutdown Cooling System)

4. Loss of a single 120VAC Class 1E Instrument Bus during an accident (e.g. LOCA)

5. Loss of a single 125VDC Class 1E Instrument Bus from at power conditions

6. Loss of Instrument Air from 100% power

7. Loss of RCP seal cooling and injection (including RCP seal failure)

8. Stuck open PZR relief valve

9. Loss of Shutdown cooling

10. Loss of Service Water/Component cooling Water

11. Turbine and Main Generator Trips

12. Seismic Event

C. Emergency Operation (using EPGs)

1. Loss of Coolant Accident (LOCA), including loss of a 480VAC Vital Bus using Optimal Recovery Guideline

2. Steam Generator Tube Rupture (SGTR) including a Cooldown in Natural Circulation using Optimal Recovery Guideline

3. Excess Steam Demand Event (ESDE) using Functional Recovery Guideline

4. Loss of All Feedwater (LOAF) using Optimal Recovery Guideline

5. Station Blackout (including recovery by starting a 480V Emergency Diesel Generator) using Optimal Recovery Guideline

6. Loss of Off-Site Power from 100% Power

7. Anticipated Transient Without Scram (ATWS) requiring Emergency Boration using Functional Recovery Guideline

D. HSI and I&C Equipment Failure Sequences

1. Complete Loss of the DPS
   a. during an accident (e.g. LOAF)
   b. during power operation {including a plant and reactor shutdown to Tech Spec Mode 3 (Hot Shutdown)}

2. Loss of power to a DIAS Segment
   a. DIAS-P during an accident (e.g. LOCA)
   b. DIAS-N at power

3. Loss of an ESF-CCS Segment
   a. loss of power from at power conditions (e.g. greater than 20% power)
   b. Multiplexer failure during an accident (e.g. LOCA)

4. Common Mode I&C Failure (Loss of PPS, DIAS-N, & ESF-CCS during LOCA)

5. Standard MCR maintenance activities (e.g., device replacements, removal from service of plant equipment, etc.)

E. Startup, Operation, & Shutdown of Systems Important to Safety

Exercise of the following systems and functions, including their applicable routine surveillances, will be incorporated in the HSI design validation scenarios.

1. Reactor Coolant System
2. CEDMECS
3. Shutdown Cooling System
4. Safety Injection & Rapid Depressurization Systems

5. Service Water/Component Cooling Water Systems
6. Containment Isolation
7. Containment Spray & Fan Cooler Systems
8. Annulus Ventilation System
9. Hydrogen Monitoring & Control
10. Fuel Pool Purification and Cooling
11. Main Steam System
12. Feedwater Systems
13. Pressurizer Pressure Control
14. CVCS
15. Reactor Coolant Gas Vent System
16. HVAC Systems
17. Instrument Air System
18. Electrical Systems & Emergency Power Sources
19. Nuclear Instrumentation
20. Reactor Protection System
21. Release Path Monitoring, Control, & Isolation

F. Offnormal or Alarm Conditions

Exercise of a selected sample of alarm conditions will be incorporated in the HSI design validation.

6.3.4.3 Performance Measures

Performance measures should provide data that are useful for identifying design problems, and sufficient to test the design against performance requirements, in areas such as:

- system safety
- crew primary tasks
- crew errors
- situation awareness
- workload
- communications and coordination
- physical movement and interaction

Two basic approaches to data generation will be used:

1. Auto event data logging - Real-time objective data used to assess overall system performance, crew primary task performance, workload levels, movement, and errors; and

2. Subjective evaluation - Observer and performer rating and comment data, to assess crew movement, positioning, coordination, communication, workload, situational awareness, and errors.

Scenario-specific objective criteria and subjective evaluation tools will be provided for each scenario.

Reference 5 provides relevant guidance on performance evaluation in simulation environments. Specifications for performance measurement must be prepared according to the requirements of Appendix B.

6.3.4.4 Operating Ensemble Validation Activities

An operating ensemble validation will be conducted by the COL Applicant to provide assurance that trained operators using the "final" plant-specific procedures in the as-built main control room (and remote shutdown room) together form an effective operating ensemble. Completion of the operating ensemble validation will satisfy all requirements on the main control room and remote shutdown room validation.

Requirements for the operating ensemble validation plan are provided in Section 19.3.1.2 of CESSAR-DC. Complete event scenarios, data, and results will be provided for COL Applicant use via OSIP.

6.3.5 Criteria

The criteria for validation of the performance of the integrated Man-Machine system for System 80+ are organized into seven categories corresponding to the seven specific validation objectives identified in Section 6.3.1. These will be provided in the form of a checklist with places to enter notes and findings. The criteria for each of these categories is as follows:

1. Validate ability to execute operator tasks required by procedure guidance:

   a. There are sufficient information and controls for the operators to perform all procedural steps, including post-trip actions, diagnostic steps, safety function status checks, and contingency actions, as specified.

   b. Proper execution of operating sequences maintains critical plant parameters within technical specification limits for normal operations.

   c. Proper execution of operating sequences maintains critical plant parameters within safety limits for off-normal operations.

   d. Operators are able to locate/retrieve particular information or control devices when required.

e. Information needed to perform a control action is available within reading distance of the control device.

f. Information and control formats (e.g., terms, units, magnitudes, etc.) correspond to procedure guideline technical contents.

g. Continuously available Reg Guide 1.97 Category 1 data is distinct from other types of data.

2. Validate the MCR configuration staffing assumptions and confirm the Task Analysis results:

a. Minimum design basis staffing for the applicable plant conditions supports timely and successful performance of required tasks.

b. A single operator can perform a plant startup and escalation from 5% power to 100% power without continuous support from another operator.

c. A single operator can perform normal operating sequences while greater than 5% power and maintain critical plant parameters within technical specification limits.

3. Validate time response for credited operator actions:

a. Operator actions credited in the Safety Analysis can be completed within the time requirements of the Safety Analysis.

b. Operators can manage emergency event scenarios and perform Critical Tasks (i.e., identified by PRA/HRA) within the time criteria specified in the Task Analysis.

c. Operators can successfully complete immediate post-trip actions for uncomplicated trips within 10 minutes (based on the number of safety function verification steps at one minute per step).

d. When there is a control system segment failure during an accident, operators are able to use alternate control devices and complete steps in the time credited in the Safety Analysis.

e. Actions outside the MCR are not required for safety prior to 30 minutes from the initial indication of the event.

4. Validate the allocations of functions and operator situational awareness:

   a. There is sufficient information to evaluate procedural conditions and actions (e.g. select applicable EPGs during an accident, Shutdown Cooling System entry conditions, conditions requiring a plant cooldown, entry conditions for Steam Generator isolation during a Steam Generator Tube Rupture, etc.).

   b. Available data is sufficient for necessary diagnosis and decision making (e.g. identifying which steam generator has a tube rupture during a steam generator tube rupture event).

   c. Operators can identify when the exit conditions for an EPG are met.

   d. Operators can take control of the following important automatic systems and control in manual (Pressurizer Pressure Control, Pressurizer Level Control, Steam Generator Level Control, Control Rod Sequence Control, Steam Bypass Control, and Emergency Diesel Generator Speed Control).

   e. Operators can perform normal plant maneuvering without propagating undesirable transients or plant conditions.

   f. Operators can identify and confirm challenges to safety functions before violations occur.

   g. Operators can identify automatic actuation of safety systems.

   h. Operators can identify critical function violations using the Integrated Plant Status Overview (IPSO).

   i. Operators can correctly determine available success paths during specified accident scenarios.

   j. Operators can identify when a safety system is bypassed or becomes inoperable.

5. Validate operator communication and team interaction:

   a. Operators are able to communicate with each other effectively (e.g. there is no excessive noise, and tasks requiring coordination were completed without excessive repetition of commands and confirmation).

b. Adequate workspace is provided so that physical interference among operators and their activities is minimized.

c. Operators are able to communicate with personnel outside the controlling work space easily (e.g. communication devices provided within easy reach at panels where continuous monitoring and control is required).

d. Control room supervisory personnel are able to interface with management, technicians, and others without excessive interference with operators in the controlling workspace.

6. Validate operation with HSI and I&C equipment failures:

a. Operators are able to promptly recognize when information or control system failures occur.

b. Operators do not use data marked questionable or invalid to make critical decisions, and are able to locate alternate sources of information when the primary source is unavailable or in doubt.

c. When there is a control system segment failure operators are able to locate and use alternate control devices (e.g. process controllers) to perform required tasks.

d. Following a complete loss of the DPS, operators are able to complete a plant shutdown without causing a reactor trip (from 100% power in Mode 1 to 0% power in Mode 3.

e. Operators are able complete all procedure steps and reach EPGs exit conditions following complete loss of the DPS.

7. Validate ability of the operator to use the alarm system effectively:

a. Operators can distinguish different states of alarm (new, existing, cleared, reset) from each other.

b. Operators can distinguish different priorities of alarm (i.e., 1, 2, and 3) from each other.

c. Operators can identify high priority alarms during an accident, and distinguish the highest priority among multiple unacknowledged alarms.

d. During normal operations (at power) there are no existing priority 1 or priority 2 alarm conditions (dark board).

e. Following an alarm system mode change (e.g. Normal Operation to Post Trip) alarms are not actuated by conditions that are normal for the new mode.

f. Operators are always audibly and visually alerted to activation of new Priority 1 alarms.

g. The alarm tones can be heard above background noise.

h. Operators can identify the location (i.e., on the MCC, AC, or SC) of a new alarm by direction of sound.

i. Operators can use either the DPS or DIAS systems to respond adequately to alarms.

j. Alarm deferral and resume buttons are located for effective use.

k. Use of deferred alarm acknowledgement does not lead to lost information and unacceptable consequences.

l. Alarms are not inadvertently acknowledged.

m. Alarm setpoints are appropriate (i.e., there is sufficient time for the operator to take appropriate action before a control action takes place, but not so close to normal operating range as to produce nuisance alarms.

n. Operators can establish an additional alarm setpoint on a condition in alarm.

7.0 SCHEDULE & MILESTONES

The V&V Program Plan outlines how ABB-CE satisfies V&V program and product requirements. However, it is not yet possible to plan a detailed, month-by-month schedule for these activities, due to commercial aspects of the design (future schedule depends heavily on external funding.) A qualitative schedule based on design activities is provided, specifying the general sequence in which these activities will be performed. Exact calendar dates for the work indicated shall remain to be determined. A detailed schedule with milestones will be developed in accordance with the requirements in Appendix B.

7.1 AVAILABILITY VERIFICATION SCHEDULE & MILESTONES

Availability verification is performed in two phases, Phase 1 and Phase 2, with Phase 1 required to be completed prior to beginning Phase 2. Availability verification produces the following four outputs:

1. Availability checklists;

2. Phase 1 findings and resolutions are sent to cognizant engineering organization for final resolution and entry into the System I&C Inventory (if required).

3. Phase 2 findings and resolutions requiring design changes are entered into the TOI database (if any are found);

4. Availability Verification Report.

The availability verification process, including inputs and outputs is illustrated on Figure 7.1.

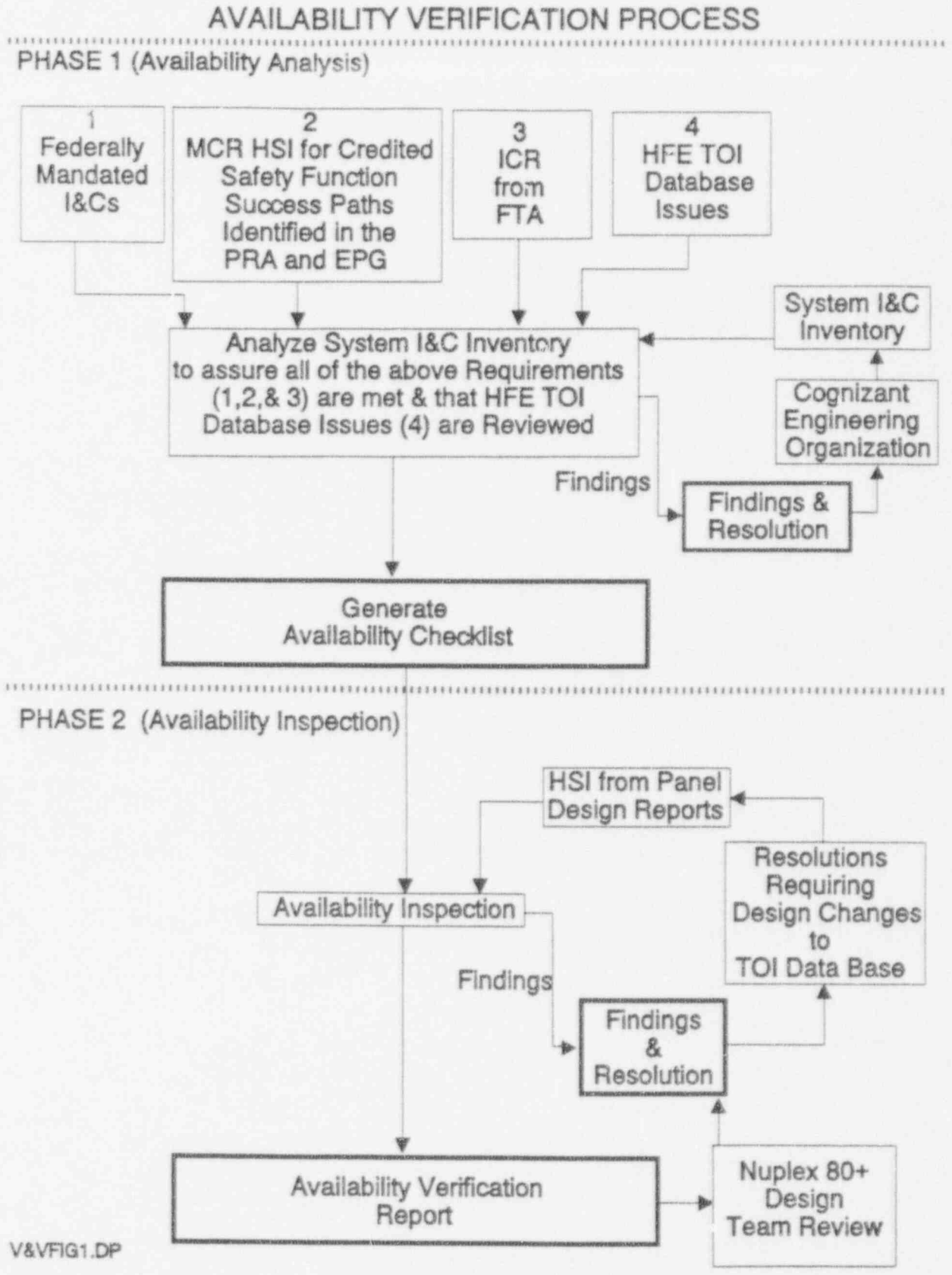

Figure 7.1 AVAILABILITY VERIFICATION PROCESS

7.2 SUITABILITY VERIFICATION SCHEDULE & MILESTONES

Conceptually, suitability follows availability. Practically, Suitability verification activities can be staggered with Availability verification activities, as long as the design implementation of each item in the Systems I&C database is verified to be suitable. Suitability verification produces the following outputs:

1. Phase 1 findings and resolutions requiring design changes for entry into the TOI database (if any are found);

2. Suitability inspection checklists;

3. Phase 2 findings and resolutions requiring design changes for entry into the TOI database (if any are found);

4. Suitability Verification Report.

The Suitability verification process, including inputs and outputs is illustrated on Figure 7.2.

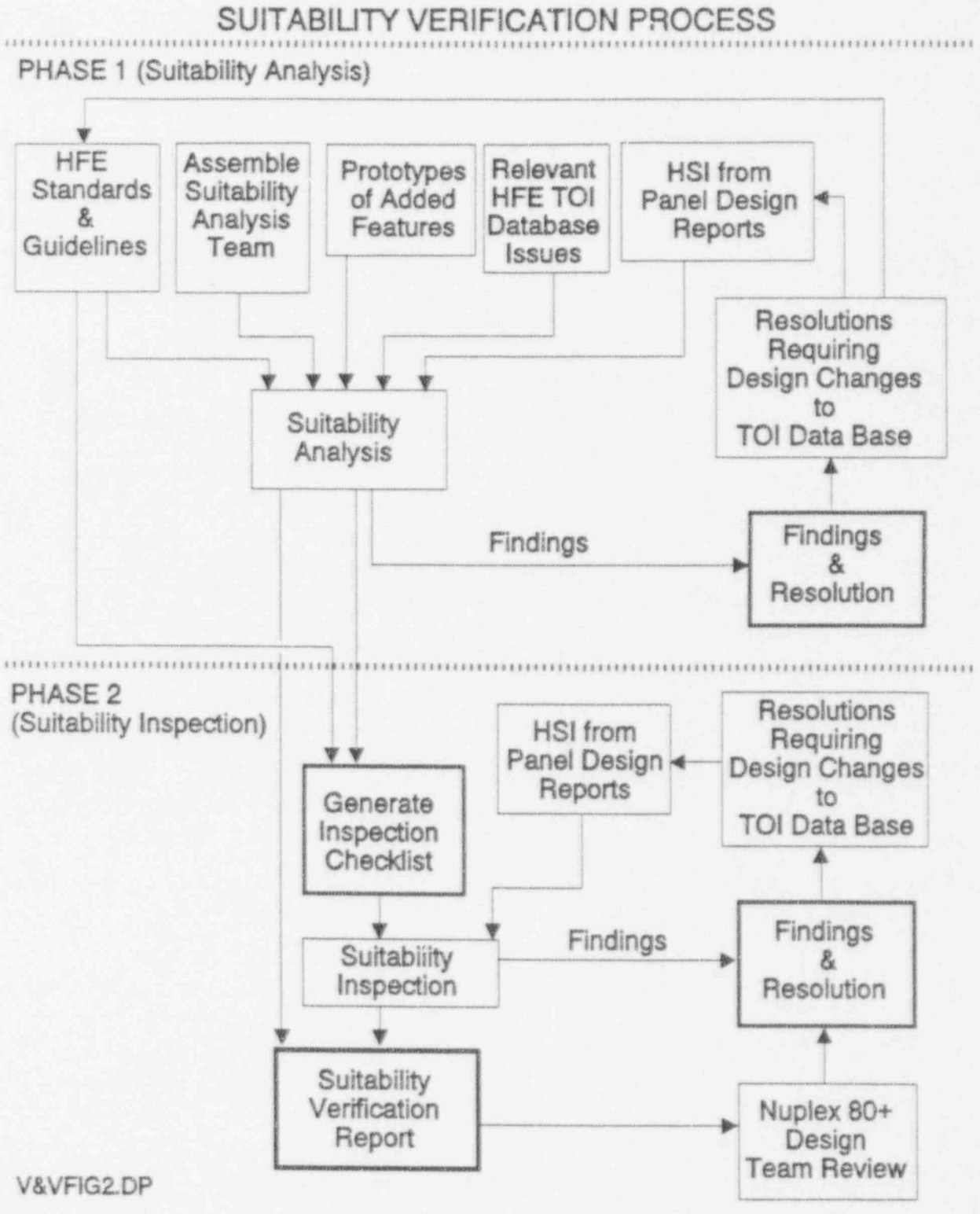

Figure 7.2 SUITABILITY VERIFICATION PROCESS

7.3 VALIDATION SCHEDULE & MILESTONES

Final design validation exercises will follow the completion of all applicable portions of the Availability and Suitability verification. Details and schedule for how the validation exercises are to be performed and how the results are to be processed will be provided in a Validation Implementation Plan. The Implementation Plan must include the treatment of issues in Appendix B of this document.

The validation scenarios and evaluation tools require the following inputs prior to completion:

1. A complete set of procedure guidance for the operating sequences in Section 6.3.4.3;

To perform the validation exercises the following must be available:

1. Validation facilities per Section 6.3.3.1;

2. A validation team including crewmembers, Operations Experts trained on Nuplex 80+/System 80+, HFE Expert(s), and systems engineers;

3. Validation scenarios and objective plant function limits and criteria for the operating sequences listed in Section 6.3.4.2;

4. Scenario-specific evaluation tools.

The results of validation exercises will be presented in Validation Reports. Closeout of validation (i.e., the final design validation report) shall include an appendix with the resolution for each formal validation finding produced during the process.

The validation process is illustrated on Figure 7.3.

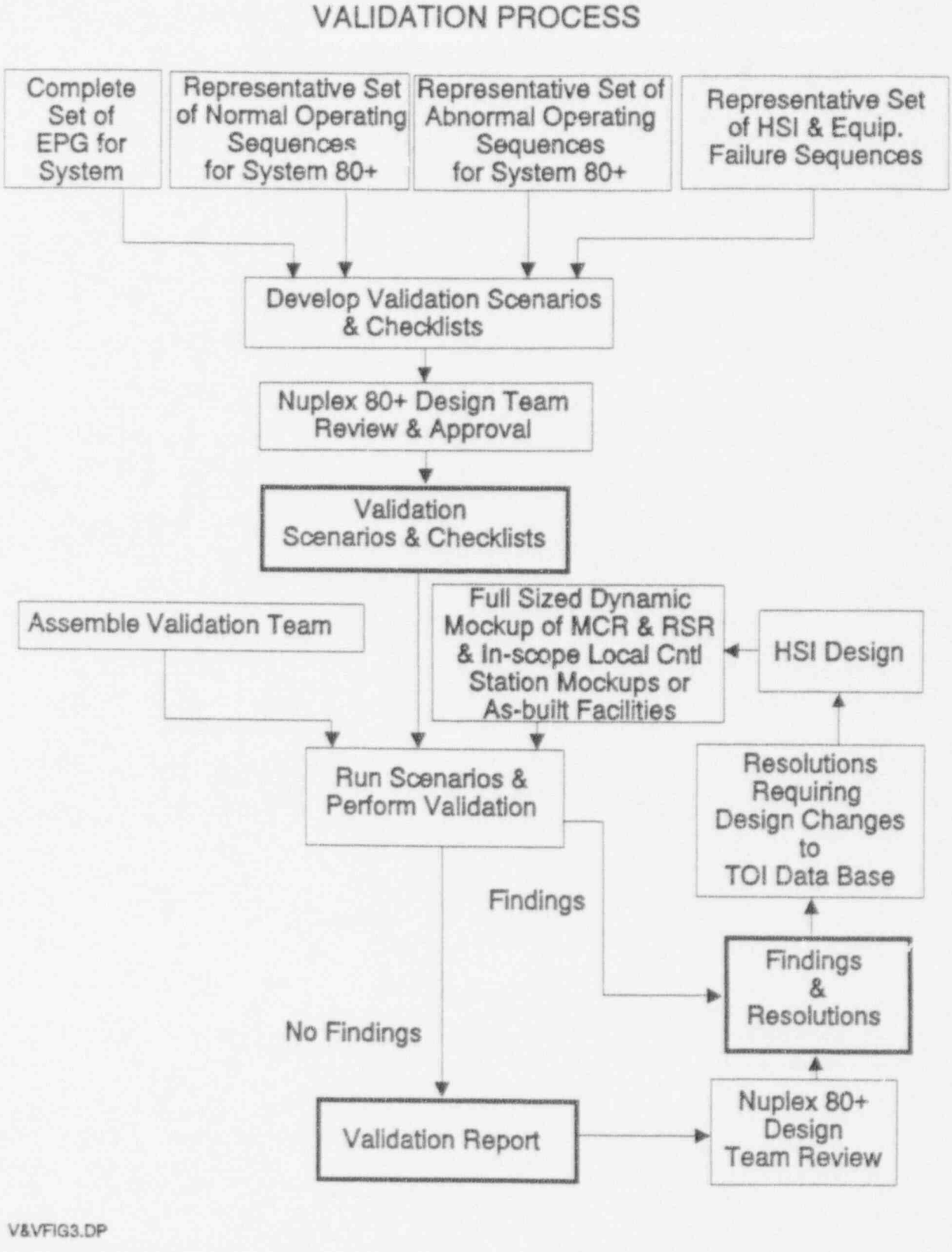

Figure 7.3 VALIDATION PROCESS

8.0 HFE V&V ADMINISTRATIVE PROCEDURES

8.1 FINDINGS REPORTING & RESOLUTION

A report will be generated for Availability Verification, Suitability Verification, and Validation to document the analyses. The HFE V&V reports will be sent to the Nuplex 80+ design team for review and comment.

The finding resolution process will consider the risk significance of tasks impacted by findings, and will qualitatively confirm that the findings as dispositioned will not lead to a risk-significant increase in error potential from that represented in the HRA, or additional risk-significant errors not modeled in the HRA.

The Responsible Management Structure of HFE V&V will ensure that all comments related to the findings and resolutions are reviewed by the design team, and any open issues tracked and resolved, per the requirements of Reference 1. The Responsible Management Structure of HFE V&V will also ensure that any finding and resolution requiring a design change is entered into the TOI database.

Availability Verification

Phase 1 availability analysis findings and resolutions (i.e. missing or unjustified entries in the System I&C Inventory) are sent to the cognizant engineering organization for formal resolution and entry into the into the design (if required by resolution). These cognizant engineering organization design changes will be documented in the System I&C Inventory.

The Phase 2 itemized findings and resolutions, as exemplified in Reference 4 will sent to the TOI database for tracking until incorporated into the design.

For any information or control item identified as unnecessary in Phase 1 (availability analysis) or Phase 2 (availability inspection), an operational review will be performed to confirm that its removal will have no operational significance.

The results of the availability verification activities {e.g. requirements-to-inventory mapping, findings, explanations (if necessary), resolution, and availability inspection checklist} will become part of the availability verification report(s). The availability verification report will be delivered to the COL applicant as part of the Operational Support Information Program (OSIP).

Suitability Verification

Phase 1 suitability verification problems and nonconformances will be incorporated as analytical findings to be evaluated and documented.

Phase 2 suitability findings identified in the inspection will be documented. The process will be repeated until the HSI panel designs are suitable.

The problems, nonconformances, completed checklists, findings, explanation, and resolution, will become part of the associated suitability verification report. The checklists will be delivered to the COL applicant as part of the OSIP.

Validation

Resolutions leading to design or other changes shall require the validation exercise to be repeated, unless this can be justified as unnecessary to complete validation.

Completed checklists, reviewers notes, findings, identified discrepancy forms, will be compiled and summarized in a formal Validation report. The report will be provided to the COL applicant as part of the OSIP.

8.2 TASK ITERATION

All V&V tasks that identify a finding will be considered for iteration as part of the Nuplex 80+ design review and comment process. If iteration of a V&V task is determined to be necessary, the Responsible Management Structure of HFE V&V will determine the level or iteration, schedule, and ensure that the associated V&V task iteration is completed. After iteration of the analysis, the V&V task will follow the HFE V&V control procedures regarding document review and comment until final resolution.

8.3 CONTROL PROCEDURES

A formal procedure will be issued to control V&V activities.

APPENDIX A NUPLEX 80+ DESIGN TEAM EVALUATION

HSI design team evaluation is done by a multi-disciplined internal review without issuing a formal HSI design team evaluation report. The Human Factors Program Plan for the System 80+ (TM) Standard Plant Design (Reference 1) describes this review process.

Significant comments received and resolved during this review process include the following:

1. The overall objectives of validation should be clearly stated and include the following: integrated system performance of the integrated HSI, including IPSO, confirm task analysis and staffing assumptions, operator communication ability, credited operator actions time response, and evaluation of function allocation and situational awareness.

2. Phase 1 verification should ensure that EPG tasks and critical tasks identified in the Probable Risk Assessment (PRA) can be accomplished with the fixed position MCR HSI alone;

3. Validation exercises should include all EPGs;

4. Validation exercises should include a special category of scenarios that include HSI and I&C equipment failures;

5. The V&V Plan should clearly identify V&V activity outputs and inputs to other design activities;

6. Part of the resolution analysis should identify whether all or a portion of the V&V activity needs repetition;

7. Findings and resolutions should feed the TOI database or the System I&C Inventory;

8. Validation should include time response tasks identified in the Task Analysis;

9. Validation criteria for operator error should be included;

10. Control/display interaction criteria should be added;

11. Validation sequences should be identified in the V&V Plan.

12. The SONGS validation program for Emergency Operating Instructions is a good example of a validation methodology that may be modified to accommodated Nuplex 80+ validation;

13. Review and comment of V&V reports should be done by the Nuplex 80+ design team;

14. Availability verification should be performed in 2 phases; phase 1 should ensure the System I&C Inventory is complete and phase 2 should verify the HSI on the Panel Design Reports includes all required System I&C Inventory;

15. Definitions are needed for ICR and System I&C Inventory;

16. Suitability analysis must be performed on HSI devices in the MCR, RSR, and those local control stations specified in the EPGs;

17. Prototypes of added features are needed for previously unanalyzed features;

18. Confirm need for HFE V&V to verify Federally mandated indication and control requirements;

19. Confirm the need to verify the System I&C Inventory for completeness;

20. Consistent terminology should be used throughout the HFE V&V Plan;

21. Plan should specify that suitability verification can be done by panel.

22. Validation criteria for the alarm system need to be developed.

APPENDIX B V&V IMPLEMENTATION DETAILS

A. AVAILABILITY VERIFICATION

1. Prior to availability verification, a detailed schedule with milestones must be provided.

B. SUITABILITY VERIFICATION

1. Prior to suitability verification, a detailed schedule with milestones must be provided.

2. Relevant findings from the DIAS alarm suitability analysis (defined in TOI entry #101) will also be implemented on the DPS, and be evaluated during the DPS suitability verification.

C. VALIDATION

1. Prior to validation, a detailed schedule with milestones must be provided.

2. Prior to validation, the operating sequences and scenarios must be detailed and documented.

3. Validation scenarios must incorporate all Critical Tasks identified in the Task Analysis from the PRA.

4. Scenario-specific objective criteria and subjective evaluation tools must be provided for each scenario.

5. Particular attention must be paid to the effectiveness of the annunciator functions provided by DIAS and DPS systems, including under high alarm conditions.

6. The data analysis methods by which the validation results are processed and validation criteria applied must be specified.

7. The validation implementation plan must specify the number of operations expert "crews" needed.

8. Prior to validation, the simulation facilities and event data logging methodology must be verified.

9. Addition of significant instrument failures to the Validation scenarios must be considered during detailed scenario development.

ATTACHMENT 4

HFE V&V-related TOI Entries

Identification Number	101	Title	DIAS Alarm Prototype
Originator	RB Fuld	Source	NRC Review
Responsible Engineer		Resolution Commit Date	

Description

A stand-alone DIAS alarm tile display prototype will be developed that permits full exercise of the alarm system HSI features, and evaluation of interactions occuring among features during use. The prototype will be employed to resolve design questions including those issues listed below. The NRC should review the prototype before the evaluations are completed to ensure that its specific concerns identified in the alarm system area are being appropriately addressed.

A dedicated Suitability verification analysis and report will be provided on the alarm prototype. Independent evaluators will be included in the process of collecting pertinent suitability data. The following issues will be included in those that are evaluated and resolved:

a. Consider eliminating cleared alarm behavior for improving conditions (TOI #35).
b. Review/determine guidance for inclusion of setpoints in DIAS alarm messages (TOI #74).
c. Ensure acceptability of difference between New and Cleared flash rates (TOI #75).
d. Minimize "Marquee Effect" due to synchronized multiple flash rates (TOI #76).
e. Multiple alarm tile states on multiple tiles may be difficult to interpret and use (TOI #78).
f. Ensure that brightness levels of New, Existing, Cleared, and Reset alarm states are mutually discriminable for relative discriminations.
g. Ensure acceptability of overall alarm system access and use, including the number of alarm conditions/setpoints within a single alarm tile.
h. Consider the use of alarm-response-procedure messaging.

Resolution

Resolution Date	Commitment Date
Responsible Engineer	
Approved By	
Resolution Comments	

Implementation

Document Number	Revision
Section	Implementation Date
Approved By	
Implementation Comments	

ATTACHMENT 5

CESSAR-DC Markups for V&V and Procedures

13.5 PLANT PROCEDURES

Information concerning the site operator's plant procedures is within the site operator's scope and shall be provided in the site-specific SAR. E

PROPOSED COL ACTION ITEM

13.5.1 Plant Operating Procedures Development Plan

A. A Plant Operating Procedures (POP) development plan (i.e., the Plan) shall be ~~provided~~ created to formally guide development of the POPs for normal, abnormal, and emergency operations.

B. The Plan shall ~~state the means~~ specify the process by which the POPs will be developed, verified, validated, revised, and maintained.

C. The scope of the ~~POP development~~ plan shall include the applicable operating procedures in Appendix A of Reference 1, including consideration of plant operations when systems or equipment are undergoing test, maintenance, or inspection. ← covered by Insert 1 Section V

D. The Plan shall ensure that POPs follow standard formats implemented through Writer's Guides (e.g., per References 2 and 9).

E. The Plan shall ~~ensure~~ specify that the POPs' technical bases are documented, and that their content is consistent with plant design basis material including applicable procedure guidelines, task analyses, and PRA, (all provided via OSIP), and applicable plant-specific aspects, per Reference 2. to ensure

F. The Plan shall ~~state the means~~ specify the process by which training of operators on the POPs and on changes to the POPs is provided and kept current.

The plan shall specify the

G. ^POP validation activities ~~shall~~ That demonstrate the acceptability of the completed ~~operating ensemble (i.e., procedures, staff, and equipment interface)~~ for the scope specified in Item C above. Confirmatory validation scenarios and ~~design~~ validation results shall be provided via OSIP as specified in the System 80+ HFE V&V Plan and System 80+ HFPP.

H. The POPs ~~shall~~ comply with the applicable requirements of References 2, 3, 4, 5, ~~and~~ 6, 7, and 8.

The plan shall specify that

13.5.1.1 [Insert 1]

Subsection 13.5.1.1.

13.5.2.1.2

References

1. Quality Assurance Program Requirements. Regulatory Guide 1.33, Revision 3, 1982 (Draft).

12. Guidelines for the Preparation of Emergency Operating Procedures. NUREG-0899, 1982.

13. Code of Federal Regulations: Energy. 10 CFR 50.34(f)2.ii 1993.

3 4. Clarification of TMI Action Plan Requirements. NUREG-0737, 1980.

4 5. Supplement 1 to NUREG-0737, Requirements for Emergency Response Capability. 1982.

5 6. ANSI 18.7-1976/ANS-3.2, 1976.

6 7. Lessons Learned from the Special Inspection Program for Emergency Operating Procedures. NUREG-1358, 1989.

7 8. Supplement 1 to NUREG-1358, Lessons Learned from the Special Inspection Program for Emergency Operating Procedures. 1992.

8 9. Techniques for Preparing Flowchart Format Emergency Operating Procedures. NUREG/CR-5228, 1989.

13.5.2 [Insert 2]

Insert 1

13.5.1./ Procedures Included in Scope of Plan

The following procedures shall be included in the scope of the Plant Operating Procedures Development Plan:

I. System Procedures. Such procedures include all system procedures that require operator action in the MCR or RSR. Procedures shall be prepared, ~~as appropriate,~~ for ~~the following~~ PWR system operation. Typical PWR systems having procedures are listed below:

a. Reactor Coolant System
b. Control Rod Drive System (including part-length rods)
c. Shutdown Cooling System
d. Emergency Core Cooling System
e. Component Cooling Water System
f. Containment
   (1) Maintaining Containment Integrity
   (2) Special Containment Systems
      (a) Atmosphere
      (b) Double-Wall Containment with Controlled Interspace
   (3) Containment Ventilation System
   (4) Containment Cooling Systems
g. Atmosphere Cleanup Systems
h. Fuel Storage Pool Purification and Cooling System
i. Main Steam System
j. Pressurizer Pressure and Spray Control Systems
k. Feedwater System (feedwater pumps to steam generator)/startup Feedwater Sys
l. Auxiliary Feedwater system
m. Service Water System
n. Chemical and Volume Control System (including Letdown/Purification System)
o. Auxiliary or Reactor Building Heating and Ventilation
p. control Room Heating and Ventilation
q. Radwaste building Heating and Ventilation
r. Instrument Air System
s. Electrical System
   (1) Offsite (circuits between the offsite transmission network and the onsite Class 1E distribution system)
   (2) Onsite
   (a) Emergency Power Sources (e.g., diesel generator, batteries)
   (b) A.C. System
   (c) D.C. System
t. Nuclear Instrument System
   (1) Source Range
   (2) Intermediate Range
   (3) Power Range
   (4) Incore System
u. Reactor Control and Protection System
v. Hydrogen Recombiner

II. Procedures for Off-Normal or Alarm Conditions. Such procedures include

all procedures for off-normal or alarm conditions that require operator action in the MCR or RSR. These correspond to the number of alarm annunciators. Each annunciator important to safety should have its own written procedure, which should normally contain (a) the meaning of the annunciator, (b) the source of the signal, (c) the immediate action that is to occur automatically, (d) the immediate operator action and (e) the long-range actions.

III. General Plant Operating Procedures. Such procedures include all general plant operating procedures that require operator action in the MCR or RSR. Procedures shall be prepared for the integrated operations of the plant. Typical general plant procedures are listed below:

a. Cold Shutdown to Hot Standby
b. Hot Standby to Minimum Load (nuclear startup)
c. Recovery from Reactor Trip
d. Operating at Hot Standby
e. Turbine Startup and Synchronization of Generator
g. Changing Load and Load Follow (if applicable)
h. Plant Shutdown to Hot Standby
i. Hot Standby to Cold Shutdown
j. Reactor coolant system operation with loops partially drained

IV. Radiation Control Procedures. Such procedures include all radiation control procedures that require operator action in the MCR or RSR. ~~including,~~ Typical radiation control procedures are listed below: ||

a. PWR Gaseous Effluent System
   (1) Collection, Storage, and Discharge
   (2) sampling and Monitoring
   (3) Air Ejector and Stack Monitoring
   (4) Ventilation Air Monitoring
b. Process radiation Monitoring System Operation
c. Meteorological Monitoring

V. Maintenance, Calibration, Inspection and Test Procedures. ~~Such procedures include~~ All portions of maintenance, calibration, inspection and test procedures that require operator action in the MCR or RSR. ~~The applicable procedures~~ will conform to the requirements of the Plant Operating Procedures Development Plan.

VI. Procedures for Emergencies, Operational Transients and Other Significant Events. Such procedures include all emergency, operational transient and other significant-event-related procedures that require operator action in the MCR or RSR. ~~including,~~ Typical procedures for emergencies, operational transients and other significant events are listed below:

a. Loss of Coolant (including significant PWR steam generator leaks), (inside and outside primary containment), (response to large and small breaks, including leak rate determination)
b. Loss of Instrument Air
c. Loss of Electrical Power (or degraded power sources, or both)
d. Loss of Core Coolant Flow/Achievement and Maintenance of Natural

Circulation, including connection of the pressurizer heaters to the emergency bus, if necessary

e. Loss of Condenser Vacuum
f. Loss of Service Water
g. Loss of Shutdown Cooling
h. Loss of Component Cooling System and Cooling to Individual Components
i. Loss of Feedwater or Feedwater System Failure (including verification of proper operation of the auxiliary feedwater system, pressurizer Power Operated Relief Valve (PORV), and steam generator level control system, as applicable)
j. Loss of Protective System Channel
k. Mispositioned Control Rod or Rods (and rod drops)
l. Inability to Drive Control Rods
m. Conditions Requiring Use of Emergency Boration or Standby Liquid Control System
n. Fuel Cladding Failure or High Activity in Reactor Coolant or Offgas
o. Fire in Control Room or Forced Evacuation of Control Room
p. turbine and Generator Trips
q. Malfunction of Automatic Reactivity Control System
r. Malfunction of Pressure Control System
s. Reactor Trip
t. Plant Fires
u. Acts of Nature (e.g., tornado, flood, dam failure, earthquake)
v. Abnormal Releases of Radioactivity
w. Hydrogen Explosions
x. Containment Isolation (including reopening of individual isolation valves following reset of safety injection or containment isolation valves)
y. Loss of Annunciators

Insert 2

~~13.6~~ 13.5.2 **Administrative Control Procedures**

Such procedures will be a COL action item including "Review and Modify Procedures for Removing Safety-Related Systems from Service~~,~~" and "Guidelines for Upgrading Other Procedures."

a facility that physically represents the MCR configuration and dynamically represents the operating characteristics and responses of the system 80+ design

18.9.3 VALIDATION

18.9.2.1 Design Validation design

The purpose of validation is to ensure that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EPG provides usable HSI ensemble that supports the successful accomplishment of the operator's required tasks using a full-size dynamic mockup of the consoles that simulates plant operational responses (i.e. validate performance of the integrated Human Machine system for System 80+). Validation includes operator interaction with the ensemble and EPGs. Specifically, validation meets the following objectives:

Design or operating sequences. design

A. Validate ability to execute operator tasks required by procedure guidance.

B. Validate the MCR configuration staffing assumptions and confirm the Task Analysis results;

C. Validate time response for credited operator actions based on the safety analysis;

D. Validate the allocation of functions and operator situational awareness;

E. Validate operator communication and team interaction;

F. Validate operation with HSI and I&C equipment failures;

G. Validate ability of the operator to use the alarm system effectively.

Each of the plant accident, abnormal, normal, and HSI and I&C equipment failure operating sequences will be performed on the full-size dynamic mockups of Nuplex 80+ consoles that simulates plant operational sequences.

The design validation team will be debriefed after each scenario for the purpose of identifying and defining discrepancies. Identified findings from this debriefing will be documented. The design validation activities will be conducted until the completed control complex is validated.

a facility that physically represents the MCR configuration and dynamically represents the operating characteristics and responses of the System 80+ design.

3.

CESSAR-DC ADDITION

18.9.3.2

~~13.5.3~~ Operating Ensemble Validation Plan

An operating ensemble validation plan shall be developed to guide validation activities that will demonstrate acceptability of the completed operating ensemble (i.e., equipment interface, plant-specific procedures, and operating staff). This will provide assurance that trained operators using "final", plant-specific procedures in the as-built control room, together form an effective operating ensemble.

The operating ensemble validation plan shall specify the scope of procedures and validation scenarios to be used. As a minimum the operating ensemble validation shall exercise the "final" version of all plant-specific procedures listed in Section 13.5.1.1 (note that the procedures validation of Section 13.5.1 may be performed in conjunction with this activity). In addition, operating tasks for plant-specific equipment that is different from the certified design shall be performed using appropriate scenarios and applicable procedures.

The operating ensemble validation plan shall specify the validation methodology including required validation team personnel, required facilities and resources, detailed operating scenarios which incorporate all critical tasks identified in the Task Analysis from the PRA, performance measures, and data collection and analysis methodology.

The operating ensemble validation plan shall specify the acceptance criteria to be used during the validation. This will include relevant acceptance criteria from the Nuplex 80+ design validation provided through OSIP and scenario-specific objective criteria for each scenario.

The operating ensemble validation plan shall specify the schedule and milestones of the validation activities.

The operating ensemble validation plan shall require administrative procedures to govern validation activities including reporting and resolution of findings.

Information concerning the site operator's operating ensemble validation is within the site operator's scope and shall be provided in the site specific SAR.

13.5-1 Site-specific plant operating Procedures 13.5.1-2

18.9-1 Site-specific operating crew table validation 18.9.3.2

TABLE 1.10-1 (Cont'd)

(Sheet 8 of 10)

COL LICENSE INFORMATION

Item Number	Subject	CESSAR-DC Section
13.1-1	Organizational structure of the site operator	13.1
13.3-1	Site-specific emergency planning	13.3.2
13.3-2	Emergency planning support facilities	13.3.3.2
14.2.1-1	Startup administrative manual	14.2.1.1
14.2.2-1	Information on organization and staffing	14.2.2.1
14.2.3-1	Initial test procedures	14.2.3
14.2.4-1	Initial test program	14.2.4
14.2.6-1	Test records	14.2.6
14.2.9-1	Trial use of plant operating and emergency procedures	14.2.9
14.2.10-1	Initial fuel loading	14.2.10.1
14.2.11-1	Test program schedule	14.2.11
14.2.12.3-1	Scoping documents containing testing objectives and acceptance criteria	14.2.3.1
14.2.12.3-2	Documents listing plant conditions required during testing	14.2.3.2
14.2.12.3-3	Reconciliation methods for test conditions	14.2.4.3
14.2.12.3-4	Preoperational and startup test procedures	14.2.3.2
14.2.13-1	Security system and its test and acceptance criteria	14.2.3.3
15.3.10-1	Liquid tank failure	15.7.3.4
17.3.1.2-1	O-RAP development and implementation	17.3.10
19.1.2.2.2-1	Vulnerability of the intake structure due to tornado-generated debris	19.7.2.1.3