

HUMAN FACTORS PROGRAM PLAN
FOR THE
SYSTEM 80+ (TM)
STANDARD PLANT DESIGN

NPX80-IC-DP790-01

Revision 02

September 29, 1993

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

Prepared by: R.B. Fuld Date: 9/29/93
R.B. Fuld, Lead Engineer, Human Factors
Reviewed by: D.L. Harmon Date: 9/29/93
D.L. Harmon, Supervisor, Man-Machine Interface Design
Approved by: T.J. Rozek Date: 9/29/93
T.J. Rozek, Manager, I&C Monitoring Systems Engineering

Issue date 9/30/93

RECORD OF REVISIONS

NO.	DATE	PAGES INVOLVED	PREPARED BY	APPROVALS
00	10/10/92	ALL	P. M. Simon	D. L. Harmon K. Scarola
01	12/15/92	ALL	R. B. Fuld	D. L. Harmon T. S. Rozek
02	09/29/93	1, 5, 47-51, 54, 55; Appendix: 5, 7, 10, 11, 15, 18, 19, 23, 26, 37, 48	R. B. Fuld	D. L. Harmon T. S. Rozek

TABLE OF CONTENTS

1 - INTRODUCTION	
1.1 - Purpose and Scope.....	5
1.2 - Goals and Philosophy.....	6
1.3 - Organization.....	12
2 - HUMAN FACTORS ANALYSES	
2.1 - Systems Analysis.....	22
2.2 - Function and Task Analysis.....	23
2.3 - Staffing and Configuration Evaluation.....	25
2.4 - Info Presentation & Panel Design Evaluation.....	27
2.5 - Verification and Validation.....	29
2.6 - Alarm Analyses and Evaluations.....	30
2.7 - Halden Reactor Studies.....	32
2.8 - Summary.....	34
3 - HUMAN ENGINEERING OF HSI AND EQUIPMENT	
3.1 - Integrated Process Status Overview Display.....	35
3.2 - DPS VDT Displays.....	37
3.3 - Alarms.....	39
3.4 - Discrete Indicators.....	41
3.5 - Process Controllers.....	43
3.6 - Flat-Panel Displays	44
3.7 - Component Control.....	45
4 - MAINTENANCE, PROCEDURES, AND TRAINING	
4.1 - Maintenance.....	47
4.2 - Procedure Development.....	47
4.3 - Training Development.....	49
5 - PLANNED HUMAN FACTORS ACTIVITIES	
5.1 - Final HF Standards, Guidelines and Bases.....	53
5.2 - Full-Scale Mockup Activities.....	53
5.3 - Prototyping and Programmable Features.....	54
5.4 - Verification Activities.....	54
5.5 - Further Task Analysis.....	54
5.6 - Static Mockup Evaluations.....	55
5.7 - Final Design Validation Activities.....	55
6 - SCHEDULE	
6.1 - Design Certification Engineering.....	56
6.2 - First-of-a-Kind Engineering.....	56
6.3 - Manufacturing & Procurement.....	57
7 - CONCLUSION.....	58

APPENDIX A - DESIGN PROCESS REQUIREMENTS

ABBREVIATIONS

ABB-CE	Asea Brown Boveri - Combustion Engineering
AC	Auxiliary Console
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
CESSAR-DC	Combustion Engineering Standard Safety Analysis Report - Design Certification
CFM	Critical Functions Monitoring
CFR	Code of Federal Regulations
Ch	Chapter
COL	Combined Operating License
CRDR	Control Room Design Review
CRS	Control Room Supervisor
CRT	Cathode Ray Tube
CVCS	Charging & Volume Control System
DBE	Design Basis Event
DE&S	Duke Engineering and Services
DIAS	Discrete Indication & Alarm System
DPE	Design Process Element
DPS	Data Processing System
DRM	Design Review Meeting
ELD	Electro-Luminescent Display
EPG	Emergency Procedure Guidelines
EPRI	Electric Power Research Institute
FOAK	First-Of-A-Kind (engineering)
FTA	Function & Task Analysis
GDC	General Design Criteria
HCG	Human-Centered Goal
HF	Human Factors
HFE	Human Factors Engineering
HFPP	Human Factors Program Plan
HRA	Human Reliability Assessment
HSI	Human-Systems Interface
I&C	Instrumentation and Control
IPSO	Integrated Process Status Overview
M/A	Manual/Auto
MCC	Main Control Console
MCR	Main Control Room
NRC	Nuclear Regulatory Commission
OSIP	Operational Support Information Program
PAMI	Post Accident Monitoring Indication
PG	Procedure Guidelines
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
QA	Quality Assurance
RCS	Reactor Coolant System
RDD	Reference Design Documentation
RSA	Remote Shutdown Area
RSP	Remote Shutdown Panel

SC	Safety Console
SGB	(HFE) Standards, Guidelines, & Bases (document)
SPDS	Safety Parameter Display System
SPM	Success Path Monitoring
SRDBE	Safety-Related Design Basis Event
TA	Task Analysis
TOI	Tracking-of-Open-Issues (database)
TSC	Technical Support Center
V&V	Verification and Validation
VDT	Video Display Terminal

1 - INTRODUCTION

1.1 - PURPOSE AND SCOPE

1.1.1 - Purpose

The Human Factors Program Plan (HFPP) for System 80+ describes the Human Factors Engineering (HFE) program for the System 80+ Standard Plant design, specifies the elements of the program, and explains how the elements are managed. The document identifies:

- 1) Human Factors (HF) activities performed for the project to date;
- 2) HF activities to be performed as part of the ongoing System 80+ Standard Plant design program;
- 3) Requirements on HF activities (Appendix A).

The document provides a consolidated basis for review of ABB-CE's human factors plans and progress. It is not intended to revise the efforts that have brought the design to its present state of completion. Rather, activities and products which are thus far complete are regarded as exemplary design practices to be repeated, where specified, in the future design of the plant. Thus, the HFPP presents the requirements on the design process, identifies what has been accomplished thus far in the design process, and relates this to the plans for continued and future activities; this provides a complete program for Human-System Interface (HSI) development.

1.1.2 - Scope

The HFPP describes activities relating to 1) the design of the Human-System Interface for the Nuplex 80+ advanced control complex for the System 80+ standard plant, and 2) HSI considerations for the balance of the System 80+ standard plant design. Specific scope requirements are presented in Appendix Section A-1.4.

The HFPP has two major components. The first part is the main body of the document. This provides the review of HF activities performed by the project to date, and the plans for HF activities to be performed by the ongoing design program. The second part, Appendix A, provides goals, requirements, and criteria for these activities, along with their supporting bases and references. These two components must be considered together in the use and evaluation of the Plan.

1.2 - GOALS AND PHILOSOPHY

1.2.1 - Philosophy of Design

The System 80+ design philosophy for both the plant and the control complex is evolutionary. Implicit in any evolutionary framework is the success of preceding generations: evolution is a process of modifying generally successful designs into improved ones. Conservative evolutionary design therefore emphasizes the solution of known problems, and the incorporation of established improvements. In turn, testing must ensure that the acceptability of preceding generations is maintained throughout the changes embodied in the new design.

The System 80+ physical systems and their operation do not differ substantially from previously licensed plants (i.e., System 80). Similarly, the Nuplex 80+ advanced control complex has sought to make evolutionary improvements in plant operations and the HSI, while assuring that the HSI remains acceptable with respect to established industry standards. Nuplex 80+ is therefore an implementation of existing HSI functions on an advanced I&C platform. Criteria for HSI acceptability include conformance to existing human factors guidance, correction of significant human error concerns that are identified during analysis, development, or verification, and demonstration of the operators' ability to perform required operating and safety functions and procedures in a timely and reliable manner (i.e., validation).

Since there is no unitary, objective measure of performance quality, nor any baseline data against which the notion of 'optimal' can be measured, ABB-CE does not make any claim regarding optimal HSI performance for Nuplex 80+. Likewise, ABB-CE does not claim quantified improvements in human operator performance over that achieved in conventional plants (although many specific improvements are held to be qualitatively clear.) Rather, the design process and acceptability criteria are directed to the practical achievement of the design goals listed in the Plan.

The two main philosophies of evolutionary design and acceptability assurance are supplemented by several subsidiary ones. These are summarized below:

Accuracy over Speed: Nuplex 80+ is designed to permit operators to perform required plant control actions without violating system-referenced time constraints. Safety features are allocated to automation so that rapid operator responses are unnecessary to ensure plant safety. This

permits operators to emphasize the criterion of accuracy, rather than speed, in their responses.

Maintain the Role of the Operator: It is a premise of the System 80+ design that the preceding System 80 plant is a safe and acceptable design. This premise has been validated by the many successful hours of operation that System 80 has logged to date. Furthermore, the operator's role is held to be a successful component of the System 80 design. Therefore, for System 80+, substantial changes to the operator's present position "in-the-loop" have been avoided.

Evaluation of Design Product by Users: The design team has placed an emphasis on assuring the operator's and other end user's extensive input to, involvement with, and feedback on the design, from the initial concept through the final validation.

Information over Data: Nuplex 80+ presents integrated, valid information, rather than disaggregate data to operators. The design philosophy is to provide necessary information in a format and at a level of detail that efficiently supports operations tasks. Data processing algorithms reliably monitor for and explicitly indicate discrepant channels (which are infrequent and potentially misleading). Detailed data is available, on demand, for diagnostic and maintenance tasks. Unnecessary and uninformative mental load is thereby reduced for operators.

No Backup: It is part of the design philosophy not to provide hardwired indicators and controls as a 'backup' certifiable HSI. Redundant indications are normally available at the control consoles so that loss of a single device will not result in a loss of information, and so that PAMI readings are provided on familiar instrumentation.

Specific Criteria: The HSI design is based on accepted industry practice and human factors criteria. Initially, general criteria from these documents were used in the design. As work progressed, these generic and sometimes conflicting methods were distilled into a specific set of HFE standards, guidelines, and bases for Nuplex 80+. This document is being maintained and updated to refine HSI guidance abreast of the needs of the design.

Certification of Process & Approval of Features: Detailed documentation is being provided on the Nuplex 80+ design process and standard features that have been exemplified by the RCS panel design. The process and standard features have been submitted for certification and approval by NRC staff. Certification approval will permit the approach to

be applied to subsequent first-of-a-kind engineering products. Design evaluations and acceptance criteria will be formally applied to these subsequent products to ensure performance adequacy and conformance to the certified design. This approach provides an effective mix of both process and product design evaluations.

1.2.2 - Goals for Design

The term "goal" lends itself to many uses in planning, design, and testing. Goals in the present document are identified in at least three distinct contexts; each of these uses of the term has merit. Thus, they are each discussed below. To avoid subsequent confusion, use of "goal" should place the term clearly in a specific context.

1.2.2.1 - Process Element Goals - Appendix A of this document defines and provides bases for eight HFE design process elements in terms of their Goals, Requirements, and Criteria (see Section A-2.2). Goals represent the idealized function or purpose of the element. Requirements, in contrast, are pragmatic and concrete, and operationalize the Goals. Criteria, are objectively verifiable quantities or qualities of acceptability against which an item is tested, to determine whether it meets the associated requirement. Appendix A presents design process elements for Nuplex 80+.

1.2.2.2 - Human-centered Design Goals - The NRC Program Review Model identifies six generic Human-Centered Design Goals (HCGs). These are general design objectives for the system HSI expressed in terms of human performance. Stated as generalities, they are at some point to be "objectively defined and [to] serve as criteria for test and evaluation activities." The HCGs are as follows:

- 1) The operating team can accomplish all assigned tasks within system-defined time and performance criteria.
- 2) The system and allocation of functions will provide acceptable workload levels to assure vigilance and to assure no operator overload.
- 3) The system will support a high degree of operating crew "situational awareness."
- 4) Signal detection and event recognition requirements will be kept within the operators' information processing limits to minimize the need for operators to mentally transform data in order for it to be used.
- 5) The system will minimize operator memory load.

- 6) The operator interfaces will minimize operator error and will provide for error detection and recovery capability.

These fairly general goals might be further summarized by stating that "The HSI shall facilitate acceptable human performance." This is already a cornerstone of Nuplex 80+ HSI philosophy (see Section 1.2.1).

However, the HCGs are somewhat more specific. Their main concern is for the concomitants and characteristic effects of operator workload, particularly mental load, as conceived by various human performance models (i.e., time stress (1), low and high arousal (2), "cognitive tunnel vision" and "operator-out-of-the-loop syndrome" (3), perceptual channel and working memory capacities (4 & 5), and error/accuracy (6)). Unfortunately, mental workload is an abstract construct, not directly observable; a "high-inference" variable prone to unreliable results. While it is desirable to avoid workloads of either extreme, workload measures thus have somewhat limited utility.

In control room design, time- and error-related observations are generally the most useful types of human performance measures. This is due to the fact that they are relatively "low-inference" variables, whose criteria can be system-referenced. For example, if valve X must be shut before time Y or a safety limit will be exceeded, then acceptable human performance has been objectively (if ad hoc) defined by the system design. Workload may then be inferred from these results.

Thus, the HCGs articulate desirable goals, but their correspondence to objective evaluation criteria is limited both on theoretical and pragmatic grounds. In the System 80+ design process the HCGs are addressed through formal analysis and subjective evaluations, as follows:

HCG 1 - System-defined Criteria: This goal captures the purpose of the Design Validation exercises (Sections 2.5, 5.7, and A-3.8) in a nutshell. Validation exercises apply standard simulator evaluation techniques to ensure the adequacy of operating staff performance on the actual control room design, using vendor procedure guidance to maintain the plant within design basis limits. In addition, preliminary evaluations of response time adequacy include response time modeling portions of the Task Analyses (see A-3.4) and SAR Chapter 15 accident analyses that credit operator action. Analyses of specific operator errors, including time response considerations, and identification of critical tasks, are performed as Human Reliability

Analysis (HRA; part of SAR Chapter 19, PRA). Finally, it is assumed that the systematic application of HFE principles (i.e., through the SGB; see Sections 5.1 and A-3.5) will generally increase performance speed and accuracy (i.e., reduce operator loading). Successful application of these principles is evaluated by Suitability Verification (see Section A-3.7).

HCG 2 - Function Allocation: This goal implies through its use of the term "allocation of functions" that there is a particular concern for the manner in which automation has been applied. In fact, many allocations of safety-related features to automation are mandated by Federal Regulations (see Section A-3.3). In addition, part of the System 80+ design philosophy has been to retain the established role of the operator as a successful facet of the preceding System 80 design. Therefore, changes to allocations have been made in a largely evolutionary fashion, only to make specific improvements in the overall design or to address specific problems (e.g., the one-sensor-per-indicator problem). Allocation of Function will be evaluated in terms of the Requirements and Criteria specified in Section A-3.3. In addition, feedback and resolution of allocation issues continues throughout design via Task Analysis (A-3.4), Verification (A-3.6 and A-3.7) and Validation (A-3.8), and applicable SAR analyses of Chapters 15 (DBE) and 19 (PRA).

HCG 3 - Situational Awareness: Use of the term "situation awareness" reflects cognizance of recent research themes in aviation HF. Like mental load and mental models, situation awareness is a "high-inference" variable. However, it is believed that many of the Nuplex 80+ design bases and resulting features can be accepted, on a priori grounds, to make improvements in this area. These features include the Critical Functions, Success Path Monitoring (SPM), IPSO, the prioritized alarm scheme, and the variety of methods applied to integrate data into information (see Section 2.7 on empirical Halden studies verifying the effectiveness of CFM, SPM, and IPSO). Validation exercises (Section A-3.8) will ensure the acceptability of crew situational awareness in terms of system-defined time and performance criteria, and subjective evaluation by operators.

HCG 4 & 5 - Perceptual & Cognitive Loading: In contrast to HCGs 1 and 3, which emphasizes the more integrated, "big-picture" aspects of the HSI, HCGs 4 and 5 express more elemental or micro-level concerns. As previously discussed, the general concern is for excessive or unnecessary mental load; references to data transformations, signal detection, and memory loading imply a specific emphasis on proper display design and panel layout, as well as the integration

of displays and information. This is primarily addressed through the Requirements and Criteria for HSI Design (Section A-3.5), including application of the SGB; the subsequent Verification of Suitability (Section A-3.7) for panels, and subjective evaluation by operators during Validation (Section A-3.8).

HCG 6 - Operator Error: As discussed previously, the focus on error as opposed to loading is somewhat the other side of the same coin. Although operator error cannot precisely be minimized, its likelihood can be reduced, or its impact mitigated, through design evaluation and revision. Much of HSI design is aimed at reducing more "error-likely situations" into less error-likely ones. Incorporation of operating experience (A-3.2), incrementally revised allocations (A-3.3), Task Analysis (A-3.4), HSI design (A-3.5), Verification (A-3.6 and A-3.7) and Validation (A-3.8), as well as SAR analyses in Ch 15 (DBEs, including operator time response) and Ch 19 (PRA, including HRA) all contribute to the goal of reducing human errors.

1.2.2.3 - Nuplex 80+ Design Goals - Section 3 of this document summarizes certain design basis information (positions held to be self-evident based on first principles, a priori assumptions, etc.) for various Nuplex 80+ design features that are available in CESSAR DC and other docketed design documents. These goals were part of the conceptual design. They were not intended to provide a source for requirements or criteria, however. They should therefore be understood simply as explanatory material.

1.2.3 - Position on Regulations

Nuplex 80+ and all other areas of System 80+ HSI meet the requirements of 10 CFR 50.34(f)(2), and other applicable federal regulations as specified in Appendix A. The design shall conform to the guidance of NUREG-0700 and its bases where these are applicable to advanced design. The design and design process also meet the current human factors design requirements of the Standard Review Plan, NUREG-0800. Other NRC regulatory documents which pertain to HFE (e.g., Regulatory Guide 1.97) have also been considered, and their requirements incorporated as specified in Appendix A of this document, and in Section 1.8 of CESSAR-DC.

In the absence of NRC guidance on advanced HSI design, the project has distilled guidance from accepted industry documents as described in Section 1.2.2; efforts have also been made to follow generic industry guidance such as EPRI NP-3659 and the EPRI ALWR Utility Requirements Document.

1.3 - ORGANIZATION

1.3.1 - Design Team

1.3.1.1 - Internal Organization - The human factors engineering at ABB-CE is an integrated discipline within the HSI design process. Full time human factors specialists are permanently employed by ABB-CE and participate throughout design development and evaluation. Use of an integrated group enables close interaction between HF specialists, operations specialists, and system designers. This permits more sharing of design knowledge, and higher frequency of iteration and feedback than would be available from a more compartmentalized organization.

The exact number of human factors engineers working on Nuplex 80+ at any given time varies depending on schedules, work in progress, and other projects which require human factors involvement. There are currently two groups at ABB-CE which include HF Specialists: the Nuclear Systems I&C Control Complex Engineering Group, and the Nuclear Services Training and Human Factors Group. The Systems group has primary responsibility for the Nuplex 80+ design; the Services group provides staff augmentation as needed for specific tasks.

Minimum requirements for HF specialists on the project include either: 1) a Master's degree in an HF-related field, plus one year of industry design experience, or 2) five years HF-related design experience in the nuclear industry, or 3) any proportional combination of 1) and 2).

There has always been at least one human factors engineer working full time on the Nuplex 80+ design. At certain points in the design, such as during Functional Task Analysis (FTA) there have been as many as four. The HFE specialists at ABB-CE bring a diverse background to the design, including nuclear navy, utility, and architect/engineer experience. Human factors specialists are one component of a group of eleven HSI designers dedicated to System 80+ work. These include experienced navy and commercial operators, individuals with expertise in display development, I&C systems, and control panel fabrication.

As previously noted, the exact staffing level of human factors engineers dedicated to System 80+ and related projects varies, and an exact number of man-months per year would be difficult to interpret. However, for comparison purposes, it can be noted that for second half of 1991, four HF specialists (three engineers and one supervisor) were assigned full-time to Nuplex 80+ and related projects.

The I&C department contains numerous engineers and specialists besides human factors. CESSAR-DC Table 18.2-1 provides design team staffing information. Former licensed commercial and navy PWR operators contribute greatly to the HSI design, especially in the walk-through and analysis portions. Software specialists, experts in control board design, and I&C systems engineers also add input. In short, HFE is part of the larger integrated design team approach to the entire System 80+ product.

The reporting structure at ABB-CE has varied over the course of the design of System 80+. The present structure for the System 80+ project is shown in Figure 1.3-1; requirements in this area are cited in Section A-3.1.2. Currently, the human factors engineers assigned to the project report to the supervisor of man-machine interface design. The man-machine interface design function is then matrixed to other function and task domains within I&C engineering and the System 80+ project. HF specialists on loan from the Nuclear Services group similarly report to the supervisor of man-machine interface design. However, when the Nuclear Services group performs independent HF tasks (such as the FTA) for the design, they remain within their normal Nuclear Services reporting structure: HF specialist to HF group supervisor, etc. and up the Nuclear Services management chain, which meets the I&C ALWR group's reporting authority at the President of ABB-CE Nuclear Power.

1.3.1.2 - Design Process - The Nuplex 80+ HSI design process is illustrated in Figures 1.3-2 through 1.3-6. These show the relationships among 'conventional' HF analyses, i.e., functional decomposition, design reviews, rapid prototypes, standardized panel layouts, and other design methods employed in the Nuplex 80+ HSI development.

The Nuplex 80+ design approach can be seen to be consistent with human factors methodology described in references such as IEEE-1023 in that:

- the design is an iterative process using HF specialists, operators, plant systems engineers, and maintenance experts;
- prototypes & mockups, DRMs, and other technical evaluations are used to develop a standard HSI design;
- the design team develops System 80+ information and control characteristics to satisfy the operators' need to perform EPGs (safety functions) and other operating tasks;

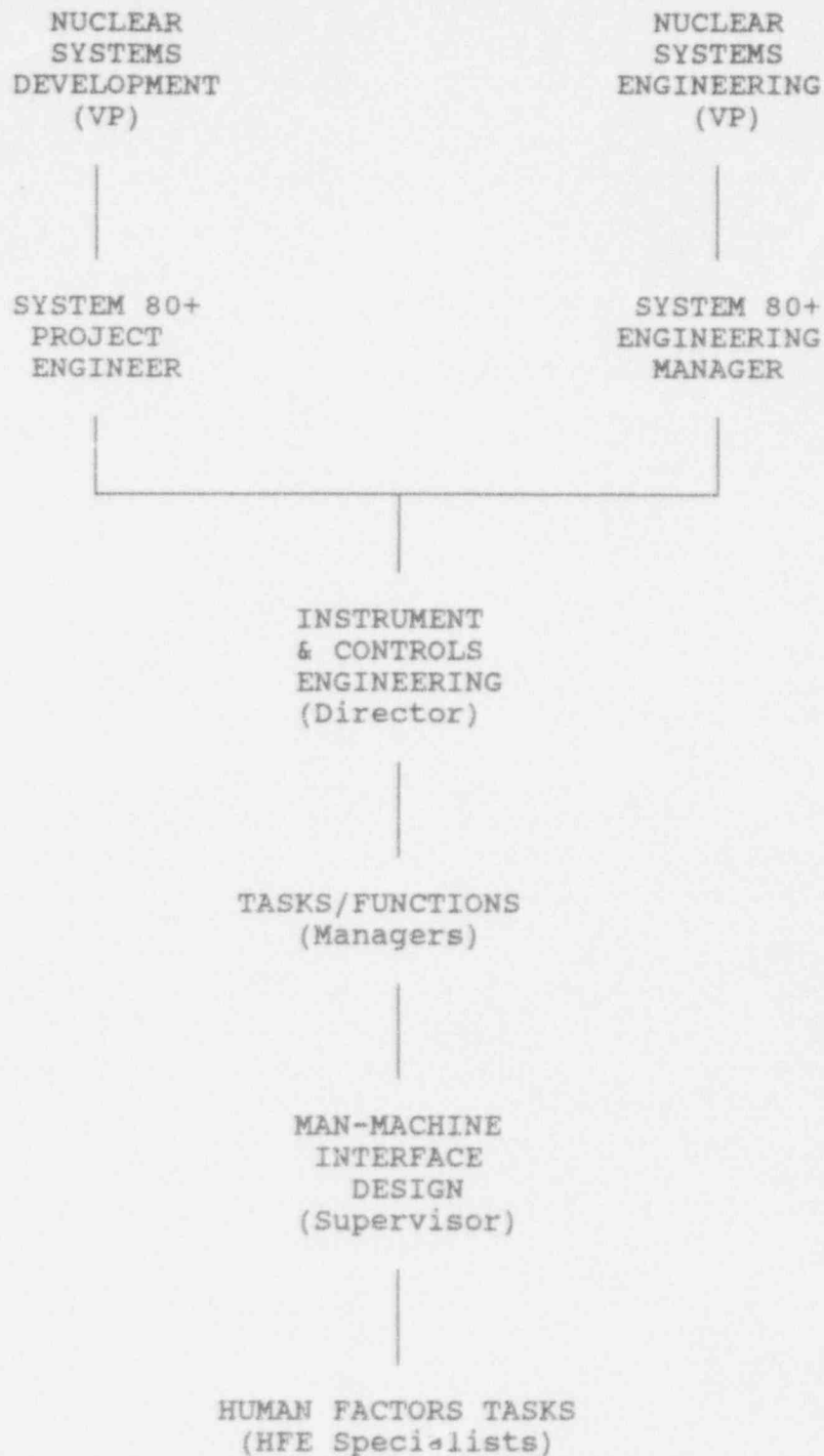


Figure 1.3-1: HFE in System 80+ Management

- the analyses' results are provided to the designers for incorporation into their work and the total design of one panel and the IPSO display;
- additional panel sections are being designed using a similar methodology, with ongoing verification work;
- the entire product will be validated on full-scope simulation facilities.

Elaborate studies and analyses were not seen as the most efficient or practical approach to upgrading the information and control interface for well-understood process systems in an evolutionary design. The ABB-CE design framework utilizes small design teams to develop system and components to meet specified design bases, and to solve existing problems, as well as emergent problems that are identified during the design process. Design flows not only from analyses but also from individual problem solving efforts, design reviews, and experience with previous plants.

1.3.1.3 - Design Review Meetings - The Nuplex 80+ design process utilizes other approaches in addition to conventional human factors analyses. One of the most frequent and important is the Design Review Meeting (DRM). In DRMs, engineer(s) present their work for interdisciplinary review and critique from other design team members. A DRM may have anywhere from three to twenty reviewers, and may include implementers, system designers, operators, or HF specialists, as appropriate to the aspect of design under review. Their frequency is determined by the progress and needs of the design.

This process is akin to what EPRI calls the "boiler room" approach, where design details are "sweated out". Alternately, DRMs can be seen as the 'test' phase of an iterative design cycle of hypothesis-and-test. Specialists in HFE use DRMs both to assure that all aspects of the design receive HF input, and to subject their own work to cross-disciplinary scrutiny. Goals of the DRM include assuring that the proposed design is feasible, useable, and compatible with existing aspects of the design. Minutes and action items from all design review meetings are documented.

These meetings provide early and specific feedback to designers and allow the product to be reviewed well in advance of any finalization. It is important to emphasize that no system is designed without design reviews.

1.3.1.4 - Human Factors Efforts by Subcontractors - Some Balance-Of-Plant (BOP) work relating to the HSI for System

80+ is being performed by Duke Engineering and Services (DE&S) as a subcontractor. ABB-CE retains final design review authority and responsibility for work performed by DE&S or other subcontractors. This work, to date, includes some of the preliminary BOP-related panel layouts and much of the physical plant configuration that impinges on HF-related maintenance and access considerations. The DE&S organization includes operations, maintenance, and testing specialists, many "on loan" from Duke Power; their input has been particularly valuable.

At specified design milestones, work produced by DE&S comes to ABB-CE for interdisciplinary review, including that of ABB-CE human factors specialists. ABB-CE also provides HFE guidance to DE&S by providing HF-related guideline documents and Nuplex 80+ design practice documents. This is to assure that DE&S's products are both sufficient in themselves, and consistent with the remainder of the System 80+ HSI.

Future System 80+ design work may be performed by other subcontractors. Should this prove the case, the same methods of review, guidance, and control will be used to assure a continued standardized and acceptable HSI.

1.3.2 - HFE Documentation

Along with CESSAR-DC, a 13-volume set of Reference Design Documentation (RDD) has been provided. Portions of the RDD relating to HF methods and results include the system descriptions for the RCS and CVCS panels, the generic Panel Layout Standard, the Control Complex Information Systems description, the CFM Systems description, and the Alarm Processing Description. These are incorporated in the design process diagrams of Figures 1.3-2 through 1.3-6. Double boxes in these figures denote documentation; documents are often shown as associated with a specific analysis or activity by an undirected, dotted line.

In the HFPP, reference is made to these and other ABB-CE documents which have been made available to the NRC, such as the HFE Standards, Guidelines, and Bases (SGB), the RCS panel FTA Report, and the RCS panel Verification Analysis Report. Documents slated for the future are also cited (e.g., the OER report, Function Allocations report, V&V plan, future TA and V&V reports, distribution records, Tracking-Open-Issues database reports, etc.). The HFPP does not detail the contents of these documents, but their existence or production is specified as part of the Plan.

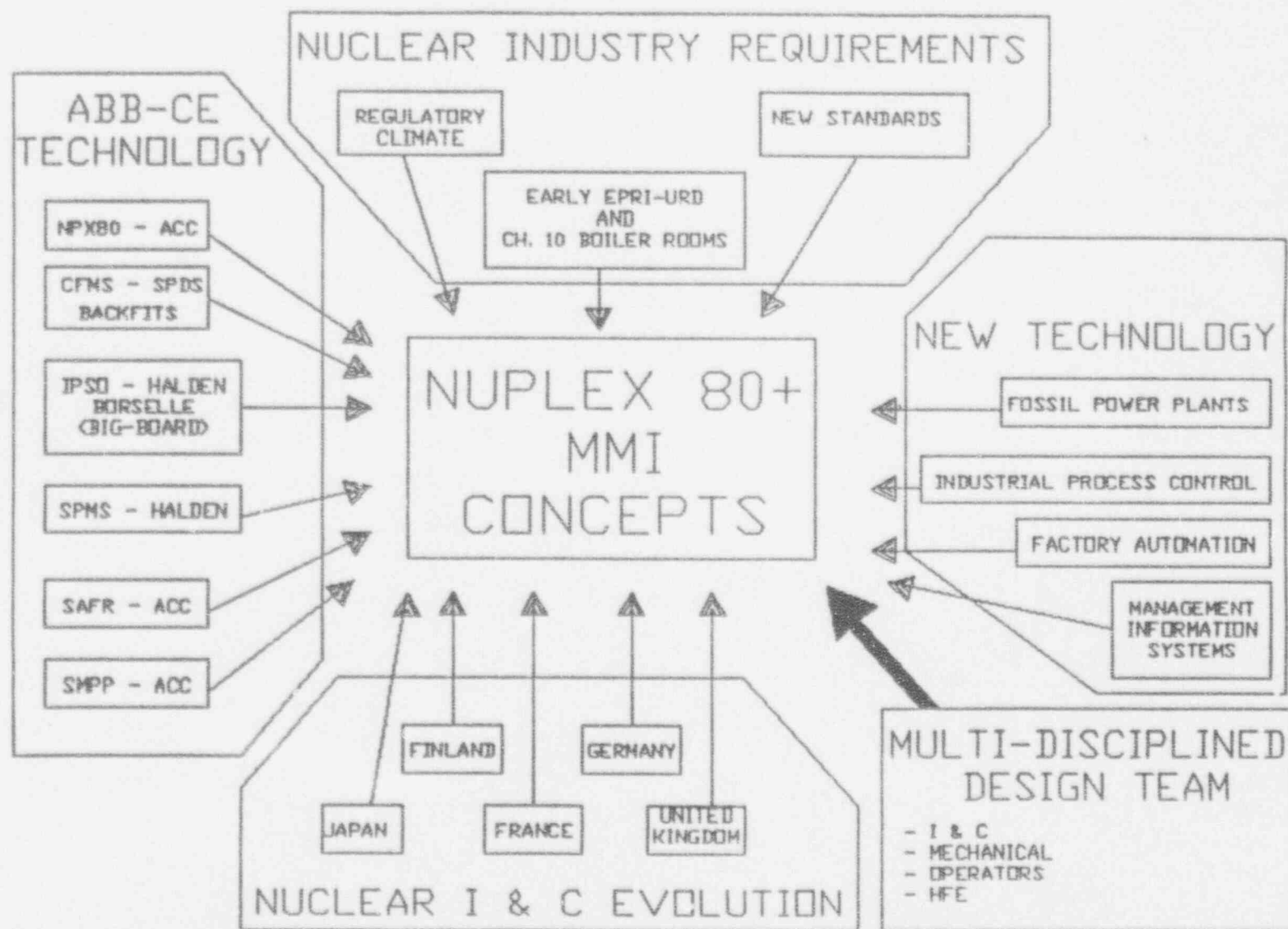


Figure 1.3-2 - Nuplex 80+ HSI Design Process

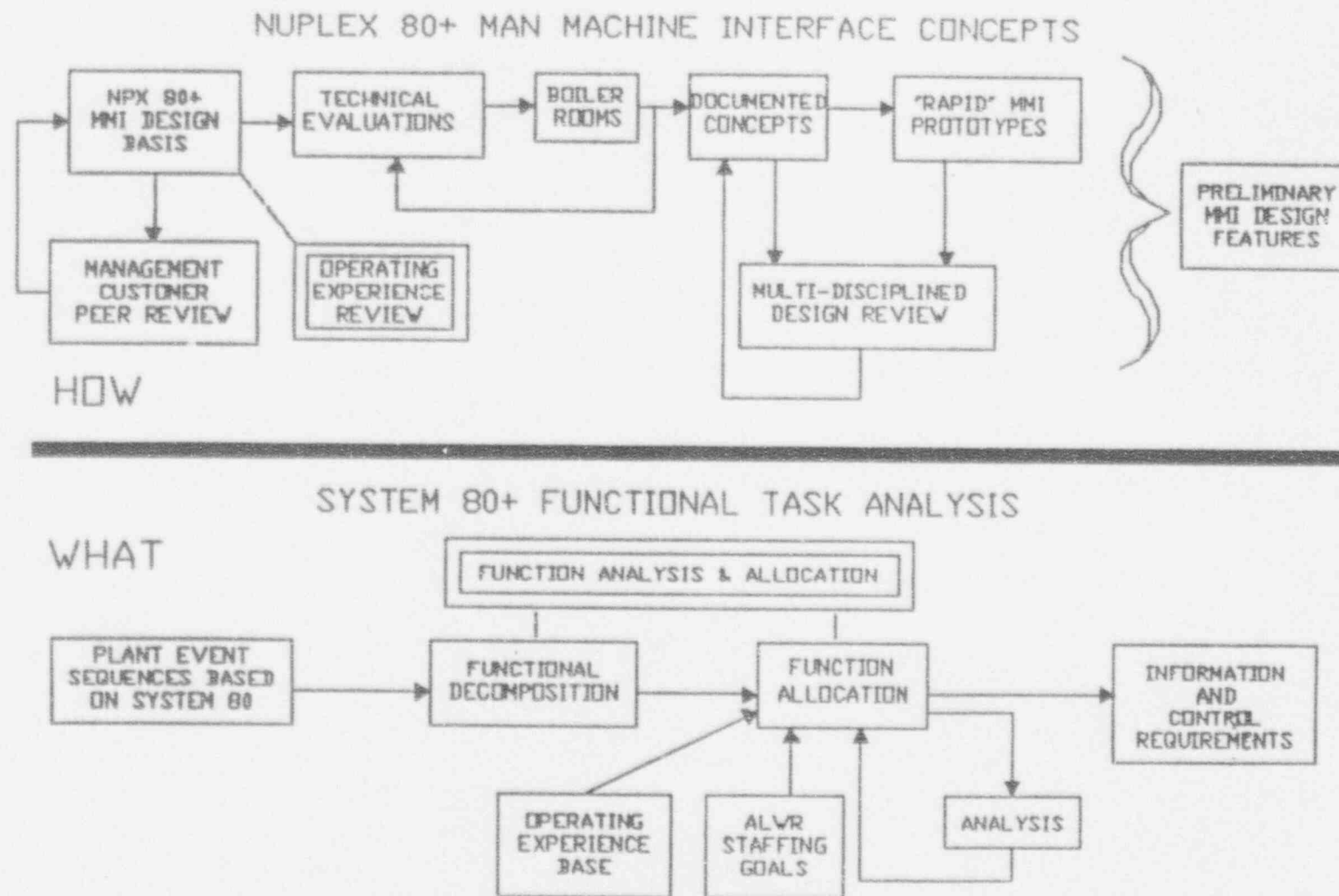


Figure 1.3-3 - Nuplex 80+ HSI Design Process

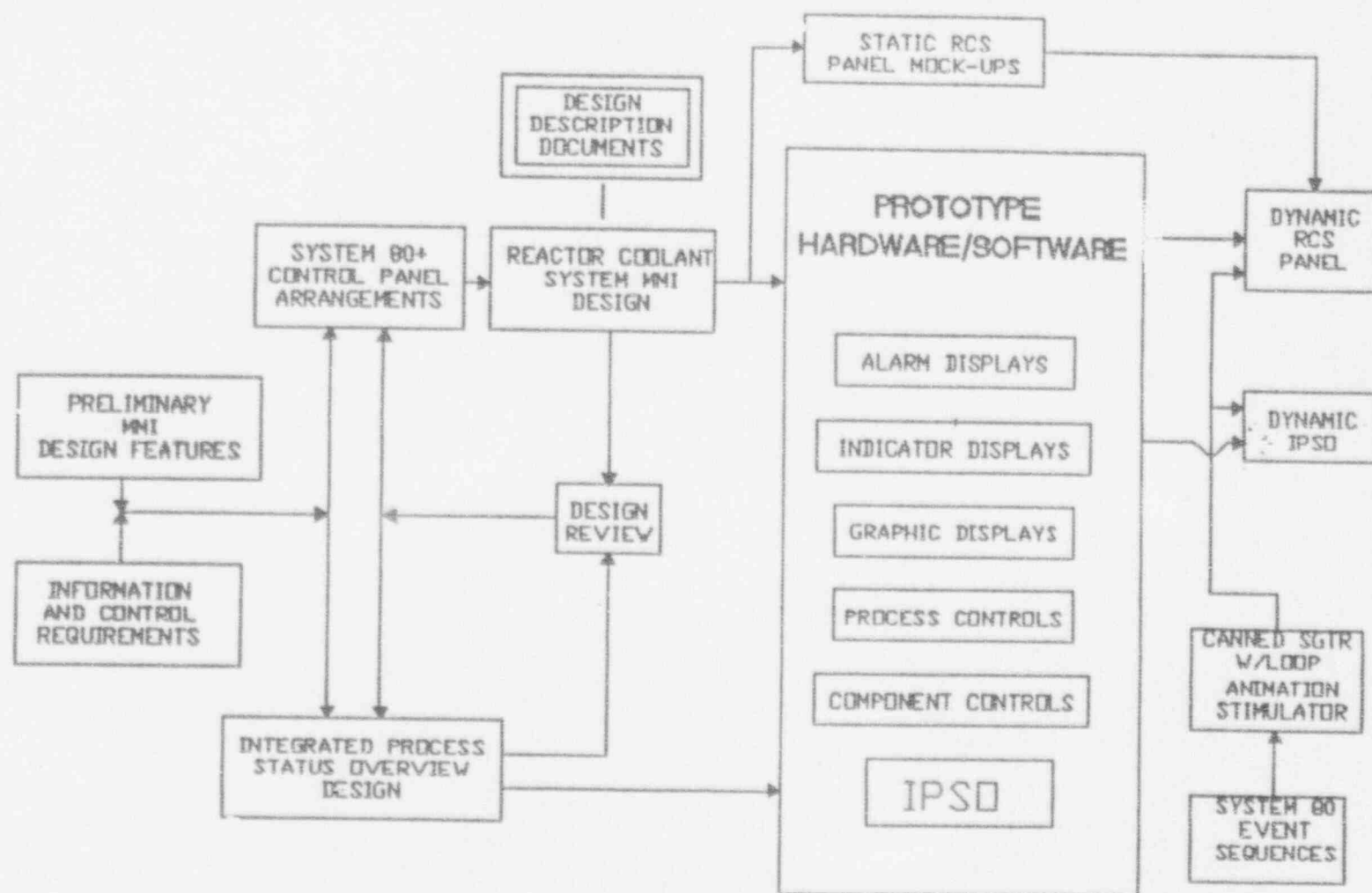


Figure 1.3-4 - Nuplex 80+ HSI Design Process

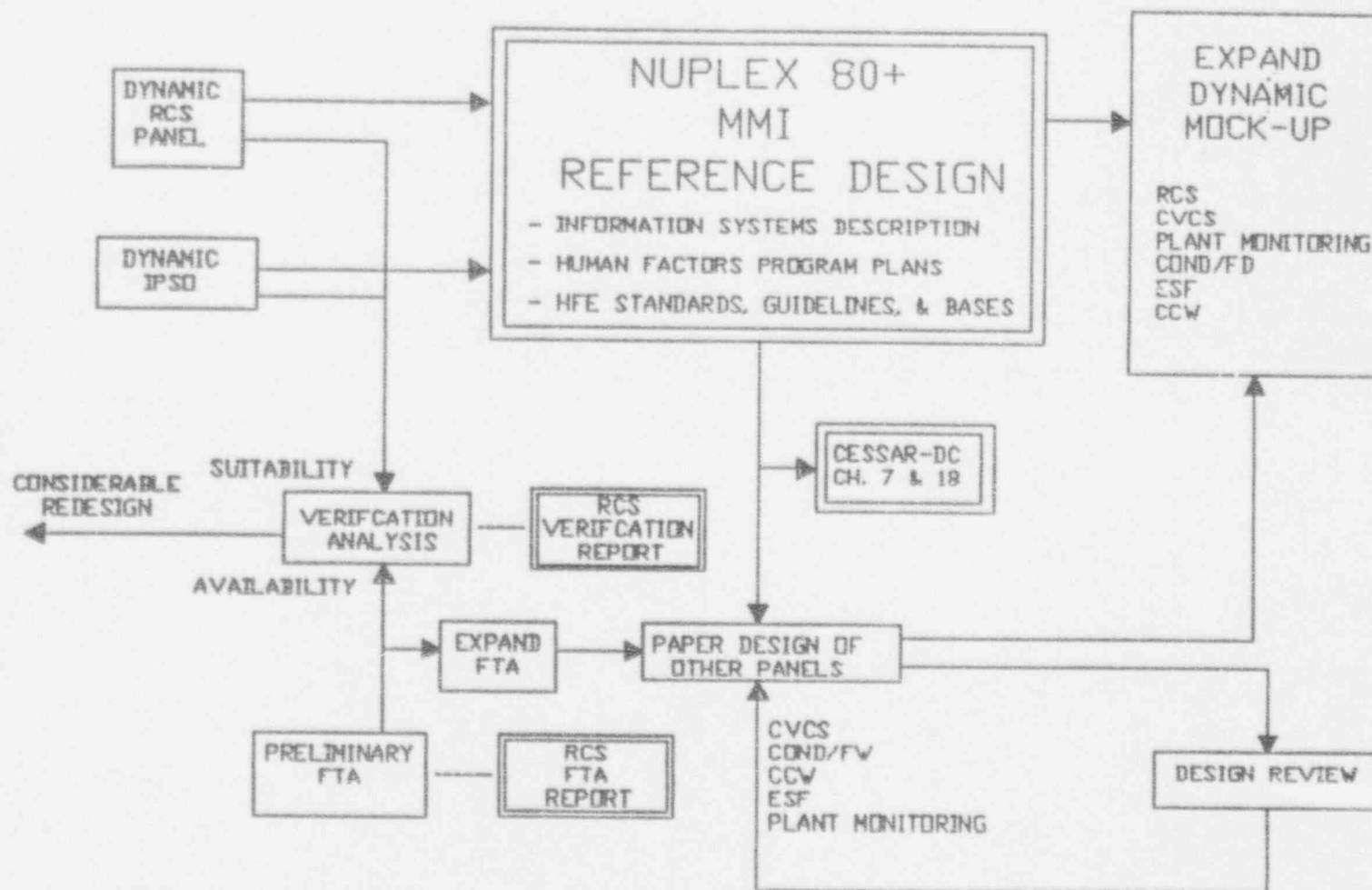


Figure 1.3-5 - Nuplex 80+ HSI Design Process

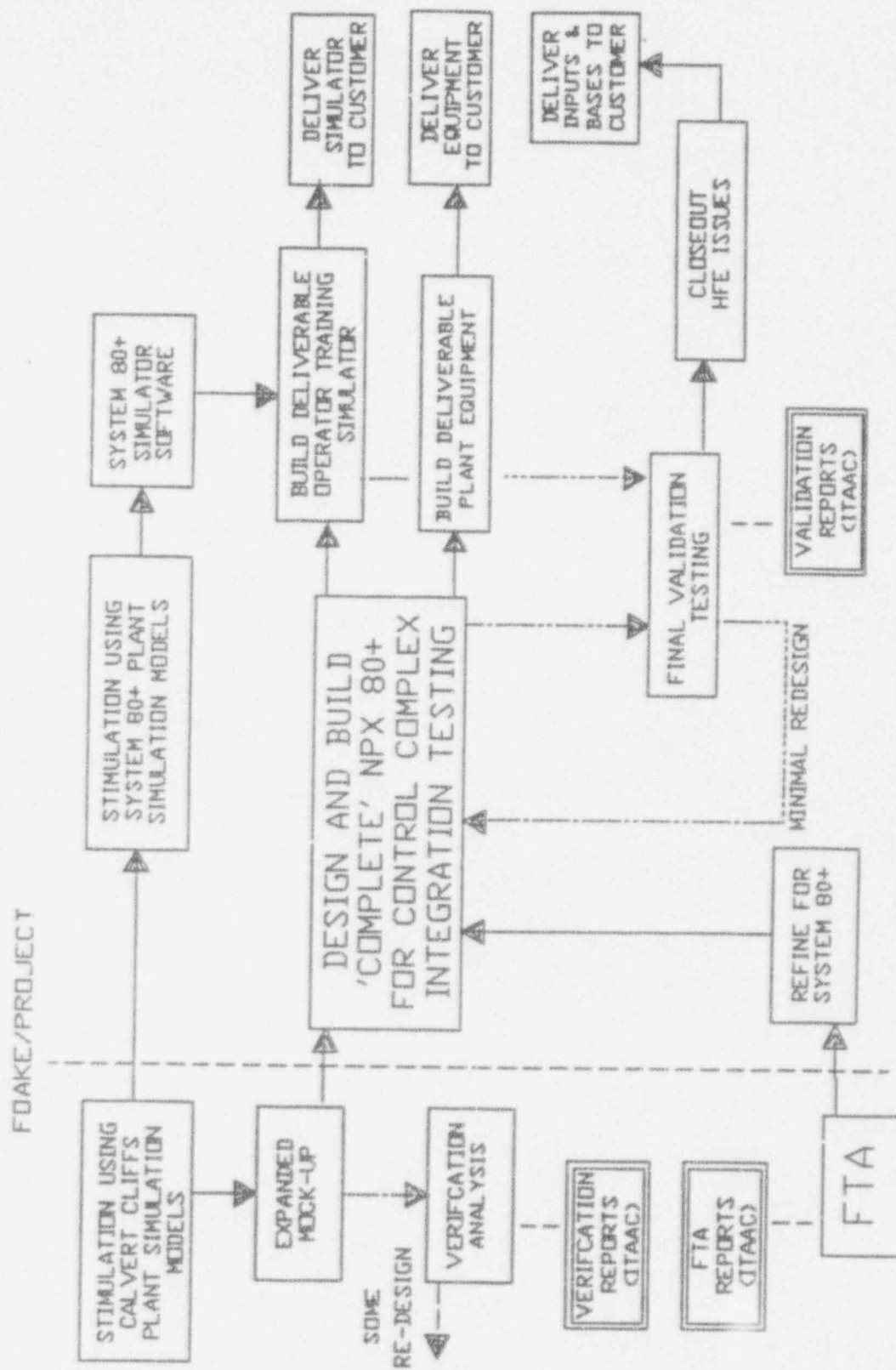


Figure 1.3-6 - Nuplex 80+ HSI Design Process

2 - HUMAN FACTORS ANALYSES

The design team has performed and plans to perform a number of formal analyses and less-structured evaluations as part of the Nuplex 80+ HSI design process. These begin with systems analysis, and progress to task analyses and the other analysis and evaluation activities which normally flow from TA, namely staffing and configuration evaluation, information and panel design evaluation, and V&V. Subsequent to the discussion of these activities, a description of other analyses and evaluations contributing to Nuplex 80+ design is presented. These are alarm analyses and the Halden Reactor studies.

2.1 - SYSTEMS ANALYSIS

A formal systems analysis, such as described in MIL-H-46855B, was not performed for the System 80+ Plant. The analysis was not necessary because the systems for the plant are essentially the same as those for previously-licensed ABB-CE units. The nature of systems and operating procedures for these units is well-established and documented. Therefore, a systems analysis would not be beneficial or necessary for System 80+. Analyses from other projects that were applicable to System 80+ (such as SONGS 2 & 3) were referenced but System 80+ takes credit for design experience as its primary justification for not needing a formal systems analysis since System 80+ represents few changes that affect the anticipated operations based on the previous design.

The results of previous systems operation knowledge have been incorporated into the Nuplex 80+ design in the following areas:

- Allocation and layout of systems in the controlling workspace has been based in part on the number, function and relationships identified between System 80+ systems.
- Crew sizes and staffing needs have been evaluated with consideration of the activities required for system operation.

2.2 - FUNCTION AND TASK ANALYSIS

The Function and Task Analysis is the first of four human factors analyses and evaluations which have been done for the System 80+ RCS, and which are planned for the other portions of the design which will appear in the advanced control complex. The subsequent three, which will be discussed in following sections, are: staffing and configuration evaluation, information presentation and panel design evaluation, and design validation.

A formal Function and Task Analysis (FTA) has been performed for the System 80+ RCS. This analysis and the subsequent report have previously been made available to the NRC in the RDD, volumes 7 & 8. The plan is to perform similar analyses for all other systems with indications and controls on the main control panel sections during the design process. The RCS FTA represents the methodology which the project team will use, with refinements based on the completed FTA work as noted in Section 5.5 of this report.

2.2.1 - Function Allocation

Function allocation, the assignment of functions to either man or machine (or a combination), has been done for System 80+ by reevaluating the allocation of the successful baseline System 80 design. The functions which must be performed by the System 80+ plant remain essentially the same as for System 80, and the role of the operator "in-the-loop" has been retained. Changes in allocations have been developed incrementally, to solve specific problems identified from operating history and experience (see Sections A-3.2 and A-3.3; also the reports indicated therein on review of operating experience and allocation of functions).

Design evaluation and revision of high level allocations has thus been performed in an evolutionary fashion for System 80+. Further allocation work is specified in Section A-3.3. Continuing feedback on allocations, and the resolution of associated concerns, will be generated by other elements of the design process (see HCG 2 under Section 1.2.2.2).

2.2.2 - Functional Task Analysis

A top-down functional task analysis was performed to identify System 80+ information and control characteristic requirements and to allow evaluation of the function allocation. The results of this analysis may be found in CESSAR-DC Section 18.5 and in the Nuplex 80+ Function and Task Analysis Report, in the RDD. In general, three areas

were given design support by the analysis. They are the aforementioned function allocation, general panel layout, and RCS panel design.

Functional requirements and controls for System 80+ were based on existing System 80 power plants. Monitoring tasks were primarily evaluated in the FTA because the monitoring portions of the HSI have the most significant changes, as compared to current plants. The System 80+ control requirements and HSI for controls is essentially the same as for System 80 plants, therefore, the System 80+ FTA relies heavily on the acceptability of the DCRDR process conducted previously for System 80 control rooms. The System 80 instrument list and panel components provided the starting point of the System 80+ FTA.

The analysis considered the four basic operator roles and broke operator functions down into subfunctions, operations, tasks, task information, and control characteristics, as described in the FTA report. Information and control requirements were then gleaned.

2.3 - STAFFING AND CONFIGURATION EVALUATION

2.3.1 - Staffing

The staffing and configuration evaluation, as described in CESSAR-DC, Section 18.6 is complete for the entire Nuplex 80+ control complex. The control panel profiles and arrangements were defined based on the results of the FTA and on HF criteria from the industry, as described in Section 18.6 of CESSAR-DC.

Prior to developing and evaluating the Nuplex 80+ control room configuration, potential and likely staffing levels for Nuplex 80+ were evaluated. First, a set of operational requirements was established, based on the EPRI ALWR URD, experience with existing ABB-CE units, and licensing considerations such as Reg. Guide 1.97. Based on these, Nuplex 80+ was configured to provide for a variety of operating crew sizes from one to six. The technical bases for these crew sizes are as follows.

One-person crew: An EPRI requirement. Reactor Trip was looked at as the limiting event for crew size (i.e., task loading was highest at this point of operations). Task Analysis found that one operator, at the master control console (MCC) could handle not only standard Hot Standby to Power operations but also immediate post trip actions. Therefore, Nuplex 80+ supports this crew size during normal power operations. Note that the additional crew members are in the main control room but only one operator is in the controlling workspace (i.e., at the panels).

Three-Person Crew: For post-trip and for start-up evolutions, the 3-person crew size was based on an evaluation of ABB-CE generic operating guidelines, on operating experience at existing ABB-CE units, and on task analysis.

Six-person crew: An EPRI requirement based on staffing practices of all utilities with ABB-CE plants in operation or on order, six is the maximum crew size. This is not a necessary crew size but Nuplex 80+ could support such a crew (which would include an STA and Control Room Supervisor). Adequate workspace is provided.

Acceptability of these crew sizes can be justified but not confirmed now. However, these crew sizes will be validated in the integration test facility for Nuplex 80+ as part of the human factors program/design process.

2.3.2 - Configuration

The Nuplex 80+ control room configuration was developed through an evolutionary process, beginning with System 80 control room configuration. This configuration was modified based on post-TMI monitoring requirements, the EPRI ALWR URD, plant design changes for System 80+, and industry and NRC human factors criteria and methods. Several candidate arrangements were evaluated based on operational and staffing requirements as described in CESSAR-DC Section 18.6. Essentially, problems with existing configurations were taken into consideration first. Design goals, such as the addition of a CRS workstation and redundant controls, addition of an overview mechanism for determining plant status, et. al. were considered next. The current Nuplex 80+ configuration is a result of factoring this evaluation into the design process described in Section 1 of this plan.

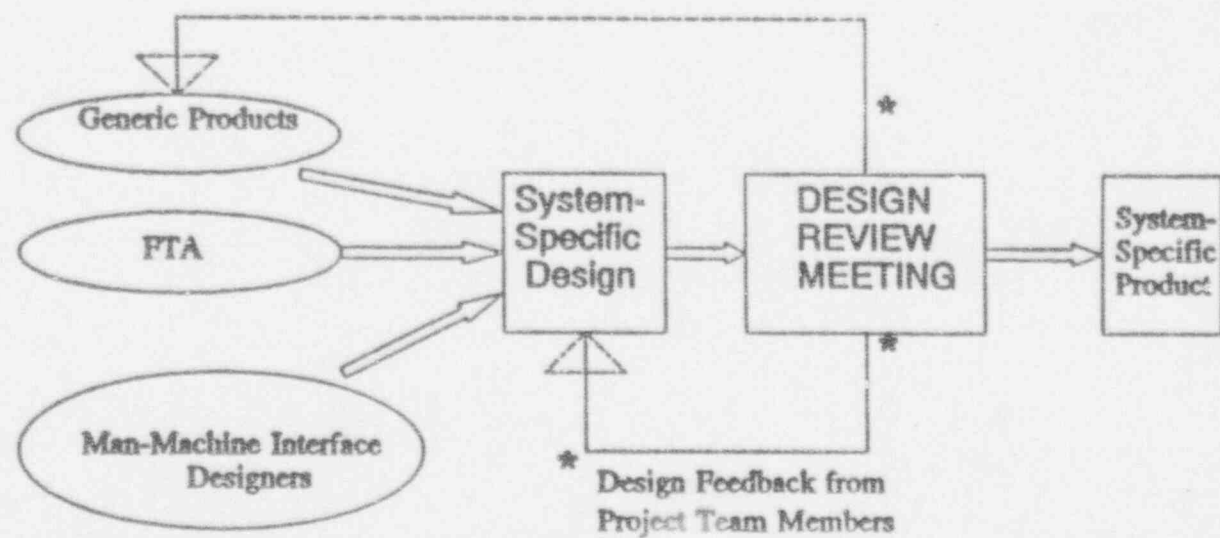
2.4 - INFORMATION PRESENTATION AND PANEL DESIGN EVALUATION

The information presentation and panel design evaluation, as documented in CESSAR-DC, the RCS and CVCS panel design reports, the Control Complex Information Systems design description (RDD vols. 5 & 6) and the SGB, has been completed for a reference design for the RCS panel and is being implemented on other panel designs for Nuplex 80+. This evaluation developed standard information and control methodologies and implemented them in panel design, based on the results of FTA. This evaluation practice will undergo additional iterations as it continues to be applied throughout the Nuplex 80+ design.

With the Nuplex 80+ HSI design philosophy as a starting point, methods were developed through evaluation of alarm, display, and control techniques (Figures in Section 1.2 illustrate this process.) This led, simultaneously, to establishing panel design criteria, and allocating information requirements to alarm, display, and control methodology. At this stage, information and control requirements from the FTA were a major input, leading to the development of information processing algorithms (algorithmic rules that relate plant data to information displays). The criteria and algorithms led, along with configuration of panel arrangement, to the design of the Nuplex 80+ control panels. Generic products resulting from this evaluation were:

- processing algorithms for raw data
- panel design criteria
- generic design documents (e.g., the SGB; and the CFM, Information Systems, and the Alarm Processing descriptions)

These products are re-evaluated on an as-needed basis during the detailed layout of subsequent control panels, and are re-verified if design changes are made or new techniques or hardware are introduced. Preceding such analysis, however, engineers and designers define and justify their proposed methods, which must then submit to the DRM process described in detail in Section 1.3.1.2 of this plan. Figure 2.4-1 illustrates the process.



Generic to Specific Design Process
Figure 2.4-1

2.5 - VERIFICATION AND VALIDATION

The purpose of Verification and Validation (V&V) is to demonstrate adequate operator task performance capabilities and the capacity to perform necessary functions in the MCR and RSA (and local control stations specified in the EPGs). Verification consists of steps necessary to review and evaluate the design adequacy of the elemental parts of the HSI design. Validation consists of an evaluation of the collected HSI design for dynamic, interactive sufficiency. (See Sections 6.4 & 6.7 concerning future V&V.)

The design team has analytically verified Availability and Suitability for the RCS panel design, as documented in the Verification Report (in the Reference Design Documentation). It is planned to pursue the same verification methodologies and provide similar levels of documentation for other control panel designs (see Sections A-3.6 for Availability requirements, and A-3.7 for Suitability requirements). Availability will be based on the procedure guideline input and task analysis data (see Sections 2.1 and A-3.4 on Task Analysis). Suitability will be based on the HSI design guidance in the SGB (see Section A-3.5 on HSI design).

In general, validation examines combinations of features, functions, and components or collective performance; initially for system refinement, finally to demonstrate system sufficiency. Specific Design Validation activities (Section A-3.8) examine the dynamic use of panel functions, yield subjective operator inputs and evaluation, and demonstrate the acceptability of required crew sizes and the executability of their required operations tasks using the design ensemble.

Design Validation will use a multi-phase approach to evaluate successively more complete subsets of the MCR ensemble, to ensure integration of the final result. These phases will consist of:

- 1) Initial validation work performed as the required component panels of the full-scale, partially dynamic Nuplex 80+ mockup are completed (e.g., MCC one-person operation can be validated before the Auxiliary and Safety Consoles are complete.)
- 2) Preliminary validation performed on the Integration Test Facility, to assure sufficiency of the final design.
- 3) Final Design Validation (see Sections 5.7 and A-3.8) performed on high-fidelity simulation facilities prior to operation, to demonstrate final design acceptability.

2.6 - ALARM ANALYSES AND EVALUATIONS

A number of power industry studies of plant alarm and annunciation systems were used as contributing material in the development of the Nuplex 80+ alarm system. Based on these, and the existing System 80 alarm systems, an evaluation of potential alarm system HSI features was performed for the Department of Energy, as part of the Advanced Instrumentation and Control Milestone B work. During the course of this work, various NRC and nuclear industry guidelines on alarm systems were reviewed. Below is a listing of some of these studies and the data they provided to the initial Nuplex 80+ alarm scheme:

EPRI-NP-3448: Provided list of problems with current schemes and data on prioritization definitions.

NUREG/CR-2776: Provided alternatives for advanced alarm display systems.

NUREG/CR-2147: Provided recommendations for solving 'classic' annunciator and alarm system problems.

NUREG-0700: Provided guidance on VDT displays, desirable alarm features, HSI characteristics (such as color, response time, etc.), and prioritization.

NUREG/CR-3217: Provided details on short-term improvements which were possible for existing System 80 plants.

NUREG/CR-3987: Provided guidelines and information used by ABB-CE for an evaluation of computer-based alarm schemes.

NUREG/CR-4463: Provided guidance and prospective methodology for a test plan for evaluating annunciator systems.

EPRI Alarm Seminar (MPR Associates, 1988): Provided bases for incorporating spatially dedicated alarms into the design.

Based on these studies, the team began Nuplex 80+ alarm system design and proceeded according to the design process described and illustrated in the other sections of this program plan.

It is important to understand that in the Nuplex 80+ alarm scheme, the alarm system is not actually necessary for accident mitigation, safe shutdown, or the successful

performance of the operators' safety and accident mitigation roles in other design basis operating scenarios. Hence, it is a non-safety system and provides what is essentially a monitoring support function. Consistent with this philosophy, the emergency procedure guidelines require no action to be taken in response to alarms and as a result, the alarm system is excluded from the FTA process.

2.7 - HALDEN REACTOR STUDIES

In 1986-88, a number of studies were performed at the Halden reactor and its simulation facilities, located in Norway. These studies and evaluations provided important input to the design of the Integrated Process Status Overview (IPSO, i.e., the big screen 6' x 8' display above the MCC), the Critical Functions Monitoring (CFM) feature, and the Success Path Monitoring function (SPM). What follows is a brief description of these studies and how they influenced the development of the Nuplex 80+ HSI design.

2.7.1 - CFM

In 1987, a study was performed at the Halden reactor facility to validate the concept of Critical Functions Monitoring on a PWR simulator. Full details on the study may be found in Volume 10 of the RDD. Simulator tests were run and it was concluded that the CFM function, which provides on-line assessment of the status of critical functions, is a valuable tool to reduce operator error, especially in conjunction with success path monitoring. This led to a decision to implement a similar CFM feature in the System 80+ design.

2.7.2 - SPM

The Success Path Monitoring feature for System 80+ is intended to be an advanced computer-based operator support function which provides an on-line assessment of the status of both availability and performance of success paths that mitigate challenges to critical functions. A prototype version of the system was developed and tested at the Halden reactor PWR simulator. The HSI was evaluated by having experienced operators cope with a series of realistic simulated transients.

Operator performance was evaluated to judge the efficacy of different information presentation systems. Operators' response times and accuracy were measured and comments were recorded. The results indicated the advantages of SPM in allowing the operator to better detect and correct success path problems before they impinged on critical functions. Based on the results of these studies, a similar SPM feature was included in the System 80+ design.

2.7.3 - IPSO

As part of an evaluation of whether to provide operators with an overview of plant status, and a determination of the best display method for this information, ABB-CE

participated in a study at the Halden reactor PWR simulator in 1986-7. IPSO was evaluated for the adequacy of its HSI in a series of studies which included experienced operators and simulations of three different phases of operation (selected to represent different task loading situations).

Subjects evaluated IPSO's use during normal and abnormal operations, as well as aspects of its HSI such as content and format. Further study investigated the use of IPSO as a focal point for decision making. Results of the studies supported the usefulness of a large-screen plant overview display. Based on these results, the design team elected to include a large screen display in the Nuplex 80+ control complex design, and modified the form and content of the display in response to user comments.

2.8 - SUMMARY

Reference design work from previously licensed and operating System 80 plants has been used as the basis to determine:

- allocation of functions
- information and control requirements
- generic operating sequences
- selection of control devices

Generic industry references and applicable NRC documents provided further input to the project design philosophy and HF guidelines. Industry alarm studies and Halden reactor studies contributed to the design of the IPSO, CFM, SPM, and the Nuplex 80+ alarm system. Operating experience from Duke and System 80 plants has influenced control complex layout, information and control requirements, and task sequences which were developed. Functional task analysis has provided direct input to panel layouts by elucidating relationships between controls, indicators, and the functions the panels must perform. As such, it has also served as an input to staffing and configuration evaluation, information presentation, and panel design analysis. Conceptual design bases have been founded on both FTA results and a priori judgements based on design reviews, knowledge of hardware, aforementioned operating experience, and input from a multi-disciplinary design team.

3 - HUMAN ENGINEERING OF HSI AND EQUIPMENT

Human Factors of detailed equipment design has been and continues to be a major part of the design team's human engineering efforts. Control room interfaces that make up the HSI include the IPSO, alarms, discrete indicators, process controllers, data processing system VDTs, and component controls. Equipment to provide these interfaces include one big screen display and a combination of VDT screens, electro-luminescent touch screens (flat panel displays, henceforth referred to as ELDs), and pushbutton controls (henceforth referred to as switches). What follows is a description of the evolution of the interface from functional design goals, with a description of design rationale. The design goals are not intended to be testable criteria with clear dependent variables but were intended instead to be objectives for the system designers and human factors engineers as the Nuplex 80+ design developed. Why particular pieces of hardware were chosen is also briefly explained.

3.1 - INTEGRATED PROCESS STATUS OVERVIEW (IPSO) DISPLAY

The IPSO, which currently uses a six foot by eight foot rear projection display, presents Critical Functions, and Success Path availability and performance status. It evolved in response to the general concern that information presented on separate, small-format devices could prevent the operators from getting an overall "feel" of plant performance, and that VDT displays could cause disorientation or narrowing of attentional focus. IPSO provides an overview to operators in the controlling workspace, continuously offering "the big picture" at a single glance. It is also visible from the Shift Supervisor's office and the Technical Support Center, so that those not directly controlling the plant but still possessing a need for high-level plant status data, can obtain the information quickly without interrupting controlling workspace activities.

The IPSO information format also exists as a display page available on all of the DPS screens in the control room and at remote facilities such as the Emergency Operations Facility. Thus, although the big board display is located behind the MCC workstation, IPSO information is widely available to maintenance and supervisory staff, visitors, and engineering personnel.

Design goals for IPSO included:

- Reduce the quantity of information to an easily understood and recognized amount;
- Provide a single location for quick assessment of key information indicative of critical power plant production and safety functions status as well as major success paths;
- Compensate for a reduction in dedicated displays by allowing a 'feel' of plant conditions, thereby promoting a critical functions rather than a systems orientation;
- Compensate for reduced staffing by providing an overview while doing detailed diagnostic tasks;
- Be viewable to not only control room operators but also Control Room and Shift Supervisors and staff in the emergency facilities.

Design basis rationale for IPSO included:

Large Screen: The Halden evaluations showed that a large screen display was preferable for monitoring and obtaining information quickly.

Level of Detail: The Halden studies also showed that highly processed information, not raw data, was preferred by users.

Spatial and Serial: Design reviews showed that spatial and serial information were best left on the panels.

IPSO uses the same criteria for display design and format as the VDT display pages (see CESSAR-DC Section 18.7.1.1); however, additional criteria are applied in order to focus and limit information included at the IPSO level (see Section 18.7.1.2.2).

The IPSO HSI was empirically evaluated through visits to hardware vendors, trying out different mounting methods and projection techniques, and application of human factors references to determine light intensity, ambient conditions, display size, and similar factors. Rear screen technology was found to interfere least with other control room tasks. A slightly tilted screen and black bezel were found to enhance viewability at all viewing locations.

3.2 - DPS VDT DISPLAYS

Every panel in the Nuplex 80+ control room has at least one DPS VDT display (some have two). In addition, DPS displays are provided in the Technical Support Center, Remote Shutdown Panel, CRS console, the Operator's office, the Shift Supervisor and CRS office, and the Emergency Operations Facility. Screens are currently envisioned to be 19 or 20 inch diagonal full color monitors which employ touch-screen CRT technology for the operator interface.

VDT pages represent the best method of presenting DPS plant information, which is available to the operator in a structured hierarchy. There are three levels of displays plus the IPSO overview. Among the functional design goals for the DPS VDT displays were:

- Provide all information required for following operating procedures within three levels of hierarchical depth (Level 1, monitoring; Level 2, controlling; Level 3, diagnostic);
- Assure an HSI that is consistent with other control room hardware and internally among display pages through the use of an information systems description document and the SGB;
- Functionally consolidate information traditionally scattered across recorders, meters, status lamps, etc. in one location;
- Provide alarm mapping and access categorization to support alarm acknowledgement and understanding through the VDTs.

Details on paging, menus, etc. may be found in Section 18.7.1.3 of CESSAR-DC.

Touch screens were chosen for the VDTs and ELD displays in order to focus operator attention and save the excess panel space which keyboards or trackballs would have required. Additionally, touch screens make use of the human inclination to point directly without these input devices. Touch screens allow the menu itself to be used for accessing and manipulating the system, which cuts down on page clutter, and allows more useful integration of menus and touch areas into the display format. Additional rationales for the DPS display format includes the ability to provide:

- Extensive details within meaningful context;
- Integrated presentation of analog and digital data;
- Integration of SPDS and general display functions;
- Redundant availability throughout the Nuplex 80+ HSI;
- Two-touch access to any screen;
- Flexible and context-rich acknowledgement of alarms.

The design bases for the VDT screens may be found in the information systems document. hardware was selected to meet criteria in NUREG-0700 as well as NRC requirements for seismic category II. The useability of the VDT displays and the hardware, i.e., its adherence to human engineering principles, is assured through the systematic application of HFE design guidance, and HFE evaluation of the resultant design in V&V.

3.3 - ALARMS

Details on the characteristics of the alarm system for Nuplex may be found in CESSAR-DC Section 18.7.1.5. These design goals and rationale, as well as system evolution are discussed below without an attempt to fully describe all features associated with alarm and annunciation in Nuplex 80+.

Design bases for the alarm system were described in Section 2.6. Design goals for the alarm system included:

- Reduce the number of generated alarms and audible annunciators, to mitigate information overload and resulting stress during emergencies;
- Provide a meaningful and orderly framework of cues and information, to help operators direct their attention to items of greatest operating priority;
- Support quick assessment of alarms' implications for plant safety and performance;
- Provide reliable, intelligent data processing of alarm inputs;
- Assure useability of elemental alarm system features.

Design features and rationale employed to meet these design goals include:

- Mode Dependency eliminates nuisance alarms, reducing unnecessary loading;
- Annunciator significance mapping: alarms and operator aids are mapped to appropriate displays (e.g. IPSO, Alarm Tiles, or VDTs only) based on the categorical significance of the data;
- Momentary audible indications of new and cleared alarms reduce auditory distractions;
- Spatial Dedication for the most significant alarms reduces search and processing time;
- Grouped alarms provide specific messages for plant conditions;
- Critical function alarm setpoints are tied to emergency operating procedures, integrating HSI directly with EPGs.

3.3.1 - Alarm Tiles

Some alarms are presented on VDT displays and/or the IPSO screen, based on the significance mapping feature. All alarms which appear on the dedicated alarm tile displays are based on alarm prioritization, a three-level scheme developed per NUREG-0700 and EPRI NP-3448. Originally, alarms defined as priority one or two were selected for display on the spatially dedicated alarm tiles but verification of design has led to a more functional approach to this aspect of HSI development.

Alarm inputs are now selected for display on the alarm tiles based on their relation to significant operator action conditions. Alarms which can result in this type of operator action, even if the prioritization system classifies them as priority three, will be displayed on the alarm tiles. The alarm presentation scheme and significant operator action conditions are discussed in the alarm processing document.

A description of the hardware rationale for the alarm system may be found in Section 3.6

3.4 - DISCRETE INDICATORS

Discrete indicators, along with the alarm displays, form the human-system interface of the Discrete Indication and Alarm System (DIAS). Discrete indicators differ from process controllers in that they do not provide the ability to control plant parameters from their screens. Control on DIAS displays is limited to the ability to page between related data on the discrete indicators and the ability to page through levels of alarms on the alarm screens.

The discrete indicators are an evolutionary successor to both analog and digital meters, and strip chart recorders. Design goals for the discrete indicators' HSI were:

- Provide a validated list display of all Reg. Guide 1.97 Category I variables;
- Provide information to allow continued operation without the DPS, including
 - a) tech spec monitoring for < 24 hr surveillances
 - b) info needed to assess personnel hazards & equipment damage
 - c) Reg Guide 1.97 Category 1 and 2 parameters not already on single parameter displays
- Provide key parameters used to assess success path performance, and status of critical power and safety functions;
- Provide access to individual sensor channels used in process representation values to allow continued operation without the DPS available;
- Provide continuous display of all SPM and CFM monitored plant data;
- Reduce the quantity of data which the operator must process in order to minimize information overload;
- Provide simple access to support data (e.g., Tech Spec and Reg Guide 1.97 information);
- Afford use of same spatially dedicated displays for normal and post accident monitoring, to ensure familiarity;
- Provide reliable, intelligent data processing;
- Provide automatic range changes as appropriate to plant situation;

The following design decisions and rationale were employed to satisfy the design goals:

- Spatially dedicated displays were chosen to reduce time to access information and improve familiarity of the HSI;
- Analog and digital information (e.g.-trends and numeric data) are presented together, replacing disintegral arrays of recorders and meters;
- Multiple channels of redundant data receive algorithmic validation and aggregation into single process information values, thereby reducing the number of displays and unnecessary manual information processing;
- System is designed so that PAMI indications are in routine normal use;
- Indicator availability and suitability meet HSI portions of Reg Guide 1.97;

In hardware considerations, the discrete information was considered for mainly VDT presentation in ABB-CE's earlier Nuplex 80 (as opposed to 80+) design. However, discussions with operators, task analysis results, and the design review process convinced Nuplex 80+ designers of the operational advantages of spatially dedicated displays. For a discussion of hardware used for discrete indication, see Section 3.6.

3.5 - PROCESS CONTROLLERS

Process controllers, located in the benchboard section of the control consoles, provide the operator with the ability to automatically or manually control plant process loops, such as closed loop controllers. As such, they represent an evolution from the traditional hardwired Manual/Auto (M/A) station found in conventional control rooms. Functional goals for process controllers were determined based on operating experience and an examination of workload, suitability, etc. in the RCS panel task analysis and subsequent verification. Resultant goals included provision of:

- A full range of functions as provided by conventional Manual/Auto stations (e.g., setpoint control, mode control, display of range and channel, current parameter value, etc.).
- A familiar HSI based on the operating conventions of traditional hardware;
- Digital display of value;
- Flexible access to multiple control loop subfunctions;
- Format, method of operation and human factors conventions consistent with the rest of the HSI

The following rationale and decisions were included in the design of the process controllers, in order to meet the design goals:

- The HSI was chosen to mimic the function and operation of conventional M/A stations;
- Master and subcontrollers for a process are integrated on one module to facilitate operation
- Controllers were located near appropriate indicators to enhance useability;
- Controls were separated from discrete indicators and DPS displays to assure operator control actions would be deliberate;

A discussion of the hardware used for process controllers may be found in Section 3.6.

3.6 - FLAT-PANEL DISPLAY HARDWARE

There are three basic types of flat-panel displays used in the main control complex: alarm displays, process controllers, and discrete indicators. A brief discussion of common features and why this technology has evolved for these portions of the Nuplex 80+ HSI is presented here.

Flat-panel technology was chosen to meet functional design goals of display clarity and reliability as well as the ability to purchase off-the-shelf, qualified displays from a number of sources. The current displays are not color, but do provide high contrast. They employ the same HSI conventions as the rest of the control room hardware. The use of color as only a back-up or secondary coding method for information on the VDT displays assures a one-to-one mapping of data coding and format techniques between the ELDs and the VDT displays.

The traditional analog indicators and hard-tile alarm systems have been superseded by flat-panel technology to consolidate volume and improve functionality of the HSI. A major design basis concern has been to maintain a familiar HSI, while incorporating technological improvements to reduce unnecessary information, unwieldy panel sizes, etc. This hardware allows ABB-CE to retain the advantages of spatial dedication in the design while still greatly reducing the overall volume of indicators and controls in the controlling workspace.

3.7 - COMPONENT CONTROL

Momentary activation-type switches, used for component control, comprise the last major HSI component type for Nuplex 80+. These controls look and feel like conventional hardwired legend switches. In size, resistance, luminance, and other HSI features, they adhere to the human factors standards of NUREG-0700, MIL-STD-1472D, EPRI NP-3659, and similar industry guidance. However, these are modular devices, that employ fiber optic multiplexing to their component control systems. Their use simplifies both construction and maintenance, permitting on-line replacement of the switch unit, and bumpless transfer of control (both avoiding needless errors). Fiber optic multiplexing also dramatically reduces the amount of panel and floor cabling required.

Types of components controlled from these switches include valves, pumps, breakers, dampers, fans, heaters, and sprays. In addition, a similar hardware type (but separately labelled and color-coded) pushbutton may be found on every panel section for lamp test. Design criteria used to identify components that should be controlled from momentary activation switches included that:

- The component is in the main flowpath of a success path;
- The component bears no relation to any process controller.

After review of reference design (i.e.-the baseline System 80 design and its evolution through Nuplex 80) and the regulatory requirements for control, the design team interviewed experienced commercial and navy PWR operators. Functional task analysis and a review of the control requirements and list of tasks and subtasks convinced the designers to employ an evolutionary approach with some momentary activation switches, for critical operating paths based on task sequences from the Emergency Procedure Guidelines. Newer technology was used to improve some aspects of the HSI while maintaining a technology of proven reliability and acceptability.

Main resulting design features were:

- Maintain conventional HSI aspects to avoid negative transfer of training, and enhance operator acceptance;
- Utilize functional mimic layouts to integrate switches into control panel schemes;

- Locate switches, like process controllers, separate from indication-only devices to assure operator control actions would be deliberate;
- Maintain compatibility and consistency with the coding, symbols, and terminology of other features of the Nuplex 80+ HSI.

4 - MAINTENANCE, PROCEDURES, AND TRAINING

This section presents the philosophy and general approach for major adjunct aspects of the System 80+ design, and explains their treatment and integration with the overall human factors program and its activities.

4.1 - MAINTENANCE

Maintenance considerations have been a continuous influence on the design of the System 80+ HSI. Maintenance-related human factors were considered in the Nuplex 80+ design through the application of industry guidance (e.g.-DOE HF Design Guidelines for Maintainability-DE 85 016790), MIL standards, operating experience, and maintenance technician input. Based on these evaluations and the team's design review process, the maintenance goals for hardware were developed. The repository for the human factors goals for maintenance is the Human Factors Engineering Standards, Guidelines, and Bases document. It is out of the scope of the program plan to list the maintenance goals and rationale pertaining to human factors. However, representative examples are provided below, at a generic level, to aid in evaluating the human factors program:

- The HSI is designed to facilitate maintenance activities while minimizing the disruption of operations;
- Equipment is off-the-shelf, preferably from more than one vendor, to reduce replacement time and interruption of operations;
- Equipment replacement at control panels is 'front-access', to reduce maintenance time;
- Information and control capabilities in Nuplex 80+ have sufficient redundancy and diversity so that panel maintenance does not preclude necessary operations.

4.2 - PROCEDURE DEVELOPMENT

For a standard plant design such as Nuplex 80+, most of the technical information required for procedure development exists prior to the site-specific construction process. This material permits design validation of the control complex to be performed prior to the completion of final, formatted procedures. In addition, it eliminates the translation of generic into plant-specific procedure

guidelines per NUREG-0899 (Figure 4.2-1), thus simplifying the procedure development process (Figure 4.2-2).

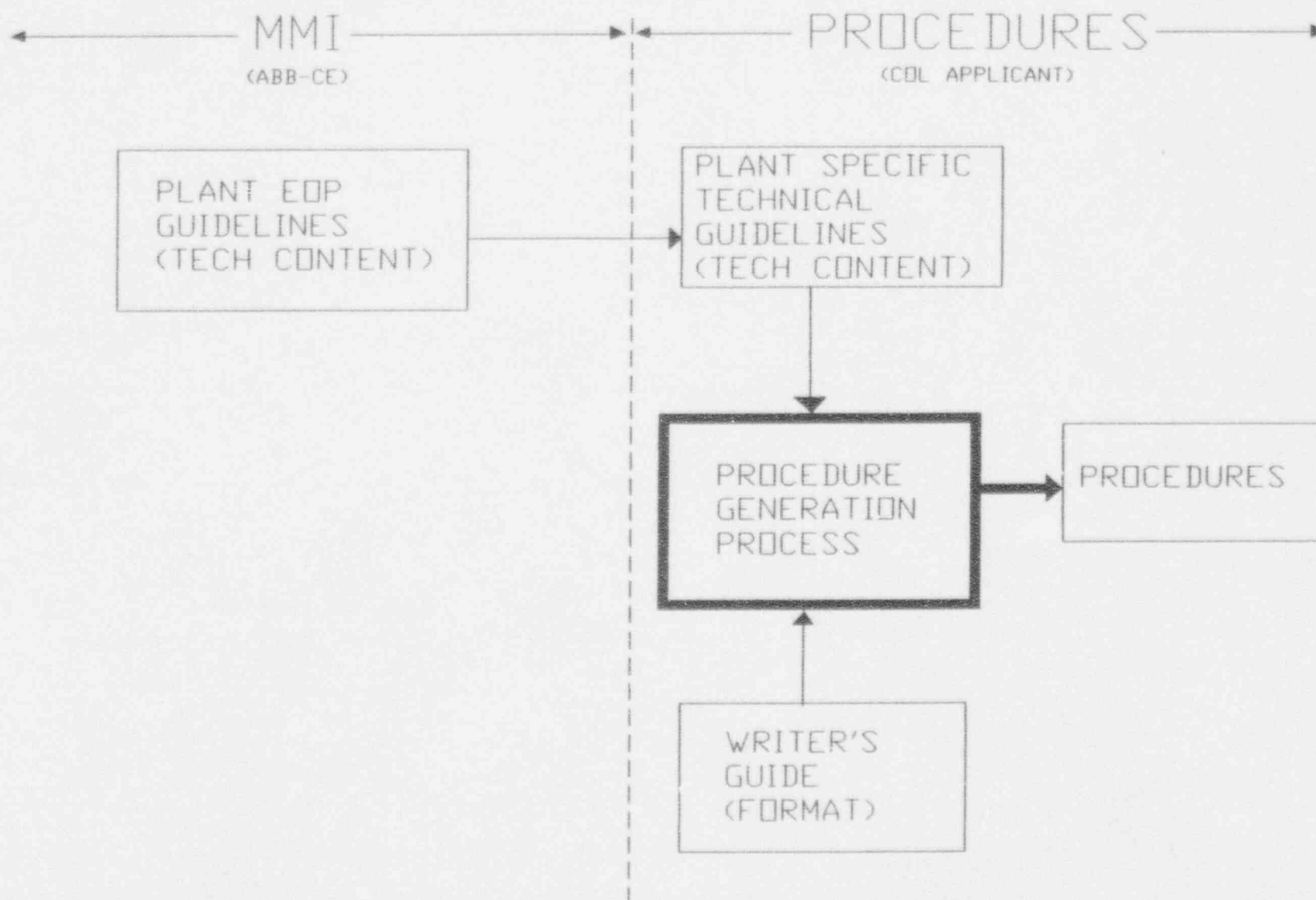
The combined design and procedure development processes are shown in Figure 4.2-3. Procedure development is a COL Applicant responsibility which is detailed as a COL Action Item in Section 13.5 of CESSAR/DC. Technical guidance and bases for procedure content are developed by ABB-CE, and provided to the COL Applicant (in System 80+, via OSIP) as input to the procedure development and training programs. A standardized procedure format (i.e., a writer's guide incorporating human factors) is developed by the COL Applicant. For each procedure, acceptable content and format are verified as part of the COL Applicant procedure development program. Procedure development activities are governed by separate requirements (10 CFR 50.34(g)(3)) and regulatory review processes (NUREG-0899), and are covered under NPOC Building Block 7. Thus, final procedure development is outside the scope of the ABB-CE Plan.

Procedure guidelines are still required by the Plan for use in Task Analysis (A-3.4), Availability Verification (A-3.6), and Design Validation (A-3.8) activities. Feedback from these analyses to procedure guideline development will be provided through the formal review of analytic results. Identified issues will be tracked to resolution (A-3.1.2.4). Thus, procedure guidelines will be utilized in design and evaluation of the HSI, and coupling of the design and HFE analyses to the procedure guidelines is assured.

Although procedure development is not managed by the Plan, several steps have been taken to provide direct links from the System 80+ design process to the COL Applicant procedure development process. Event scenarios, acceptance criteria, data and results of the Nuplex 80+ design validation will be provided to the COL Applicant for use during the operating ensemble validation using "final" plant-specific procedures. The HFPP requires these and other human factors products to be delivered to the COL Applicant through OSIP (A-3.1.2.5, A-3.8.2.4). Thus, integration of the control room and operating procedures is assured, and the intent of Element 7 (Plant and Emergency Operating Procedure Development) of NUREG-5908 is met.

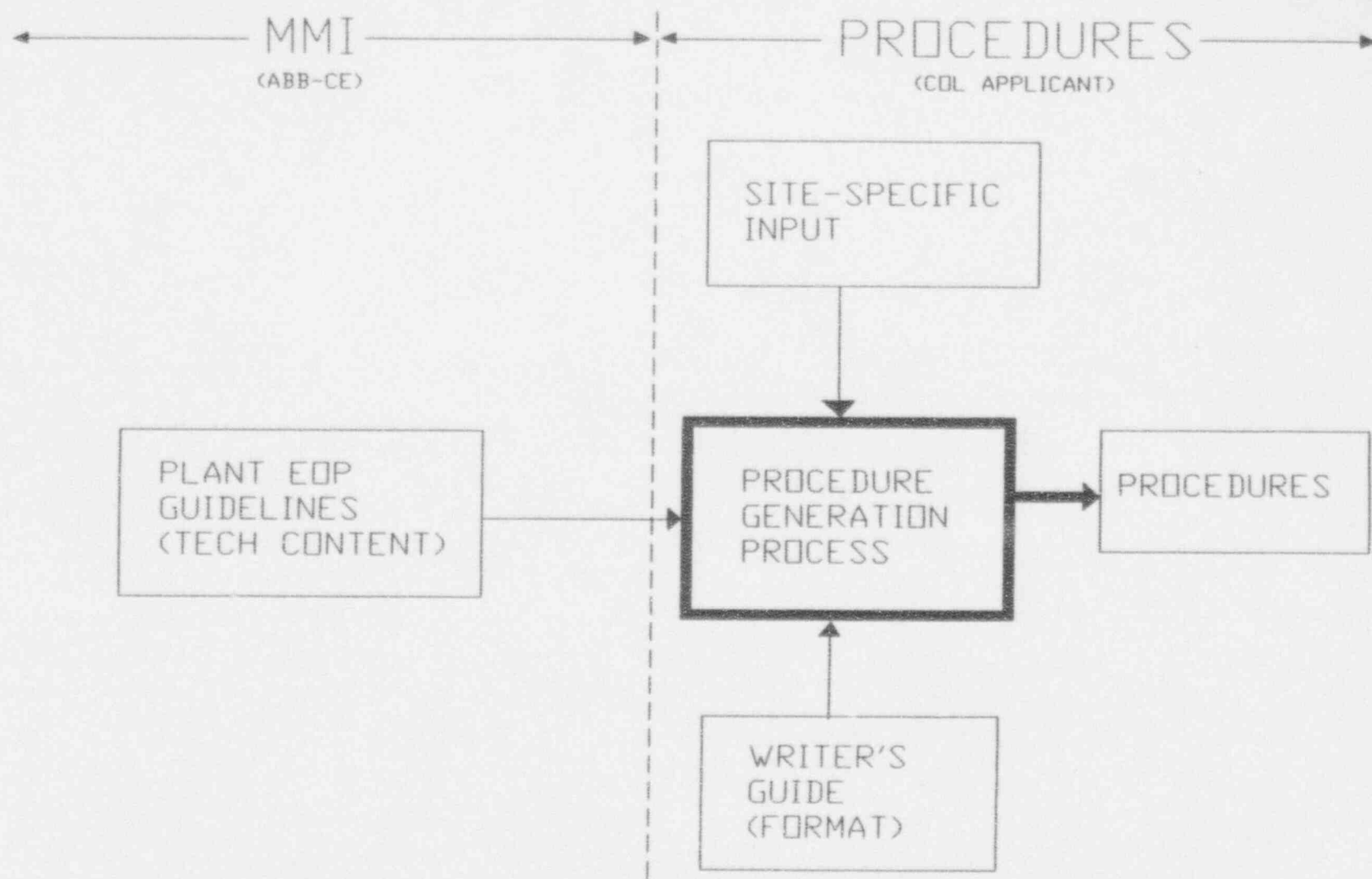
4.3 - TRAINING DEVELOPMENT

Like procedure development, training of operators, maintainers, and other personnel is not part of the design certification HF program. Training is handled by COL Applicant programs and specialists in these areas. Training



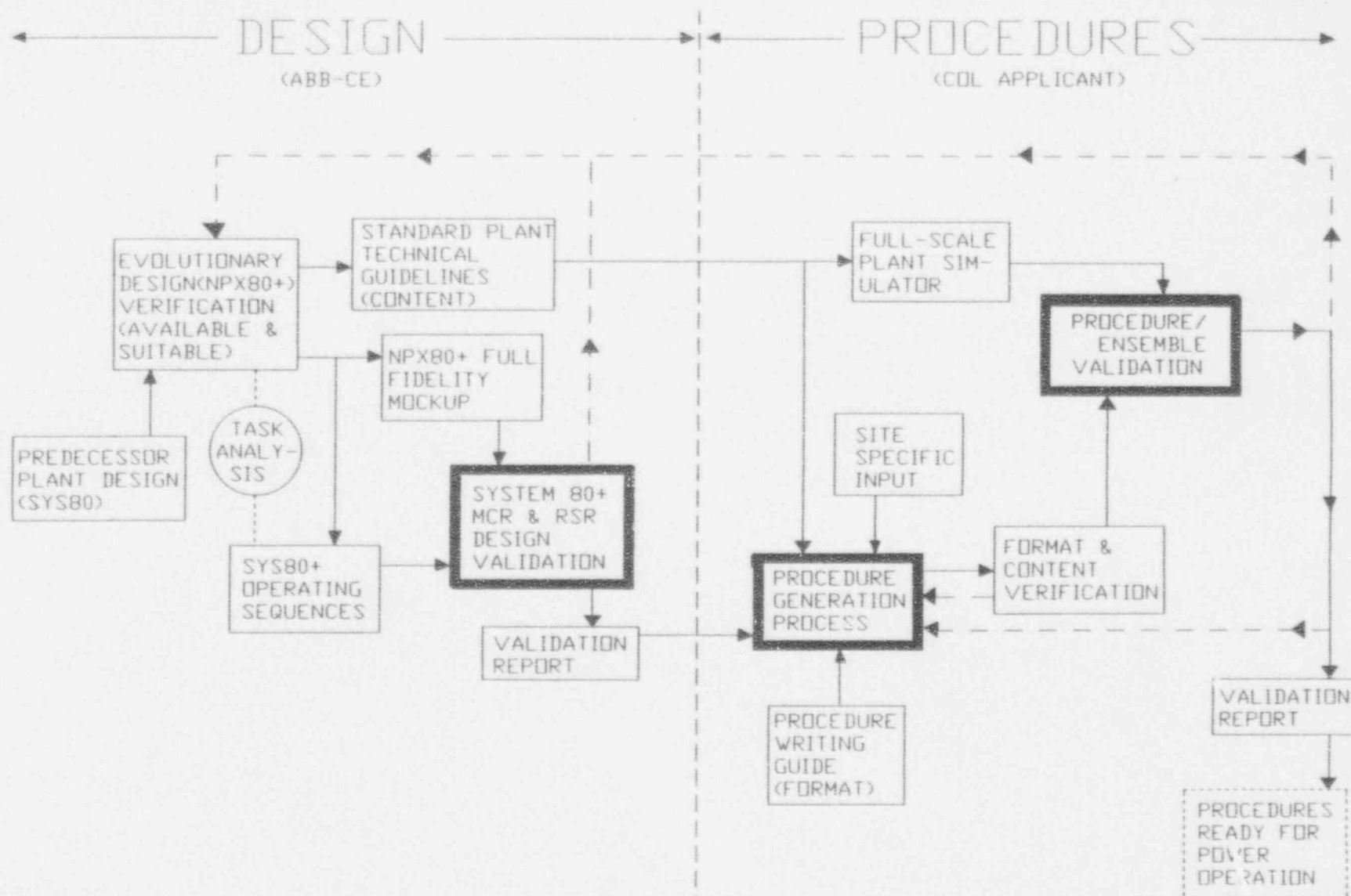
EOP Development Process (NUREG-0899)

Figure 4.2-1



Procedure Development Process
for Nuplex 80+ Standard Plant

Figure 4.2-2



DESIGN & PROCEDURE VALIDATIONS

Figure 4.2-3

will be based on the entire design and the nature of the tasks involved, not merely on human factors. Vendor task analyses and procedure guidelines, will be provided as an input to operator training development. However, training development and delivery are not managed under the HFPP.

5 - FUTURE HUMAN FACTORS ACTIVITIES

In addition to the ongoing interdisciplinary design process described in the earlier sections of this plan, a number of specific human factors activities and analyses are planned as the design of the System 80+ HSI progresses. This section contains a brief explanation of these activities to enhance understanding of what is planned. Refer again to the figures in Section 1.2 for an understanding of the integrated design process. This process is similar to that outlined in IEEE-1023 and a comparison between Figures 1.1-2 through 1.3-6 and the design process figure of the IEEE document provides a useful insight into the relationship between the generic (IEEE) design process and that pursued for System 80+.

5.1 - FINAL HUMAN FACTORS STANDARDS, GUIDELINES, AND BASES

A complete, design-specific version of the Nuplex 80+ HFE Standards, Guidelines and Bases (SGB) is provided for System 80+. The SGB affords all designers and evaluators on the team with a controlled compendium of human engineering information to assure a standardized HSI across the project. The bases include source materials from which the guidance was culled, and justifications for design-specific implementations, to support tradeoff evaluation (see Section A-3.5, HSI Design).

5.2 - FULL SCALE MOCKUP ACTIVITIES

The use of mockups of control panel arrangements, a key step in human factors design efforts, is an ongoing process for the Nuplex 80+ design. Currently, a static, full scale MCR panel arrangement exists. Actual layouts on these panels are not yet done, though efforts are ongoing. This static mockup will provide a location for future analyses and a basis for design reviews pertaining to board layouts.

A dynamic Nuplex 80+ mockup currently exists for the MCC and one SC panel. This mockup contains functioning VDTs plus some DIAS displays, switches, and process controllers. Some controls on this mockup are static representations and the layouts are not final. This mockup serves as an evolving demonstration and design tool for the HSI (see Section A-3.5, HSI Design). Future work includes further evaluation and testing of the hardware and layouts, and upgrade of the static portions of the mockup to a more dynamic version for preliminary design validation (see Section A-3.8).

5.3 - PROTOTYPING AND PROGRAMMABLE FEATURES

As the work on the dynamic mockup progresses, the current VDT and Switch hardware, as well as the IPSO undergo continuous prototyping. New display features and hardware are implemented and evaluated for performance and useability. The Nuplex 80+ Information Systems Description Document, prepared by human factors specialists on the design team, is used by prototype designers to implement the human engineering aspects of display screens. Future iterations and improvements will incorporate the results of relevant analyses into the integrated design.

5.4 - VERIFICATION ACTIVITIES

Described as part of the test and evaluation plan, it is important to further note that verification activities are an ongoing process. Additional verification on subsequent panels and features will be performed following Certification, as part of the ITAAC processes. Some design goals of this future verification work include:

- Comparing information and control requirements to actual inventory
- Identifying missing or superfluous controls and indicators
- Ensure final design details are compatible with SGB

Basically, this activity will be the panel by panel verification of Availability (A-3.6) and Suitability (A-3.7) as generally described in Section 2.5.

5.5 - FURTHER TASK ANALYSIS

The task analysis process described in the FTA report for Nuplex 80+ (See Section 2.2) will be continued to completion. Each panel section of the control complex (MCC and RSA) and all local control stations required by emergency procedure guidelines will be subject to analysis, and the results incorporated in the task analysis database prior to detailed design. Task analysis requirements are provided in Section A-3.4. Current task analysis methodology is presented in Section 18.5 of CESSAR-DC.

5.6 - STATIC MOCKUP EVALUATIONS

A phase of future HF evaluation activities which was not envisioned in the original design is the evaluation of the HSI at a full-scale static mockup of the Nuplex 80+ controlling workspace. The static mockup is being developed for Nuplex based on human factors rationale as described in EPRI-NP-2411 (final chapter). As such it provides a venue for human factors analyses and evaluations and an ability to rapidly an inexpensively prototype candidate arrangements of the HSI. Activities which are planned for the static mockup include:

- traffic and motion evaluations
- evaluation of the anthropometry of the HSI
- verification of useable control panel layouts based on task sequences (operator walkthroughs)
- evaluation of candidate control panel arrangements
- preliminary design validation exercises

The availability of the static mockup in a much earlier stage of the design than the integration test facility will assure that these evaluations can be performed before a stage in the process when it is extremely difficult to make design changes. Further, since full panel layouts are not needed to evaluate traffic and motion or anthropometry, some portions of the static mockup evaluations can begin prior to detailed panel layout work.

5.7 - FINAL DESIGN VALIDATION ACTIVITIES

Final human factors testing for the Nuplex 80+ control complex is the Validation of the HSI design (Section A-3.8). These exercises will utilize procedure guidelines, safety and transient analysis-based operating sequences, and high fidelity dynamic facilities to demonstrate the integrated usability of the HSI design for the execution of plant operations tasks. Findings from this analysis will be resolved so that the standard plant technical guidelines accurately reflect the HSI design, and the design meets acceptance criteria. Following the resolution of the design Validation findings, the design will be considered to be complete, and will provide the necessary environment for operating ensemble Validation by the COL applicant (see Section 4.2). Subsequent changes to the software-based HSI by the COL Applicant can be easily executed, if desired.

6 - SCHEDULE

The HFPP outlines how ABB-CE satisfies HFE design 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 phases 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.

6.1 - DESIGN CERTIFICATION ENGINEERING

The following activities/deliverables are performed and the results submitted prior to certification:

- Halden Evaluations (IPSO, CFM, SPM); Industry Alarm Evaluations (Figure 1.3-2)
- Operating Experience Review (Figure 1.3-3)
- Evaluation : Allocation of Systems' Functions Report (Figure 1.3-3)
- Mockup of exemplar panel & standard features (Figure 1.3-4)
- HF Program Plans & Requirements (Figure 1.3-5)
- Staffing and Configuration Evaluation (Figure 1.3-5; CESSAR-DC 18.7.6)
- Task Analysis Methodology (& exemplar RCS Panel FTA report; (Figure 1.3-5)
- HFE Standards, Guidelines, and Bases Document (Figure 1.3-5)
- Availability & Suitability Verification Methodologies (& exemplar RCS Panel analysis report; Figure 1.3-5)

6.2 - FIRST-OF-A-KIND ENGINEERING

The following activities are performed during First-Of-A-Kind (FOAK) Engineering:

- Task Analyses of additional panels (Figure 1.3-6)
- Prototyping & mockups of additional panels (Figure 1.3-6)
- Availability & Suitability Verification of additional panels (Figure 1.3-6)

6.3 - MANUFACTURING AND PROCUREMENT

The following activities are performed during Manufacturing and Procurement (i.e., prior to Startup testing):

- Validation of control center ensembles (Figure 1.3-6)
- Final closeout of tracked HFE items (Figure 1.3-6)

7 - CONCLUSION

This program plan has provided an overview of human factors engineering activities for the Nuplex 80+ Advanced Control Complex and the overall System 80+ standard plant design. Past, current, and future activities have been described and references provided to project documents which provide further details.

An effort has been made to describe the entire human engineering program, identify its elements, and explain how they are managed. Thus, it provides a partial basis for review of progress as well as that of product. The program plan provides information to show how and when ABB-CE has satisfied or will satisfy all human factors performance, design and program requirements specified by the regulatory agency.

It has not been possible to plan to a detailed, month-by-month schedule due to the commercial aspects of the design (i.e., to a great extent future schedule will depend on funding, both internal and external). However, wherever possible, the approximate timeline and the sequence or order which activities will follow regardless of the exact calendar date for the work has been shown.

New co-operation with Asian and European ABB entities and project participants will likely expand the available experience and expertise resources available in the future. For instance, prototyping assistance is being provided at this time from ABB-Atom in Sweden.

In summary, human factors is part of an integrated and wide-ranging design effort, but not the only driving force in the design. Nevertheless, human factors experts on the design team assure that an adequate HSI has been and will be maintained throughout the design.

Appendix A - Design Process Requirements and Criteria

DESIGN PROCESS REQUIREMENTS

TABLE OF CONTENTS

A-1	Introduction	
A-1.1	Summary.....	A - 3
A-1.2	Definitions.....	A - 4
A-1.3	Objectives.....	A - 8
A-1.4	Scope.....	A - 10
A-1.5	Method.....	A - 12
A-1.6	References.....	A - 14
A-2	Framework Description	
A-2.1	Design Process Elements.....	A - 16
A-2.2	Element Structure.....	A - 17
A-2.3	Element Products.....	A - 18
A-3	Element Descriptions	
A-3.1	HFE Program Management.....	A - 20
A-3.2	Incorporation of Industry Experience.....	A - 27
A-3.3	Evaluation and Allocation of System Functions...	A - 29
A-3.4	Task Analysis.....	A - 32
A-3.5	Human-System Interface Design.....	A - 36
A-3.6	Availability Verification.....	A - 40
A-3.7	Suitability Verification.....	A - 44
A-3.8	Design Validation.....	A - 47

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

A-1 Introduction

A-1.1 Summary

Appendix A states human factors-related goals, requirements, criteria, and bases for the Nuplex 80+ Human-System Interface (HSI) design process. These specifications have been developed based on similar industrial, regulatory, and military models. A design process that conforms to these specifications satisfies Federal Regulations and NRC Requirements, as well as the need for formal and systematic HSI design.

A-1.2 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 (Reference 9).

Bypassed and Inoperable Status of Safety Systems - Per Reg. Guide 1.47 (Reference 6).

Calendar-referenced - Use of specific, quantitative dates; compare to 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 detailed by Reference 9).

Design Process Elements (DPEs) - The eight functional units in which the design process requirements are organized.

Employ - To utilize in a responsible capacity.

Goal - Goals are the idealized functions of the eight DPEs.

HFE Design Guidance - Equipment and system design guidance (e.g., Chapter 6 of Reference 9) 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).

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

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.

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.

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 HSI systems, respectively, without regard for specific implementation.

Interdisciplinary - A philosophy which incorporates 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 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. The 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 HFE Specialists and/or Operations Experts in the process.

Nuplex 80+ - Nuplex 80+ refers collectively to the Main Control Room (MCR), the Technical Support Center (TSC), and the Remote Shutdown Panel (RSP).

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

Post-Accident Monitoring Indications - Per Reg. Guide 1.97 (Reference 12).

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

Requirements - The constituents that operationalize the DPE Goals, and thus pragmatically define the DPEs, based on applicable regulations from Reference 5.

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

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, as defined.

Schedule-referenced - The use of a relative, 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 denoting 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 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 9).

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

System 80+ - System 80+ refers to the entire plant including the Nuplex 80+ control complex, and all local control stations.

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

Technical Resources - Technical expertise (e.g., HFE Specialists) which the program is required to Employ.

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

Verification - Availability and Suitability analyses; part of process (along with Validation) by which HSI design sufficiency is confirmed (per Section 3.7 of Reference 9).

Validation - Evaluation of a dynamic operating ensemble to demonstrate trained users' ability to successfully perform their anticipated role (e.g., emergency procedures) in the afforded task environment (e.g., the control room design) under anticipated operating conditions (e.g., the Validation scenarios). Part of process (along with Verification) by which the HSI design sufficiency is confirmed (per Section 3.8 of Reference 9).

A-1.3 Objectives

The Code of Federal Regulations (CFR) includes Nuclear Regulatory Commission (NRC) regulations governing the design, review, and certification of nuclear power plants. As is true of the products of all engineering disciplines, 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) of Reference 5.

In particular, 10 CFR 50.34(f)(2)(iii) is the key regulation that explicitly 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 (not required, but for information only) to the post-TMI action plans for a Control Room Design Review (CRDR) process outlined in NUREG-0660 (Reference 7). The purpose of 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 (Reference 11), NUREG-0700 (Reference 9), NUREG-0800 (Reference 13), and NUREG-0801 (Reference 10). 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 design process requirements presented in this document.

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

One issue to emerge from the control room design review process for design certification is that fully detailed Human-System Interface (HSI) design information may not be available for review prior to certification. Thus, certification must be based in part on the approval of a design process. 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 Reference 13), a regulatory precedent and basis for such a review is not available. However, a satisfactory design process must include a sufficient set of analyses, requirements, and acceptance criteria to lead to a valid and certifiable design product.

This document provides guidance for the vendor organization to verify the adequacy of the design process, specifically in the context of evolutionary, pressurized-water reactor designs. The specific objectives of this effort are:

1. To identify a set of design process elements that are sufficient and practical requisites to the design of usable HSIs.
2. To specify requirements and acceptance criteria by which the adequacy of the design process can be evaluated.
3. To specify the relationship between the design process requirements and NRC regulations.

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

A-1.4 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, A-3.6.)

Control Room - The present approach is focussed on the process of HSI 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. In addition, HSI guidance promulgated as part of this process shall apply to other operations and control centers (e.g., the Operations Support Center and in-scope portions of the Emergency Operating Facility; see A-3.5.2.1.2), and all identified Procedure Guideline "critical tasks" shall be fully evaluated as part of Task Analysis (A-3.4), HSI Design (A-3.5), Availability Verification (A-3.6), Suitability Verification (A-3.7), and Design Validation (A-3.8) activities.

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 COL Applicant.

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 technical content or bases, training development, licensing examinations, reliability analysis, quality assurance, OSHA, ALARA, fire protection, security, or emergency planning.

Operating Procedures Development - Procedure guidelines are developed by ABB-CE as technical input to the COL Applicant procedure development program. They provide

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

guidance for content (i.e., operations) and not format (i.e., human factors). Thus, the development of the procedure guidelines and their contents is not a human factors-centered activity. Procedure format is instead accomplished as part of the development and validation of the actual procedures by the COL Applicant. For these reasons, the human factors of procedure format is excluded from the scope of the Plan. The Plan conforms to the requirements of 50.34(g)(3) of Reference 5, and forms part of an approach that meets the intent of Element 7 of Reference 14. See Section 4.2 for additional information on operating procedures development.

A-1.5 Method

The CRDR process that was developed in response to Reference 7, and successfully implemented in existing plant evaluations, embodies a "systems approach" to 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., References 1, 2, 4, and 15), and the military HFE requirements (e.g., Reference 3) all tend to reiterate a number of features that typify this 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 HSI design guidance
- Verification of necessary indication and control availability
- Validation of operating ensemble sufficiency

Thus the literature suggests that a satisfactory process for incorporating HFE in design should have these features. In turn, the requirements and criteria for the design process should verify proper incorporation of these 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.

¹ A more elaborate, but also more tentative, interpretation of 10 CFR 50.34(f)(2)(iii) than presented under **Objectives**.

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

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 products are provided elsewhere, as specified (e.g., in the SGB).

Design process adequacy thus focusses on ensuring that the necessary functional content has been incorporated in design activities. To establish what is necessary, Reference 5 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 regulations have served as the core for the contents of the requirements for each element. The Design Process Elements are identified in A-2.1; their contents (goals, requirements, and acceptance criteria) are detailed in A-3.

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

A-1.6 References

- 1) Booher, H. R. (Ed.) (1990). MANPRINT: An Approach to Systems Integration. New York, NY: Van Nostrand Reinhold.
- 2) DeGreene, K. B. (Ed.) (1970). Systems Psychology. New York, NY: McGraw Hill.
- 3) Department of Defense (1979). Human Engineering Requirements for Military Systems, Equipment, and Facilities (MIL-H-46855B).
- 4) Meister, D. (1985). Behavioral Measurement Methods. New York, NY: Wiley-Interscience.
- 5) Office of the Federal Register (1992). Code of Federal Regulations, Title 10, Chapter I - Nuclear Regulatory Commission (10 CFR Parts 0-199).
- 6) U.S. Nuclear Regulatory Commission (1973). Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Reg Guide 1.47).
- 7) U.S. Nuclear Regulatory Commission (1980). NRC Action Plan Developed as a Result of the TMI-2 Accident (NUREG-0660).
- 8) U.S. Nuclear Regulatory Commission (1980). Clarification of TMI Action Plan Requirements (NUREG-0737).
- 9) U.S. Nuclear Regulatory Commission (1981). Guidelines for Control Room Design Reviews (NUREG-0700).
- 10) U.S. Nuclear Regulatory Commission (1981). Evaluation Criteria for Detailed Control Room Design Review (NUREG-0801).
- 11) U.S. Nuclear Regulatory Commission (1982). Requirements for Emergency Response Capability (NUREG-0737, Supplement 1).

DESIGN PROCESS REQUIREMENTS
A-1 Introduction

- 12) 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).
- 13) U.S. Nuclear Regulatory Commission (1987). Standard Review Plan (NUREG-0800).
- 14) U.S. Nuclear Regulatory Commission (1992). HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors (Draft).
- 15) Van Cott, H. P. & Kinkade, R. G. (Ed.s) (1972). Human Engineering Guide to Equipment Design. Washington, DC: U.S. Government Printing Office.
- 16) Harmon, D. L. (1992). Distribution of Human Factors and Man-Machine Interface Documents (internal memorandum IC-92-316). ABB Combustion Engineering: Windsor, CT

DESIGN PROCESS REQUIREMENTS
A-2 Framework Description

A-2 Framework Description

A-2.1 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 (DPEs), which are detailed in A-3, are as follows:

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

DESIGN PROCESS REQUIREMENTS
A-2 Framework Description

A-2.2 Element Structure

A generic structure consisting of goals, requirements, and criteria, is the framework within which the DPEs 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.

A-2.2.1 Goals

The goal statement expresses the idealized function of the DPE, 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 each DPE, but also focus the questions of defining practical constituents and operationalizing their tests. This helps avoid confusion between intentions and capabilities.

A-2.2.2 Requirements

Requirements are the specific constituents that pragmatically define what must be provided or achieved by the DPE. Requirements are based on consideration of specific, applicable regulations from 10 CFR (as cited under the individual Elements in A-3) 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.

DESIGN PROCESS REQUIREMENTS
A-2 Framework Description

Note that, since these are functional rather than structural DPEs, 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.

A-2.2.3 Acceptance Criteria

Acceptance criteria are 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 criteria do not serve to detail the requirements. Rather, where further evaluation of the functional effectiveness of a DPE function is desired, attention should instead be turned to evaluation of the design product, to see if problems (e.g., unsuitabilities) have resulted in the HSI. Product review is the domain of Availability, Suitability, and Design Validation activities (Sections A-3.6, A-3.7, and A-3.8).

A-2.3 Element Products

Reference 14 indicated that each Element should produce separate plans, analyses, and evaluation reports. The present program has provided plans wherever programs of future work are indicated. However, plans have not been provided for past work completed. Analysis reports are specified for each analysis. These will include methodology, as well as results. Instead of generating separate evaluation reports, analysis reports will be subject to a formal interdisciplinary review and comment resolution process (Reference 16). The formal distribution mechanism in Reference 16 provides draft copies of all HFE and HSI documents to a multidisciplinary review group. This includes Instrumentation and Controls Engineering Department managers and selected supervisors, individuals responsible for each CESSAR-DC chapter, and licensing and project engineering personnel. This

DESIGN PROCESS REQUIREMENTS
A-2 Framework Description

ensures review by all disciplines represented in the SAR. Completed documents are also provided to the above individuals for their subsequent use. Reference 16 contains an ABB-CENP Document Distribution and Approval form template for use in preparing the review and distribution transmittals. This approach meets the intent of the evaluation report of Reference 14 in an expeditious manner.

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

A-3 Element Descriptions

A-3.1 HFE Program Management²

A-3.1.1 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 HSIs to plant operators, that 2) the final HSI 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.³

A-3.1.2 Requirements

A-3.1.2.1 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 following⁴:

- A-3.1.2.1.1 **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.

² This Design Process Element corresponds to Element 1 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

³ 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.

⁴ These requirements contribute to satisfying the requirements of 10 CFR 50.34(f)(3)(vii) to provide management plans for design and construction activities.

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

- A-3.1.2.1.2 **Technical Resources** - The technical resources (i.e., HFE Specialists, Operations Experts) employed by the applicant to address usability issues in the design.
- A-3.1.2.1.3 **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 A-3.5, HSI Design.
- A-3.1.2.1.4 **Method of Design Control** - The details of the method by which design control is exercised among team members.
- A-3.1.2.1.5 **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) Human-System Interface Design
 - e) Availability Verification
 - f) Suitability Verification
 - g) Design Validation

Goals and requirements for these elements are provided in remaining subsections of Section A-3. However, it is not required that program plans be organized in terms of this, or any other, particular set of process elements.

A-3.1.2.2 Responsibility

- A-3.1.2.2.1 **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 program requirements, and c) the resolution of all issues entered in the HFE Tracking System.

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

- A-3.1.2.2.2 **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.
- A-3.1.2.2.3 **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 HSI design products for usability concerns.
- A-3.1.2.2.4 **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) program⁵. 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.

A-3.1.2.3 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 completion of construction of the facility⁶.

A-3.1.2.4 Tracking

- A-3.1.2.4.1 **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 analyses and evaluations.

⁵ As implemented per the requirements of 10 CFR 50.34(a)(7), and 10 CFR 50.34(f)(3)(iii) for QA programs.

⁶ These requirements are in keeping with the requirements of 10 CFR 50.34(a)(8).

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

- A-3.1.2.4.2 **System Entries** - TOI entries shall include the source and a description of the issue; a Calendar-referenced commitment date for resolution; and a deadline for its implementation.
- A-3.1.2.4.3 **Resolution of Entries** - Resolution of TOI entries shall include the source and description of the resolution; and a Calendar-referenced commitment date for its implementation.
- A-3.1.2.4.4 **Implementation of Resolutions** - Closeout of TOI entries shall include a description of the final implementation; and verification of the properly completed implementation by a representative of the Responsible Management Structure.
- A-3.1.2.4.5 **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.
- A-3.1.2.4.6 **TOI Database Closeout** - Following completion of the design's V&V activities specified by the HFPP, and the resolution of all TOI entries, a TOI database closeout report shall formally verify the closure of all TOI database items.

A-3.1.2.5 COL Applicant Turnover

The following products and results of the HFE Program shall be delivered to the COL Applicant via OSIP or equivalent method at the completion of the design process:

- Task analysis data and reports
- HFE Standards, Guidelines, & Bases
- Verification & Validation plans, data and reports
- Design Validation scenarios & operating sequences
- TOI database and closeout report

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

A-3.1.3 Acceptance Criteria

A-3.1.3.1 Program Plan

- A-3.1.3.1.1 **Effective Date** - A formal HFE Program Plan as described in A-3.1.2.1 is in effect.
- A-3.1.3.1.2 **Responsible Management Structure** - The Responsible Management Structure presented in the HFE Program Plan a) shows the chain of HFE accountability from the level of technical origination to the representatives 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 individual(s) in each position.
- A-3.1.3.1.3 **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 available for review; their qualifications meet the definitions and requirements stated in the Program Plan.
- A-3.1.3.1.4 **Method of Interdisciplinary Interaction** - The HFE Program Plan provides an explanation of the interdisciplinary design process as described in A-3.1.2.3.
- A-3.1.3.1.5 **Method of Design Control** - The HFE Program Plan details or references overall design program procedures for applicable design control methods including review and sign-off of HFE analysis results.
- A-3.1.3.1.6 **Design Process Elements** - Criteria for the various DPEs are provided within each Element.

A-3.1.3.2 Responsibility

- A-3.1.3.2.1 **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 these requirements (as indicated by their sign-

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

off per A-3.1.3.5), and c) resolution and implementation of all TOI items.

A-3.1.3.2.2 **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.

A-3.1.3.2.3 **Operations Experts**

- a) Operations Experts (as defined in the Introduction) are Employed by the Responsible Management Structure;
- b) Operation Experts have reviewed all milestone HSI design products as documented by official memoranda.

A-3.1.3.3 Scheduling

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

A-3.1.3.4 Tracking

A-3.1.3.4.1 **System Provision** - A TOI is defined that accommodates the information specified in A-3.1.2.4., and is in place upon acceptance of the HFE Program Plan.

A-3.1.3.4.2 **System Implementation** - Selective audit of the TOI system indicates that it is being implemented as specified by the requirements of A-3.1.2.4, including that all commitments have been met, or their entries suitably updated.

DESIGN PROCESS REQUIREMENTS
A-3.1 HFE Program Management

A-3.1.3.5 COL Applicant Turnover

The products and results of the HFE Program listed in A-3.1.2.5 are formally transmitted to the COL Applicant at the completion of the design process.

DESIGN PROCESS REQUIREMENTS
A-3.2 Incorporation of Experience

A-3.2 Incorporation of Industry Experience⁷

A-3.2.1 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.

A-3.2.2 Requirements

A-3.2.2.1 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.

A-3.2.2.2 References and Studies

Prior to certification, a list of industry and regulatory references (e.g., NRC, EPRI, INPO, NUMARC, etc.) shall be developed and evaluated as input to the design.

A-3.2.2.3 Formal Treatment of Safety Issues

- A-3.2.2.3.1 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.

⁷ This Design Process Element corresponds to Element 2 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

DESIGN PROCESS REQUIREMENTS
A-3.2 Incorporation of Experience

A-3.2.2.3.2 GSI and USI processing shall be controlled by formal procedures implemented prior to certification.

A-3.2.3 Acceptance Criteria

A-3.2.3.1 Administrative Procedures

Administrative procedures for evaluating and disseminating operating, design, and construction experience as described in A-3.2.2.1 are provided in an official project document. Audit of transmittal records verifies that the procedures have been actively implemented.

A-3.2.3.2 References and Studies

A report summarizing the contents of the references identified in A-3.2.2.2, and the resolution of resulting issues that are potentially relevant to the design, is provided as an official project document.

A-3.2.3.3 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.

DESIGN PROCESS REQUIREMENTS
A-3.3 Evaluation/Allocation of Functions

A-3.3 Evaluation and Allocation of System Functions⁸

A-3.3.1 Goals

The collective 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.)

A-3.3.2 Requirements

A-3.3.2.1 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

⁸ This Design Process Element corresponds to Elements 3 and 4 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

DESIGN PROCESS REQUIREMENTS
A-3.3 Evaluation/Allocation of Functions

containment isolation signals; 10 CFR
50.34(f)(2)(xiv)(C).

- 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).

A-3.3.2.2 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.

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". Alternately, or if no predecessor system is extant, a formal systems analysis may be provided.

⁹ 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.

DESIGN PROCESS REQUIREMENTS

A-3.3 Evaluation/Allocation of Functions

A-3.3.2.3 HFE Evaluation of Allocations

The Task Analysis (Section A-3.4), Availability Verification (Section A-3.6), Suitability Verification (Section A-3.7), and Design Validation (Section A-3.8) 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 A-3.1.2.4.

A-3.3.3 Acceptance Criteria

A-3.3.3.1 Mandated Allocations

Mandated allocations, as stated in A-3.3.2.1, have been verified through review of the appropriate systems designs, and documented in official project documents or memoranda.

A-3.3.3.2 Critical Safety Functions

An 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 A-3.3.2.2.

A-3.4 Task Analysis¹⁰

A-3.4.1 Goals

Task Analysis should identify the human operator's detailed input and output requirements for a representative set of control room, and remote shutdown tasks, and any local control tasks required by the EPGs. 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 safety¹¹.

A-3.4.2 Requirements

A-3.4.2.1 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."

A-3.4.2.2 Design Basis Task Inventory

The inventory of tasks subject to TA shall include the contents of the emergency operating procedure guidelines, including any local control station tasks, as well as a representative selection of MCR and RSA tasks. Both normal operations and anticipated operating occurrences shall be represented, 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.

A-3.4.2.3 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.

A-3.4.2.4 Methodology

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

- A-3.4.2.4.1 **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 A-3.6.2.3.2.
- A-3.4.2.4.2 **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 A-3.1.2.4.

A-3.4.2.5 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).

A-3.4.2.6 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). Reports shall receive formal interdisciplinary review from the design team.

A-3.4.2.7 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.

A-3.4.2.8 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 A-3.6.

A-3.4.3 Acceptance Criteria

A-3.4.3.1 Operational Basis

A-3.4.3.1.1 Task Analysis Report(s) have been produced based on referenced procedural sources as described in A-3.4.2.1.

A-3.4.3.1.2 Task Analysis Report(s) have been co-originated by at least one Operations Expert, in addition to a Human Factors Specialist.

A-3.4.3.2 Design Basis Task Inventory

A-3.4.3.2.1 The Task Analysis Report(s) describes analyses which include all emergency operating procedure tasks, and an additional selection of control room normal and abnormal operating procedures,

DESIGN PROCESS REQUIREMENTS
A-3.4 Task Analysis

including startup, design basis load transients, shutdown, and uncomplicated reactor trip.

- A-3.4.3.2.2 The Task Analysis Report(s) describe the basis for identifying the set of evaluated tasks as representative of all tasks required by anticipated operating occurrences. TA report(s) have been originated and disseminated as specified in A-3.4.2.6.

A-3.4.3.3 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.

A-3.4.3.4 Methodology

- A-3.4.3.4.1 The TA method is demonstrated by example to provide the data required by Section A-3.6.2.3.2.
- A-3.4.3.4.2 The TA method provides a criterion, basis, and evaluation of operator loading.

A-3.4.3.5 Staffing Assumptions

- A-3.4.3.5.1 The design basis staffing and staffing assumptions incorporated in the analysis have been identified in the TA Report(s).
- A-3.4.3.5.2 Operator loadings have been evaluated in the TA Report(s) for the design basis minimum staffing.

A-3.4.3.6 Reporting of Results

Reports at a minimum include the information required by Section A-3.4.2.6. All cases of results in which analyzed conditions exceeded the loading criterion of A-3.4.2.4.2 have been entered as TOI issues.

DESIGN PROCESS REQUIREMENTS
A-3.5 Human-System Interface Design

A-3.5 Human-System Interface Design¹²

A-3.5.1 Goals

The goal of Human-System Interface (HSI) design is to ensure that the final facility provides a thoroughly sufficient HSI, and a control room that reflects the State-of-the-Art in HFE. Stated differently, the aim is for the HSI designer's products to support the HSI user's needs. This is also the overall goal of HFE efforts; the specific efforts identified under HSI 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 HSI (e.g., labelling, layout, etc.)¹³

A-3.5.2 Requirements

A-3.5.2.1 HFE Design Guidance

A-3.5.2.1.1 **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 HSI design as HFE Design Guidance.

A-3.5.2.1.2 **Applicability** - The HFE Design Guidance shall be applicable to the HSIs in all engineering operations and control centers, including the Main Control Room, the Remote Shutdown Area, local

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).

DESIGN PROCESS REQUIREMENTS
A-3.5 Human-System Interface Design

control stations, the Technical Support Center, the Operations Support Center, and in-scope portions of the Emergency Operations Facility.

A-3.5.2.1.3 **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.

A-3.5.2.1.4 **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 the topics is provided for information only, and is not itself required.

A-3.5.2.1.5 **Promulgation** - The HFE Design Guidance shall be formally promulgated by the Responsible Management Structure to the design team for implementation in the design.

A-3.5.2.1.6 **Systematic Process** - The reference design for the MCR and RSR indications and controls (i.e., screen design, panel layout, etc.) shall be detailed through a systematic process incorporating HFE design guidance. Documentation for this process shall include the results of design reviews.

A-3.5.2.1.7 **Control** - The HFE Design Guidance document(s) shall be subject to program design document control measures as applicable under A-3.1.2.2.4.

DESIGN PROCESS REQUIREMENTS
A-3.5 Human-System Interface Design

A-3.5.2.1.8 **Role in Suitability** - The HFE Design Guidance shall provide the criteria for the Verification of Suitability specified in A-3.7.

A-3.5.2.2 HFE Design Assumptions

A-3.5.2.2.1 **Workspace Conditions** - The HSI 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.

A-3.5.2.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the HSI 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.

A-3.5.2.3 Reference Design

A-3.5.2.3.1 **Documentation** - The Reference Design for main control room and remote shutdown area HSI systems and equipment shall be detailed within official program documents.

A-3.5.2.3.2 **Interdisciplinary Review** - Reference Design documents shall receive a documented interdisciplinary review, including participation of HFE Specialist(s) and Operations Expert(s).

A-3.5.2.3.3 **Mockup Development** - The Reference Design documentation of A-3.5.2.3.1 shall be the basis for corresponding HSI mockups constructed for use in Suitability Verification.

A-3.5.3 **Acceptance Criteria**

A-3.5.3.1 HFE Design Guidance

A-3.5.3.1.1 **Provision** - A body of HFE Design Guidance has been assembled by the design team. Original guidance therein has been developed by HFE Specialists.

A-3.5.3.1.2 **Applicability** - The HFE Design Guidance, either through its contents or promulgation, formally indicates its applicability as specified under A-

DESIGN PROCESS REQUIREMENTS
A-3.5 Human-System Interface Design

3.5.2.1.2.

- A-3.5.3.1.3 **Basis** - A technical basis for the HFE Design Guidance has been provided as specified under A-3.5.2.1.3. If original, it has been explained by an HFE Specialist.
- A-3.5.3.1.4 **Content** - The HFE Design Guidance includes coverage of the topics specified under A-3.5.2.1.4.
- A-3.5.3.1.5 **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.

A-3.5.3.2 HFE Design Assumptions

- A-3.5.3.2.1 **Workspace Conditions** - The HSI 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.
- A-3.5.3.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the HSI 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.

A-3.5.3.3 Reference Design

- A-3.5.3.3.1 The Reference Design for HSI systems and equipment documented and reviewed per the Requirements of A-3.5.2.3.
- A-3.5.3.3.2 Corresponding mockups are verified to have been constructed for the Reference Design HSI.

DESIGN PROCESS REQUIREMENTS
A-3.6 Availability Verification

A-3.6 Availability Verification¹⁴

A-3.6.1 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) for required emergency procedure tasks, and required for operators to perform other necessary operating tasks in the main control room and the remote shutdown area, per GDC 13 and 19 of 10 CFR 50, Appendix A.¹⁵

A-3.6.2 Requirements

A-3.6.2.1 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).

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).

DESIGN PROCESS REQUIREMENTS
A-3.6 Availability Verification

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

A-3.6.2.2 I&C Inventory

A-3.6.2.2.1 **Database** - An I&C Inventory database shall be provided:

- a) that allows the elements of the Task Inventory identified in A-3.4.2.2 (i.e., their inputs and outputs) to be indexed and tracked against 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.

A-3.6.2.2.2 **Control** - The I&C Inventory shall be subject to program design control measures to maintain it current with the design configuration as applicable under A-3.1.2.2.4.

DESIGN PROCESS REQUIREMENTS
A-3.6 Availability Verification

A-3.6.2.3 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.

A-3.6.2.4 Methodology

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

A-3.6.2.5 Analysis Report

Report(s), 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, and receive formal interdisciplinary review from the design team.

A-3.6.2.6 Discrepancies

Discrepancies between required and actual I&C availability specified by A-3.6.2.1 or A-3.6.2.2 shall be entered as TOI issues per the Requirements of A-3.1.2.4.

A-3.6.3 Acceptance Criteria

A-3.6.3.1 Mandated Availability

The design makes Available the Federally mandated indication and control features identified in A-3.6.2.1, or provides a technical justification for why they are no longer functionally required for plant operation. This is verified in an official project document.

A-3.6.3.2 I&C Inventory Database

An I&C Inventory database has been provided in the Availability Analysis Report that meets the requirements of A-3.6.2.3.

DESIGN PROCESS REQUIREMENTS
A-3.6 Availability Verification

A-3.6.3.3 Formal Analysis

A formal Availability Verification analysis has been performed and disseminated as stated in A-3.6.2.3.3.

A-3.6.3.4 Methodology

The methodology to be used in the formal Availability analysis has been demonstrated as stated in A-3.6.2.3.4.

A-3.6.3.5 Analysis Report

A report as specified in A-3.6.2.4.2 has been produced.

A-3.6.3.6 Discrepancies

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

DESIGN PROCESS REQUIREMENTS
A-3.7 Suitability Verification

A-3.7 Suitability Verification¹⁶

A-3.7.1 Goals

The goal of Suitability Verification is to ensure that the HSI's various Indication and Control Features (as defined in the Introduction) afforded by the main control room, the remote shutdown area, and the local control stations required for executing emergency procedures, are Usable designs that will support the operator's successful task accomplishment per the applicable HFE Design Guidance.¹⁷

A-3.7.2 Requirements

A-3.7.2.1 Formal Analysis

Formal Suitability Analysis shall be performed by HFE Specialist(s) to evaluate the Usability of the HSI Indication and Control Features of the main control room, the remote shutdown room, and any local control station tasks required by the EPGs shall be observed and documented in terms of the HFE Design Guidance of A-3.5.

A-3.7.2.2 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.

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).

DESIGN PROCESS REQUIREMENTS
A-3.7 Suitability Verification

However, HFE Design Guidance shall provide the primary reference against which Suitability is evaluated.

A-3.7.2.3 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.)

A-3.7.2.4 Methodology

Prior to certification, the Suitability analysis methodology shall be demonstrated by example.

A-3.7.2.5 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. Reports shall receive formal interdisciplinary review from the design team.

A-3.7.2.6 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.

A-3.7.3 Acceptance Criteria

A-3.7.3.1 Formal Analysis

Suitability has been formally Verified for the HSIs in all engineering control centers as specified in A-3.7.2.1 and documented in A-3.7.3.4.

A-3.7.3.2 Relationship to HFE Design Guidance

The Suitability Analysis Report indicates that the designs have been evaluated against the HFE Design Guidance Document of A-3.5.

DESIGN PROCESS REQUIREMENTS
A-3.7 Suitability Verification

A-3.7.3.3 Fidelity

Mockups and any other design representations used to verify Suitability embody the evaluated characteristics specified in A-3.7.2.3, as recorded in an official project document.

A-3.7.3.4 Methodology

The methodology to be used in the Suitability analysis has been demonstrated as stated in A-3.7.2.3.4.

A-3.7.3.5 Analysis Report

Report(s) have been provided and disseminated as specified in A-3.7.2.4.

A-3.7.3.6 Discrepancies and Concerns

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

DESIGN PROCESS REQUIREMENTS
A-3.8 Design Validation

A-3.8 Design Validation¹⁸

A-3.8.1 Goals

The goal of design Validation is to ensure that the sum of the various HSI design features afforded by the main control room, the remote shutdown area, and local control stations required for executing emergency procedures, provide Usable design ensembles that support the successful accomplishment of the operator's functional role (i.e., as specified by training and procedures) under dynamic, real-time conditions.¹⁹

A-3.8.2 Requirements

A-3.8.2.1 Formal Evaluation

Prior to the combined operating license, formal, final design Validation exercises for the main control room, the remote shutdown area, and any local control station tasks required by the EPGs shall be observed and documented by a team including HFE Specialist(s) and Operations Expert(s). Subjective feedback from the tested operators shall be a formal component of the evaluation.

A-3.8.2.2 Relationship to Design Basis

Prior to certification, the set of design Validation scenarios to be performed shall be specified, along with the plant-referenced operating, tech spec, and

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).

DESIGN PROCESS REQUIREMENTS
A-3.8 Design Validation

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 operations, and all SRDBEs (as defined in the Introduction)²⁰ which credit operator actions in their analysis.

A-3.8.2.3 Fidelity

The Validation facilities shall physically represent the MCR and RSR configurations, and dynamically represent the operating characteristics and responses of the System 80+ design. Design Validation shall employ vendor procedure guidelines and actual operators in the evaluations.

A-3.8.2.4 Evaluation Report

Design Validation report(s), describing the methodology and scenarios, the applicable criteria, and the summary results of formal design Validation exercises, shall be originated jointly by observers including HFE Specialist(s), Operations Expert(s), and Safety (i.e., DBE) Analyst(s). Validation reports shall include any failure to meet the detailed acceptance criteria of the exercises, particularly any case in which prior SRDBE analysis that has taken credit for operator action was not limiting in comparison to the corresponding Validation exercise. Validation reports shall receive formal interdisciplinary review from the design team.

A-3.8.2.5 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 A-3.1.2.4.

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).

DESIGN PROCESS REQUIREMENTS
A-3.8 Design Validation

A-3.8.3 Acceptance Criteria

A-3.8.3.1 Formal Evaluation

Validations for the main control room, the remote shutdown area, and local control station tasks required by the EPGs have been performed and documented as described in A-3.8.2.1.

A-3.8.3.2 Relationship to Design Basis

Official program documentation has indicated the scenarios to be performed, and criteria to be applied, as specified in A-3.8.2.2.

A-3.8.3.3 Fidelity

Facilities and guidance as specified in A-3.8.2.3 have been utilized for the Validation exercises.

A-3.8.3.4 Evaluation Report

Official program documentation indicates that the Validation report(s) have been originated and disseminated as specified in A-3.8.2.3.

A-3.8.3.5 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.

ATTACHMENT 2