HUMAN FACTORS EVALUATION

AND ALLOCATION OF

SYSTEM 80+ FUNCTIONS

NPX80-IC-RR790-02

Revision 01

March 15, 1993

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

TABLE OF CONTENTS

ABBREVIATIONS

ABB-CE	Asea Brown Boveri - Combustion Engineering
AC	Alternating Current
AFW	Auxiliary Feedwater
Alt	Alternate
ANS	American Nuclear Society
ANSI	American National Standards Institute
APS	Auxiliary Protection System
ATWS	Anticipated Transient Without Scram
Auto	Automatic
AVS	Annulus Ventilation System
CEA	Control Element Assembly
CFR	Code of Federal Regulations
CIAS	Containment Isolation Actuation Signal
Cntl	Control
Comp	Complementary
CSAS	Containment Spray Actuation Signal
Ctmt	Containment
CVCS	Charging and Volume Control System
DBE	Design Basis Events
DC	Direct Current
DG	Diesel Generator
DVI	Direct Vessel Injection
EFAS	Emergency Feedwater Actuation Signal
EFW	Emergency Feedwater
EFWST	Emergency Feedwater Storage Tank
GDC	General Design Criterion
LOOP	Loss Of Offsite Power
IEEE	Institute of Electrical and Electronics Engineers
Init	Initiate, Initiation
MSIS	Main Steam Isolation Signal
NRC	Nuclear Regulatory Commission
Par	Parallel
PORV	Power Operated Relief Valve
PPS	Plant Protection System
PWR	Pressurized Water Reactor
PZR	Pressurizer
RCGV	Reactor Coolant Gas Vent
RCGVS	Reactor Coolant Gas Vent System
RCS	Reactor Coolant System
RD	Rapid Depressurization
RDS	Rapid Depressurization System
RG	Regulatory Guide
RPS	Reactor Protection System
Rx	Reactor
SCS	Shutdown Cooling System
SDS	Safety Depressurization System

SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection System
SIAS	Safety Injection Actuation Signal
SIT	Safety Injection Tank
SPS	Supplementary Protection Signal
S/U	Start Up
Xfmr	Transformer

DEFINITIONS

Allocation of Function - The decision to use manual or automatic control in the design of a particular system operating feature. This is described as falling into one of five categories of configuration: 1) Fully manual, 2) fully automatic, 3) Complementary, 4) Alternate, or 5) Parallel (see Section x).

Automatic - A type of control in which the main switching and/or regulating features are governed by machine devices, without need for human supervision or intervention.

Critical Safety Functions - The safety functions for the System 80+ design and its predecessors.

Critical Operator Actions - Human operator tasks identified by the PRA to contribute significantly to overall risk in the System 80+ design.

Design Basis Events - Events evaluated by CESSAR-DC Chapter 15 safety analyses (Reference 4).

Manual - A type of control in which the main switching and/or regulating features are governed by human operator(s).

Mixed Allocation - A combination of automatic and manual control used in one of several configurations (i.e., Complementary, Alternate, or Parallel; see Section 4.4).

Non-safety System - A system not relied on to remain functional during design basis events.

Operating Bypass - Inhibition of the capability for a protective action that could otherwise occur in response to plant conditions.

Protective Action - The generation of signal(s) by the process monitoring and equipment command features to initiate reactor trip and/or engineered safety feature operation (i.e., protective systems).

Protective System - A system relied on (i.e., credited in CESSAR-DC Chapter 15 analyses) to mitigate DBEs by performing the specified safety function.

Safety Functions - Physical processes, conditions, or actions relied on to maintain the plant within acceptable design basis

limits, i.e. to prevent core melt and to ensure radiation releases do not exceed the limits of 10 CFR 100.

Segment - In Appendix B, a segment is any unit of functional decomposition (function, subfunction, task, etc.) proposed for allocation. This generic term is used to avoid invoking preconceptions about system hardware that might be implied for some readers by more frequently used systems terminology.

Success Path - A set of physical process commodities and equipment that, if available, are sufficient to perform a particular safety function in the design.

Unanticipated Systems Interaction - The undesired propagation of results to one system (subsystem, division, train, component, structure, segment, etc.) due to a single credible failure within another system, by means of inconspicuous interdependencies between the systems (per NUREG-1229, Reference 5).

1.0 INTRODUCTION

1.1 Background

The identification of system functional requirements, and the subsequent allocation of the functions to man and machine are part of a generic, top-down approach to systems design (Reference 1 & 2). The general concern, from a human factors standpoint, is that the task demands on human operators consistently remain within the effective limits of their abilities. One specific goal is to avoid excessive (or insufficient) levels of workload. A second, related goal is that the supervisory activity normally required of operators ensures their awareness of process status, and their readiness to perform safety-related functions. Concerns that automated systems can give rise to problems in these areas has led to an increasing emphasis on the allocation of functions in design.

Of course, these are not the only concerns in allocation. Of greatest importance in nuclear power plant design is the maintenance of plant safety. To this end, a variety of specific requirements on the allocation of certain safety-related functions exist that must be met by the design (e.g., Reference 3). The operator's present role in existing plants has evolved within these constraints.

As an evolutionary Pressurized Water Reactor (PWR) design, System 80+ has been developed in light of the success and experience accrued from prior generations of similar Combustion Engineering plants (see Reference 4, Table 1.3-1). In particular, the ABB-CE Critical Functions (i.e., safety functions) have proved themselves to be a sufficient and effective framework for emergency operations and maintaining plant safety.

1.2 Purpose

The purpose of the present report is to explain how System 80+ conforms to the existing Critical Functions framework to meet the applicable requirements and intentions of industry guidance for plant safety and emergency operations. The report identifies:

1) requirements and guidelines applicable to the issues of functional analysis and allocation;

2) the ABB-CE plant operators' role as it has evolved and culminated in System 80+, with an emphasis on safety functions; and

3) how System 80+ meets the safety-related requirements.

This report responds to the requirements of the ABB-CE Human Factors Program Plan (Reference 6, Section A-2.3). In addition, it addresses Elements 3 and 4 of Appendix E of Reference 2, per the agreements of Reference 7. The commitments of Reference 7 included the submission of the present report, an "explanation-of-functions" paper grounded in System 80+ Critical Safety Functions that describes:

1) the baseline system;

2) its functional objectives, requirements and allocations to human and machine elements;

3) changes to these requirements effected by the new system;

4) auditable bases for the allocations;

5) analyses of particular allocation problems in predecessor plants; and

6) activities confirming that personnel can properly perform tasks allocated to them.

The present report addresses each of these areas. Further details may be obtained from References 4 and 8, and future evaluation activities; see Section 3.4.

1.3 Scope

The scope of the present report is on the Safety Functions and Success Paths required to accommodate design basis events. The Safety Functions and their Success Paths are the means by which the System 80+ design safely accommodates all anticipated operating occurrences during normal, abnormal, and emergency conditions. Events beyond design basis, such as severe accidents or unanticipated systems interactions (Reference 5), are not addressed by this evaluation.

In addition, passive or inherent functions are generally outside the realm of the allocation concept. However, where these are credited for achieving Safety Functions, they have been treated as automatic functions in the evaluation.

2.0 REQUIREMENTS

A variety of federal regulations, industry standards, and regulatory guidelines apply to the issues of PWR plant functional design and the allocation of functions to human and/or machine control. Both general and specific items are found. Relevant portions are reviewed here to identify specific requirements governing allocation. The resulting criteria are specified under Section 3.3 of the Approach, for application in the subsequent Evaluation.

Please note that references within a document description refer to the numbering scheme used in that document; references to other documents will identify the document specifically; references to the present report, where used, will parenthetically indicate to "see" the indicated Section. Material is not presented word for word or in its entirety from the original sources; it has been paraphrased for brevity and clarity. While it is felt that the original authors' intentions have been retained, readers with specific concerns should consult the original sources.

2.1 10 CFR 50 - Code of Federal Regulations: Nuclear Regulatory Commission (Reference 3)

Part 50, "Domestic licensing of production and utilization facilities," provides several specific allocation requirements.

2.1.1 **General Design Criteria** (10 CFR 50, Appendix A)

Automatic initiation of protective systems including reactivity control systems and associated systems and components important to safety; GDC 20.

2.1.2 **Additional TMI-related requirements** (10 CFR 50.34(f))

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

b) Automatic and manual initiation of auxiliary (and/or emergency) feedwater systems; 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; 50.34(f)(2)(xiv)

d) No automatic reopening of automatically closed containment isolation valves on reset of automatic containment isolation signals; 50.34(f)(2)(xiv)(C).

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

2.1.3 **Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants** (10 CFR 50.62)

Automatic initiation of turbine trip; 50.62(c).

2.2 ANSI/ANS 58.8-1984 - Time Response Design Criteria for Nuclear Safety-related Operator Actions (Reference 11)

These criteria specify time test requirements to be met by design and nuclear-safety analyses, for credit to be taken for manual operator actions that initiate and/or control nuclear-safety system actions. If the manual time test requirements cannot be met, then additional control automation (or other mitigating steps) are necessary for resolution. The response time criteria of the Standard are based on simulator data; 95% confidence levels are established for the sufficiency of the defined intervals to permit opera or action (these have since been validated as conservative with further testing for an upcoming revision of the Standard.)

The criteria of ANSI/ANS 58.8 are applied as part of the safety analyses during design, and the final results are provided in Chapter 15 of CESSAR-DC. Any issues identified in Chapter 15 are addressed as part of the safety analysis and Standard Review, and the results incorporated in the System 80+ design and design basis documentation. The ANSI/ANS 58.8 criteria will thus not be utilized further in the present report.

2.3 IEEE 279-1971 - IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations (Reference 12)

Section 4.17, "Manual Initiation" (to which RG 1.62 replied; see Section 2.9) presented specific requirements relating to allocations. However, for the purposes of function allocation, this document has been incorporated in and superseded by the current version of IEEE 603.

2.4 IEEE 603-1991 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Reference 13)

This Standard is an update of IEEE 603-1980, primarily in response to the comments of RG 1.153 (whose technical input was, essentially, incorporated by the revision.) The following requirements from IEEE 603-1991 are relevant to functional analysis and allocation:

2.4.1 **Safety System Design Basis** (Section 4)

The following are part of the design basis documentation requirements for protective actions corresponding to safety functions in each design basis event:

Solely Manual Initiation (4.5.2) - The justification must be documented for permitting initiation, or control subsequent to initiation, solely by manual means.

Range of Environmental Conditions (4.5.3) - The range of environmental conditions imposed on the operator in which the manual operations must be performed shall be documented.

2.4.2 **Safety System Criteria** (Section 5)

The following are system functional and design requirements to ensure that plant parameters are maintained within acceptable limits for each design basis event:

Completion of Protective Action (5.2) - Safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis [i.e., that can prevent a system from accomplishing its function] or the provision for deliberate operator interventions.

Human Factors (5.14) - Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals.

2.4.3 **Sense and Command Features - Functional and Design Requirements** (Section 6)

In addition to the functional and design requirements of Section 5, these requirements apply to sense and command features:

Automatic Control (6.1) - Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.

Manual Control (6.2) - Means shall be provided in the control room to manually initiate all automatically initiated protective actions at the division level, and to manually initiate and control protective actions identified in 4.5 that have not been selected for automatic control under 6.1.

Operating Bypasses (6.6) - Whenever applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass, or initiate the appropriate safety function. If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically do one of the following (6.6):

1) Remove the appropriate active operating bypass(es).
2) Restore plant conditions so that permissive conditions once again exist.
3) Initiate the appropriate safety function.

2.4.4 **Executive Features - Functional and Design Requirements** (Section 7)

In addition to the functional and design requirements of Section 5, these requirements apply to executive features:

Automatic Control (7.1) - Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis [i.e., the variables monitored as the basis for control].

Manual Control (7.2) - If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 [i.e., single failure criteria] and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.

Completion of Protective Action (7.3) - The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11, or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal.

Operating Bypasses (7.4) - [As for 6.6.]

2.5 IEEE 1023-1988 - IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Reference 14)

Section 6, "Implementation in the Design, Operations, Testing, and Maintenance Process," includes guidance for planning, documentation, and review of experience. It proposes a typical program plan (see Figure 1) that includes analysis and allocation of functions for new designs, but not for modifications to existing ones (any evolutionary design is some balance of the two). The specific guidance provided is as follows:

a) Functional Analysis - Functions required to meet the system design objectives should be determined (6.1.1.3).

b) Function Allocation - Functions should be allocated to the human operator(s) and maintainer(s), to machines, or to a combination of humans and machines (6.1.1.4).

2.6 NUREG-0700 - Guidelines for Control Room Design Reviews (Reference 1)

Appendix B, "Systems/Operations Design Analysis Techniques," provides high-level guidance on the overall systems design

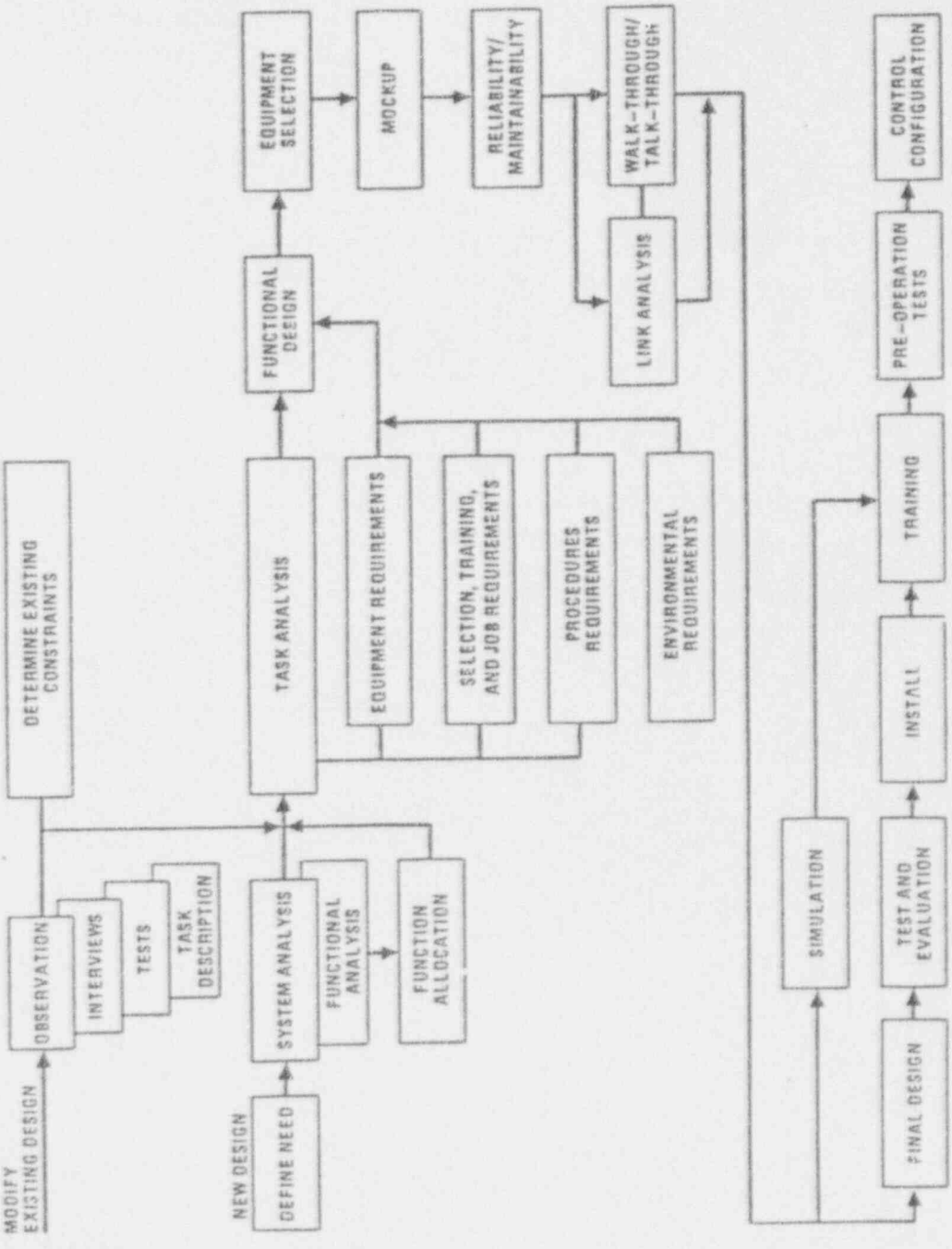

Fig 1
Typical Comprehensive Application of HFE in the Design Process

process, including function analysis and allocation. It is based on Reference 9, and is generally consistent with the approach of NUREG/CR-3331. It includes human performance-related allocation criteria in the form of a Fitts list, which has been included in the present report as an aid to designers and evaluators (see Appendix A).

2.7 NUREG/CR-3331 - A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control (Reference 15)

This document describes a method by which formal allocation can be included in the systems design process. Based on this document, evaluative criteria in the form of a decision algorithm have been provided as an aid to designers and evaluators in this report (see Appendix B).

2.8 Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Reference 16)

This document expanded upon Section 4.13 of IEEE 279-1971, which has been superseded by IEEE 603 (see Section 2.4), as well as on 10 CFR 50.34(f)(2)(v) (see Section 2.1.2.a). In general, the concern was that administrative procedures alone were insufficient to ensure operator cognizance of safety system operability; the Regulatory Position recommended automatic (supplemented by manual) bypassed and inoperable status indication for protection systems. IEEE 603-1991 incorporates similar standards in Section 5.8.3. System 80+ conformance to RG 1.47 is addressed in Chapter 7, Section 7.1.2.21 of CESSAR-DC, and is not further treated as an allocation issue in the present report.

2.9 Regulatory Guide 1.62 - Manual Initiation of Protective Actions (Reference 17)

This document expanded upon IEEE 279-1971, which has been superseded by IEEE 603 (see Section 2.4). In general, there was a concern for an excessive number of component actions required in the manual initiation of safety functions. While the concerns of RG 1.62 have been accommodated by subsequent versions of IEEE 603 (see Section 2.11), the allocation-related concerns presented in the Regulatory Position section of RG 1.62 are summarized here for the sake of completeness.

1) Means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation) at the system level, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve) (C.1).

2) Manual initiation of a protective action at the system level should perform all actions performed by automatic initiation such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to assure correct valve position, and providing the required action-sequencing functions and interlocks (C.2).

3) The switches for manual initiation of protective actions at the system level should be located in the control room and be easily accessible (C.3); manual initiation should depend on the operation of a minimum of equipment (C.5).

System 80+ conformance to RG 1.62 is addressed in Chapter 7, Section 7.1.2.22 of CESSAR-DC, and is not further treated as an allocation issue in the present report.

2.10 Regulatory Guide 1.97 - Instrumentation for Light-water-cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident (Reference 18)

Regulatory Guide 1.97 has no allocation requirements, per se, but specifies information requirements including Type A variables (supporting fully manual safety actions) similar to 5.8.1 of IEEE 603-1991.

The criteria of RG 1.97 have been met by preceding generations of ABB-CE plants, and have been applied to the System 80+ design. Conformance to RG 1.97 is addressed in Chapter 7, Section 7.1.2.26 of CESSAR-DC, and is not further treated as an allocation issue in the present report.

2.11 Regulatory Guide 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems (Reference 19)

This document largely endorsed IEEE 603-1980, with a small number of modest caveats. These remaining issues, in that they related to allocation, have been incorporated in IEEE 603-1991 (see Section 2.4).

3.0 APPROACH

System 80+ is an evolutionary design. It incorporates improvements that reflect experience gained from the design and operation of prior generation(s) of ABB-CE plants. However, the major characteristics of the System 80+ physical plant remain similar to and consistent with those of its forbearers (see Table 1.3-1 of Reference 4 for an overview). Such incremental improvement to a successful design reflects a safe and conservative approach to engineering.

Like the physical plant systems, the plant critical functions, and the operator's role in maintaining them, have been modified and improved in light of experience and technological progress. However, given the safe operating history of ABB-CE designs, and the successful operation of licensed System 80 plants, there have been no fundamental changes in these areas. Again, this reflects a conservative engineering approach.

Section 3 states the goals and specifies the criteria that will be applied to evaluate the past and present acceptability of the allocation of functions in these areas of the ABB-CE designs. In addition, Section 3 states the framework for the evaluation, and identifies the relationship of subsequent design process activities to those of allocation.

3.1 Allocation Goals

The following goals direct the efforts of this portion of the design process, and should be met by any final allocation of nuclear power plant safety functions:

a) Maintain Critical Safety Functions - The ensemble of facility systems must maintain the provision of certain operating functions (i.e., Critical Safety Functions) to ensure successful performance, particularly in the area of the health and safety of the public.

b) Complementary Human and Machine Roles - As part of a defense-in-depth philosophy, the human and machine elements within the system ensemble should play complementary roles that make the successful accomplishment of these functions highly likely.

c) Ensure Suitable Allocation - 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.)

3.2 Framework

The critical functions and their success paths, and the operators role in implementing them, for System 80 and System 80+ shall be compared to verify their similarity and consistency. The System 80+ success paths shall then be evaluated against the identified allocation criteria to verify the acceptability of the allocation of control of safety functions in the System 80+ design.

3.3 Criteria

The following criteria shall be applied to evaluate the acceptability of the allocation of control of safety functions in the System 80+ design.

10 CFR 50

Critical Functions shall be consistent with the federally mandated allocations identified in Section 2.1 from 10 CFR 50.

IEEE 603-1991

Not superseding the criteria of 10 CFR 50, the following additional allocation criteria result from the requirements identified in Section 2.4

a) Justification for requiring initiation or control of any protective actions solely by manual means, including assurance of necessary habitability, shall be documented.

b) In all other cases, means shall be provided to:

1) automatically initiate and control protective actions,

AND

2) manually initiate all automatic protective actions (at the division level from the control room).

NUREG/CR-3331

Not superseding the criteria of 10 CFR 50 and those resulting from IEEE 603-1991, the additional allocation criteria resulting from NUREG/CR-3331 (see Appendix B) shall be applied to verify

compatibility of the allocated functions with human factors guidelines.

3.4 Subsequent Evaluations and Allocation Issues

Throughout the life of the design, feedback on design decisions is generated. In particular, during the design process, various analysis and development efforts (not limited to human factors) may produce results that have allocation implications. In particular, Task Analysis, Availability Verification, Suitability Verification, control room Validation, PRA, and procedure guideline development may be a source of further issues.

However, findings thus identified, including allocation issues (if any), shall be resolved using general program mechanisms as specified in the HFPP (Reference 6). Emergent feedback is not a unique problem in the allocation area, and no unique process is necessarily indicated for the resolution of subsequent allocation issues. This approach satisfies the intent of Section 5.14 of IEEE 603-1991, Appendix B of NUREG-0700, and Elements 3 and 4 of the NRC HFE Program Review Model.

4.0 EVALUATION

This section provides a top-down descriptive evaluation of the allocation of plant safety functions. This description will be sufficient to permit understanding of the operator's safety-related role in the overall system design, and in design basis evaluations performed to establish the adequacy of the System 80+ Critical Safety Functions.[1] The description will take 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"[2]. This is provided as an alternative to a formal systems analysis, which would be more appropriate if System 80+ had no direct predecessor system.

4.1 Critical Safety Functions

Safety functions are physical processes, conditions, or actions relied on to maintain the plant within acceptable design basis limits, i.e. to prevent core melt and to ensure radiation releases do not exceed the limits of 10 CFR 100. These functions may be performed by automatic or manual actuation and/or regulation, from passive system performance, or from natural feedback in the plant design.

The composition of the safety functions is relatively unchanging for a given type of plant design. Table 1 compares a list of CE plant safety functions (i.e., the Critical Safety Functions, or CSFs) as described in 1980 (Reference 10; note that this substantially predates System 80), with those for the System 80 and System 80+ designs. Three changes should be noted in the table.

One change is to the relative priority of the functions: "Vital Auxiliaries" moved to a higher priority in the Emergency Procedure Guidelines in response to operational considerations (Reference 20). Specifically, the provision of vital power is a prerequisite for actively managing most other CSFs; thus,

---

[1] This requirement is 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."

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

verification of vital power precedes other CSF verifications for efficiency ("Reactivity Control" is the exception to this rule for its primary safety significance, its passive safety functionality, and for the importance of prompt response).

A second change is that "Indirect Radioactivity Release Control" has evolved to "Radiation Emission." This acknowledges that releases from plant systems may require management to minimize overall safety consequences.

The third change is that "Containment Temperature and Pressure" and "Combustible Gas Control" have been combined under the heading "Containment Environment." This reflects not so much a change in the required actions or the overall function, but that their aggregation under a single concept remains coherent, but is more procedurally efficient.

The aforementioned modifications reflect changes in operation, rather than design, and have been validated to be effective in actual use on System 80 and other ABB-CE plants. No additional changes in the CSF framework are planned for System 80+. Thus, CSFs have received only small evolutionary refinements, rather than any major changes, over the generations of Combustion Engineering plant design.

Table 1 - **SAFETY FUNCTIONS**

ORIGINAL LIST (1980)		SYSTEM 80 & SYSTEM 80+	
Function	Purpose	Function	Purpose
Reactivity Control	Shut reactor down to reduce heat production	Reactivity Control	Shut reactor down to reduce heat production
RCS Inventory Control	Maintain a coolant medium around core	Maintenance of Vital Auxiliaries	Maintain operability of systems needed to support safety systems
RCS Pressure Control	Maintain coolant medium in proper state	RCs Inventory Control	Maintain a coolant medium around core
Core Heat Removal	Transfer heat out of core into coolant system medium	RCS Pressure Control	Maintain coolant medium in proper state
RCS Heat Removal	Transfer heat out of coolant system medium	Core Heat Removal	Transfer heat out of core into coolant system medium
Containment Isolation	Close containment penetrations to prevent radiation release	RCS Heat Removal	Transfer heat out of coolant system medium
Containment Temperature & Pressure Control	Avoid equipment damage & maintain containment integrity	Containment Isolation	Close containment penetrations to prevent radiation release
Combustible Gas Control	Remove/redistribute H_2 to prevent fire or explosion & maintain containment integrity	Containment Environment	Control containment temperature pressure, hydrogen concentration, and radiation levels; maintain containment integrity and minimize potential release
Maintenance of Vital Auxiliaries	Maintain operability of systems needed to support safety systems	Radiation Emission	Control radiation release
Indirect Radioactivity Release Control	Contain misc. stored radioactivity to protect public and avoid distracting operators from protection of larger sources		

4.2 Success Paths

For each safety function there are multiple, diverse success paths. A success path is a set of components and resource commodities that is capable of satisfying a particular safety function. The purpose of diverse success paths is to provide multiple alternative means to accomplish a safety function goal (see Figure 2). Individual success paths may have further redundancy as well. This is part of the defense-in-depth philosophy. Although each safety function has one or more safety-grade success paths, additional success paths may be afforded by non-safety grade systems. Success paths join safety function to plant structure, providing a unitary framework tc organize displayed information and integrate written procedures. The System 80+ CSFs and their success paths are portrayed graphically in Figure 3.

A high level "functional" comparison of the major success paths for the System 80 and System 80+ CSFs is provided in Table 2. Essentially, changes to the success paths have been few, and reflect evolutionary improvements to the ABB-CE design. These changes, are summarized briefly here and in Table 3:

a) Safety Depressurization - The Safety Depressurization System consists of two major subsystems: 1) the Reactor Coolant Gas Vent System (RCGVS), and 2) the Rapid Depressurization System (RDS).

   The RCGVS was part of the System 80 design, although its success path function (depressurization to SCS entry conditions during natural circulation cooldown) was not credited in full for safety (System 80 also credited Aux Spray; see Non-safety CVCS, below.)

   The RDS can be used to depressurize the plant while using SIS/DVI to inject water into the core. This accomplishes heat removal via feed-and-bleed (i.e., "once-through cooling"). RDS is an added success path for beyond-design basis and severe accident scenarios. While it provides increased redundancy and diversity of the RCS heat removal success paths, its operation does not require frequent, rapid, unique, or complex actions, and it is not the preferred means or a safety-credited system for this function. Once-through cooling was formerly available using PORVs manually on some earlier ABB-CE plants; the function was removed when PORVs were eliminated from the design (see D.6). Thus, though the RDS is itself new, its addition does

not represent a significant change of the System 80+ operators' role or responsibilities from that of System 80.

b) Hydrogen Ignitors - H_2 Ignitors were not part of the System 80 design, but have been proven in operation on other plants. They has been added to System 80+ for increased redundancy and diversity of the Hydrogen control success paths, and for severe accident management. They are not the initial means of Hydrogen control, their operation does not require frequent, rapid, unique, or complex actions, and they are not credited as a safety system. Thus, the incorporation of H_2 Ignitors in the design does not represent a significant change of the System 80+ operators' role or responsibilities from that of System 80.

The following differences apparent in Table 2 are not operationally significant changes, from the CSF success path perspective, between the System 80 and System 80+:

a) Non-safety-grade CVCS - The System 80+ CVCS is no longer a safety-grade system. In System 80, portions of the CVCS system had to be safety grade because they were credited by safety analysis for achieving certain functions. In particular, CVCS was credited for borating at high pressure (reactivity control), and depressurizing from high pressure, via Aux Spray (RCS pressure control). In System 80+, however, these functions receive credit via the SIS pumps, and the Reactor Coolant Gas Vent System of SDS, respectively. Thus, CVCS is not required to be a safety-grade system; however, it remains available in System 80+ as a success path for these functions.

b) Safety-grade Offsite Power - There are differences between the System 80 and System 80+ electrical system configurations, including some changes in nomenclature. However, from the CSF success path perspective, the basic function of the Startup Transformers (System 80) and the Reserve Auxiliary Transformers (System 80+) are similar. Both provide alternate off-site grid sources (separate from the Unit Main Transformer), as well as automatic fast bus transfer from the Unit Main on loss of power.

c) Safety-grade Emergency Feedwater - The Emergency Feedwater System has not changed significantly from System 80 to System 80+. However, it has in the past been referred to as the Auxiliary Feedwater System at sites where Westinghouse plants already exist, for consistency.

Thus, the CSF Success Paths have changed little, consistent with the evolutionary nature of the plant. Additional details are provided in Section 4.3; in general, however, the detailed design of physical systems and their operation are beyond the scope of the present analysis.

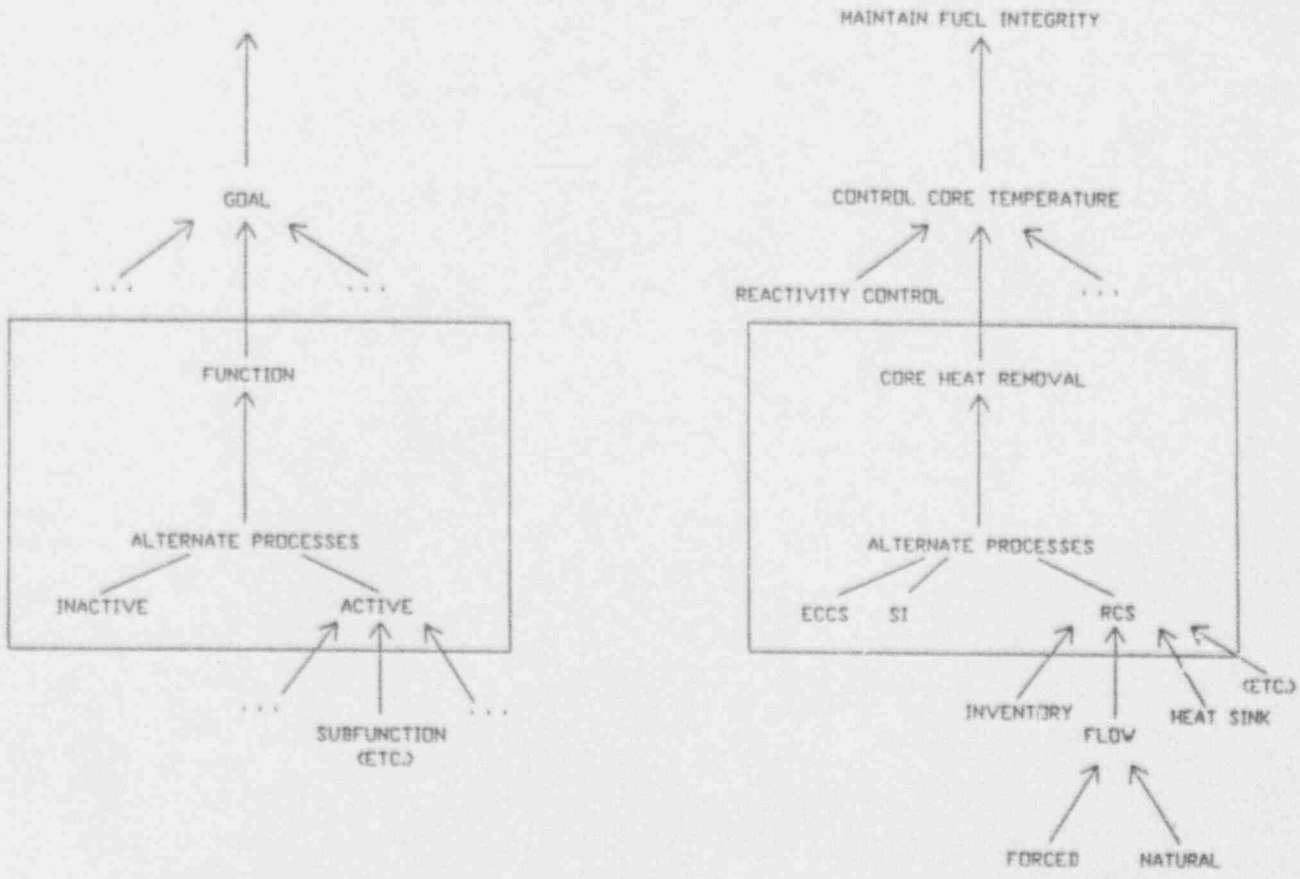

Figure 2 - Goal-Means Hierarchy

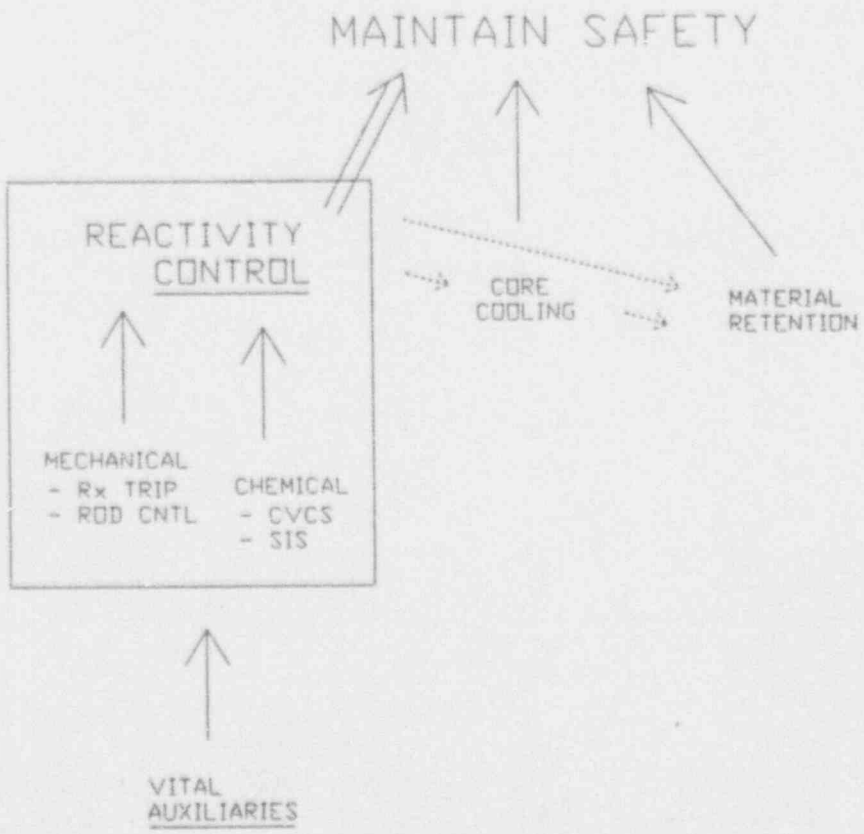

Figure 3 - System 80+ CSFs and Success Paths (page 1 of 3)

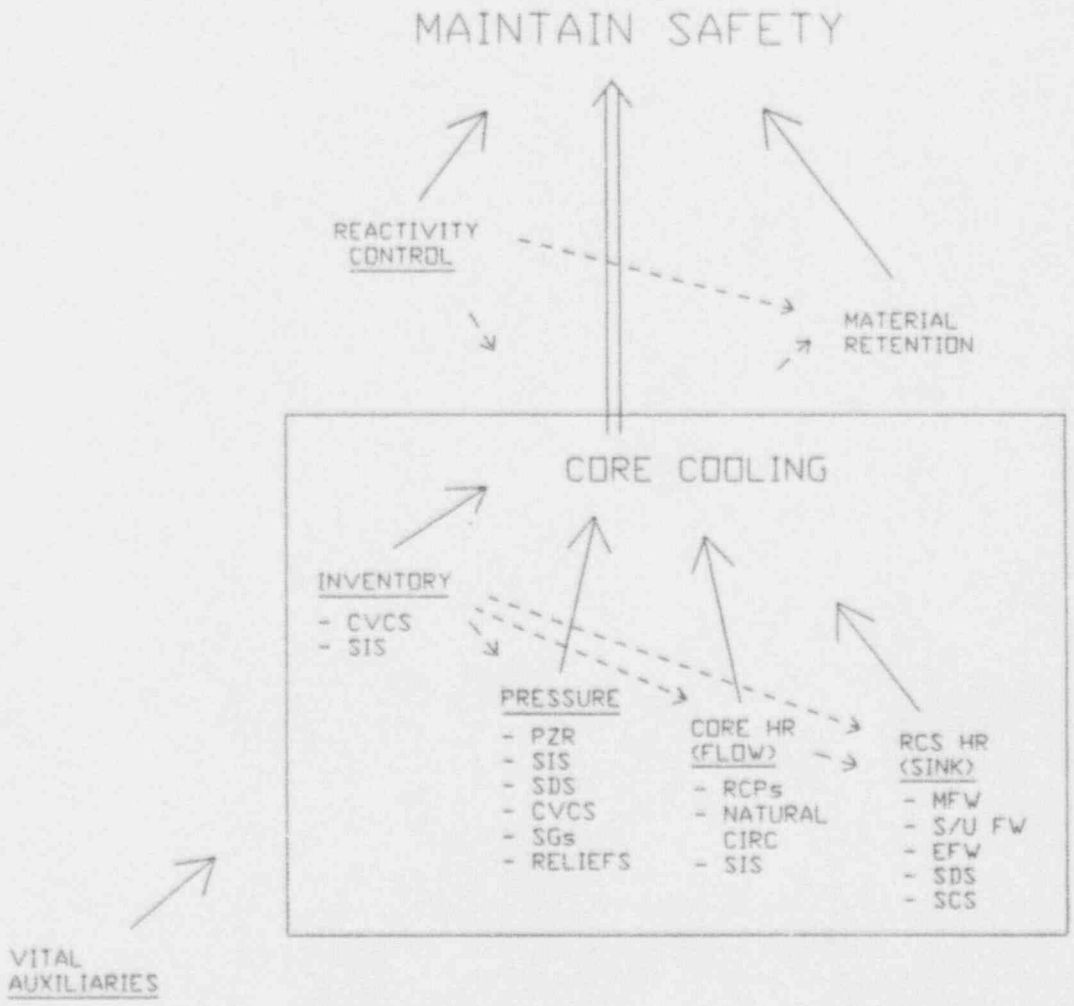

Figure 3 - System 80+ CSFs and Success Paths (page 2 of 3)

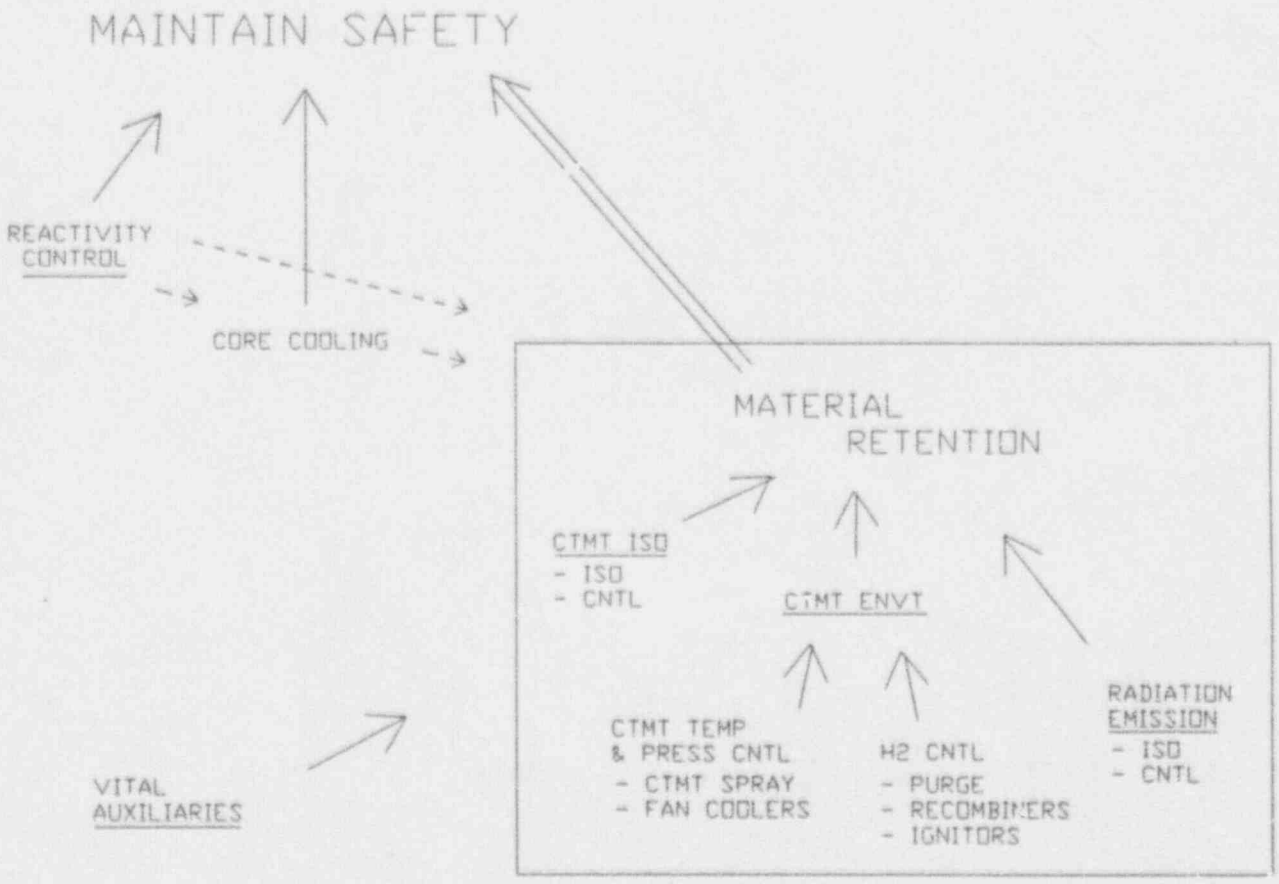

Figure 3 - System 80+ CSFs and Success Paths (page 3 of 3)

Table 2 - **SUCCESS PATHS** (Based on CEN-152 and CESSAR-DC)

Critical Function	SAFETY GRADE		NON-SAFETY GRADE	
	System 80	System 80+	System 80	System 80+
Reactivity Control	- Reactor trip - Safety injection - CVCS boration	- Reactor trip - Safety injection	- Rod control	- Rod control - CVCS boration
Maintenance of Vital Auxiliaries	- Emergency diesels - Startup xfmrs - Station batteries	- Emergency diesels - Reserve Aux xfmrs - Station batteries	- Unit xfmr backfeed - Alternate generator - Station batteries	- Unit xfmr backfeed - Alternate generator - Station batteries
RCS Inventory Control	- Safety injection	- Safety injection	- CVCS charging & letdown	- CVCS charging & letdown
RCS Pressure Control	- Safety injection - Rx coolant gas vent - CVCS aux spray - Primary reliefs	- Safety injection - Rx coolant gas vent - Primary reliefs	- PZR heaters & sprays - CVCS charging & letdown - SG steaming	- PZR heaters & sprays - CVCS charging & letdown - CVCS aux spray - SG steaming
Core Heat Removal	- Natural circulation - Safety injection	- Natural circulation - Safety Injection	- Forced circulation	- Forced circulation
RCS Heat Removal	- Emergency (Aux) feed - Shutdown cooling	- Emergency feed - Rapid depressurization - Shutdown cooling	- Main feed - Startup feed	- Main feed - Startup feed
Containment Isolation	- Penetration flowpath isolation	- Penetration flowpath isolation	- Penetration flowpath control	- Penetration flowpath control
Containment Environment	- Containment spray - H_2 recombiners	- Containment spray - H_2 recombiners	- Fan coolers - H_2 purge	- Fan coolers - H_2 purge - H_2 igniters
Radiation Emission	- Release path isolation	- Release path isolation	- Release path monitoring & control	- Release path monitoring & control

Table 3 - CSF SUCCESS PATHS: FUNCTIONAL DESIGN STATUS

CSF	SUCCESS PATH	UNCHANGED	MODIFIED	NEW	DELETED
REACTIVITY CONTROL	Reactor Trip	X			
	Safety Injection	X			
	Rod Control	X			
	CVCS Boration	X			
VITAL AUXILIARIES	Emergency Diesels	X			
	Reserve Aux Xfmrs	X			
	Station Batteries	X			
	Unit Xfmr Backfeed	X			
	Alternate Generator		X		
RCS INVENTORY CONTROL	Safety Injection	X			
	CVCS Charging & Letdown	X			
RCS PRESSURE CONTROL	Safety Injection	X			
	Reactor Coolant Gas Vent	X			
	Primary Reliefs	X			
	PZR Heaters & Sprays	X			
	CVCS Charging & Letdown	X			
	SG Steaming	X			
	CVCS Aux Spray	X			
CORE HEAT REMOVAL	Forced Circulation	X			
	Natural Circulation	X			
	Safety Injection	X			
RCS HEAT REMOVAL	Main Feed	X			
	Startup Feed		X		
	Emergency Feed	X			
	Rapid Depressurization			X	
	Shutdown Cooling	X			
CONTAINMENT ISOLATION	Penetration Path Iso	X			
	Penetration Path Cntl	X			

Table 3 - **CSF SUCCESS PATHS: FUNCTIONAL DESIGN STATUS**

CSF	SUCCESS PATH	UNCHANGED	MODIFIED	NEW	DELETED
CONTAINMENT ENVIRONMENT	Containment Spray	X			
	Fan Coolers	X			
	H_2 Purge	X			
	H_2 Recombiners	X			
	H_2 Igniters			X	
RADIATION EMISSION	Release Path Isolation	X			
	Release Path Control	X			

4.3 Operators' Role and Safety Functions

The operator, along with automated systems and inherent and passive plant features, is part of the defense-in-depth approach to assure that safety functions are maintained. Specifically, the operators' role in executing safety functions (Reference 10) can be summarized as follows:

1) monitor the plant to verify that the safety functions are accomplished;

2) actuate and control those systems that are not fully automated;

3) intervene where the automatically actuated systems are not operating as intended.

Item 2) above represents primary manual allocations (i.e., to human operators); Item 1) represents a supervisory role; Item 3) represents backup manual allocations (implying that the design provides automatic, passive or inherent system features as a first line of defense. Manual and automatic allocations in safety system operation are identified in the present Section of this report. Detailed specification of the operators' role in executing safety functions is provided by the actions and contingencies of the Emergency Procedure Guidelines.

After reviewing the requirements identified in Section 2.0, and the resulting criteria in Section 3.3, it is evident that the design process has sought to remove the need for the operator to respond with immediate control actions at the onset of events. This approach increases reliability of overall system protective actions by 1) reducing reliance on sustained human vigilance, and 2) reducing time stress on human performance, which induces errors. Further allocation decisions tend to be based on experience and precedent.

4.4 Allocation Data

To evaluate the acceptability of allocations to the operators' safety role, Table 4 provides a summary of the System 80+ safety function allocations in comparison to the Section 3.3 criteria.

The data fields of Table 4 are defined as follows:

Critical Functions & Success Paths - Per the contents of Tables 1 and 2.

Protective System or Commodity? - Whether or not this is a system relied on (i.e., credited) by CESSAR-DC Chapter 15 safety analyses to mitigate DBEs by performing the specified safety function.

10 CFR 50 Allocation Requirements - General or specific allocation requirements from 10 CFR 50 as summarized in Section 2.1 of the present report.

NUREG/CR-3331 Allocation Requirements - The acceptance path resulting from application of the criteria in Appendix B of the present report.

Auto Init - The equipment-generated (i.e., automatic) Protective Action that initiates a Protective System to achieve the Safety Function.

Manual Init - Whether or not the operator is afforded a means to manually initiate the Protective Action.

Control - After initiation, the manual and automatic elements of a control system configuration maintain the safety function throughout the limiting DBE. These are categorized as follows:

1) Automatic (Auto) - A configuration that is completely automatic, i.e., without means for manual action to execute the basic function.

2) Parallel (Par) - A configuration affording both manual and automatic control modes in which the operator has discretion to provide manual input at any time, but not to defeat the equivalent automatic processing (excluding resets and operating bypasses; e.g., reactor trip initiation). This strategy tends to increase the likelihood of executing the function.

3) Alternate (Alt) - A configuration affording both manual and

automatic control modes in which the operator has discretion over which mode of control is in use (e.g., pressurizer spray control). This strategy tends to provide increased flexibility to the operator (e.g., to balance workload or manage unusual conditions).

4) Complementary (Comp) - A configuration in which there is sharing of responsibilities between the human and machine components. While there may be some functional overlap, there is not complete redundancy. (An example is the use of SI for heat removal. SI is not initiated automatically in response to degraded core heat removal conditions, per se. If initiated, the automatic alignmment of SI is sufficient for initial core heat removal. However, the SI configuration must be manually adjusted and realigned to suit plant conditions.

5) Manual - A fully manual configuration (i.e., other than transmission); all actions are executed on plant equipment by operators.

The mixed configurations (parallel, alternate, and complementary) are depicted schematically in Figure 4.

Justification for solely manual init/cntl of protection (IEEE 603-1991) - For protective systems, an explanation of why some portion of achieving a safety function has not been automated. This is provided, as required, for the protective systems whose control responsibilities are described as either Alternate, Complementary, or fully manual (Parallel implies manual control is redundant to fully automatic control). Also used as an overall comment field, as indicated.

Additional explanation of the CSF success paths and their allocations, and the allocation rationale (in terms of satisfied Appendix B criteria), is provided in the remainder of this Section.

A. Reactivity Control

A.1 Reactor Trip - Reactor trip is a protective feature whose rapid and reliable initiation is of the utmost importance to safety. Automatic initiation of reactor trip is mandatory, and occurs in response to RPS or APS trip signals (see Reference 4, Sections 7.2 and 7.7.1.1.11, respectively); manual initiation is also provided to enable operators to perform assigned supervisory and backup roles. Operator actions will be performed under normal MCR habitability

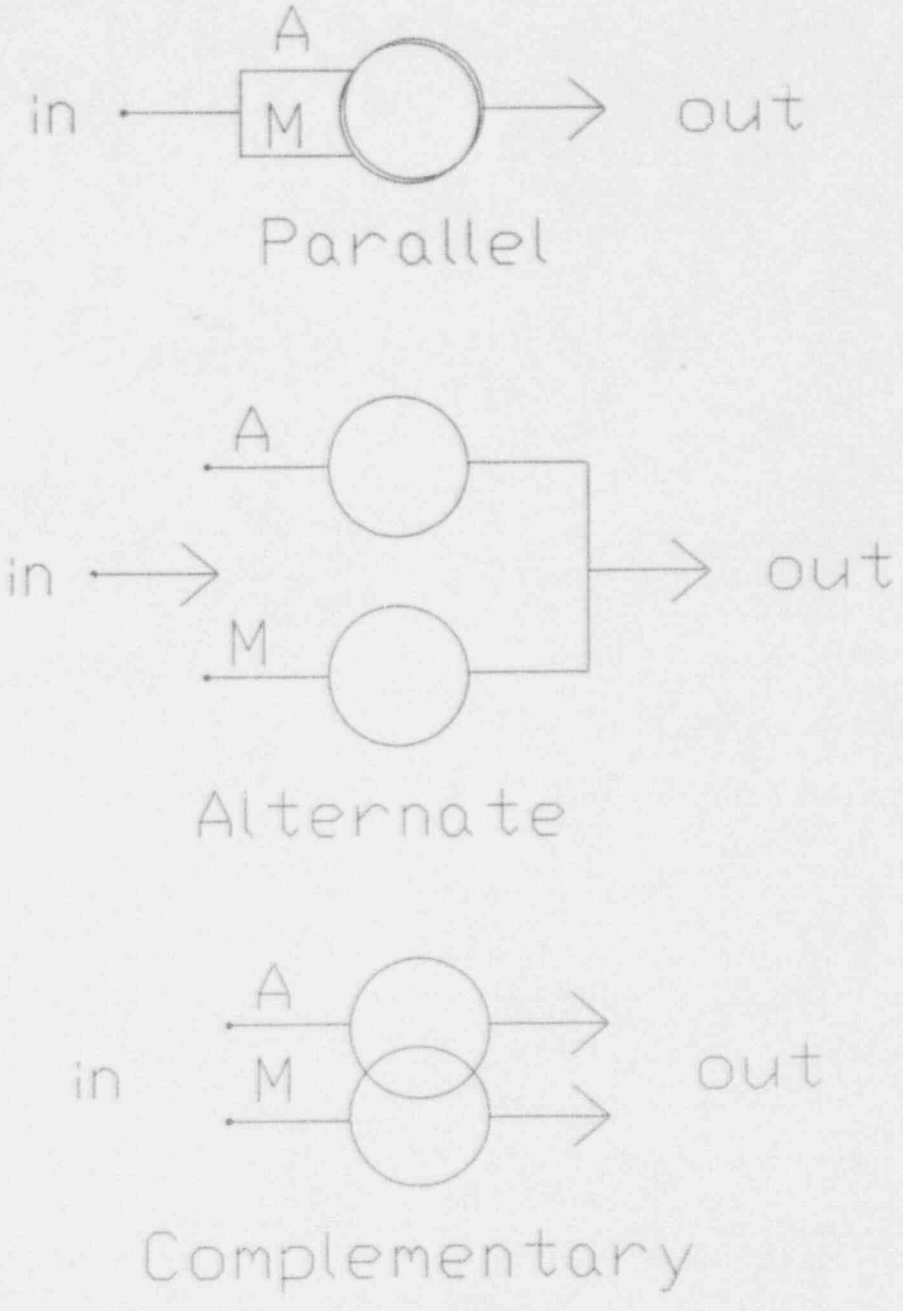

Figure 4 - Mixed Allocation Configurations

conditions. As a discrete function, Reactor Trip has no continuous control component to be allocated. These System 80+ allocations are unchanged from those in System 80.

A.1 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual initiation is desirable for flexibility and reliability (9d & 9e).

A.2 Safety Injection - The SI system performs Reactivity Control by direct high pressure injection of borated water into the Rx vessel. This occurs automatically, when a SIAS is generated by the ESF system. Note that SIAS is not generated automatically in order to shut the reactor down, per se; however, SI boration rate is sufficient to maintain shutdown margins even if the reactive rod were ejected from the core (see Chapter 7, Reference 4). Manual initiation is provided to enable operators to perform assigned supervisory and backup roles. Following initiation, operators have the responsibility to evaluate, adjust, and/or terminate SI. These System 80+ allocations are unchanged from those in System 80.

A.2 **Allocation Rationale:** Automation is preferable based on precedent (5a), and in preference to human performance (5b) based on characteristics of the function (e.g., per 7a, 7b, 7d, 7e). Manual operation is desirable for flexibility and reliability (9d & 9e).

A.3 Charging & Volume Control (Boration) - The CVCS can be used to inject borated water into the RCS. However, it is a relatively slow, long-term means of adjusting core reactivity, and is not a credited safety system for Reactivity Control. Boration is not a standard lineup for the CVCS, and it is performed and initiated manually from the control room. However, once aligned, the CVCS can be operated in either automatic or manual modes. These System 80+ allocations are unchanged from those in System 80.

A.3 **Allocation Rationale:** The function is suitable for allocation to the operator (8a, 8b, & 8c).

A.4 Rod Control - Rod control provides a backup success path that can be used if rod(s) stick or otherwise fail to return to their bottom travel positions following a reactor trip.

This is accomplished by reshutting the trip breakers and energizing the rod drive mechanisms, then attempting to actively drive the rods inward using the rod control system. The rod control system is not a protective means of reactivity insertion, it is not a credited safety system for Reactivity Control, and the execution of this task is fully manual. These System 80+ allocations are unchanged from those in System 80.

A.4 **Allocation Rationale:** Given the suitability of the associated tasks (e.g., per 8a, 8b, & 8c), human performance is clearly preferable for this application (6a, or 3b) due to the need to deliberately shut the Reactor Trip Breakers as part of the process.

B. Vital Auxiliaries

The configuration of equipment and resource commodities used to maintain Vital Auxiliaries is part of the overall design of the electrical system. Electrical system design and operation is explained in Chapter 8 of CESSAR-DC (Reference 4).

B.1 Emergency Diesel Generators - Emergency DG operation is initiated automatically on Loss of Offsite Power, and by SIAS or EFAS signals. Startup and vital loading are performed by automatic load sequencing. Manual startup and loading is also possible. Given automatic initiation, the operator is responsible to evaluate continued DG operation, modify its loading as necessary (particularly to satisfy subsequent CSFs), and transfer fuel oil to Fuel System (before the seven day fuel supply is exhausted; see Section 9.5.4.1.1 of Reference 4). The auto sequencer must complete its function before sequenced loading can be manually modified. Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

B.1 **Allocation Rationale:** Automation is mandatory because of federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically prover (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, & 9f).

B.2 Reserve Aux Transformers - The Reserve Aux Transformers provides an offsite supply grid connection that is separate from the Unit Main Transformer grid. Use of the Reserve Aux Transformer is automatically initiated via fast bus transfer

on loss of the Unit Main Transformer. Manual transfer is also possible. The operator is responsible to evaluate the electric plant and modify its loading and configuration as necessary (particularly to satisfy subsequent CSFs). Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

B.2 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, and 9f).

B.3 Vital Station Batteries - Vital Station Batteries are normally on their bus in some form of standby charging or discharging operation. Thus, "initiation" is to place or retain the battery on the bus; "control" is to load or unload the bus. On loss of vital AC power, initial loading established by auto trips and load shedding. No immediate operator action is required. However, the operator will evaluate operating conditions, and will shed unnecessary loads manually to extend battery life from 2 to 8 hrs (see Section 8.3.2.1.2.1.2 of Reference 4) while taking steps to restore AC power. Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

B.3 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, & 9f).

B.4 Alternate Generator - System 80+ provides a permanently installed Alternate Generator (i.e., a combustion turbine) as a separate and diverse source of onsite generating capacity. This increases the redundancy and diversity of the AC power success paths in System 80+. Alternate Generator operation is initiated automatically on LOOP (along with Diesel Generator initiation). Loading is by auto sequencing of permanent non-vital bus loads; however, vital bus loads can be assumed manually if DGs fail. The operator is responsible to evaluate continued Alternate Generator operation, and modify its

loading as necessary. The Alternate Generator is not credited as a safety system for Vital Auxiliaries. The System 80 design did not include a permanently installed Alternate Generator, although they have been provided as options. The allocations of Alternate Generator control are consistent with those for DG control in System 80 and System 80+.

B.4 **Allocation Rationale**: Since this is described in Table 3 as a "modified" success path, the steps through the criteria of Appendix B are given in full:

1. Is automation mandatory?
   a. Are working conditions hostile to humans: No
   b. Are tasks included which humans cannot perform: No
   c. Is automation required by law or regulations: No
   d. Is automation required to assure plant safety or protection: No

   No (all) - Go to step 3.

3. Is human performance mandatory?
   a. Is automation technically infeasible: No
   b. Is human required to retain policy-level or ultimate control: No
   c. Is human required by law or regulation: No

   No (all) - Go to step 5.

5. Is automation clearly preferable to human operators?
   a. Is automation technology well-established as suitable (i.e., effective, reliable, cost-effective, etc.): Yes
   b. Is human performance acknowledged as less satisfactory: Yes (due to time requirements of Alternate Generator S/U)

   Yes (all) - Tentatively allocate to auto; go to step 9.

9. Reconsider the tentative automatic allocations in terms of their negative impact on human operator performance.
   a. Would manual performance of the task help to keep the operator engaged with the plant, informed of process status, or prepared to plan and solve problems: No
   b. Would manual performance of the task provide the operator with important opportunities to develop or maintain valuable skills or knowledge: No
   c. Will absolute implementation of the automatic feature(s) contribute to operator underloading (e.g., boredom): No
   d. Would the option for manual control from the control room afford desired flexibility: Yes
   e. Would the option for manual control from the control room afford more reliable performance of the function: Yes
   f. Would the option for manual control from the control room

be desirable for testing, maintenance, or management of off-normal conditions: Yes

Yes (any) - Make a tentative allocation to automation with operator discretion. If operator discretion is subordinate (man may initiate but not override automatic action), go to step 12 (Step 12, "Consider the residual role of the human operator in support of the automated function," alludes to detailed design tasks that are addressed during human-system interface design.)

B.5 Unit Main Transformers - The Unit Main Transformer provides a connection to an offsite supply grid that is separate from the Reserve Aux Transformer grid. The Unit Main is the default offsite AC power source, and is not credited as a safety system for Vital Auxiliaries. Normally, at power, the Unit Main Transformers are on line connecting the plant electrical system to supply power to the offsite grid; on turbine trip, the Main Transformer breakers remain shut, allowing power to be drawn from the grid to supply plant electrical demands (i.e., "backfeed"). The operator is responsible to evaluate the electric plant and modify its loading and configuration as necessary. These System 80+ allocations are unchanged from those in System 80.

B.5 **Allocation Rationale**: The function is suitable for allocation to the operator (8a, 8b, & 8c).

B.6 Non-Vital Station Batteries - Non-Vital Station Batteries are normally on their bus in some form of standby charging or discharging operation. Thus, "initiation" is to place or retain the battery on the bus; "control" is to load or unload the bus. Non-vital station batteries are not credited as a safety system for Vital Auxiliaries. On loss of non-vital AC power, initial loading established by auto trips and load shedding. No immediate operator action is required. However, the operator will evaluate operating conditions, and will shed unnecessary loads manually to extend battery life while taking steps to restore AC power. These System 80+ allocations are unchanged from those in System 80.

B.6 **Allocation Rationale**: Automation is mandatory because of sustained monitoring and rapid response time requirements (1b). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, & 9f).

C. RCS Inventory Control

C.1 Safety Injection - The SI system performs Inventory Control by direct high pressure injection of borated water into the Rx vessel (see Section 6.3, Reference 4). This occurs automatically, when a SIAS is generated by the ESF system (see Section 7.3, Reference 4), or passively, if RCS pressure falls below SIT pressure. Manual initiation is also provided to enable operators to perform assigned supervisory and backup roles. Following initiation, operators have the responsibility to evaluate, adjust, and/or terminate SI; however, after initiation, operation can continue for one to three hours without manual intervention (Reference 4, Section 6.3.3.4). Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

C.1 **Allocation Rationale**: Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, & 9f).

C.2 Charging & Volume Control (Charging & Letdown) - The CVCS can be used to inject water into the RCS. However, it is a long term, relatively slow, backup means of adding core inventory, and is not a credited safety system for Inventory Control (see Section 9.3.4, Reference 4). CVCS is initiated manually from the control room. However, once initiated, the CVCS can be operated in either automatic or manual modes. These System 80+ allocations are unchanged from those in System 80.

C.2 **Allocation Rationale**: The function is suitable for allocation to the operator (8a, 8b, & 8c).

D. RCS Pressure Control

D.1 Safety Injection - The SI system performs Pressure Control by high pressure injection of borated water into the RCS (see Section 6.3, Reference 4). This occurs automatically, when a SIAS is generated by the ESF system (see Section 7.3, Reference 4), or passively, if RCS pressure falls below SIT pressure. Manual initiation is also provided to enable operators to perform assigned supervisory and backup

roles. Following initiation, operators have the responsibility to evaluate, adjust, and/or terminate SI; however, after initiation, operation can continue for one to three hours without manual intervention (Reference 4, Section 6.3.3.4). Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

D.1 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is desirable for flexibility, reliability, and management of unusual conditions (9d, 9e, & 9f).

D.2 Rx Coolant Gas Vent System - The Reactor Coolant Gas Vent System (RCGVS) is a portion of the SDS. It permits controlled RCS depressurization to SCS entry conditions during natural circulation cooldown scenarios (see Section 6.7, Reference 4). Rapid response of this function is not required, since cooldown typically takes 8-12 hours. Thus, automatic initiation is not necessary or even desirable. Instead, operators have responsibility to initiate and control RCS depressurization by the RCGVS. Operator actions will be performed under normal MCR habitability conditions. Manual operation of RCGVS in System 80+ is an unchanged allocation from System 80, although System 80 credited Aux Spray for permitting depressurization with natural circulation. Likewise, Aux Spray was manually allocated in System 80, and remains so in System 80+. Thus, these System 80+ allocations are unchanged from System 80.

D.2 **Allocation Rationale:** Automation could be argued to be mandatory because of general regulations for automatic protective actions under GDC 20 (1c). However, although this is a credited safety system, it is not required to make immediate or rapid (i.e., protective) responses in its safety role. In addition, the uncertain conditions of its use, and concerns for inadvertent initiation make human performance preferable (6).

D.3 PZR Heaters & Sprays - Normal RCS Pressure Control is provided by the operation of PZR heaters and sprays to control PZR saturation conditions. This system is described as manually initiated in that it is operated in either automatic or manual modes at operator discretion; normally it would be on line in auto. It is not credited as a safety system for

RCS Pressure Control. These System 80+ allocations are unchanged from those in System 80.

D.3 **Allocation Rationale:** Automation is preferable because of the repetitive and predictable nature of the function (5); the system is normally left on-line to cycle in automatic. However, manual operation affords necessary flexibility and improved reliability (9d-f).

D.4 Charging & Volume Control - The CVCS provides PZR Aux Spray as an alternate means (i.e., during natural circulation cooling, without RCP head to provide PZR Main Spray) to reduce RCS pressure under saturated PZR conditions. CVCS can also be used to control RCS pressure with a solid PZR by adjusting RCS inventory. The CVCS is not a credited safety system for Pressure Control. CVCS operation is initiated manually from the control room. The CVCS can be operated in either automatic or manual modes, but manual mode is specified for solid plant operations due to the possibility of rapid pressure excursions. Although the System 80+ CVCS is a fully non-safety system (a change from System 80; see Section 4.2) the operation of the CVCS, and the allocation of these System 80+ functions, are unchanged from those in System 80.

D.4 **Allocation Rationale:** The uncertainty of conditions involved in the need for or control of RCS Pressure via CVCS make human performance preferable (6).

D.5 SG Steaming - Controlled heat removal through the SGs (see Section 10, CESSAR-DC) can be used to control RCS pressure, particularly when solid, by manipulating (i.e., contracting) available RCS inventory. Steaming and feeding in this case are initiated and controlled manually from the control room to avoid excessive pressure excursions. The Sgs are not a credited safety system for RCS Pressure Control. These System 80+ allocations are unchanged from those in System 80.

D.5 **Allocation Rationale:** The uncertainty of conditions involved in the need for or control of RCS Pressure via SG Steaming make human performance preferable (6).

D.6 Pressure Reliefs - Design basis overpressure relief for vessel protection is provided without the option for manual initiation. Some older units (predating System 80) used Power-Operated Relief Valves; PORVs permitted both manual and automatic operation. However, experience has dictated a return to more simple and standard (i.e., hydromechanical)

relief valve designs in recent plants (including System 80). Thus, these System 80+ allocations are unchanged from System 80.

D.6 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual operation is not necessary or desirable.

E. Core Heat Removal

E.1 Natural Circulation - Initiation and control of natural circulation flow are essentially passive (equivalent to automatic) functions. The operator has responsibility to evaluate Heat Removal performance, and to maintain an effective heat sink. Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from System 80.

E.1 **Allocation Rationale:** Automation can be viewed as mandatory because of federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). As a passive function, manual operation can be viewed as either implicit, or inapplicable.

E.2 Forced Circulation (RCPs) - Initiation of forced circulation (i.e., RCP flow) is manual (the discrete "pump run" function has no continuous control component). Core Heat Removal via forced circulation is the normal means of Core Heat Removal during operations, but is not credited for safety. These System 80+ allocations are unchanged from System 80.

E.2 **Allocation Rationale:** The function is suitable for allocation to the operator (8a, 8b, & 8c).

E.3 Safety Injection (DVI) - The SI system performs Core Heat Removal by direct high pressure injection of borated water into the Rx vessel. For DBEs, unavailability of natural circulation may imply RCS pressure or inventory problems, and SI actuation is thus a resultant possibility. However, DVI is not the preferred means for Core Heat Removal, and SIAS is not generated in response to Heat Removal problems, per se. Following either automatic, passive, or manual SIAS initiation, the DVI lineup is automatically established;

operation can then continue for one to three hours without manual intervention (Reference 4, Sections 6.3.2.7 & 6.3.3.4). The operator has responsibility to evaluate Core Heat Removal performance, to modify the SI lineup to suit plant conditions, and to maintain effective RCS Heat Removal. Operator actions will be performed under normal MCR habitability conditions. Changes to the SI injection points are improvements in the physical plant configuration; however, the related System 80+ allocations are unchanged from System 80.

E.3 **Allocation Rationale**: Automation could be argued to be mandatory because of general regulations for automatic protective actions under GDC 20 (1c). However, although this is a credited safety system, it is not required to make immediate or rapid (i.e., protective) responses in its safety role. The uncertainty of conditions involved in the need for or performance of Core Heat Removal via SIS make human performance preferable (6).

F. RCS Heat Removal

F.1 Main Feed - The Main Feed system provides heat removal for the RCS using the SGs and Main Feed Pumps. This is the normal means of heat removal for power operation. It is initiated manually, but may be controlled in either manual or automatic modes. Main Feed is not a credited safety system. These System 80+ allocations are unchanged from those in System 80.

F.1 **Allocation Rationale**: The function is suitable for allocation to the operator (8a, 8b, & 8c).

F.2 Startup Feed - The Startup Feed system provides heat removal for the RCS using the SGs and Startup Feed Pump. This is the normal means of heat removal for very low power (0 to 5%) operation. Startup Feed is automatically initiated on reactor trip with complete loss of MFW, providing diversity and defense in depth against total loss of feed. The system can also be manually initiated and controlled. Startup Feed is not a credited safety system. The addition of automatic initiation and control of Startup Feed is a change to the prior System 80 allocation.

F.2 **Allocation Rationale**: Since this is described in Table 3 as a "modified" success path, the steps through the criteria of Appendix B are given in full:

1. Is automation mandatory?
 a. Are working conditions hostile to humans: No
 b. Are tasks included which humans cannot perform: No
 c. Is automation required by law or regulations: No
 d. Is automation required to assure plant safety or protection: No

No (all) - Go to step 3.

3. Is human performance mandatory?
 a. Is automation technically infeasible: No
 b. Is human required to retain policy-level or ultimate control: No
 c. Is human required by law or regulation: No

No (all) - Go to step 5.

5. Is automation clearly preferable to human operators?
 a. Is automation technology well-established as suitable (i.e., effective, reliable, cost-effective, etc.): Yes
 b. Is human performance acknowledged as less satisfactory: Yes (due to risk reduction and utility requirements)

Yes (all) - Tentatively allocate to auto; go to step 9.

9. Reconsider the tentative automatic allocations in terms of their negative impact on human operator performance.
 a. Would manual performance of the task help to keep the operator engaged with the plant, informed of process status, or prepared to plan and solve problems: Yes
 b. Would manual performance of the task provide the operator with important opportunities to develop or maintain valuable skills or knowledge: No
 c. Will absolute implementation of the automatic feature(s) contribute to operator underloading (e.g., boredom): No
 d. Would the option for manual control from the control room afford desired flexibility: Yes
 e. Would the option for manual control from the control room afford more reliable performance of the function: No
 f. Would the option for manual control from the control room be desirable for testing, maintenance, or management of off-normal conditions: Yes

Yes (any) - Make a tentative allocation to automation with operator discretion. If operator discretion is subordinate (man may initiate but not override automatic action), go to step 12 (Step 12, "Consider the residual role of the human operator in support of the automated function," alludes to detailed design tasks that are addressed during human-system interface design.)

F.3 Emergency Feed - The Emergency Feedwater system assures that secondary plant heat removal capacity remains available if normal feedwater sources are lost. Initiation of EFW occurs automatically when an EFAS is generated by the PPS; manual initiation is also provided to enable operators to perform assigned supervisory and backup roles (this satisfies specific requirements of Section 2.1.2.b). EFW control requires no operator intervention until .5 hrs after limiting DBE (CESSAR-DC 10.4.9); operators have the responsibility to operate ADVs, ensure adequate level in the Sgs, provide makeup to the EFWSTs, and evaluate, adjust or terminate EFW function. Operator actions are performed under normal habitability conditions. These System 80+ allocations are unchanged from those in System 80.

F.3 **Allocation Rationale**: Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual initiation is desirable for reliability (9e).

F.4 Rapid Depressurization (RD) - The RD portion of the SDS can be used to depressurize the plant while using SIS/DVI for Core Heat Removal. This accomplishes heat removal via feed-and-bleed, also known as "once-through cooling." It is not the preferred means for RCS Heat Removal, and it is not a credited safety system for controlling RCS heat removal on System 80+. However, if no Sgs are available for steaming (i.e., total loss of feed, a beyond-design-basis event) then this provides an added, diverse success path. The operator has responsibility to evaluate and control RCS Heat Removal performance, and to maintain an adequate RCS inventory. Control of RD itself is a discrete function (i.e., start/stop only; no throttling). Operator actions will be performed under normal MCR habitability conditions. Once-through cooling using PORVs was available on some earlier ABB-CE plants. However, due to PORV problems, they were eliminated from newer designs (see D.6), and once-through cooling was not afforded on System 80 (i.e., not at Palo Verde; however, RD is being installed in Korea). The manual allocation of the RD "bleed" function in System 80+ is consistent with similar allocations in preceding ABB-CE plant designs.

F.4 **Allocation Rationale**: Since this is described in Table 3 as a "new" success path, the steps through the criteria of Appendix B are given in full:

1. Is automation mandatory?
a. Are working conditions hostile to humans: No
b. Are tasks included which humans cannot perform: No
c. Is automation required by law or regulations: No
d. Is automation required to assure plant safety or protection: No
No (all) - Go to step 3.

3. Is human performance mandatory?
a. Is automation technically infeasible: No
b. Is human required to retain policy-level or ultimate control: No (The distinction between this question and 3a is somewhat subjective.)
c. Is human required by law or regulation: No
No (all) - Go to step 5.

5. Is automation clearly preferable to human operators?
a. Is automation technology well-established as suitable: No
b. Is human performance acknowledged as less satisfactory: No
No (any) - Go to step 6.

6. Is human performance clearly preferable to automation?
a. Is human performance regarded as clearly necessary, or superior to automation: Yes (given the suitability of the required tasks, and due to the uncertain conditions of the use of RD and the concerns for spurious actuation.)
Yes - Allocate to human; go to step 11. (Step 11, "Consider residual automated and control system support for the operator," alludes to detailed design tasks that are addressed during human-system interface design.)

F.5 Shutdown Cooling - SCS is not initially useful as success path in DBEs initiated from higher mode operation; SCS is placed on line as part of the normal transition to lower modes. Rapid initiation of SCS is not required (cooldown to SCS entry conditions typically takes 8-12 hours); on the other hand, spurious system actuation would be problematic. Thus, automatic actuation is not necessary or even desirable, while manual actuation is acceptable. Operator actions will be performed under normal MCR habitability conditions. Certain changes have been made to the SCS design from System 80 (e.g., it no longer shares pumps with SI, and has a higher pressure rating, permitting removal of a suction valve trip that was a chronic cause for loss of SCS; see Reference 4, Chapter 5). However, these are improvements in the physical plant

configuration; the related System 80+ allocations are similar to those in System 80.

F.5 **Allocation Rationale:** Automation could be argued to be mandatory because of general regulations for automatic protective actions under GDC 20 (1c). However, although this is a credited safety system, it is not required to make immediate or rapid (i.e., protective) responses in its safety role. In addition, the uncertain conditions of its use, and concerns for inadvertent initiation make human performance preferable (6).

G. Containment Isolation

G.1 Penetration Flowpath Isolation - Containment Flowpath Isolation is performed by automatically shutting containment isolation valves on CIAS actuation. CIAS may also be actuated manually, to enable operators to perform assigned supervisory and backup roles. CIAS does not shut penetrations used for accident mitigation, RCP operation, or safe shutdown; these are isolated manually, if necessary. If a CIAS is actuated, explicit manual reset is required before any of the flowpaths can be reopened (to prevent inadvertent release, per 10 CFR 50.34(f)(2)(xiv)); subsequent reopening of the valves must also be done manually (remote manual controls are provided for all automatically isolated valves). As a discrete function (i.e., shutting the valves), Containment Flowpath Isolation has no continuous control component. Operator actions are performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

G.1 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual initiation is desirable for reliability (9e).

G.2 Penetration Flowpath Control - Containment Flowpath Control is performed by individually selecting and shutting containment isolation valves using component control systems. This is fully manual, enabling operators to perform assigned supervisory and backup roles, and providing flexibility and reliability in the overall system. If a CIAS has already actuated, the CIAS must be manually reset before any of the flowpath control valves can be reopened (to prevent inadvertent release, per 10 CFR 50.34(f)(2)(xiv)). As a discrete function (i.e., to shut the valves), Containment

Flowpath Control has no continuous control component. Operator actions are performed under normal MCR habitability conditions. This is not a credited safety system. These System 80+ allocations are unchanged from those in System 80.

G.2 **Allocation Rationale:** The function is suitable for allocation to the operator (8a, 8b, & 8c).

H. Containment Environment

H.1 Containment Spray - The Containment Spray system actively removes heat from a sealed Containment Environment so that containment temperature and pressure remain within limits under anticipated accident conditions. Initiation of Containment Spray occurs automatically when a CSAS is generated by the PPS; manual initiation is also provided, to enable operators to perform assigned supervisory and backup roles. Following initiation, operators have the responsibility to evaluate, adjust, and/or terminate Containment Spray. Additionally, operators can reconfigure the system to use SCS or an external water source if the preferred containment spray lineup is unsuccessful. Normally, however, manual action is indefinitely unnecessary, as the water is continuously recirculated through the IRWST. Operator actions will be performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

H.1 **Allocation Rationale:** Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual initiation is desirable for reliability (9e).

H.2 Fan Coolers - The Containment Fan Coolers actively remove heat from the Containment Environment to control containment temperature (and pressure, in a sealed containment). Containment Fan Coolers are manually started and are normally in operation; additional coolers may be manually started as an emergency mode supplement. Operator actions will be performed under normal MCR habitability conditions. This is not a credited safety system. These System 80+ allocations are unchanged from those in System 80.

H.2 **Allocation Rationale:** The function is suitable for allocation to the operator (8a, 8b, & 8c).

H.3 H_2 Recombiners - The H_2 Recombiners are a portable, externally connected means to maintain Hydrogen levels within limits in a sealed Containment Environment under anticipated accident conditions. They are not the initial success path for containment Hydrogen control. H_2 Recombiners are manually aligned and started, by procedure, within 72 hours following a LOCA. After startup, the H_2 Recombiners run continuously; operators are responsible to evaluate and/or terminate continued H_2 Recombiner operation. Operator actions will be performed in the Nuclear Annex Building under acceptable post-accident habitability conditions. These System 80+ allocations are unchanged from those in System 80.

H.3 **Allocation Rationale**: Automation could be argued to be mandatory because of general regulations for automatic protective actions under GDC 20 (1c). However, although this is a credited safety system, it is not required to make immediate or rapid (i.e., protective) responses in its safety role. The function is suitable for allocation to the operator (8a, 8b, & 8c).

H.4 H_2 Purge - H_2 Purge is a permanently installed means to control containment Hydrogen levels. H_2 Purge is accomplished using portions of the Annulus Ventilation System, and the Containment Low Volume Purge System. H_2 Purge is manually initiated. After startup, operators are then responsible to evaluate, adjust, and/or terminate H_2 Purge operation; H_2 Purge is automatically isolated on CIAS actuation. This function does not require any immediate or rapid responses, and operator actions will be performed under normal MCR habitability conditions. This is not a credited safety system. Although the containment annulus vent system is part of an improved containment design for System 80+, these allocations for the System 80+ H_2 Purge success path are unchanged from those in System 80.

H.4 **Allocation Rationale**: Given the suitability of the associated tasks (e.g., per 8a, 8b, & 8c, or 4), human performance is preferable for this application (6a, or 3b & 3c) due to the potential for inadvertent release during a severe accident.

H.5 H_2 Ignitors - The H_2 Ignitors are a permanently installed means to maintain Hydrogen levels within limits in a sealed Containment Environment. If H_2 Purge and Recombiners are not available, H_2 Ignitors can be manually started on indication of high Hydrogen levels in containment. After startup, operators then are responsible to evaluate, adjust, and/or terminate H_2

Ignitor operation. Operator actions will be performed under normal MCR habitability conditions. This success path was not part of the System 80 design, but has been proven in operation on other systems. It has been added for System 80+ for increased redundancy and diversity of the Hydrogen control success paths. It is not a credited safety system. This does not represent a significant change of the System 80+ operators' role or responsibilities from those in System 80.

H.5 **Allocation Rationale:** Since this is described in Table 3 as a "new" success path, the steps through the criteria of Appendix B are given in full:

1. Is automation mandatory?
   a. Are working conditions hostile to humans: No
   b. Are tasks included which humans cannot perform: No
   c. Is automation required by law or regulations: No
   d. Is automation required to assure plant safety or protection: No

   No (all) - Go to step 3.

3. Is human performance mandatory?
   a. Is automation technically infeasible: No
   b. Is human required to retain policy-level or ultimate control: No (The distinction between this question and 3a is somewhat subjective.)
   c. Is human required by law or regulation: No

   No (all) - Go to step 5.

5. Is automation clearly preferable to human operators?
   a. Is automation technology well-established as suitable: No
   b. Is human performance acknowledged as less satisfactory: No

   No (any) - Go to step 6.

6. Is human performance clearly preferable to automation?
   a. Is human performance regarded as clearly necessary, or superior to automation: Yes (given the suitability of the required tasks, and the concern for equipment damage due to inadvertent actuation)

   Yes - Allocate to human; go to step 11. (Step 11, "Consider residual automated and control system support for the operator," alludes to detailed design tasks that are addressed during human-system interface design.)

I. Radiation Emission

I.1 Release Path Isolation - Containment-to-environment release paths are automatically isolated on high radiation and CIAS. They can also be manually isolated, to enable operators to perform assigned supervisory and backup roles. As a discrete function (i.e., to shut the valves), Release Path Isolation has no continuous control component. Operator actions are performed under normal MCR habitability conditions. These System 80+ allocations are unchanged from those in System 80.

I.1 **Allocation Rationale**: Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and pragmatically available (2b). Manual initiation is desirable for reliability (9e).

I.2 Release Path Control - Containment-to-environment release paths can be individually isolated by selecting and manually shutting individual valves through the component control systems, to enable operators to perform assigned supervisory and backup roles. Operator actions are performed under normal MCR habitability conditions. This is not a credited safety system. These System 80+ allocations are unchanged from those in System 80.

I.2 **Allocation Rationale**: The function is suitable for allocation to the operator (8a, 8b, & 8c).

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 1 of 10)

CRITICAL FUNCTION: A. Reactivity Control	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATH		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Reactor Trip	Yes	Auto init (GDC 20)	1b-d; 2; 9d,e	RPS APS	Yes	-	
2. Safety Injection	No	-	5; 9d,e	SIAS	Yes	Comp	
3. CVCS (boration)	No	-	8	No	Yes	Alt	
4. Rod Control	No	-	6	No	Yes	Manual	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 2 of 10)

CRITICAL FUNCTION: B. Maintenance of Vital Auxiliaries	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Emergency Diesel Generators (AC)	Yes	Auto init (GDC 20)	1c-d; 2; 9d,e,f	LOOP SIAS EFAS	Yes	Comp	
2. Reserve Aux Transformers (Site AC)	Yes	Auto init (GDC 20)	1b-d; 2; 9d,e,f	Loss of Unit Main Xfmr	Yes	Comp	
3. Vital Station Batteries (DC)	Yes	Auto init (GDC 20)	1b-d; 2; 9d,e,f	Loss of vital AC	Yes	Comp	
4. Alternate Generator (AC)	No	-	5; 9d,e,f	LOOP	Yes	Comp	
5. Unit Main Transformer (Site AC)	No	-	8	No	Yes	Alt	
6. Non-vital Station Batteries (DC)	No	-	1b; 2; 9d,e,f	Yes	Yes	Alt	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 4 of 10)

CRITICAL FUNCTION: C. RCS Inventory Control	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Safety Injection	Yes	Auto Init (GDC 20)	1b-n, 2; 9d,e,f	SIAS	Yes	Comp	
2. CVCS (Charging & Letdown)	No	-	B	No	Yes	Alt	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 5 of 10)

CRITICAL FUNCTION: D. RCS Pressure Control	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Safety Injection	Yes	Auto init (GDC 20)	1b-d; 2; 9d,e,f	SIAS	Yes	Comp	
2. Rx Gas Vent System (Safety Depressurization,	Yes	Auto init (GDC 20)	(1c); 6	No	Yes	Manual	System is credited for providing depressurization ability to SCS entry conditions. Rapid response is not required (cooldown typically takes 8-12 hours), but spurious system actuation could compromise safety. Thus, auto initiation is not necessary or desirable. Operator actions performed under normal MCR habitability conditions.
3. PZR Heaters & Sprays	No	-	5; 9d-f	No	Yes	Alt	
4. CVCS (Charging & Letdown, Aux Spray)	No	-	6	No	Yes	Alt	
5. SG Steaming	No	-	6	No	Yes	Alt	
6. Pressure Reliefs	Yes	Auto init (GDC 20)	1b-d; 2	Pressure Set point	No	Auto	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 6 of 10)

CRITICAL FUNCTION: E. Core Heat Removal	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Natural Circulation	Yes	Auto init (GDC 20)	1c,d; 2	Passive	Yes	Comp	
2. Forced Circulation	No	-	8	No	Yes	-	
3. Safety Injection (Direct Vessel Injection)	Yes	Auto Init (GDC 20)	(1c); 6	No	Yes	Comp	DVI provides an added success path (not the preferred means) for Core Heat Removal. For DBEs, loss of natural circ may imply prior RCS Pressure or Inventory problems and possible auto SI initiation, but not for Heat Removal per se. With SI initiation, DVI lineup is automatically established. Operator has responsibility to evaluate Core Heat Removal performance, to modify SI lineup to best suit plant conditions, and to initiate and maintain heat sink performance.

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 7 of 10)

CRITICAL FUNCTION: F. RCS Heat Removal	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Main Feed	No	-	8	No	Yes	Alt	
2. Start Up Feed	No	-	5; 9a,d,f	Yes	Yes	Comp	
3. Emergency Feed	Yes	Auto & Manual init (GDC 20; 50.34(f)(2)(xii); 50.62(c)	1b-d; 2; 9e	EFAS	Yes	Comp	
4. Rapid Depressurization System (Safety Depressurization)	No	-	(3b; 4); 6	No	Yes	Manual	
5. Shutdown Cooling	Yes	Auto init (GDC 20)	(1c); 6	No	Yes	Alt	SCS not initially useful as success path in DBEs, and inadvertent initiation is problematic; thus, manual operation is desirable. Actions performed under normal MCR habitability conditions.

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 8 of 10)

CRITICAL FUNCTION: G. Containment Isolation	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Penetration Flowpath Isolation	Yes	Auto init, Manual reset (GDC 20; 50.34(f)(2)(xiv)	1b-d; 2; 9e	CIAS	Yes	-	
2. Penetration Flowpath Control	No	-	8	No	Yes	Manual	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 9 of 10)

CRITICAL FUNCTION: H. Containment Environment	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Containment Spray	Yes	Auto init (GDC 20)	1b-d; 2; 9e	CSAS	Yes	Comp	
2. Fan Coolers	No	-	8	No	Yes	Alt	
3. H_2 Recombiners	Yes	Auto init (GDC 20)	(1c); 8	No	Yes	Manual	H_2 Recombiners are not necessary prior to 72 hrs after start of limiting DBE. Operator has responsibility to setup, initiate, evaluate, and adjust or terminate Recombiner function. Actions performed in Nuclear Annex under acceptable post-accident habitability conditions.
4. H_2 Purge	No	-	(3b,c; 4); 6	No	Yes	Manual	
5. H_2 Igniters	No	-	6	No	Yes	Manual	

Table 4 - **SUCCESS PATH ALLOCATIONS** (page 10 of 10)

CRITICAL FUNCTION: 1. Radiation Emission	Protective System or Commodity?	Allocation Requirements		SYSTEM 80+			
SUCCESS PATHS		10 CFR 50	NUREG/CR-3331	Auto Init	Manual Init	Control	Justification for solely manual init/cntl of protective system (IEEE 603-1991)
1. Release Path Isolation	Yes	Auto init (GDC 20; 50.34(f)(xiv)(E)	1b-d; 2; 9e	Hi Rad CIAS	Yes	-	
2. Release Path Monitoring & Control	No	-	8	No	Yes	Manual	

4.4 Other Allocations Supporting System Safety/Operator Performance

The present section reviews some other significant facets of the System 80+ design. While these items are beyond the scope of the present evaluation, they identify additional points of change and improvement of prior design allocations in terms of the criteria of this report.

4.4.1 **Added Functions/Features**

a) Validated Aggregation of Data - The cross-checking of redundant data channels, and the aggregation of redundant data into representative (i.e., process representation) values has long been recommended as appropriate for automation, and an unnecessary burden on the human operator. The Nuplex 80+ system implements such features with easy access to individual datum, if desired.

b) Mode Dependency of Alarms - Alarm mode dependency is now a system feature, reducing the number of nuisance alarms. Mode shifts are fully automated post-trip, and partially automated in other cases (requiring the operator to respond to a prompt.)

c) Explicit Display of Derived Parameters - Important derived operating data such as heatup and cooldown rates, and density compensations, are directly displayed by the system rather than requiring operator calculation or inference.

d) Low Power Feedwater Control - This has historically been a problem task for human operators and a source of unnecessary trips due to long lags and complex dynamics in the process. The automatic Low Power Feedwater Control system has been proven as an operational success on the System 80 plant, and improves power production reliability.

e) Automatic Testing Features - Digital technology has proven the successful automation of various test features possible. Automatic digital PPS surveillance features have been proven as an operational success on Arkansas Nuclear Unit 2, and will be implemented in Nuplex 80+. Computer Automated Testing (COMAT) algorithms will also be provided for specific systems as support for manual testing activities, by confirming correct 1) test lineups, 2) test performance, and 3) system restoration.

f) Automatic Load Dispatch - The Megawatt Demand Setter allows changing load demands from the grid to be processed automatically, including maintenance of appropriate operating margins. This system has already been approved and installed on earlier generations of Combustion Engineering plants (specifically, LP&L's Waterford 3 and ANO1's Unit 2).

4.4.2 Removed Functions/Features

a) Automatic Closure of SCS Isolation Valves - This equipment protection feature was a common cause of loss of SCS. Redesign of the system for a higher operating pressure has eliminated the need for the trip.

b) Recirculation Actuation - The change to the In-containment Refuelling Water Storage Tank has eliminated the need to automatically (or manually) switch SI pumps from the RWST to the containment sump on low tank level, thus improving reliability.

c) Required Boronation for Maneuvering Reactivity Control - The addition of four CEAs, and the change from part-length to part-strength (i.e., "grey") control rods, permits plant maneuvering in response to load transients without the need to change soluble boron concentration. The CEA maneuvering response can be performed automatically (see 4.1.1.f) or manually. Boronating remains a manual function, but is no longer required as part of this evolution.

d) Automatic Isolation of Emergency Feedwater - The addition of cavitating venturis to the EFW headers, which limit feed flow to Sgs with a steam or feed line rupture, makes the automatic isolation feature that formerly mitigated these events unnecessary. Manual isolation of the EFW headers remains possible.

4.4.3 Miscellaneous 10 CFR Conformance

The single remaining allocation criterion of Section 2.1 that has not yet been addressed is met as follows:

Automatic Initiation of Turbine Trip - Automatic turbine trip presently is in use at all operating Combustion Engineering units, and will be incorporated as a standard System 80+ feature.

5.0 RESULTS

As a descriptive evaluation, this report did not aim to create or revise the design. Perhaps its main benefit has been to improve the author's understanding of the System 80+ design. Nonetheless, some constructive if miscellaneous observations on the evolution and incorporation of certain design details are collected here, and could be viewed as "results".

5.1 Emergency Procedure Guidelines

One important perspective on the use of plant systems to maintain CSFs is provided by the EPGs. It is notable that developing the present report provided a nexus for the discussion of operating issues that resulted in some useful feedback to the EPG developers. For example, the draft revision of the EPGs showed both Hydrogen Purge and the Ignitors being started concurrently. However, this would be undesirable; they should be successive and independent success paths. Also, the present report anticipated the addition of the SDS system to the Heat Removal recovery guidelines. While these points only reflect, rather than effect, the design, they do suggest that the evaluation has been a coherent, even constructive effort.

5.2 Reg Guide 1.97

The results of this study informally reiterate the ABB-CE response to DSER Open Item 7.5.2.1-1; i.e., that there are no manual protective functions (and thus no Type A variables or Class 1E alarms) in the System 80+ design.

5.3 Operating Experience

Virtually all of the changes described in Sections 4.4.1 and 4.4.2 of this report are a direct result of incorporating operating experience with similar plants in the design of System 80+.

5.4 Functional Task Analysis

Improved operator support by adjustments to the "allocation" of information display functions were suggested by the results of initial task analysis (Reference 21). The concerns were based on estimated operator task loadings (time required vs. time available); resolutions were suggested in keeping with the Appendix A criteria. These results are being addressed in the detailed design (as will any subsequent task analysis results), to ensure acceptable task workload levels are maintained.

6.0 CONCLUSIONS

This report has been a descriptive evaluation of the allocation of critical safety functions in the System 80+ design. The analysis assumes that existing plants of similar design with extensive, successful operating histories are a valid reference point from which to evaluate evolutionary changes and improvements. The conclusions of this evaluation are summarized as follows:

1. Critical Safety Functions (CSFs) have not changed between System 80 and the System 80+ plants.

2. CSF Success Paths and their control allocations are similar in System 80 and System 80+; changes and additions have been few, and afford well-considered improvements to overall plant performance.

3. System 80+ meets all safety-related requirements for allocation of function. No additional allocation concerns have been identified.

4. System 80+ provides improvements through revised allocations in areas of known concern to operator performance.

5. Evaluation of the interaction between the human and machine elements of the plant control system, and resolution of specific problems identified, will continue as part of Task Analysis, PRA, Verification & Validation, and procedure development activities.

6. This report satisfies the requirements of Section A-3.3.2.2 of the System 80+ HFE Program Plan (Reference 6), and of Elements 3 and 4 of the HFE Program Review Model (Appendix E of Reference 2) for System 80+ Certification.

7.0 REFERENCES

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

2) Advanced Control Room Design Review Guidelines (NUREG-5908; draft). U.S. Nuclear Regulatory Commission (1992).

3) Code of Federal Regulations, Title 10, Chapter I - Nuclear Regulatory Commission, Part 50 - Domestic Licensing of Production and Utilization Facilities (10 CFR 50). Office of the Federal Register (1992).

4) System 80+ Standard Safety Analysis Report (CESSAR-DC). ABB Combustion Engineering, Inc.

5) Regulatory Analysis for Resolution of USI A-17 (NUREG-1229). U.S. Nuclear Regulatory Commission (1989).

6) Human Factors Program Plan for the System 80+ Standard Plant Design (NPX80-IC-DP790-01, Rev 1). ABB Combustion Engineering, Inc. (1992).

7) Minutes of Public Meeting (September 10 and 11, 1992; Windsor, CT) between representatives of the NRC Human Factors Branch Staff and the ABB Combustion Engineering MMI Group regarding Human Factors Engineering design issues.

8) Operating Experience Review for System 80+ MMI Design (NPX80-IC-RR790-01, Rev 0). ABB Combustion Engineering, Inc. (1992).

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

10) The Operator's Role and Safety Functions (TIS-6555A). ABB Combustion Engineering (1980).

11) Time Response Design Criteria for Nuclear Safety Related Operator Actions (ANS 58.8-1984). American Nuclear Society (1984).

12) IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE 279-1971). Institute of Electrical and Electronics Engineers (1971).

13) IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE 603-1991). Institute of Electrical and Electronics Engineers (1991).

14) IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (IEEE 1023-1988). Institute of Electrical and Electronics Engineers (1988).

15) A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control (NUREG-3331). U.S. Nuclear Regulatory Commission (1983).

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

17) Manual Initiation of Protective Actions (Reg Guide 1.62). U.S. Nuclear Regulatory Commission (1973).

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

19) Criteria for Power, Instrumentation, and Control Portions of Safety Systems (Reg Guide 1.153). U.S. Nuclear Regulatory Commission (1985).

20) Emergency Procedure Guidelines (CEN-152, Rev 3). ABB Combustion Engineering, Inc.

21) System 80+ Function & Task Analysis Report (NPX80-IC-DP790-02). ABB Combustion Engineering, Inc. (1989).

22) Advanced Light Water Reactor Requirements Document (EPRI URD, Rev B). Chapter 10, Man-Machine Interface Systems. Electric Power Research Institute (1989).

APPENDIX A

FITTS LIST CRITERIA

(from NUREG-0700)

Humans Excel In	Machines Excel In
Detection of certain forms of very low energy levels	Monitoring (both personnel and equipment
Sensitivity to an extremely wide variety of stimuli	Performing routine, repetitive, or very precise operations
Perceiving patterns and making generalizations about them	Responding very quickly to control signals
Detecting signals in high noise levels	Exerting great force, smoothly and with precision
Ability to store large amounts of information for long periods--and recalling relevant facts at appropriate moments	Storing and recalling large amounts of information in short time-periods
Ability to exercise judgment where events cannot be completely defined	Performing complex and rapid computations with high accuracy
Improvising and adopting flexible procedures	Sensitivity of stimuli beyond the range of human sensitivity (infrared, radio waves, etc.)
Ability to react to unexpected low-probability events	Doing many different things at one time.
Applying originality in solving problems: i.e., alternative solutions	Deductive processes
Ability to profit from experience and alter course of action	Insensitivity to extraneous factors
Ability to perform fine manipulation, especially where misalignment appears unexpectedly	Ability to repeat operations very rapidly, continuously, and precisely the same way over a long period
Ability to continue to perform when overloaded	Operating in environments which are hostile to humans or beyond human tolerance
Ability to reason inductively	

APPENDIX B

FUNCTION ALLOCATION CRITERIA

(from NUREG/CR-3331)

FUNCTION ALLOCATION CRITERIA

The following guidelines and criteria are adapted from NUREG-CR/3331, A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control. Tradeoff mechanisms and Fitts list-type human performance criteria are provided in the form of a decision algorithm (see also Appendix A, "Fitts List Criteria"). The algorithm can be applied at any level of detail; however, engineering judgment must be applied to determine when the design description is sufficiently detailed for the purpose at hand. This provides an expedient framework for designers and evaluators to verify appropriate allocations of plant control functions in any aspect of the design.

---

1. **Is automation mandatory?**

   a. Are working conditions hostile to humans?
   b. Are tasks included which humans cannot perform?
   c. Is automation required by law or regulations?
   d. Is automation required to assure plant safety or protection?

   Yes (any) - Go to step 2.
   No (all) - Go to step 3.
   (If automation is required only in part, then the design description may be detailed to identify that part.)

2. **Is automation technically feasible?**

   a. Are proven technologies available?
   b. Are the costs and development/delivery times acceptable?

   Yes (all) - Tentatively allocate to auto; go to step 9.
   No (any) - Redefine the function(s), allocation, or engineering solution.

3. **Is human performance mandatory?**

   a. Is automation technically infeasible?
   b. Is human required to retain policy-level or ultimate control?
   c. Is human required by law or regulation?

   Yes (any) - Go to step 4.
   No (all) - Go to step 5.
   (If a human operator is required only in part, then the design description may be detailed to identify that part.)

4. **Is human performance a feasible solution?**

   a. Can humans perform the specified tasks?
   b. Are the costs and development/delivery times of the necessary support (e.g., procedures, training, etc.) acceptable?

   Yes (all) - Allocate to human; go to step 11.
   No (any) - Redefine the function(s), allocation, or engineering solution.

5. **Is automation clearly preferable to human operators?**

   a. Is automation technology well-established as suitable? (i.e., effective, reliable, cost-effective, etc.)
   b. Is human performance acknowledged as less satisfactory?

   Yes (all) - Tentatively allocate to auto; go to step 9.
   No (any) - Go to step 6.
   (If automation is preferable only in part, then expand the design description sufficiently to identify that part.)

6. **Is human performance clearly preferable to automation?**

   a. Is human performance regarded as clearly necessary, or superior to automation?

   Yes - Allocate to human; go to step 11.
   No - Go to step 7.
   (If a human operator is preferable only in part, then the design description may be detailed to identify that part.)

7. **Is the segment a suitable candidate for automation?**

   a. Is the segment comprised of mechanistic or repetitive tasks?
   b. Does the segment require sustained vigilance?
   c. Does the segment require extremely rapid or consistent responses?
   d. Is the segment comprised of well-defined and highly predictable conditions, actions, and outcomes?
   e. Is the segment likely to be required at the same time as a large (i.e., excessive) number of other tasks?
   f. Does the segment require the collection, storage, manipulation, or recall of data in substantial amounts, or with high accuracy?

   Yes (any) - Tentatively allocate to auto; go to step 9.
   No (all) - Go to step 8.

8. **Is the segment suitable for human operator performance?**

   a. Is it within the realm of human strengths and capabilities?
   b. Will the task form an appropriate and satisfactory part of an operators job? (i.e., cannot be trivial, demeaning, or comprised of leftovers)
   c. Will it allow the operator to maintain satisfactory workload? (i.e., neither too high nor too low)

   Yes (all) - Allocate to human; go to step 11.
   No (any) - Go to step 10.

9. **Reconsider the tentative automatic allocations in terms of their negative impact on human operator performance.**

   a. Would manual performance of the task help to keep the operator engaged with the plant, informed of process status, or prepared to plan and solve problems?
   b. Would manual performance of the task provide the operator with important opportunities to develop or maintain valuable skills or knowledge?
   c. Will absolute implementation of the automatic feature(s) contribute to operator underloading (e.g., boredom)?
   d. Would the option for manual control from the control room afford desired flexibility?
   e. Would the option for manual control from the control room afford more reliable performance of the function?
   f. Would the option for manual control from the control room be desirable for testing, maintenance, or management of off-normal conditions?

   Yes (any) - Make a tentative allocation to automation with operator discretion. If operator discretion is superordinate (man selects auto or manual modes) then go to step 11. If operator discretion is subordinate (man may initiate but not override automatic action), go to step 12.
   No (all) - Allocate to automation; go to step 12.

10. **If any segments remain unallocated, apply the following criteria:**

   a. Comparative cost of human and automated options
   b. Consistency with preceding design goals and selections
   c. Available technologies
   d. Customer preference
   e. Operator acceptance

   or, redefine the function(s), allocation, or engineering solution.

   If allocated to automation, go to step 9.
   If allocated to human operator, go to step 11.

11. **Consider residual automated and control system support for the operator:**

    a. Data display and integration
    b. Monitoring of limits and detection of abnormalities
    c. Hierarchical access to indicating and control options
    d. Automatic control of inner loops
    e. "Fail safe" controls
    f. (etc.)

    Complete any required documentation.

12. **Consider the residual role of the human operator in support of the automated function:**

    a. Policy-level control (e.g., initiation of transitions to less conservative plant states)
    b. Awareness of automatic system status, transitions, availability, etc.
    c. Detection of abnormalities and management of failures, including those in "hidden" or low-level features
    d. Emergency initiation or shutdown
    e. Override of selected interlocks under specified conditions
    f. Removal of equipment from service
    g. Status of local transfer or test switches

    Complete any required documentation.