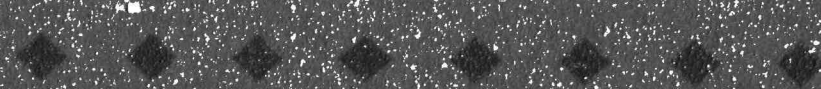


Westinghouse Non-Proliferation Class 2



AP600 Functional Requirements Analysis and Function Allocation

Westinghouse Energy Systems



9610210284 961009
PDR ADOCK 05200003
A PDR

Westinghouse Non-Proprietary Class 3



WCAP-14644
Revision 0

AP600 Functional Requirements Analysis and Function Allocation

Westinghouse Energy Systems



9610210284 961009
PDR ADOCK 05200003
A. PDR

AP600 DOCUMENT COVER SHEET

Form 58202G(5/94) [t:\xxxx.wpf:1x]

AP600 CENTRAL FILE USE ONLY:

TDC: _____ IDS: I _____ S _____

0058.FRM

RFS#:

RFS ITEM #:

AP600 DOCUMENT NO. <i>005-J1-010</i>	REVISION NO. <i>0</i>	Page 1 of _____	ASSIGNED TO
---	--------------------------	-----------------	-------------

ALTERNATE DOCUMENT NUMBER: *WCAP-14644* WORK BREAKDOWN #: *3.3.2.4.5*

DESIGN AGENT ORGANIZATION: *Westinghouse Electric*
PROJECT:

TITLE: *AP600 Functional Requirements Analysis and Function Allocation*

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:	
CALCULATION/ANALYSIS REFERENCE:		
ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION

(C) WESTINGHOUSE ELECTRIC CORPORATION 19*96*

☒ WESTINGHOUSE PROPRIETARY CLASS 2

This document contains information proprietary to Westinghouse Electric Corporation; it is submitted in confidence and is to be used solely for the purpose for which it is furnished and returned upon request. This document and such information is not to be reproduced, transmitted, disclosed or used otherwise in whole or in part without prior written authorization of Westinghouse Electric Corporation, Energy Systems Business Unit, subject to the legends contained hereof.

☐ WESTINGHOUSE PROPRIETARY CLASS 2C

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Corporation and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

COMPLETE 1 IF WORK PERFORMED UNDER DESIGN CERTIFICATION OR COMPLETE 2 IF WORK PERFORMED UNDER FOAKE.

1 ☐ DOE DESIGN CERTIFICATION PROGRAM - GOVERNMENT LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-AC03-90SF18495.

☐ DOE CONTRACT DELIVERABLES (DELIVERED DATA)

Subject to specified exceptions, disclosure of this data is restricted until September 30, 1995 or Design Certification under DOE contract DE-AC03-90SF18495, whichever is later.

EPRI CONFIDENTIAL: NOTICE: 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ CATEGORY: A ☒ B ☐ C ☐ D ☐ E ☐ F ☐

2 ☐ ARC FOAKE PROGRAM - ARC LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-FC02-NE34267 and subcontract ARC-93-3-SC-001.

☐ ARC CONTRACT DELIVERABLES (CONTRACT DATA)

Subject to specified exceptions, disclosure of this data is restricted under ARC Subcontract ARC-93-3-SC-001.

ORIGINATOR <i>C.S. Brockoff</i>	SIGNATURE/DATE <i>S.P. Beul</i> <i>per CSB</i> <i>per tele con</i> <i>10/8/96</i>
AP600 RESPONSIBLE MANAGER <i>J.B. Reid</i>	SIGNATURE* <i>David J. Vantini</i> APPROVAL DATE <i>10/9/96</i>

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

Form 58202G(5/94)

LIMITED RIGHTS STATEMENTS

DOE GOVERNMENT LIMITED RIGHTS STATEMENT

- (A) These data are submitted with limited rights under government contract No. DE-AC03-90SF18495. These data may be reproduced and used by the government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacturer nor disclosed outside the government; except that the government may disclose these data outside the government for the following purposes, if any, provided that the government makes such disclosure subject to prohibition against further use and disclosure:
- (i) This "Proprietary Data" may be disclosed for evaluation purposes under the restrictions above.
 - (ii) The "Proprietary Data" may be disclosed to the Electric Power Research Institute (EPRI), electric utility representatives and their direct consultants, excluding direct commercial competitors, and the DOE National Laboratories under the prohibitions and restrictions above.
- (B) This notice shall be marked on any reproduction of these data, in whole or in part.

ARC LIMITED RIGHTS STATEMENT:

This proprietary data, furnished under Subcontract Number ARC-93-3-SC-001 with ARC may be duplicated and used by the government and ARC, subject to the limitations of Article H-17.F. of that subcontract, with the express limitations that the proprietary data may not be disclosed outside the government or ARC, or ARC's Class 1 & 3 members or EPRI or be used for purposes of manufacture without prior permission of the Subcontractor, except that further disclosure or use may be made solely for the following purposes:

This proprietary data may be disclosed to other than commercial competitors of Subcontractor for evaluation purposes of this subcontract under the restriction that the proprietary data be retained in confidence and not be further disclosed, and subject to the terms of a non-disclosure agreement between the Subcontractor and that organization, excluding DOE and its contractors.

DEFINITIONS

CONTRACT/DELIVERED DATA — Consists of documents (e.g. specifications, drawings, reports) which are generated under the DOE or ARC contracts which contain no background proprietary data.

EPRI CONFIDENTIALITY / OBLIGATION NOTICES

NOTICE 1: The data in this document is subject to no confidentiality obligations.

NOTICE 2: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for limited purposes only. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited except as agreed to in advance by the Electric Power Research Institute (EPRI) and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted.

NOTICE 3: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for use only in evaluation tasks specifically authorized by the Electric Power Research Institute (EPRI). Any use, disclosure to unauthorized persons, or copying this document or parts thereof is prohibited except as agreed to in advance by EPRI and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted. This document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 4: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is being revealed in confidence and trust only to Employees of EPRI and to certain contractors of EPRI for limited evaluation tasks authorized by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. This Document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 5: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. Access to this data is given in Confidence and Trust only at Westinghouse facilities for limited evaluation tasks assigned by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. Neither this document nor any excerpts therefrom are to be removed from Westinghouse facilities.

EPRI CONFIDENTIALITY / OBLIGATION CATEGORIES

CATEGORY "A" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is contained in an issued report.

CATEGORY "B" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is not contained in an issued report, except for computer programs.

CATEGORY "C" — Consists of CONTRACTOR Background Data except for computer programs.

CATEGORY "D" — Consists of computer programs developed in the course of performing the Work.

CATEGORY "E" — Consists of computer programs developed prior to the Effective Date or after the Effective Date but outside the scope of the Work.

CATEGORY "F" — Consists of administrative plans and administrative reports.

WCAP-14644

**AP600 Functional Requirements
Analysis and Function
Allocation**

C. S. Brockhoff
R. J. Mumaw
E. M. Roth
T. L. Schulz

AP600 Design Certification Project

September 1996

Westinghouse Electric Corporation
Energy System Business Unit
P.O. Box 355
Pittsburgh, PA 15230-0355

© 1996 Westinghouse Electric Corporation
All Rights Reserved

TABLE OF CONTENTS

LIST OF TABLES	v
LIST OF FIGURES	vi
ACRONYMS	vii
1.0 INTRODUCTION	1-1
1.1 Objectives	1-1
1.2 Overview of AP600 Functional Requirements and Function Allocation Methodology	1-2
1.3 Overview of the Role of the Operator in AP600	1-3
1.4 Scope of Analysis	1-5
1.4.1 CSFs and Success Paths	1-6
1.4.2 Westinghouse PWR Reference Plant	1-8
1.5 Supporting Westinghouse Reference Documents	1-9
1.5.1 WCAP-13793, AP600 System/Event Matrix (Reference 11)	1-9
1.5.2 AP600 Emergency Response Guidelines (Reference 6)	1-10
1.5.3 AP600 Emergency Response Guidelines Background Document (Reference 7)	1-12
1.5.4 AP600 Standard Safety Analysis Report (Reference 12)	1-12
1.5.5 AP600 Probabilistic Risk Assessment (Reference 8)	1-14
1.5.6 WCAP-13856, AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process (Reference 13)	1-15
1.5.7 WCAP-14477, The AP600 Adverse System Evaluation Report (Reference 10)	1-15
1.5.8 AP600 Shutdown Evaluation Report (Reference 14)	1-15
2.0 AP600 FUNCTIONAL REQUIREMENTS ANALYSIS	2-1
2.1 Description of Methodology	2-1
2.1.1 AP600 CSFs (Table 1)	2-2
2.1.2 AP600 CSF Success Paths (Table 2)	2-2
2.1.3 Comparison of CSF Success Paths Between AP600 and Generic Westinghouse PWR Reference Plant (Table 3)	2-4
2.2 Results	2-7
2.3 Verification and Updating of Functional Requirements Analysis	2-8
3.0 AP600 INITIAL FUNCTION ALLOCATION	3-1
3.1 Methodology for Function Allocation	3-1
3.1.1 The General Approach to Function Allocation	3-1
3.1.2 Westinghouse Function Allocation Process	3-3

TABLE OF CONTENTS (Cont.)

3.1.3	Integration of Automation and Operators	3-10
3.1.3.1	Guidelines for the Residual Role of the Operator for Functions Allocated to Automation	3-10
3.1.3.2	Guidelines for the Residual Role of Automation for Functions Allocated to Human Performance	3-17
3.1.3.3	Implementation Schemes	3-17
3.2	AP600 Function Allocation Summary (Table 4)	3-18
3.3	AP600 Function Allocation Basis (Table 5)	3-24
3.4	Results	3-24
4.0	HUMAN FACTORS CONSIDERATIONS IN FUNCTION ALLOCATION	4-1
4.1	Human Factors Input Early in the Design Process	4-1
4.2	Human Factors Evaluation of the Integrated Role of the Operator	4-2
4.3	Mechanisms for Modifying Function Allocations Based on Analysis Results	4-4
5.0	CONCLUSIONS	5-1
6.0	REFERENCES	6-1

LIST OF TABLES

Table 1	Westinghouse ERG Critical Safety Functions	T-1
Table 2	Success Paths	T-3
Table 3	Success Path Status	T-8
Table 4	Success Path SSC Allocations	T-19
Table 5	Function Allocation Basis	T-40
Table 6	Function Allocation Questions	T-45

LIST OF FIGURES

Figure 1	Function Allocation Decision Process	T-47
----------	--	------

ACRONYMS

ADS	Automatic Depressurization System
AFW	Auxiliary Feedwater System
ALWR	Advanced Light Water Reactor
AMSAC	ATWS Mitigation System Actuation Circuitry
ASI	Adverse Systems Interactions
ATWS	Anticipated Transient Without Scram
CCS	Component Cooling Water System
CFR	Code of Federal Regulations
CMT	Core Makeup Tank
CVS	Chemical and Volume Control System
CSF	Critical Safety Function
DAS	Diverse Actuation System
DDS	Data Display and Processing System
ELS	Plant Lighting System
EOP	Emergency Operating Procedure
ERG	Emergency Response Guideline
ESF	Engineered Safety Feature
FBTA	Function-Based Task Analysis
GDC	General Design Criteria
HFE	Human Factors Engineering
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air-Conditioning
HX	Heat Exchanger
IAEA	International Atomic Energy Agency
I&C	Instrumentation & Control
IIS	Incore Instrumentation System
IRC	Inside Reactor Containment
IRWST	In-Containment Refueling Water Storage Tank
LOCA	Loss-of-Coolant Accident
M-MIS	Man-Machine Interface System/Human System Interface
MCC	Motor Control Center
MCR	Main Control Room
MG	Motor-Generator
MSIV	Main Steamline Isolation Valve
MTC	Moderator Temperature Coefficient
NSR	Nonsafety-Related
OCS	Operation and Control Centers
ORC	Outside Reactor Containment
OSA	Operational Sequence Analysis
PCS	Passive Containment Cooling System

ACRONYMS (cont.)

PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PORV	Power-Operated Relief Valve
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PRM	Human Factors Program Review Model
PWR	Pressurized Water Reactor
PXS	Passive Core Cooling System
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RNS	Normal Residual Heat Removal System
RWST	Refueling Water Storage Tank
RV	Reactor Vessel
SFS	Spent Fuel Pool Cooling System
SG	Steam Generator
SI	Safety Injection
SR	Safety-Related
SRP	Standard Review Plan
SSAR	Standard Safety Analysis Report
SSC	Systems, Structures, and Components
SSPS	Solid State Protection System
SWS	Service Water System
TS	Technical Specifications
UPS	Uninterruptible Power Supply
URD	Utility Requirements Document

1.0 INTRODUCTION

Element 3 of the Human Factors Program Review Model (PRM) specifies requirements for performing functional requirements analyses and function allocation in support of establishing and documenting design decisions with respect to the level of plant automation (NUREG-0711) (Ref. 1). Similar analysis and documentation requirements, with respect to function allocation decisions, are specified in the Advanced Light Water Reactor Utility Requirements Document (ALWR URD) (EPRI, 1992) (Ref. 2) and in international man-machine interface design standards and guidelines documents that address the design of power plant control rooms (including IAEA-TECDOC-663 and IEC964, Ref. 3 and 4.)

The objective of this report is to document the methodology used by Westinghouse to arrive at the AP600 level of automation for plant functions, processes, and systems involved in maintaining plant safety, and to document the results and rationale for function allocation decisions for the AP600 plant. The report also describes human factors activities that are conducted as part of the AP600 man-machine interface system (M-MIS) design process to verify the adequacy of function allocation decisions, and to establish the ability of operators to perform the role assigned to them. This report satisfies the requirements of Element 3 of the PRM.

This document employs the same definitions of function requirements analysis and function allocation provided in NUREG-0711. Consistent with NUREG-0711:

- *Functional requirements analysis* is defined as the "identification of those functions that must be performed to satisfy plant safety objectives, that is, to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public." (NUREG-0711, pg. 4-1).
- *Function allocation* is defined as the "analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup)" (NUREG-0711, pg. 4-1).

1.1. Objectives

This document has three primary objectives:

- To describe the Westinghouse approach to functional requirements analysis and present the results for the AP600 critical safety functions (CSFs)

- To describe the Westinghouse approach to initial function allocation and present the results for the AP600 CSFs
- To describe the methods by which human factors considerations, with respect to function allocation, are addressed as part of the AP600 design process

Section 2.0 provides a description of the Westinghouse approach to functional requirements analysis and presents the results for AP600 CSFs. The results include a description of AP600 systems, structures, and components (SSCs) involved in maintaining the AP600 CSFs. The section also includes a similar analysis for generic Westinghouse pressurized water reactor (PWR) designs to provide a comparison of where the AP600 plant differs from current Westinghouse PWR designs. The section includes an explicit comparison of the AP600 design with the reference plant design and identifies SSCs that are new or modified, relative to the reference plant design. This includes changes in the level of automation.

Section 3.0 describes the Westinghouse approach to initial function allocation and presents the results for AP600 CSFs. The results include specification of the level of automation and the responsibility of personnel for the AP600 CSFs. The results also document the rationale for function allocation decisions for the AP600 CSFs.

The report also describes human factors activities that are conducted as part of the AP600 M-MIS design process to verify the adequacy of function allocation decisions and to establish the ability of operators to perform the role assigned to them.

Section 4.0 describes how human factors considerations, with respect to function allocation, are addressed as part of the AP600 design process. This includes the following:

- How human factors input is provided early in the design process
- How the integrated role of the operator, across all systems, is confirmed for acceptability
- The mechanisms available for reconsidering and, if necessary, changing AP600 function allocations in response to developing design specifics, operating experience, and the outcomes of on-going analyses and trade studies

1.2. Overview of AP600 Functional Requirements and Function Allocation Methodology

In the Westinghouse design process, functional requirements analysis and preliminary function allocation are largely the responsibility of system designers. As explicitly recognized in the International Atomic Energy Agency report on the role of automation and humans in nuclear power plants (IAEA-TECDOC-668), as well as in NUREG-0711, functional requirements analysis and function allocation decisions for a new plant are rarely generated from a clean slate. Functional requirements and function allocation decisions for AP600 have

been strongly guided by regulatory requirements (e.g., 10 CFR 50), industry requirements (e.g., URD requirements), design goals, and experience with predecessor plants, as is typically the case with new plant designs. Details on the specific requirements and decision processes that entered into AP600 function allocations are provided in Section 3.0.

Human factors considerations in function allocation are incorporated in the design process at several points. Initial allocation, while largely constrained by external requirements and design goals, takes into account the strengths and limitations of human operators and automated systems. As mentioned previously, the initial allocation is the responsibility of system designers. The system designers consider the relative capabilities of human and automated systems in making allocation decisions. The role of the human operator in system operation is specified in cases where decisions are made to automate processes. This typically includes monitoring the operation of the automated system. Depending on the system, it may also include the ability to manually initiate the system, to initiate a backup system should the primary system perform improperly, and/or the ability to take over manual control if required. As part of the design process, the system designers specify the sensors and controls to be provided to support the operator's role in system operations. A methodology adapted from NUREG/CR-3331 (Ref. 5) has been used to document the rationale for initial allocation decisions. The methodology was developed by an interdisciplinary team that included human factors and system design engineers. The methodology is presented in subsection 3.1 and the results are presented in subsection 3.2.

The adequacy of the allocation is further evaluated throughout the AP600 design process. Function-based task analyses (FTBAs) are used to verify that the sensors and controls provided are sufficient to enable operators to perform the role assigned to them in system performance. Workload analyses are used to evaluate the adequacy of the integrated role assigned to operators across systems. Final integrated system validation is used to establish the adequacy of the function allocation using man-in-the-loop tests in dynamic simulated plant conditions. Should deficiencies in function allocation be identified at any point in time, formal mechanisms are available in the AP600 design process for making design changes, if determined to be necessary. Section 4.0 describes in more detail the processes that will be employed as part of the AP600 M-MIS design process to address human factors concerns related to function allocation during all phases of the design.

1.3 Overview of the Role of the Operator in AP600

In Reference 24, the role of the operator is defined as "the integration of the responsibilities that the operator performs in the fulfillment of the mission of plant systems and functions, where responsibilities are defined with regard to a spectrum of control modes" (page 9). The

primary focus is on the operator's control authority and responsibility, with respect to the plant functions and systems in which the operator is a part of the control loop.

Subsection 3.2 provides detailed descriptions of the specific operator responsibilities associated with the SSCs involved in CSFs. The results in Section 3.2 constitute a detailed description of the operator role in AP600 CSFs. An overview of the role of the operator in maintaining CSFs is provided in this section.

At a high level, the role of the operator in maintaining CSFs in the AP600 plant remains the same as in current plants. This can be seen by examining the AP600 Emergency Response Guidelines (ERGs) (Ref. 6). An overview of the AP600 ERGs and the activities that operators are expected to engage in when responding to emergency situations can be found in the introduction of the AP600 ERG background document (Ref. 7).

As in current plants, operator response to emergency events will be guided by Emergency Operating Procedures (EOPs). The operator's role includes the following:

- Monitoring plant state and verifying plant parameters
- Monitoring automatic operation of safety-related (SR) and nonsafety-related (NSR) systems, including:
 - Verifying operation of, or the need for operation of, the nonsafety-related defense-in-depth systems
 - Verifying operation of, or the need for operation of, the passive safety-related systems
- Controlling the operation of nonsafety-related systems
- Terminating operation of the safety-related systems when plant conditions have been stabilized following an event and EOP termination criteria are determined to be met

These operator activities are similar to the activities required of operators in responding to emergency events in current plants. As in current plants, the operator functions as supervisory controller of automated systems. The operator monitors the state of the plant, verifies that automatic systems have actuated and are responding as required, and takes manual action when necessary. As in current plants, the operator's performance will be guided by EOPs.

The difference between the role of the operator in the AP600 plant and in current plants is one of degree, and not a fundamental change in character. At a detailed level, there will be differences in the specific activities performed by operators due to differences in safety-

related systems, increased automation, and the availability of improved M-MIS. The M-MIS includes displays that integrate information to facilitate assessment of plant state and supervisory monitoring of automated systems, and a computerized procedure system that facilitates utilization of the EOPs.

Some of the distinctions in equipment type that are important from a design and licensing perspective, should be relatively transparent from an operational perspective. In particular, the AP600 employs safety-related, passive systems that automatically protect the plant in the event of an accident, without the need for immediate operator actions. The AP600 also employs nonsafety-related, defense-in-depth systems that, if available, can automatically protect the plant for the more probable postulated transients and accidents. If these defense-in-depth systems are available and operate correctly, they will prevent the need for the operation of the safety-related, passive systems. The AP600 ERGs integrate the use of the nonsafety-related, defense-in-depth systems and the safety-related, passive systems to maximize the protection of the plant for design basis and beyond-design-basis accidents. During transients, operators are required to monitor the status of both nonsafety-related and safety-related systems, and are guided in the use of both types of systems.

Another aspect of the AP600 plant that is different from current plants is in the use of safety-related, passive systems. The passive systems rely on natural forces such as gravity or compressed gases, instead of mechanical forces such as pumps, to perform their functions. From the perspective of the role of operators, passive systems can be considered a different form of automation. As with other automatic systems, operators are responsible for monitoring the availability and operational status of the passive systems. Operators are responsible to verify the operation of, or the need for operation of, the passive systems. When termination criteria are met, operators are responsible for terminating the operation of the systems. Monitoring and control activities associated with passive systems are guided by EOPs.

In the design of the M-MIS procedures and training the passive systems are treated as a type of automated system. The M-MIS will be designed to support supervisory monitoring and control of the passive systems. While the passive systems are different in how they operate, they should not pose fundamentally different challenges for M-MIS design or operator supervisory control. In addition, some specific passive systems, such as the accumulators, have been installed in current plants and function identically for the AP600.

1.4 Scope of Analysis

The scope of this report is to address the functional requirements analysis and the function allocation process for the AP600 CSFs for both design basis and beyond-design-basis events. The CSFs are contained in the AP600 ERGs.

1.4.1 CSFs and Success Paths

CSFs are physical processes, conditions, or actions taken using the safety-related and nonsafety-related SSCs to maintain the plant conditions within the acceptable design basis. SSCs are the physical equipment used to initiate and control the processes that achieve the CSF.

A success path for a CSF is the specific combination of safety-related and nonsafety-related, defense-in-depth SSCs that are capable of accomplishing that particular CSF. The CSFs may be accomplished by automatic or manual actuation, or control, and can be supplemented by passive processes.

The CSFs and their associated success paths are the means by which the AP600 design accommodates anticipated operational occurrences during normal, abnormal, and emergency conditions.

The CSFs for the AP600 have been developed considering the specific plant design basis, in conjunction with extensive Westinghouse PWR operating experience and with the previous experience in the development of ERGs for current plants.

The AP600 CSFs, as identified in Reference 6, include the following:

- Subcriticality
- Core cooling
- Heat sink
- Reactor Coolant System (RCS) integrity
- Containment
- RCS inventory

Table 1 provides an overview of the AP600 CSFs, including a brief summary of the purpose for each CSF and the primary AP600 plant parameters monitored to confirm the status of the associated CSF. The development of these CSFs for the AP600 is discussed in subsections 1.5.1 and 1.5.2. Additional information on each CSF is also provided in the ERG Background Document (Reference 7).

These six CSFs provide protection for events initiating from both at-power and shutdown conditions. Therefore, the functional requirements analysis and the function allocation process described in this report addresses plant SSCs that are used to mitigate events that initiate from both at-power and shutdown conditions.

The specific AP600 SSCs that form the CSF success paths and are addressed as part of the functional requirements analysis and the function allocation process include the following:

- Safety-related passive SSCs (such as core makeup tanks (CMTs) and accumulators)
- Nonsafety-related, defense-in-depth SSCs (such as chemical and volume control system (CVS) and startup feedwater systems)
- Other nonsafety-related SSCs that support the CSF success paths as identified in References 6 and 7 (such as the main feedwater system)

As appropriate, the inherent passive processes that provide actuation and control functions for safety-related SSCs identified in the various success paths are also addressed as part of the function allocation process described in this report.

The definition of a success path is based on identifying the SSCs that accomplish the CSFs in the various tables. References to the phrase "SSCs" in the context of success paths for this evaluation are meant to encompass the following:

- The actual equipment and components that accomplish the CSF, such as the system piping, valves, pumps, other mechanical and electrical components in the flowpaths or supporting the flowpaths (such as air-operated valve control solenoids), and components such as tanks, including those that may actually be integral to building structures, like the in-containment refueling water storage tank (IRWST)
- The equipment and components that provide support for the functioning of the SSCs, such as instrumentation and control (I&C) system actuation and control functions, or electrical power generation and distribution equipment functions
- The physical plant and system processes associated with the operation of the SSCs in mitigating the consequences of the accident and ultimately accomplishing the CSFs (such as fluid system injection, depressurization flow, or reactor neutron kinetics processes related to control rod motion on a reactor trip or boration).

Since this report addresses the functional requirements analysis and the function allocation process incorporated for the AP600 ERGs, severe accident events are not included as part of this evaluation. Severe accident response is evaluated in the AP600 Probabilistic Risk Assessment (PRA) (Ref. 8) and addressed in WCAP-13913, Framework for AP600 Severe Accident Management Guidance (Ref. 9).

Unanticipated and adverse systems interactions are implicitly included in the ERG response since this aspect of the operation of the safety-related and nonsafety-related systems SSCs has

been evaluated in WCAP-14477, The AP600 Adverse Systems Interactions (ASI) Evaluation Report (Ref. 10) and considered in the development of the ERGs.

The actuation, control, continuing operation, and operator monitoring of the various SSCs for the CSF paths implicitly requires operation of both I&C systems and electrical power systems. Following a loss of electrical power, the nonsafety-related emergency diesel-generators automatically start and load the appropriate nonsafety-related, defense-in-depth systems. The diesel-generators also provide electrical power to both the ac and dc power systems, thereby providing operating power for nonsafety-related components such as pumps and fans, as well as power for actuation, control, and monitoring instrumentation. These safety-related and nonsafety-related SSCs are included in the following AP600 systems:

Instrumentation and Control Systems

- Protection and Safety Monitoring System (PMS) (safety-related)
- Plant Control System (PLS) (nonsafety-related)
- Diverse Actuation System (DAS) (nonsafety-related)
- Data Display and Processing System (DDS) (nonsafety-related)
- Incore Instrumentation System (IIS) (nonsafety-related)
- Operation and Control Centers (OCS) (safety-related)
- Radiation Monitoring System (RMS) (safety-related)
- Plant Lighting System (ELS) (nonsafety-related)

Electrical Power Systems

- Main ac Power System (nonsafety-related)
- Class 1E dc and uninterruptible power supply (UPS) System (safety-related)
- Non-Class 1E dc and UPS System (nonsafety-related)
- Onsite Standby Power System (includes the nonsafety-related emergency diesel-generators)

1.4.2 Westinghouse PWR Reference Plant

Element 3 of the PRM (NUREG-0711) specifies that in conducting a functional requirements analysis, safety functions and processes of the new plant should be compared to those of predecessor plants. The predecessor plants provide a reference for identifying and documenting functions and processes that have been modified (i.e., are new, changed or deleted) and functions and processes that are unchanged relative to the reference plant.

The generic PWR design for currently licensed Westinghouse nuclear power plants functions as the reference plant in performing the function requirements analysis for the AP600. As shown in Table 1, the CSFs for the AP600 plant are identical to the CSFs for current

Westinghouse PWR plants. This is because a similar design basis is used for the AP600 plant as for the current generic Westinghouse PWR design.

The functional requirements analysis and the function allocation process provides appropriate comparisons to the generic PWR reference plant design. They identify differences in the success paths that must be considered in completing the function allocation process.

1.5 Supporting Westinghouse Reference Documents

A number of reference documents were used to support the functional requirements analysis and function allocation process and may be referenced as appropriate in this evaluation. Together, these documents provide a comprehensive and complementary summary of the pertinent aspects of the plant design needed to support the function allocation process. This process includes the design, operation, accident mitigation response, and safety importance of the various plant systems and components. These supporting reference documents follow.

1.5.1 WCAP-13793, AP600 System/Event Matrix (Reference 11)

The design basis for the Westinghouse PWRs, including the AP600, requires protecting the three fission product barriers following design basis events. The AP600 System/Event Matrix (Ref. 11) is a design document that identifies four design basis safety functions that are required to provide this protection for the fission product barriers. These four design basis safety functions identified in the design document were expanded into the six CSFs in writing the symptom-based AP600 ERGs.

Along with Reference 6, the System/Event Matrix provides much of the basis for the activities described in this report. The System/Event Matrix provides an integrated summary of the plant accident mitigation response and has been used throughout the design process.

The System/Event Matrix document identifies the following four safety-related, post-accident mitigation functions that are required as part of the design basis for the AP600 to protect the integrity of the three fission product barriers in the plant (the fuel matrix and cladding, the RCS pressure boundary, and containment):

- Reactor shutdown
- RCS inventory control
- Core decay heat removal
- Containment cooling

The design basis of the plant requires safety-related SSCs that can perform these safety-related functions for design basis events. The nonsafety-related SSCs also perform defense-

in-depth functions that complement the safety-related SSCs in performing these safety-related functions.

For each event, the System/Event Matrix document provides simplified flow diagrams that present the prioritized sequence for the operation of the various safety-related and nonsafety-related, defense-in-depth SSCs that are used to protect the reactor core and to mitigate the consequences of each event. Flow diagrams are provided for events initiated from both operating and shutdown conditions.

The document also provides tables for each event that shows the following:

- Safety-related and nonsafety-related I&C system support requirements (actuation/control) for each success path
- Actuation mode (automatic/manual) for each of the success paths
- Safety-related and nonsafety-related electrical power support requirements for each success path

This document is used in the functional requirements analysis and the function allocation process since it specifies how the AP600 safety-related and nonsafety-related systems are used to maintain CSFs during the specific events (i.e., which systems are used, and in what sequence, during each event).

1.5.2 AP600 Emergency Response Guidelines (Reference 6)

The AP600 ERGs provide functional guidelines for terminating accidents and transients that affect plant safety. The ERGs are a standardized document that was initially developed in a program by the Westinghouse Owners' Group (WOG) to provide control room operators with symptom-based technical guidance for response to emergency transients.

The ERGs provide a diagnostic process to direct operator actions based on plant symptoms, and do not require immediate identification of the cause (i.e., the specific initiating event) of the symptoms to determine the required actions. The recovery actions identified in the standardized ERGs for Westinghouse PWRs are based on satisfying the six CSFs listed in subsection 1.4.1.

The detailed plant EOPs that provide step-by-step actions for use by the control room operators in the plant, will be developed using the high-level functional guidelines provided in the ERGs. The ERGs provide the technical basis for development of the EOPs.

This document is used in the functional requirements analysis and the function allocation process since it provides the specific operator actions required to support the recovery guidelines, following a plant transient, and the function restoration guidelines (including both verification activities and control actions) that maintain the success paths for the CSFs.

AP600 ERG Development

The AP600 ERGs were developed using the System/Event Matrix document as the plant response design basis and following the standardized process for ERG development for Westinghouse PWRs. The design approach described in the System/Event Matrix document organizes the identified safety-related and nonsafety-related SSCs into the appropriate groups that perform the four safety-related design functions. In the AP600 ERGs, the same groups of safety-related and nonsafety-related SSCs in the System/Event Matrix are used to perform their basic design functions. But they are organized somewhat differently from the System/Event Matrix to support development of symptom-based functional guidelines that can be used more effectively by the operators.

The four safety-related functions (listed in subsection 1.5.1) from the System/Event Matrix document are now replaced by six equivalent CSFs (listed in subsection 1.4) for use in the ERGs. This can be seen by studying the tables provided later in this report to support the AP600 function allocation process, and comparing them to the tables and flow charts in the System/Event Matrix document.

The relation between the System/Event Matrix and the ERG development is also discussed in the ERG background document, that also includes the specific System/Event Matrix flow diagrams for the various events in the background document introduction.

Consolidation of At-Power and Shutdown ERG CSFs

The AP600 ERGs are arranged to provide two sets of CSF status trees and two sets of CSF restoration guidelines for the operators -- one for use following events initiated from at-power conditions and one for use following events initiated from shutdown conditions. This helps to simplify and improve operator response following an event. The six CSFs listed in subsection 1.4 form the basis for both sets of guidelines.

These CSF success paths in the ERGs were developed from one common list of success paths for events (both at-power and shutdown) that was provided in the System/Event Matrix document. The System/Event Matrix flow diagrams were split into two groups (at-power and shutdown) to support the ERG development.

This report uses the ERG success paths from a consolidation of the two sets of ERG guidelines for each CSF. This consolidation simply adds the SSCs in the success path for

each shutdown CSF to the SSCs to the success path for the same at-power CSF. This approach greatly simplifies the number of cases that must be displayed, since in many cases, the same success paths are used to satisfy the same CSF for events from both conditions. For example, accumulator injection is part of the success path following partial RCS depressurization for at-power events or for shutdown events initiated at reduced RCS pressures.

Tables 2, 3, 4, and 5 support the functional requirements analysis and the function allocation process described in this report, and include success paths that are applicable to at-power events only, both at-power and shutdown events, and shutdown events only. Those specific success paths that apply only during shutdown conditions (such as when the reactor vessel head is removed and the refueling cavity is flooded up) are identified with the word "shutdown" in parentheses after the list of the SSCs in the success path. The shutdown SSCs are listed last in the success paths provided in each table.

1.5.3 AP600 Emergency Response Guidelines Background Document (Reference 7)

The AP600 ERG Background Documents provide a brief overview of the ERG development and explanations of specific actions included in the ERG functional guidelines. The background document provides a comprehensive discussion of the actions taken by the operators including the purpose of the actions, the basis for actions taken, and the instrumentation, controls, and equipment used by the operators to accomplish the specific actions.

This document is used in the functional requirements analysis and the function allocation process since it provides the required background information to understand the basis for the accident mitigation actions identified in the ERGs.

1.5.4 AP600 Standard Safety Analysis Report (Reference 12)

The safety-related and nonsafety-related SSCs that are included in the CSF success paths discussed in this evaluation are described in the appropriate sections throughout the AP600 Standard Safety Analysis Report (SSAR). The AP600 SSAR provides four important categories of design information that are helpful in understanding the function allocation process addressed in this evaluation. The individual SSAR sections describe this information for each system included in the CSF success path:

- The design basis for the system
- The individual components within each system
- The operation of each system including accident mitigation response
- The associated I&C.

For example, the safety-related passive core cooling system (PXS) is described in subsection 6.3 of the SSAR and the nonsafety-related, defense-in-depth chemical and volume control system (CVS) is described in subsection 9.3.6 of the SSAR.

Chapter 7 of the SSAR provides the following information related to the I&C systems, that was used to support the function allocation process:

- The design of the safety-related PMS that is used to actuate and control safety-related SSCs, and the design of the nonsafety-related PLS that is used to actuate and control the nonsafety-related SSCs, are described in subsection 7.1 of the SSAR.
- The safety-related reactor trip functions of the PMS are described in subsection 7.2 of the SSAR and reference functional diagrams for each of the reactor trip functions and other related plant functions included in the function allocation process. These same trip functions are credited in the safety analyses, as described in Chapter 15 of the SSAR.
- The PMS actuation functions for the safety-related engineered safety features SSCs in the various CSF success paths are described in subsection 7.3 of the SSAR and reference functional diagrams for each of the engineered safeguards functions included in the function allocation process. These same engineered safeguards functions are credited in the safety analyses, as described in Chapter 15 of the SSAR.
- The instrumentation used by the operator to monitor the operation of the various plant SSCs in the CSF success paths for the various events is described in subsection 7.5 of the SSAR.
- The safety-related PMS control systems and the nonsafety-related PLS control systems are described in subsection 7.7 of the SSAR. These control functions addressed in the function allocation process and considered in the safety analyses, as described in Chapter 15 of the SSAR.

Chapter 8 of the SSAR provides a description of the electrical power systems that are used to provide normal and emergency power for operation of the various SSCs in the CSF success paths. Chapter 8 also describes the normal and emergency electrical power sources for the I&C systems that was used to actuate and control the various SSCs in the CSF success paths.

Chapter 15 of the SSAR provides the accident analyses that confirm the design basis for the AP600. These safety analyses incorporate the appropriate automatic and manual actuation that result from the function allocations specified for each of the SSCs in the various CSF success paths and confirm that the design basis for the plant is met. The safety analyses can be used to support the function allocation process, for example, by identifying automatic

actuation and control functions that may be necessary. The safety analyses completed to support Chapter 15 provide conservative and bounding design basis analyses that assume the most limiting single failures of various components, including failures of the nonsafety-related control systems.

Chapter 18 of the SSAR describes the overall human factors engineering (HFE) process that was included as part of the AP600 design process.

This document is used for the functional requirements analysis and the function allocation process since it is one of the sources of specific design information for the various plant SSCs, including information related to SSC actuation and control. The SSAR also provides the design basis analyses to confirm the accident mitigation capabilities of the various SSCs and a description of the overall HFE process.

1.5.5 AP600 Probabilistic Risk Assessment (Reference 8)

The AP600 design certification application includes a PRA that provides an evaluation of the design, including the plant, containment, and typical site analyses for both internal and external events, and for both at-power and shutdown plant conditions. The PRA modeled and evaluated various accident prevention and mitigation systems in achieving the required safety-related functions identified in the System/Event Matrix document and the ERGs. The major PRA activities included modeling and analysis of specific safety-related and nonsafety-related systems (including associated automatic and manual actuation and control) that provide accident mitigation support, human reliability analysis, common-cause failure analysis, severe accident analysis, and other related accident phenomena analysis.

The PRA evaluation analyses, completed as part of the PRA, provide more realistic evaluations of the plant success path response than the conservative SSAR Chapter 15 safety analyses. The PRA uses best estimate analyses that consider a comprehensive range of credible component failures, with component failure data compiled from operating plant component performance data. The PRA also includes the effects of common-mode failures of similar components.

The PRA is used in the functional requirements analysis and the function allocation process since it is one of the basis documents that evaluates plant accident response. The PRA was also used to identify the need for, and evaluate the success of, manual and automatic actuation and control for various SSCs that are used in the CSF success paths.

1.5.6 WCAP-13856, AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process (Reference 13)

This report summarizes the evaluation performed to determine the significant nonsafety-related SSCs for the AP600 and the appropriate additional regulatory oversight associated with these SSCs. The evaluation considers the impact of a range of important accident mitigation issues related to the nonsafety-related systems for both at-power and shutdown events.

This report is used in the functional requirements analysis and the function allocation process. It systematically considers nonsafety-related systems, evaluates them against ten important probabilistic and deterministic criteria related to accident mitigation, and helps to identify the most important nonsafety-related systems.

1.5.7 WCAP-14477, The AP600 Adverse Systems Interactions Evaluation Report (Reference 10)

This report provides a systematic approach to evaluate systems interactions and their impact on plant safety. The report summarizes the various interactions between safety-related systems and other safety-related systems and between safety-related systems and nonsafety-related systems. The report also describes how these interactions have been considered in the analyses and evaluations presented in the AP600 SSAR and the AP600 PRA. Insights for both the AP600 ERGs and the M-MIS design were identified in this report to preclude potential operator errors that could result in unintended adverse interactions and that could lead to degradation of the plant safety during an accident.

This report is used in the functional requirements analysis and the function allocation process since it discusses and evaluates the interactions between the various systems that must potentially be considered as part of operator event mitigation actions.

1.5.8 AP600 Shutdown Evaluation Report (Reference 14)

This report provides a comprehensive evaluation of the AP600 plant safety during shutdown modes. It describes features of the AP600 design that address issues of shutdown risk and provides an evaluation of these features, with respect to their ability to reduce this risk and mitigate the consequences of events initiated from shutdown conditions. The report provides descriptions of the AP600 SSCs that are designed to operate during shutdown modes and discusses their shutdown operations. It also includes an evaluation for the range of credible events that can initiate during shutdown conditions and provides an overview of the shutdown risk assessment included in the AP600 PRA.

This report is used in the functional requirements analysis and the function allocation process since it discusses and evaluates the CSF success paths and the associated accident mitigation response, specifically for events initiated during shutdown conditions.

2.0 AP600 FUNCTIONAL REQUIREMENTS ANALYSIS

According to Element 3 of NUREG-0711, functional requirements analysis is the identification of those functions that must be performed to satisfy plant safety objectives, that is, to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public.

NUREG-0711 states that:

"Functional requirements analysis is conducted to (1) determine the objectives, performance requirements, and constraints of the design; (2) define the functions that must be accomplished to meet the objectives and required performance; (3) define the relationships between functions and plant processes (e.g., plant configurations or success paths) responsible for performing the functions; (4) provide a framework for understanding the role of controllers (whether personnel or system) for controlling plant processes." (pg. 4-1)

This section describes the Westinghouse approach to functional requirements analysis and presents results for AP600 safety functions.

2.1 Description of Methodology

Following the basis provided in NUREG-0711, a functional requirements analysis begins with identification of safety functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant processes (plant system configurations or success paths) that are responsible for or capable of carrying out the function need to be clearly defined.

In the case of the AP600, the CSFs are the safety functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each CSF, the success paths that are capable of carrying out the CSF have been defined.

Functional requirements analysis is performed by system designers in support of plant system design and function allocation. This section describes the methodology used by Westinghouse to document the success paths that support CSFs for the AP600 plant. Section 2.2 documents the results of the functional requirements analysis for the AP600 CSFs.

A related functional requirements activity is conducted by the M-MIS design group in support of FBTA and display design. Section 18.5 of the AP600 SSAR describes the goal-means decomposition of plant functions that is conducted as part of the M-MIS design process. The goal-means decomposition is developed by M-MIS designers as a way to represent plant functions as input to FBTAs and M-MIS design activities. The goal-means

decomposition of plant functions contains two major branches that correspond to the two major goals of the plant: (1) generate electricity and (2) prevent radiation release. The AP600 CSFs correspond to high-level nodes under the "Prevent Radiation Release" branch. The goal-means decomposition is derived from system design documents, and as such, is consistent with the functional requirements analysis of CSFs presented here.

The functional requirements analysis presented in subsection 2.2 specifies the AP600 success paths involved in CSFs for the AP600 plant. It also provides a comparison between the AP600 success paths and the success paths involved in CSFs for the generic Westinghouse PWR plant, which serves as the reference plant. The comparison with the reference plant enables differences in the SSCs involved in the success paths for the AP600 plant and a typical current Westinghouse PWR plant to be identified.

2.1.1 AP600 CSFs (Table 1)

As discussed in subsection 1.4, Table 1 provides an overview of the AP600 CSFs that form the basis for the approach used for the functional requirements analysis and the function allocation process. The table summarizes the purpose of each CSF and also identifies the primary plant parameters monitored in the associated ERG status tree for each CSF. This reinforces the specific focus of each CSF.

Additional information on each CSF and its associated ERG status tree and function restoration guidelines is provided in the AP600 ERGs (Ref. 6) and the ERG Background Document (Ref. 7). As noted earlier, the AP600 CSFs are the same as the CSFs for the reference plant.

Table 1 also shows the correlation between the six CSFs in the AP600 ERGs and the four associated design basis safety functions identified in the AP600 System/Event Matrix document. This demonstrates the consistency of the AP600 ERGs with the design basis for the plant.

As discussed in subsection 1.5, the success paths for the ERG CSFs are based on the design basis success paths identified in the System/Event Matrix document. The ERGs were developed to address the design basis safety functions for events initiated from both at-power and shutdown conditions.

2.1.2 AP600 CSF Success Paths (Table 2)

For each AP600 CSF identified in Table 1, there are multiple success paths to accomplish the safety function. As discussed in subsection 1.4, a success path for a CSF is a specific combination of safety-related and nonsafety-related, defense-in-depth SSCs that are capable of accomplishing that particular CSF.

The overall goal of the defense-in-depth philosophy for the AP600 design is to provide multiple, diverse success paths that provide alternative means to accomplish each CSF. Each AP600 CSF has several safety-related success paths and additional success paths are provided by nonsafety-related, defense-in-depth SSCs. Individual success paths may have further redundancy as well.

Table 2 provides a list of the AP600 success paths for each CSF and a high-level functional comparison of the major success paths for the AP600 and a generic Westinghouse PWR plant, that serves as the reference plant. For each CSF, Table 2 lists the safety-related SSCs in the success path for that CSF and compares them to the safety-related SSCs in the same success path for the generic reference Westinghouse PWR plant. Table 2 also provides this same comparison for the nonsafety-related SSCs in the success paths for the CSF. The table organization, based on the six AP600 CSFs, is similar to the structure that is used in the subsequent tables that support the functional requirements analysis and the function allocation process.

Table 2 was compiled using the success paths identified in both the AP600 ERGs and the System/Event Matrix document.

The SSCs identified in Table 2 for the CSF Integrity are treated somewhat differently from the perspective of actuation, control, and operator actions than the SSCs for other CSFs. The CSFs, other than Integrity, are successful when the SSCs actuate and perform their specified functions. For example, core cooling is successful when the passive residual heat removal (PRHR) System/Event and other safety-related and nonsafety-related SSCs that provide core cooling actuate. The CSF restoration guidelines direct the operators to confirm satisfactory operation of the required SSCs or to take actions to initiate operation of required SSCs that have failed to start.

Similarly, the CSF Integrity is satisfied when the identified SSCs in the success path successfully actuate and are successfully controlled during their operation. However, challenges to Integrity occur when the required SSCs either actuate when not required, or when they successfully actuate and a control malfunction subsequently occurs. The AP600 design provides safety-related design basis protection. But beyond-design-basis malfunctions of the actuation or control functions for the identified SSCs in the success paths cause either overcooling (such as excessive steam flow through the turbine bypass valves) or overpressurization (excessive RCS makeup flow from the CVS makeup pumps). Therefore, to mitigate the consequences of these failures, most of the actions in the function restoration guidelines for Integrity direct the operator to respond in an opposite fashion from that of the other CSFs – to identify the malfunctioning SSCs that are operating in an unacceptable manner and to manually control or isolate the SSC, as appropriate.

2.1.3 Comparison of CSF Success Paths Between AP600 and Generic Westinghouse PWR Reference Plant (Table 3)

Once the AP600 CSF success paths are identified, the next step in the functional requirements analysis is to identify where the AP600 success paths are different from the success paths for the generic Westinghouse PWR plant, which serves as the reference plant.

For the purposes of the function allocation process for this evaluation, differences are identified only where they are operationally significant to the system and its function allocation.

For success paths that are unchanged from the reference plant, operating experience from existing plants becomes an important source of input for establishing the technical basis and rationale for the functional requirements and the function allocations.

Table 3 summarizes the results of a comparison of the success paths for AP600 and the generic Westinghouse PWR reference plant. The SSCs for the AP600 success paths for each CSF in Table 2 are listed in Table 3. For each success path, the results of the comparison of the AP600 success path with the corresponding success path (if any) for the reference plant are characterized in Table 3, using the following three categories to describe the differences:

- Unchanged
- Modified
- New

Two aspects are considered in determining whether an AP600 success path is unchanged, modified, or new. The first aspect relates to the overall system design configuration or system arrangement. This is represented in Table 3 by the letter "D" for "design." The second aspect relates to whether there are any differences in person-machine function allocation. The set of SSCs associated with an AP600 success path may be the same as for the generic Westinghouse PWR reference plant but there may be changes in level of automation. This second aspect of the comparison between the AP600 success paths and the corresponding success paths for the reference plant is represented in Table 3 by the letter "A" for "allocation." As a result, each success path in Table 3 includes the entries, "D" and "A." Each of these entries are placed in one of three columns that correspond to three categories – unchanged, modified, and new.

The notes in the last column of Table 3 provide a brief summary description where there are differences between the AP600 and the reference plant for the SSCs in the various success paths.

The three categories used in Table 3 to describe the differences that exist, if any, between the AP600 success path and the corresponding success path for the reference plant, are defined as follows:

Unchanged *This category is selected for an AP600 success path where there are no operationally significant changes in either the SSC design or function allocation from the equivalent success path in current plants.*

AP600 SSCs that normally operate to support power generation and can be used for accident mitigation such as main feedwater, RCS pressure control (pressurizer heaters and spray), and steam generator water level control are functionally and operationally equivalent to current plants, and their design is categorized as unchanged. This is consistent with the treatment for typical Westinghouse plants where there may be some slight differences in the exact pump designs or the number of specific valves, but these differences do not represent operationally significant differences. For these systems, the function allocation would also be categorized as unchanged.

There are no significant operational differences for nonsafety-related, defense-in-depth systems such as component cooling water or service water between current plants and AP600. Therefore, both their design and function allocation would be categorized as unchanged. For the component cooling water system and many other nonsafety-related and defense-in-depth systems, the primary difference between current plants and AP600 is that the piping and component classification is nonsafety-related instead of safety-related. The system operation is essentially identical, since the component classification changes do not affect design or automation.

The accumulators are a passive safety injection subsystem that are identical to the configuration in current plants and both their design and function allocation would be categorized as unchanged.

Modified *This category is selected for an AP600 success path where either the SSC design or its function allocation may be similar to the success path operation in typical Westinghouse PWRs, but where there are also some significant operational differences that must be considered for the functional requirements analysis.*

Although the high-level functions of the nonsafety-related CVS are essentially the same for the AP600 and for current plants (RCS purification, makeup, boration, letdown, etc.), the elimination of the reactor coolant pump seals results in only intermittent automatic makeup and manual letdown operations. Both AP600 and current plants do maintain continuous purification and the

purification components are similar (ion exchangers, filters, control valves, etc.), but the AP600 purification loop is designed for higher system pressure. Therefore, both the design and function allocation for this system is categorized as modified.

The design of the AP600 startup feedwater system would be categorized as unchanged since it is functionally similar to current plants. However, the function allocation is categorized as modified since the AP600 startup feedwater flow control valves are automatically controlled to reduce post-accident operator workload. In current plants, the equivalent auxiliary feedwater flow control valves actuate to a fully-open position on system startup. They must be manually throttled by the operators to reduce total feedwater soon after system actuation to prevent steam generator overfill and RCS overcooling. This is required early in an event when there are many conflicting demands on the operator.

New

This category is selected for an AP600 success path that may have a functional equivalent in current plants, but where a new system design feature is employed to perform specific functions in mitigating the consequences of an event. For example, the CMTs employ passive processes to provide high-pressure injection that is provided by high head safety injection pumps in current plants.

The AP600 design includes passive core cooling and containment cooling systems that include new design features and, therefore, new function allocations for the associated components. Many of the actuation signals for the AP600 are similar or identical to the actuation of the functionally equivalent systems on a typical Westinghouse plant.

The differences in engineered safety features (ESFs) design for the AP600 are primarily due to the following five new passive, safety-related SSCs included in the Table 3 success paths:

- The PRHR System/Event functions to transfer core decay heat from the RCS to the in-containment refueling water storage tank (IRWST).
- The CMTs function to provide high-pressure gravity injection at the existing RCS pressure and initiate automatic depressurization when the contained CMT inventory decreases and the other passive, safety injection sources are needed.
- The IRWST functions to provide a heat sink for the PRHR System/Event following PRHR actuation and a gravity injection source,

once the RCS has been depressurized. The IRWST performs similar functions to the refueling water storage tank (RWST) in current plants, except that the IRWST is now located at a high elevation inside the containment to provide gravity injection.

- The automatic depressurization system (ADS) functions to automatically depressurize the RCS when the CMTs begin to empty and a transition to the other passive, safety injection sources is required.
- The passive containment cooling system (PCS) functions to remove heat from containment (by convective and evaporative heat transfer) through gravity drain of water over the outside of the containment shell.

2.2 Results

Table 1 provides an overview of the Westinghouse ERG CSFs that form the basis for the AP600 function allocation. The table shows that there is overlap and consistency between the AP600 design basis safety functions provided in the System/Event Matrix and the ERGs. The ERGs are used to develop the symptom-based EOPs for use by the plant operators.

Table 2 provides a comparison of AP600 and reference plant success paths. The table shows the improved defense-in-depth capabilities that have been incorporated into the AP600 through the use of the safety-related, passive systems. The function allocation process must address each of the AP600 SSCs listed in this table.

Table 3 provides a comparison of the design and function allocation differences between AP600 and the reference plant for each SSC in the CSF success paths. The table shows that most of the differences that exist are related to one of the following four considerations:

- The use of safety-related, passive systems for safety injection and decay heat removal
- The use of advanced, digital I&C systems
- Automation of SSC actuation and control functions that help to reduce operator workload during critical periods following an event
- Recommended design improvements (from operating plant experience, the AP600 PRA, etc.) that help to improve overall plant safety

2.3 Verification and Updating of Functional Requirements Analysis

A number of activities are conducted to verify the adequacy of the functional requirements analysis specifying the functions, systems, and processes involved in maintaining CSFs. The design basis safety analysis presented in Chapter 15 of the SSAR establishes the adequacy of the functions, systems, and processes for design basis events. PRA analyses provide further verification of the adequacy of the description of functions, systems, and processes involved in maintaining CSFs for beyond-design-basis events. In addition, the FBTAs that are performed by the M-MIS group as part of task analysis activities, provide verification that the set of sensors and controls that have been specified by system designers are sufficient to support operators in performing the role they have been assigned in system function.

Mechanisms are available within the AP600 design process for updating the functional requirements analysis as the design proceeds. The process by which design changes are proposed, evaluated, tracked, and implemented is described in the AP600 Simplified Passive Advanced Light Water Reactor Plant Program, Program Operating Procedures (WCAP-12601, Ref. 19).

3.0 AP600 INITIAL FUNCTION ALLOCATION

Function allocation involves the analysis of the requirements for plant control and the assignment of control functions to one of the following:

- Personnel (i.e., manual control)
- System elements (i.e., automatic I&C systems and passive, self-controlling phenomena)
- Combinations of personnel and system elements (e.g., shared control using automatic systems with manual backup)

The goal of function allocation is to maximize overall plant safety and reliability by exploiting the strengths of personnel and system elements, including improvements that can be achieved through assignment of overlapping and redundant responsibilities.

This section describes the Westinghouse methodology for initial function allocation of the AP600 CSFs and presents the results. The results include documentation of the rationale for function allocations for AP600 CSFs.

3.1 Methodology for Function Allocation

A review of the literature, including references cited in NUREG-0711, revealed no single standard or accepted function allocation methodology, either in the general HFE literature or in nuclear power industry-specific documents. Instead, there are a number of proposed approaches to function allocation, many of which share a similar philosophy.

3.1.1 The General Approach to Function Allocation

The general approach to function allocation can be captured by the following:

1. Identify the functions that need to be allocated
2. Allocate as best as possible using a set of guidelines and heuristics
3. Document and justify the reasons for allocation
4. Test the allocation and fix the problems through iterative design-and-test cycles

The primary example of this approach is found in NUREG/CR-3331. The approach outlined there begins with a specification of system functions. It then identifies the desired role of the

human operator. The allocation, however, is also driven by justifications for automating functions. In fact, this allocation algorithm starts with the following sequence:

- Identify functions for which automation is mandatory
- Identify functions for which human performance is mandatory

For each function, a list of possible reasons is offered as to why the allocation should be mandatory. The process considers the feasibility of the allocation such as cost, capabilities, technology, schedule, etc. Not all functions will receive a mandatory allocation. Therefore, the function allocation in subsequent steps of the process is assigned based on weaker allocation criteria. The analyst must then identify reasons why an allocation would be clearly preferable. This decision is split into two steps:

- Identify functions for which automation is strongly preferred
- Identify functions for which human performance is strongly preferred

The first two allocation decision sequences should identify functions for which strong evidence supports a specific allocation. Remaining are functions that might be tailored to work either way, as automated or assigned to human performance. For these functions, a series of guidelines are used to determine which allocation best suits that function. These guidelines, which are perhaps better labelled heuristics, primarily concern performance requirements and relevant capabilities of humans and automation. There are a number of "tables of relative merit" (e.g., Fitts, 1951, Ref. 15) that are used to match task characteristics with strengths of humans and machines. The common form of these tables is one list of task characteristics for which humans have superior capabilities and one list of task characteristics for which automation has superior capabilities.

Further, during this phased allocation process, there is an option to break a function into smaller segments (individual tasks or processes) that better lend themselves to allocation. That is, a single function, as initially defined, may have a mix of performance characteristics that make it difficult to allocate one way or the other. In this case, the analyst is asked to redefine the function to identify smaller segments that are more easily allocated.

When this allocation process is complete, that is, after all functions have been given an initial assignment to either automation or human performance, a set of more in-depth questions must be answered having to do with ensuring that the allocations can truly be supported in the system design. For example, for functions that will be assigned to automation, there is a need to determine the extent to which the human operator will have the capability for manual backup or to be aware of the activities of the automated process.

The allocation process, therefore, allows one to make initial assignments and to identify related groups of tasks assigned to humans and automation. However, because there is a

strong dynamic component to task performance, it is necessary to evaluate the initial assignments in the context of actual performance (typically in a simulated control room). Therefore, the design needs to remain open to the possibility for re-allocation, depending on the outcome of design tests. Especially important are issues of appropriate operator workload, which are best assessed in a dynamic simulation.

A recent International Atomic Energy Agency (IAEA) document (IAEA-TECDOC-668) lays out an allocation process with the same form although there are fewer details regarding the criteria for each allocation decision. Recent analysis of the System 80+ by ABB/Combustion Engineering (Reference 23) borrows heavily from the NUREG/CR-3331 method.

This general approach will be exploited for function allocation. The specific AP600 methodology begins with the core of the NUREG/CR-3331 process. The specifics of the approach are described in the next section.

3.1.2 Westinghouse Function Allocation Process

Figure 1 shows the flow diagram that represents the AP600 approach to function allocation (Note that this diagram shows the flow through the process. The specific checklist items contained in each box are shown in Table 6). This diagram borrows heavily from the NUREG/CR-3331 process.

The initial question is "Is automation mandatory?" (box 1). This set of checklist items asks the analyst to determine whether there is a requirement to allocate the function to automation. The first two items assess whether there are conditions that prohibit the involvement of humans (hostile conditions, or tasks that are impossible for humans to conduct). The third item is used to reveal regulatory or industry requirements that might remove the option for human operator control. A variety of regulatory and industry requirements and guidelines must be considered. Some of these requirements and guidelines are specifically related to HFE activities, while others indirectly affect the function allocation through the impact on the design of specific plant systems and the associated system actuation and control requirements. The following are various regulatory and industry documents that are considered in the function allocation process described in this report:

Part 50 of the Code of Federal Regulations

From a regulatory perspective, the overall nuclear power plant design is controlled through the licensing requirements specified in Part 50 of Title 10 of the Code of Federal Regulations (10 CFR 50), and this document forms the basis for many of the design requirements, including those that directly or indirectly affect function allocation. Appendix A of 10 CFR 50 provides the General Design Criteria (GDC) for nuclear power plants, that contain high-

level design requirements that must be met as part of the plant licensing basis. There are 55 GDCs that include the following requirements:

- Overall requirements
- Protection by Multiple Fission Product Barriers
- Protection and Reactivity Control Systems
- Fluid Systems
- Reactor Containment
- Fuel and Reactivity Control

Some of these GDCs contain design requirements directly related to automation of actuation and control functions. GDC 20 (Protection System Functions) is one of the more important for function allocation. It contains generic GDC requirements for the automatic actuation of protective functions for the appropriate systems and components that are important to safety, including the reactivity control system. There are other GDCs that also address automatic actuation and control related to various SSCs, including instrumentation, electrical power, main control room habitation, reactivity control, emergency cooling, containment penetrations, and radioactive ventilation discharge.

In addition, the CFR contains other groups of miscellaneous design requirements that may directly or indirectly affect function allocation. These include the TMI-related requirements provided in 10 CFR 50.34(f) and special requirements for some individual safety issues such as Anticipated Transient Without Scram (ATWS) in 10 CFR 50.62 and loss of all alternating current (station blackout) in 10 CFR 50.63.

These general criteria are supplemented by more specific and detailed design criteria that are contained in other supporting regulatory documents. These other documents are not part of the CFR, but they reference the appropriate Appendix A requirements that the detailed requirements or guidelines are intended to support.

Other Regulatory Documents

The other important groups of regulatory documents that are considered and addressed in both the system design and the function allocation processes include the following:

- Standard Review Plan (NUREG-0800)
- Regulatory Guides
- Generic and Unresolved Safety Issues (NUREG-0933)
- Advanced Light Water Reactor (ALWR) Certification Issues (SECY 93-087)
- Generic Letters and Bulletins

These documents support and reference the high-level requirements in the GDCs. For example, Standard Review Plan (SRP) subsection 6.3 (Emergency Core Cooling System), provides specific design acceptance criteria for the NRC staff reviewers to confirm that in accordance with the GDC requirements, "the primary mode of actuation for the emergency core cooling system must be automatic, and [that] actuation must be initiated by signals of suitable diversity and redundancy." The AP600 PXS is designed with automatic actuation of isolation valves for some components controlled by I&C system signals, and for other components controlled by inherent natural (passive) processes, as described later in this report.

Note that as part of the AP600 design and design certification process, the AP600 design has been systematically and comprehensively assessed against the design requirements in these regulatory documents. Therefore, the AP600 overall design, including the function allocation, comprehensively addresses the requirements and guidelines provided in these regulatory documents. The results of these assessments are provided in either the appropriate sections of the AP600 SSAR or the WCAP reports listed below:

- General Design Criteria
SSAR, subsection 3.1
- Standard Review Plan
WCAP-13054 (Ref. 21)
- Regulatory Guides
SSAR, Appendix 1A
- Generic and Unresolved Safety Issues/Human Factors Issues
SSAR, subsection 1.9.5
- TMI Issues SSAR, subsection 1.9.5
- ALWR Certification Issues
SSAR, subsection 1.9.5
- Generic Letters and Bulletins
WCAP-13559 (Ref. 22)

One of the important considerations in the specific design criteria for automation of SSC actuation functions is related to the timing of manual operator actions for safety-related SSCs. In addition to the specific function allocation requirements identified in the system design requirements, there are also regulatory and industry efforts to develop appropriate guidelines for automatic function actuation based on establishing a time criterion for safety-related operators actions. Additional information is provided in Unresolved Safety Issue B-17, Criteria for Safety-Related Operator Actions, in NUREG-0933 (Ref. 16) and ANSI/ANS 58.8-1984, Time Response Design Criteria for Nuclear Safety-Related Operator Actions, (Ref. 17). These documents discuss the time criterion (10 minutes) to be met by the plant design related to automatic and manual actuation of safety-related SSCs, as confirmed by nuclear safety analyses presented in Chapter 15 of the SSAR.

Industry Design Requirements

In addition to these regulatory requirements, there are industry design requirements that must be considered as part of the AP600 design. The industry design requirements are contained in the EPRI Advanced Light Water Reactor Utility Requirements Document (ALWR URD) for the ALWR Passive Plant (Ref. 2). This document includes both high-level and specific industry design criteria that affect the AP600 plant and system design.

The AP600 design process also includes a comprehensive assessment of the AP600 design against the URD design requirements. The URD design criteria can also affect the AP600 function allocation and, therefore, are considered as part of the process. The URD requirements include two specific design basis requirements (30 minutes and 72 hours) related to operator action times.

Function Allocation

The function allocation flow diagram shows that if any question in box 1 receives a "YES," meaning that it must be allocated to automation, then the next question becomes "Is automation technically feasible?" (box 2). This decision requires an engineering analysis to determine whether issues such as cost, technology, scheduling, or implementation will prohibit the development of automation. If there is no concern, the function is tentatively allocated to automation and control is passed to box 10. If there are concerns about the development of automation, the analyst is asked to redefine the function or rethink the analysis. Often, in this case, segments (individual tasks or processes) of the function can be defined for easier allocation.

If all items in box 1 receive a "NO," the flow diagram passes control to box 3 to ask "Is human performance mandatory?" The first checklist item in this box determines whether it is impossible to develop an adequate automation capability, which would preclude the use of automation and require an allocation to human performance. Note that this item also serves as a check for the feasibility of automation for the remainder of the flow diagram. The other item concerns mandatory allocation to a human operator based on a design requirement or regulation. If there is a "YES" response to either of these items, the next question asked is "Is human performance a feasible solution?" (box 4). This decision requires two judgments. First, are human operators capable of performing the tasks specified? Secondly, the analyst is asked to judge the operator workload to determine whether this allocation to a human operator will exceed a manageable workload.

If the analyst determines that there are no significant concerns about human capabilities or workload, the function is tentatively allocated to human performance and control is passed to box 11. If there are concerns about allocation to a human operator, the analyst is asked to

redefine the function or rethink the analysis. Often, in this case, segments (individual tasks, processes) of the function can be defined for easier allocation.

If there is a determination in box 3 that an allocation to human performance is not mandatory, the second phase of assessment begins -- that is, the assessment moves from a mandatory allocation to an allocation that is preferred. As before, allocation to automation is tested first. Thus, the next question (box 5) is "Is automation clearly preferable to human operators?" The first checklist item found here focuses on whether automation technology can be implemented effectively. The second item is concerned with different types of analysis that indicate that an allocation to automation would clearly be preferred.

Westinghouse identified four possible reasons why automation would be preferred at this point. First, automation could be important, based on operating experience from predecessor plants. An analysis of operating experience may reveal that either the function was automated and this allocation worked well, or that the function was allocated to human performance and there were documented problems with this allocation.

Second, the PRA analysis may show that although automation is not mandatory, it can provide a benefit to plant safety for specific event sequences. For example, following a loss of core cooling during reduced RCS inventory conditions (mid-ioop operations). Although the operator has sufficient time to mitigate this event, credit for operator action has a very small PRA benefit and automatic actuation of IRWST injection provides a more significant benefit. Another example is the addition of backup, safety-related heat removal functions through automatic actuation of the CMT. Although manual feed and bleed operation of the RCS is also modeled in the PRA, the automatic CMT actuation, using diverse actuation from the PRHR actuation signals, provides a more significant PRA benefit than the manual feed and bleed process. Therefore, this design feature was implemented in the AP600 design as safety-related, defense-in-depth protection in the event of beyond-design-basis failures of the PRHR System/Event.

Third, the plant design may include passive design features that actuate on inherent, passively controlled actuation and therefore, preclude human performance. For example, actuation and control of accumulator injection depend on the pressure differential between the RCS and the accumulator following an event, and are independent of manual actuation or control.

Fourth, there is a judgment about the likelihood of operator overload if an SSC is not automated. When there is a high likelihood of overload, the allocation to automation is strongly preferred. For example, the startup feedwater flow control valves have been automated in AP600 so that steam generator water level is automatically controlled after system actuation. This is an improvement over current plants where manual actions are required to control feedwater flow shortly after an event initiates, in order to prevent steam

generator overfill and/or RCS overcooling. In current plants, these manual actions are required at a time very early in an event, where the potential for operator overload is high. This automation is very beneficial.

These four items are considered to determine whether automation is clearly preferred. Thus, if both checklist items receive a "YES" response, the function is tentatively allocated to automation and control is passed to box 10.

If the response to either checklist item is "NO," control is passed to box 6, which asks, "Is human performance clearly preferable to automation?" This box provides an opportunity to identify special reasons that a human operator has significant advantages over automation, such as the need for an operator judgment prior to actuation. If this item receives a "YES," the function is tentatively allocated to human performance, and control is passed to box 11.

If the response to box 6 is "NO," then the analyst probably needs to begin thinking about splitting the function into meaningful segments that can be more easily allocated. That is, if there is no strong reason to allocate the whole function to either automation or human performance, there may be a need to evaluate meaningful segments of the function to determine if there are segments that are better suited to one or the other.

Control is initially passed to box 7, which asks "Is the segment a suitable candidate for automation?" The checklist items found in box 7 provide the analyst with a set of criteria that suggest the value of allocating to automation. Thus, if any of these criteria are met (i.e., a "YES" response), the segment (and perhaps the bulk of the function) is tentatively allocated to automation. If none of the criteria is met (i.e., all "NO" responses), then control is passed to box 8.

Box 8 asks, "Is the segment suitable for human operator performance?" As with box 7, this box provides a set of checklist items that suggest the value of allocating to a human operator. The first item is a general one that should lead the analyst back to a "table of relative merit" listing, such as the one found in Fitts (1951). The analyst can use this type of list to determine whether there are specific capabilities that are more characteristic of humans and are needed to perform the designated function. If the analyst identifies some aspect of performance from this list, the segment (and perhaps the bulk of the function) is tentatively allocated to human performance. If one of the criteria is met (i.e., any "NO" response), then control is passed to box 9.

Box 9 provides a final opportunity to allocate, after all compelling reasons to allocate one way or the other have been reviewed and dismissed. This box allows the analyst to consider items such as cost and operator preference. Again, any allocations that occur at this late stage in the process are likely to apply to parts of functions instead of entire functions as

initially defined. This is also the last opportunity to split a function into meaningful segments if this option had not been selected in previous steps of the process.

Thus, through this phased process, all functions (or function segments) should be allocated to either automation or to human performance. It is insufficient to stop at this point and test the allocations in a dynamic simulation. Instead, the analyst needs to consider how the allocations will be integrated into the larger design. Thus, box 10 asks the analyst to revisit the functions allocated to automation and determine the role of the human operator, which needs to be coordinated with the automated processes. Similarly, box 11 asks the analyst to consider how human performance needs to be supported by the control room interface and coordinated with automated systems.

The flow diagram can be used to make allocations to automation. The process can also be specified so as to identify all decision paths that lead to an automation allocation and that apply to AP600. From all of the possible allocation decision paths that exist in the flow diagram, the following eight paths to an allocation to automation were used as part of the AP600 function allocation process. (Following each is the path through the flow diagram. The numbers identify the questions that receive "YES" responses):

- A1. The operator is not able to perform the required task due to human limitations. (1b, 2, 10)
- A2. Automation is necessary due to regulatory design requirements. (1c, 2, 10)
- A3. Automation is necessary due to utility design requirements. (1c, 2, 10)
- A4. Automation provides a safety benefit as identified in the PRA. (5a, 5b(2), 10)
- A5. Automation is preferred based on operating experience. (5a, 5b(1), 10)
- A6. Automation is preferred due to concerns for operator overload. (5a, 5b(4), 10)
- A7. Automation is inherent in the passive design. (5a, 5b(3), 10)
- A8. Tasks are not well suited to human performance and are better suited to automation. (7a-f, 10)

These eight items are used to specify the basis for the automation allocation provided in the function allocation basis column of Table 5. If none of these criteria is met, there would be an allocation to human performance. As shown here, each specification is equivalent to a path through the flow diagram.

The flow diagram can also be used to make allocations to human performance. The process can be specified so as to identify all decision paths that lead to a human performance allocation and that apply to AP600. The following are the possible paths to an allocation to

human performance. (Following each is the path through the flow diagram. The numbers identify the questions that receive "YES" responses):

- M1. Human performance is required because automation is not technically feasible. (3a, 4, 11)
- M2. Human performance is required by design recommendations or requirements. (3b, 4, 11)
- M3. Human performance is preferred because of consideration of safety requirements, task complexity, cost/benefit considerations to implement automation, and the value of human judgement. (6a, 11)

These items are used to specify the basis for human performance allocation provided in the function allocation basis column of Table 5. As shown here, each specification is equivalent to a path through the flow diagram.

3.1.3 Integration of Automation and Operators

Boxes 10 and 11 in the function allocation decision process (Figure 1) are the points at which an initial allocation to automation or to human performance needs to be integrated into the larger design. These boxes, described in the following subsections, present the set of guiding principles embedded within the methodology. That is, after the initial allocations to either automation or human performance, Westinghouse integrates the complementary capabilities according to the principles found here.

3.1.3.1 Guidelines for the Residual Role of the Operator for Functions Allocated to Automation

When a plant function is automated, the designer needs to specify the role that the human operator will play in that function. There are traditional roles for nuclear power plant operations, which are described here and split out into three components: actuation, control, and termination.

Actuation

For automatic actuation, which is the automatic initiation of an SSC, the operator could be assigned any of the following roles.

1. To manually actuate a specific automatic function in a pre-emptive fashion:

This allows the operator to be proactive in maintaining safety during plant operation by manually actuating an SSC if it is recognized that an automatic actuation set point

is being approached and mitigation actions are expected to be inadequate to prevent the automatic actuation.

2. To be a back-up for the automatic actuation:

That is, when the actuation criteria are met and the automatic system fails, the human operator has the capability to actuate the system manually.

3. To take the role of a supervisor when an automatic actuation occurs in determining that the automatic function has actuated completely and is performing appropriately, that is, achieving correct functional and operational goals
4. To take actions to mitigate the event by maintaining or restoring plant conditions to prevent reaching a condition that requires an automatic actuation:

For example, recovering RCS pressurizer level control by starting CVS makeup pumps can prevent actuation of the CMTs or low-pressure reactor trip due to decreasing pressurizer level. The operator prevents the automatic actuation function by preventing the requisite condition for the automatic actuation rather than by interfering with the actuation function.

It is important to note the roles that operators are not explicitly given for automatic actuation. Operators are not provided with the capability to prevent automatic actuation. Thus, the operator has the capability to provide manual actuation at any time, but does not have the capability to defeat the automatic actuation. The need for automation is based on an inability of the function to be performed manually under all conditions. Therefore, the operator is normally prohibited from being able to defeat the automatic isolation.

For several specific actuation functions in a very limited number of situations, the operator must be able to defeat the automatic actuation function (using operational blocks or actuation resets), where it is required to support some plant operation such as plant startup, shutdown, or recovery following an accident. For example, the operator is directed by procedures to block low-pressure safety injection prior to reaching a specified pressure limit during plant cooldown and depressurization. This is required to allow plant shutdown without initiating an unnecessary and undesirable safety injection. This function is not automated because operator judgement is used in determining that satisfactory conditions exist to block the safety injection function. Similarly during a reactor startup, operator judgement is required to block the excore nuclear instrumentation source range high flux trip, after confirming proper operation and overlap of the intermediate range instrumentation, to allow the reactor startup to continue without a reactor trip.

The operator also has the capability to override individual inputs that may contribute to automatic actuation functions under certain very specific conditions. For example, there are a large number of individual plant parameters that can actuate a reactor trip or other safety-related actuation (such as low pressurizer pressure, low reactor coolant loop flow, low pressurizer level, etc.). The I&C system designs must provide the capability to address component failures. This is provided by allowing defeat of the individual inputs from a failed instrument channel that actuates the specific function. The function within the affected channel can be placed in a bypassed condition to allow repair of the failed sensor or channel. This individual channel capability does not eliminate the automatic actuation function, but can defeat one of the multiple, redundant instrumentation channels that determine if the actuation function is required. In a bypass condition, the actuation coincidence logic for that function is automatically reduced to two-of-three instead of two-of-four, but the operator has not defeated the automatic actuation function.

Functional diagrams for the automatic reactor trip and engineered safeguards functions are provided in subsection 7.2 of the AP600 SSAR.

Control

An automated system, after it has been actuated, can also be automatically controlled without operator inputs. As with actuation, however, a significant role is assigned to the human operator. In many cases such as the startup of the nonsafety-related startup feedwater system, manual control is an option selected by the operator. That is, the design allows the operator to select whether the system is automated or under manual control. Thus, even though in most cases the system is actuated and controlled automatically, there are reasons why the operator may want to place the system under manual control:

1. *A manual back-up is needed when the automated control process fails. This defines a manual override or intervention in which the operator must determine that the automated system is not working and manual control is needed.*

For example, manual control would be required to override an automatic control function that fails because of an I&C system failure, such as a circuit board or an input sensor. The digital I&C design provides capabilities such as self-checking of internal components and identifying when sensors fail beyond an allowable or expected range. There is still a need to provide the operator with the capability to take manual control of control functions.

2. *Manual control of the system is needed prior to disabling automatic functions for preventive or corrective maintenance or post-maintenance testing.*

It is possible to perform some preventive or corrective maintenance and post-maintenance testing on parts of an automatic control instrumentation channel while in automatic control. However, there are some parts of the circuitry that may require maintenance or testing and that preclude simultaneous automatic control operations.

These discussions are not intended to imply that manual control is not a concern during steady state conditions, when there are no significant plant operational transients or events in progress. The design intent is to use automatic control, where installed and when possible, because an unplanned transient or event can occur at any time. In this case, automatic response is expected to provide a more effective response for transients that occur too quickly to rely on manual actuation, and especially during the initial part of any transient or event where operator overload precludes effective manual control.

There are variations in the difficulty of the manual control for the various automated control functions. For some plant control functions, such as the rod control system during power operation at a constant power level, long-term manual control is less onerous and may be acceptable (note that accidents can result in a reactor trip, which obviates the need for this specific automatic control function). In most situations, manual control is not difficult for short periods of time or during stable plant conditions, following the failure of the automatic control function while repairs or adjustments are being made.

The Role of Passive Systems - Actuation and Control

For SSCs that actuate by passive processes, the operator cannot prevent component actuation, although there may be indirect control over plant conditions related to the actuation. For example, the initiation of accumulator injection is controlled by the RCS and accumulator pressure differences that open the accumulator discharge check valves. During plant depressurization following ADS actuation, the depressurization sequence actuates accumulator injection independent of operator action. However, for some low-pressure events that do not involve ADS actuation, the operator could potentially take corrective actions to restore RCS pressure or inventory, precluding the need to initiate accumulator injection, although the operator has no direct control over the accumulator discharge valve operation.

The operator can take actions to initiate safety-related, passive processes for those that are actuated by operation of specific components, such as initiation of automatic depressurization. These anticipatory actions can be taken by operators at any time prior to reaching the automatic actuation set point.

For most SSCs that are controlled by passive processes, the operator has no direct control over the component performance, such as CMT injection flow or ADS valve vent flow, although there may be indirect control over plant conditions that affect the passive process. For example, recovering RCS inventory by providing CVS makeup will maintain sufficient inventory to preclude the need for further CMT injection.

Termination

Termination of an automated process is performed by the human operator. The fundamental goals of the ERGs and the EOPs are to mitigate the consequences of an event and to stabilize plant conditions, thereby placing the plant in the appropriate condition to facilitate plant recovery. Therefore, at some point during the event, the operator is required to determine when stable plant conditions have been established. At this time, repair, recovery, or re-start actions are expected to be initiated and the safeguards systems must be restored to the conditions required to provide design basis protection for the existing operational mode determined by Technical Specifications (TS).

The operator is assigned the role of evaluating plant conditions against specified criteria in the EOPs to determine if the termination criteria have been met. If the EOP safeguards actuation termination criteria are met, the operator is directed to reset the appropriate safeguards actuation signals provided by the I&C systems, to restore the required safeguards equipment to the proper standby conditions, and to recover the plant. These manual safeguards equipment termination actions override the automatic actuation signals for the associated equipment, provided that the actuation criteria and signals are no longer present. Based on the existing plant conditions, the automatic actuation functions are then restored as appropriate by the I&C system actuation circuitry.

If manual actions are attempted to isolate safeguards equipment and to restore it to a standby condition, or to otherwise manually defeat automatic actuation and control functions without terminating the actuation signals, the operator will be unable to override the automatic actuation and control signals.

In previous Westinghouse plant designs, the use of manual termination had the potential to place the operator in a goal-conflict situation. However, the AP600 passive safety injection systems provide a benefit over the forced-flow safety injection systems in the reference plant in relation to the termination of safety injection systems following an accident.

Following a safeguards actuation signal in the reference plant, the operation of the pumped safety injection systems results in very large quantities of water being provided to the RCS. For most events, unless there is a relatively large break, this forced flow from the high head, intermediate head, and low head safety injection pumps can potentially cause RCS overfill. It can also re-pressurize the RCS to either the shutoff head of the operating pumps or the

pressurizer safety valve setpoint, whichever is less. The potential for overfill and RCS overpressurization provides the operators with conflicting goals -- maintaining safety injection flow until the event is stabilized versus terminating the safety injection signal as soon as possible to prevent overfill.

The AP600 passive safety injection systems have been designed to provide the required safety injection flow for design basis events. The passive systems provide lower injection flow rates than the reference plant (for the same condition) and flow is controlled by passive processes, based on the need for injection. Therefore, passive components and the passive process control features are expected to result in slower transients.

For example, the CMT high-pressure injection flow provides significant benefits over high head injection in the reference plant, with regard to overfill and operator goals conflicts in terminating safety injection. Three features tend to naturally limit the potential for the CMT to cause RCS overfill. First, the injection volume that the CMTs can provide is physically limited by the CMT volumes. The CMT volume is much less than the RWST volume available to the high head safety injection pumps in the reference plant. Second, the CMT flow rate is controlled by passive processes, such as gravity injection and natural circulation conditions, and the injection flow is affected by the plant conditions that are related to the need for injection. For example, CMT injection flow is much greater when significant RCS voiding exists than for non-voided conditions. Third, the PRHR automatically actuates when the CMTs are actuated, thereby, reducing RCS temperatures. The subsequent RCS shrinkage tends to provide more margin to RCS overfill.

Therefore, for non-Loss of Coolant Accident (LOCA) events and smaller LOCA events, the potential for RCS overfill is reduced for the AP600. The operator has more time to stabilize plant conditions and to terminate safety injection, than for similar events in the reference plant.

The passive systems also provide the capability to respond to more severe transients when required. For example, a large-LOCA event results in a very rapid RCS depressurization and the passive safety injection systems must be capable of mitigating these rapid events. The accumulators are designed to rapidly inject into the RCS to flood and refill the reactor vessel following a large-LOCA. However, for smaller LOCA events, the accumulator injection will be slower since it is passively controlled, based on pressure differences between the RCS and the accumulators.

The differences in operation of the passive safety-related systems is expected to reduce operator goal conflict in AP600, when compared to the reference plant.

Functional diagrams that clarify the termination capability for the specific engineered safeguards functions are provided in subsection 7.2 of the AP600 SSAR.

Information Needs

To allow the operator to take these various roles that include supervisory monitoring, support, or back-up of automated SSCs, the M-MIS must provide an appropriate set of instrumentation to the operator. The AP600 SSAR describes the instrumentation available to the operator for each plant system. In addition, subsection 7.5 of the AP600 SSAR contains the identified post-accident monitoring instrumentation provided to the operator to confirm required plant conditions and to verify proper operation of, or the need for manual actuation of, the safety-related and nonsafety-related, defense-in-depth SSCs that are used to mitigate the consequences of an accident. The regulatory guidelines for this instrumentation are provided in Regulatory Guide 1.97 (Ref. 18) and plant conformance with these guidelines is discussed in Appendix 1A of the AP600 SSAR. The M-MIS design activities will determine how to best display this information to support each of these operator roles.

Summary

There are several fundamental principles related to automation and the role of the operator that are considered in function allocation, including the following:

- Automatic actuation and control functions are needed for a variety of regulatory and design reasons -- for example, when the operator is not fast enough or is too busy to perform required actuation and control functions.
- For SSC actuation, the human operator serves primarily as a back-up to the automated system.
- For SSC control, the human operator serves as a back-up when automation fails, but for certain operating conditions, the use of manual control is preferred.
- The human operator is used always for termination.
- The operator has limited control over passively-actuated and passively-controlled functions.

3.1.3.2 Guidelines for the Residual Role of Automation for Functions Allocated to Human Performance

When a function has been allocated to the human operator, the system designer needs to apply guidelines for integrating the capabilities of the M-MIS and plant systems to support the operator in manual operations. In general, the following are applied through the M-MIS design process:

- Develop displays that aid the operator in thinking about the process from both physical and functional perspectives (present plant state indications to aid the operator in understanding the current situation)
- Use plant systems to monitor for set point violations and other significant changes to aid the operator in identifying important changes
- Use plant systems for monitoring parameter values that are needed in completing procedures and then informing the operator about the status of those parameters in the context of the procedure step
- Aid the operator in locating and accessing important plant state information that may become relevant to operations

Chapter 18 of the AP600 SSAR provides a detailed discussion of the HFE design process, including the human system interface (M-MIS: Section 18.8 of the AP600 SSAR).

3.1.3.3 Implementation Schemes

After decisions have been made regarding the use of automation and human operators, it is possible to classify the various implementation schemes that have been used at a system level. For actuation, there are five possible implementation schemes that are discussed in detail in subsection 3.2. These five implementations schemes include the following:

1. Passive The actuation of the SSC depends on an inherent, natural process and is independent of operator action.
2. Parallel The operator has the capability to actuate the SSC manually at any time. Although the function is actuated automatically, the operator does not have the capability to defeat automatic actuation (excluding certain required resets and operating bypasses).

3. Selectable The operator has the capability to select whether the SSC can be manually or automatically actuated. Selecting manual actuation can defeat the automatic function.
4. Complementary
 There is sharing of actuation responsibilities between the human operator and automation.
5. Manual The human operator is solely responsible for actuation.

For control, there are four possible implementation schemes that are discussed in detail in subsection 3.2. These four implementations schemes include the following:

1. Passive The control of the SSC depends on an inherent, natural process and is independent of operator action.
2. Selectable The operator has the capability to select the mode of control, which can defeat the automatic function.
3. Complementary
 There is sharing of control responsibilities between the human operator and automation.
4. Manual The human operator is solely responsible for control.

Note that there is no implementation scheme in which actuation or control is solely achieved by I&C automation (see "Automatic" on page 3-18). These implementation schemes are identified in Table 4.

Subsection 3.1 provides a discussion of the methodology used for the function allocation process. Subsections 3.2 and 3.3 provide the results of this process and subsection 3.4 provides a summary of the important results from Tables 4 and 5, which documents the function allocation results.

3.2 AP600 Function Allocation Summary (Table 4)

Table 4 was developed to provide a comprehensive summary of the AP600 function allocation for the safety-related and nonsafety-related defense-in-depth SSCs. The table organization is based on the six CSFs, similar to the structure provided in Tables 1, 2, and 3. For each of the AP600 CSFs, the table identifies the same success paths and appropriate SSCs in each success path that were compiled in the earlier tables.

For each of the SSCs in the success paths, Table 4 provides the following information needed to understand the function allocation:

- A description of the SSC actuation
- A description of the SSC control
- Specific summary comments about each SSC in the success path
- An overview of the type of protection provided by the success path

As discussed previously, a success path can be made up of a single SSC or a group of SSCs that work together to accomplish a CSF. Table 4 provides information for each of the SSCs in each success path to understand the function allocation for that SSC.

The sequence of the success paths in Table 4 for each CSF is listed in the order that the success paths are expected to be actuated. The nonsafety-related, defense-in-depth SSCs are normally automatically actuated first. The safety-related, passive components are not expected to be required for an event, unless there are failures of the defense-in-depth systems. For beyond-design-basis events where multiple, safety-related SSC failures have occurred, backup success paths using either safety-related SSCs, nonsafety-related SSCs, or combinations of the two groups of SSCs are listed in the order that they are expected to be implemented. The success paths that are expected to be used either during shutdown or after shutdown conditions have been established following an event, are listed last in the table and are indicated with the word "shutdown" in parentheses.

For example, nonsafety-related main feedwater pumps and startup feedwater pumps are the first success paths to provide core cooling, and the safety-related PRHR System/Event would not be expected to actuate following events unless both of these success paths were unavailable. If the design basis protection provided by the PRHR also fails, backup success paths using the CMTs, accumulators, normal residual heat removal system (RNS), IRWST, and ADS are available, as indicated.

SSC Actuation Functions

Table 4 includes two columns to describe the SSC actuation. The first column is used to indicate when the SSC is automatically actuated and the entry in this column describes the type of actuation for that SSC. The second column is used to indicate when the SSC is manually actuated. If there are no automatic actuation capabilities for an SSC, then there will be no entries in the automatic column.

Most of the AP600 SSCs are actuated by the plant I&C systems -- the safety-related PMS, the nonsafety-related PLS, or the nonsafety-related DAS. The I&C systems are designed to provide a manual actuation capability for SSCs that are automatically actuated. This capability allows the operator to proactively initiate success path SSC functions when

necessary, as well as functioning as a backup in the event that the automatic actuation function fails to properly actuate an SSC.

The following actuation capabilities exist for the AP600:

Passive (Pass)

The SSC accomplishes safety function(s) through naturally inherent passive actuation processes (such as doppler reactivity feedback, natural circulation flow, passive heat removal and injection, or mechanical overpressure relief protection) that are independent of both I&C system actuation and operator action.

Accumulator injection is initiated passively by the pressure differential that opens the discharge check valves when RCS pressure decreases below accumulator static pressure. Injection is controlled by the pressure differential between the accumulator and the RCS.

Automatic (Auto)

The SSC actuation is completely automatic, without a means for manual actuation.

There are no AP600 SSC actuation functions in this category. The AP600 automatic actuation features also have the capability for manual actuation.

There are certain interlocks and permissives that are contained within the high-level actuation functions addressed as part of the function allocation process, and that contain automatic actuation features (without the capability for manual operator interfaces). These are internal to the specific high-level actuation function circuitry and are not appropriate to address, based on the intent of the function allocation process. These automatic features on the I&C circuitry are limited to specific interlocks or permissives that are contained within larger actuation circuits and are only mentioned for clarification and completeness of this evaluation. See the functional diagrams in Chapter 7 of the AP600 SSAR for more details.

For example, opening of the RNS pump suction isolation valves (that are used to establish closed-loop RNS cooling during shutdown conditions) is a "manual" actuation function. However, the actuation circuitry includes an automatic interlock to prevent the operator from opening these valves if RCS pressure is above a certain setpoint to prevent overpressurizing the RNS. The operator cannot disable or defeat this interlock. As part of the function allocation process,

actuation of the RNS is appropriately categorized as "manual," but the manual actuation circuitry contains this automatic interlock feature.

Parallel (Para)

The SSC actuation can be provided both manually and automatically. The operator has the capability to provide manual actuation at any time, but does not have the capability to defeat the automatic actuation (excluding resets and operating bypasses, such as the block low-pressure safety injection to allow plant cooldown without initiating safety injection).

The majority of the AP600 safety-related automatic actuation functions are in this category, such as the CMTs and ADS. It is required that the SSCs have the capacity to automatically actuate by plant technical specifications.

Selectable (Sel)

The SSC actuation can be provided both manually and automatically. The operator has the capability to select the mode of actuation, which can defeat automatic actuation.

The majority of the AP600 nonsafety-related, defense-in-depth automatic actuation functions are in this category, such as the startup feedwater or CVS makeup pumps. The automatic actuation can be defeated, for example, if a component malfunction occurs and repairs are being performed.

Complementary (Comp)

The SSC actuation can be provided both manually and automatically. There is sharing of actuation responsibilities between the operator and the I&C systems or the passive SSCs. While there may be some functional overlap, there is not complete redundancy.

This actuation scheme exists because the operator has a continuous manual interface that affects the actuation setpoint for the component. For example, the CVS and steam dumps have control setpoints for some operating modes that affect the actuation of the appropriate SSCs.

An example is the actuation of steam dumps in the "steam pressure" operating mode. The operator manually selects the desired steam generator pressure set point and the steam dumps actuate open and closed (and also modulate) as necessary to maintain the established set point, based on the reactor core decay heat rate. The operator has enabled automatic control (and established the specific operating condition) and can defeat automatic operation if desired for any reason.

Manual (Man) *The SSC actuation is completely manual, without a means for automatic actuation. (For this type of control scheme, there are no entries in the automatic column in the table.)*

The discussion in subsection 3.1.1 provides additional information related to manual actions to override automatic actuation and control signals by terminating safeguards actuation signals as part of the plant recovery following an event.

SSC Control Functions

Table 4 includes two columns to describe the SSC control. The first column is used to indicate when the SSC is automatically controlled and the entry in this column describes the type of control capabilities for that SSC. The second column is used to indicate when the SSC is manually controlled. If there are no automatic control capabilities for an SSC, then there will be no entries in the automatic column.

Most of the AP600 SSCs are controlled by the same plant I&C systems that provide the actuation functions, the safety-related PMS or the nonsafety-related PLS. (The other SSCs are controlled by passive processes.) The I&C systems provide a manual control capability for SSCs that can be automatically controlled, similar to the manual backup for the automatic actuation functions. This capability allows the operator to perform manual control of success path SSC functions when necessary and to provide a backup in the event that the automatic control function fails to properly control an SSC.

The following control capabilities exist for the AP600:

Passive (Pass) *The SSC accomplishes safety function(s) through naturally inherent passive control processes (such as ~~doppler~~ reactivity feedback, natural circulation flow, passive heat removal and injection, or mechanical overpressure relief protection) that are independent of both I&C system action and operator action.*

Accumulator injection flow is controlled passively by the pressure differential between the accumulator and the RCS.

Automatic (Auto) *The SSC control function is completely automatic, without a means for manual actuation to execute the basic function.*

There are no AP600 control functions in this category.

Parallel (Para) *The SSC control can be provided both manually and automatically. The operator has the capability to provide manual input into the control function at any time, but does not have the capability to defeat the automatic control function.*

There are no AP600 control functions in this category.

Selectable (Sel) *The SSC control can be provided both manually and automatically. The operator has the capability to select the mode of control, which can defeat automatic control.*

All of the AP600 control functions provided by the I&C systems are in this category. (The only AP600 plant control functions that are not in this category are those controlled by passive processes that are identified in Table 4.)

Complementary (Comp) *The SSC control can be provided both manually and automatically. There is sharing of control responsibilities between the operator and the I&C systems or the passive SSCs. While there may be some functional overlap, there is not complete redundancy.*

This control scheme exists because the operator has a continuous manual interface that affects the control setpoint for the component. For example, the CVS and steam dumps have control setpoints for some operating modes that affect the continuous operation of the appropriate SSCs.

An example is the reactivity control success path where the CVS provides boration for the RCS. The operator must input specified boron concentration, flow rate, and volume parameter values to the control system and then manually actuate the boration process. The CVS then automatically controls the system operation to supply the specified volume and concentration at the specified flow rate.

Manual (Man) *The SSC actuation is completely manual, without a means for automatic control of the SSC. (For this case, there are no entries in the automatic column.)*

The discussion in subsection 3.1.1 provides addition information related to manual actions to override automatic actuation and control signals by terminating safeguards actuation signals as part of the plant recovery following an event.

3.3 AP600 Function Allocation Basis (Table 5)

Table 5 identifies the basis for the function allocations for the AP600 SSCs in the CSF success paths. The table lists the SSCs for the AP600 success paths for each CSF (the same list as provided in Table 3) and provides a cross-reference to the detailed success path function allocation and description provided in Table 4.

Table 5 identifies the specific function allocation basis for each AP600 success path. The development of the specific function allocation basis is described in subsection 3.1.2 and the resulting function allocation basis codes that are specifically applicable to the AP600 are identified at the end of the subsection. These allocation basis codes are also listed at the end of Table 5.

For comparison, Table 5 indicates whether the equivalent or identical function is automated for the reference plant and also provides comments related to the function allocation basis.

3.4 Results

Table 4 provides an overview of the success path allocations, that includes summaries of the integrated actuation and control functions for the SSCs in each success path. The success paths for each CSF are listed in the sequence that is expected to be followed by the operator during an event. The comments for each success path help to explain the overall operation of the components in the success path and identify the protection basis for each path. Table 4 identifies the specific actuation and control scheme for each of the SSCs.

Table 5, which provides the basis for the function allocation for the SSCs in each CSF success path, shows that the basis for the majority of the function allocations can be grouped into several important categories:

- The safety-related, passive SSCs are required to be automated by regulatory or utility requirements.
- Many of the nonsafety-related, defense-in-depth systems must be automated by default since they are designed to actuate before the safety-related, passive systems (that must be automated) to prevent unnecessary actuation of the passive SSCs.
- Design improvements have resulted in automation of some SSC actuation and control functions to help reduce operator workload during critical periods following an event or to improve plant safety.
- A number of SSCs can be manually actuated because they serve defense-in-depth functions where there are significant layers of defense-in-depth SSCs that must fail

before those SSCs are needed and where there is significant time for the SSC to be manually actuated, when compared to the reference plant.

- Many of the nonsafety-related SSCs that perform equivalent functions to those for the reference plant are equivalently automated, except where design improvements in the automatic functions were implemented based on plant experience or human factors considerations.

4.0 HUMAN FACTORS CONSIDERATIONS IN FUNCTION ALLOCATION

Human factors considerations in function allocation are incorporated in the design process at several points. Initial allocation, while largely constrained by external requirements and design goals, takes into account the strengths and limitations of human operators and automated systems. The adequacy of the allocation is further evaluated throughout the AP600 design process. FBTAs are used to verify that the sensors and controls that are provided are sufficient to enable operators to perform the role assigned to them in system performance. Workload analyses are used to evaluate the adequacy of the integrated role assigned to operators across systems. Final integrated system validation is used to establish the adequacy of the function allocation using man-in-the-loop tests in dynamic simulated plant conditions. This section provides a detailed description of the processes, employed as part of the AP600 M-MIS design process, that address human factors concerns related to function allocation during all phases of the design.

4.1 Human Factors Input Early in the Design Process

Figure 1 captures the decision process that was used by system designers to make initial allocations (see subsection 3.1 for a description of the use of this diagram). As shown in Figure 1, there is an explicit consideration of limitations in human capabilities in the following ways:

1. Tasks are not assigned to human operators when it is known that they will be unable to perform with sufficient speed to accomplish critical safety actions in a timely fashion.
2. Tasks are not assigned to human operators when they are complex or not routinely performed and the likelihood of error is great, or when there is likely to be an overwhelming workload due to the initiation of a transient.
3. Tasks are not assigned to human operators when operating experience indicates that human capabilities are inadequate to execute tasks with sufficient skill.
4. Tasks are not assigned to human operators when a PRA analysis indicates that human error probabilities are too high for safe operation.
5. Tasks are not assigned to human operators when activities are not well-suited to human strengths; for example, the activities require sustained vigilance.
6. Design improvements have resulted in modifying AP600 tasks to reduce the likelihood of situations that present conflicting goals to the operator (such as some

post-accident conditions in current plants where human operators are required to throttle safety systems to prevent RCS overfill).

These allocation decisions were based on operating experience reviews and PRA and Human Reliability Analysis (HRA) analyses that allowed early tests of proposed roles for the operator. Further, the design of automated systems uses a set of guiding principles for establishing appropriate roles for human operators. For example, human operators are provided information to support supervisory monitoring, to ensure the process is achieving its goals, and to provide the possibility for manual intervention, when the automated process fails to achieve its goals.

4.2 Human Factors Evaluation of the Integrated Role of the Operator

Initial function allocation results and rationale focus primarily on the responsibilities of an operator with respect to an individual function, system, or process. However, in an operational setting, operators have responsibilities across multiple systems. As a result, in defining and evaluating the role of the operator, one must consider the total integration across plant functions and systems of the operator's responsibility. In this section the human factors activities are discussed that are performed as part of the M-MIS design process and that are intended to verify the adequacy of function allocation and to create an M-MIS that supports the integrated role of the operator across plant functions and systems.

These issues will be addressed as part of task analyses, workload analyses, M-MIS design, and verification and validation activities.

The AP600 Task Analysis Implementation Plan describes two types of task analyses that will be conducted in support of M-MIS design. One type of task analysis is referred to as a "FBTA". The objective of the FBTA is to determine the process plant data needed to support operators in monitoring and controlling the plant to achieve primary plant safety and energy production goals.

The FBTA involves superimposing a set of questions derived from an operator decision-making model onto the nodes of a function decomposition goal-means structure to define the plant process data and controls that are necessary to support operator performance. The answers to these questions serve as a specification of the plant parameter information and controls that need to be presented to operators to support monitoring, situation awareness, planning, and control activities.

This information and control requirements for supervisory monitoring and control of automated systems, must include the safety-related, passive SSCs and provide the information necessary to determine the following:

- Availability of automated systems and initiation criteria (i.e., are the systems available and when will they come on?)
- Performance of automated systems (i.e., are they performing correctly?)
- The need for manual backup, manual intervention, or manual override (i.e., is manual intervention required to initiate, throttle, or terminate an automated system?)

The output of the FBTA provides a completeness check on the availability of needed indications, parameters, and controls. It provides a verification of the adequacy of the I&C available to support the operator's role in function achievement.

A second type of task analysis that will be conducted as part of task analyses is the operational sequence analysis (OSA). The OSA is one of the primary tools for verifying the adequacy of the integrated role of the operator. The OSA will be conducted on a representative set of operational tasks. The tasks will be selected to represent the full range of operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions. As part of the OSA, workload analyses will be conducted on a subset of operational tasks (OSA-2).

The OSA, and in particular the workload analyses, will provide verification that the operational tasks assigned to operators that are integrated over multiple plant functions and systems, are within the operator's capability, and can be accomplished without too high or too low of a workload. The OSA will take into account control room staffing assumptions. If it is determined that the workload is too high or too low, options include making changes in staffing assumptions, or modifying the person automated system allocation.

The final integrated system validation that will be conducted in an AP600-specific training simulator will provide a final check on the adequacy of the function allocation. The integrated system validation to be performed by Westinghouse is described in the M-MIS verification and validation implementation plan.

In the design and evaluation of the control room M-MIS for the AP600, particular attention will be paid to the need to support the operator's role as supervisory controller and system monitor of automated systems, including the following considerations:

- Situation awareness, including awareness of status and operation of the automated systems (i.e., ability to detect and understand changes in automated system performance)
- Ability to detect degradation in automated system performance and establishing manual control
- Ability to make smooth transition from use of nonsafety-related SSCs to safety-related SSCs
- Monitoring and supervisory control of passive systems (including decisions and actions to mitigate events before necessitating a transition to actuation of safety-related, passive SSCs)
- Moderate operator workload and workload transitions
- Operator vigilance and the need to keep the operator involved and knowledgeable of the plant status

4.3 Mechanisms for Modifying Function Allocations Based on Analysis Results

Section 4.2 described the human factors activities that are conducted as part of the M-MIS development process to evaluate the adequacy of function allocations. These activities address the ability of operators to perform the role assigned to them, the adequacy of the information and controls provided to support task performance, and the resulting workload. If at any point, deficiencies such as lack of necessary sensors or controls to support operator performance or excessive workload are identified, then action will be taken to remediate the problem. Options available include the following:

- Changing the M-MIS (e.g., integrating available sensor information to create "synthetic" values that provide information at the level the operator requires it and reduces the operator workload associated with data gathering and integration)
- Changing system designs (e.g., to provide new sensors or to alter manual-automation system allocation assumptions)
- Changing staffing assumptions

The preferred option, whenever possible, is to make changes to the M-MIS. If a problem in function allocation is identified that cannot be dealt with through changes in the M-MIS, then it may be possible to make changes to system designs and function allocations. Finally, if the problem cannot be dealt with either through changes in the M-MIS or changes in the system designs and function allocations, then it may be possible to consider changes in the plant staffing assumptions. For example, while the design goal is to have plant operations controlled by a single operator, it may be determined that under certain plant conditions (such as plant startup, shutdown, or emergency conditions) additional staffing will be needed.

The AP600 design process includes a formal design configuration change control process that is used to control and implement changes to the plant design. It is used when the design to be changed has been previously released in a document for use and placed under configuration control. A design change proposal is the vehicle used to initiate and document review of proposed design changes. Design change proposals include identification of impacts of the proposed design change from affected functional groups. Design change proposals are maintained in a data base that is used to track the status of each design change proposal from initiation through implementation and closure. A description of the Systems Engineering Procedures for the AP600, including the design configuration change control process, is provided in WCAP-12601, AP600 Simplified Passive Advanced Light Water Reactor Plant Program, Program Operating Procedures (Ref. 19).

5.0 CONCLUSIONS

This report provides the AP600 functional requirements analysis and function allocation process for the CSFs that must be accomplished during design basis and beyond-design-basis events. The analysis is based on comparisons with the generic Westinghouse PWR design used for current plants that provide an extensive experience base of successful operating histories that form a valid reference point from which to evaluate the design changes and improvements provided in the AP600 design. The conclusions of this evaluation include the following:

1. The AP600 CSFs are the same as those used for current Westinghouse plants and satisfy the similar design basis requirements for both the AP600 and the reference plant designs.
2. The critical success paths and the function allocations for the safety-related and nonsafety-related SSCs are similar in the AP600 and the reference design.
 - The addition of safety-related, passive SSCs provides some new success paths and resulting function allocations that perform equivalent safety functions to the corresponding SSCs in the reference plant.
 - Where necessary, there have also been some changes to the traditional SSCs success path functions and allocations due to the following reasons:
 - Specific changes that provide improvements in the SSC design or operation based on operational experience
 - Consequential changes in the SSC design or operation as a result of other improvements in the AP600 design
3. The AP600 meets the safety-related requirements for function allocation. No additional allocation concerns have been identified.
4. The AP600 provides improvements through revised allocations in areas of known concern to operator performance.
5. The evaluation of the interaction between the human and machine elements of the plant actuation and control systems, and the resolution of specific problems identified, will continue as part of the FBTA, PRA, verification and validation, and procedure development activities.

6. This report satisfies the complete review level requirements for Element 3 of the AP600 HFE Program Plan (Ref. 20) and the HFE Program Review Model for the AP600 design certification (Ref. 1), and the requirements of NUREG/CR 3331 (Ref.5).

6.0 REFERENCES

1. NUREG-0711, "Human Factors Engineering Program Review Model," U. S. Nuclear Regulatory Commission, Washington, D.C., July, 1994.
2. EPRI Advanced Light Water Reactor Utility Requirements Document, Electrical Power Research Institute, Rev. 6, 1993.
3. IAEA-TECDOC-668. The Role of Automation and Humans in Nuclear Power Plants, 1992 (International Atomic Energy Agency - International Working Group on NPP Control and Instrumentation).
4. IEC 964. Design for Control Rooms of Nuclear Power Plants, 1989 (International Electrochemical Commission).
5. Pulliam, R., Prince, H.E., Bongarra, J., Sawyer, C.R., and Kisner, R.A. (1983). *A methodology for allocating nuclear power plant control functions to human and automatic control*. NUREG/CR 3331. Washington, DC: Nuclear Regulatory Commission.
6. AP600 Emergency Response Guidelines, Rev. 2 April 1996.
7. AP600 Emergency Response Guidelines Background Document, Rev. 1A, August 1996.
8. AP600 Probabilistic Risk Assessment, Rev. 6, November 1995.
9. WCAP-13913, Framework for AP600 Severe Accident Management Guidance.
10. WCAP-14477, The AP600 Adverse Systems Interactions Evaluation Report, February 1996
11. WCAP-13793, AP600 System/Event Matrix, June 1994.
12. AP600 Standard Safety Analysis Report.
13. WCAP-13856, AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process Summary Report, Rev. 0, Sept 1993.
14. AP600 Shutdown Evaluation Report.
15. Fitts, P.M. (1951). *Human engineering for an effective air navigation and traffic control system*. Washington, DC: National Research Council.

16. Unresolved Safety Issue B-17, Criteria for Safety-Related Operator Actions, NUREG 0933.
17. ANSI/ANS 58.8-1984, Time Response Design Criteria for Nuclear Safety-Related Operator Actions.
18. Regulatory Guide 1.97, Revision 3, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs During and Following an Accident, 5/83.
19. WCAP-12601, AP600 Simplified Passive Advanced Light Water Reactor Plant Program, Program Operating Procedures.
20. AP600 Standard Safety Analysis Report, Chapter 18, HFE Program Plan.
21. WCAP-13054, AP600 Compliance with SRP Acceptance Criteria (GW GL 001 Rev.0), January 1993.
22. WCAP-13559, Operational Assessment for AP600 (GW GLR 001), December 15, 1992.
23. Human Factors Evaluation and Allocation of System 80+ Functions, NPX80-IC-RR790-02, Revision 01, March 15, 1993, ABB Combustion Engineering, Inc., Windsor, CT.
24. Letter from W. C. Huffman (NRC) to N. J. Liparulo (Westinghouse), Nuclear Regulatory Commission (NRC) Response to AP600 Open Item and Related Follow on Questions, May 15, 1995.

TABLE 1 (Subsection 2.1.1)
WESTINGHOUSE ERG CRITICAL SAFETY FUNCTIONS

ERG Critical Safety Functions	Equivalent Safety Functions from WCAP-13793	Purpose	Primary Parameters Monitored by the ERGs to Confirm Critical Safety Function Status
1. Subcriticality	Reactor Shutdown	Control core reactivity to limit the heat generated by the reactor core to only core decay heat	Core reactivity as monitored by excore nuclear instrumentation
2. Core Cooling	Core Decay Heat Removal and RCS Inventory	Provide adequate RCS inventory to remove core decay heat, preventing core heatup due to inadequate core cooling, and assuring that core integrity will be maintained.	Core exit temperatures as monitored by core exit thermocouples
3. Heat Sink	Core Decay Heat Removal	Provide a heat sink for heat removal from the RCS either to containment (through either the PRHR heat exchangers or a feed and bleed process) or to the plant heat sink (through the steam generators)	Passive residual heat exchanger operation and steam generator level, feedwater flow, and pressure
4. Integrity	Core Decay Heat Removal and RCS Inventory	Mitigate the effects of events (excessive RCS cooldown or overpressurization) that can challenge reactor vessel integrity due to pressurized thermal shock or cold overpressure	RCS temperature and pressure conditions
5. Containment	Containment Cooling	Maintain containment integrity to prevent the release of radioactivity following an event	Containment conditions including pressure, floodup water level, and radiation levels
6. Inventory	Reactor Coolant System Inventory	Maintain RCS inventory and prevent reactor vessel void formation following an event	RCS pressurizer level

NOTES for TABLE 2

- ¹ A list of abbreviations is provided at the beginning of this document.
- ² The reactor is shut down by negative moderator temperature coefficient (MTC) as the coolant heats up. This capability requires automatic RCS pressure relief, turbine trip, and heat removal (auxiliary feedwater or PRHR actuation). AP600 which has a more negative MTC, includes a DAS, similar ATWS functions as ATWS Mitigation System Actuation Circuitry (AMSAC), has main feedwater, startup feedwater, and PRHR systems, and CMTs and CVS for boration.
- ³ The SSCs identified in the CSF Integrity are treated somewhat differently, from the perspective of actuation, control, and operator actions, than the SSCs for other CSFs. The CSFs other than Integrity are generally successful when the SSCs actuate and perform their specified functions. For example, core cooling is successful when the PRHR heat exchanger (HX) and other safety-related and nonsafety-related SSCs that provide core cooling actuate. The CSF restoration guidelines generally direct the operators to confirm satisfactory operation of the required SSCs or to take actions to initiate operation of required SSCs that have failed to start.

Similarly, the CSF Integrity is generally satisfied when the identified SSCs in the success path successfully actuate and are successfully controlled during their operation. However, challenges to Integrity occur when the required SSCs either actuate incorrectly when not required or when they actuate successfully and a control malfunction occurs. The AP600 design provides safety-related design basis protection, but beyond-design-basis malfunctions of the actuation or control functions for the identified SSCs in the success paths cause either overcooling (such as excessive steam flow through the turbine bypass valves) or overpressurization (excessive RCS makeup flow from the CVS makeup pumps).

Therefore, to mitigate the consequences of these failures, most of the actions in the function restoration guidelines for Integrity direct the operator to respond in an opposite fashion from that of the other CSFs; to identify the malfunctioning SSC(s) that are operating in an unacceptable manner and to manually control or isolate the SSC, as appropriate.

**TABLE 2 (Subsection 2.1.2)
SUCCESS PATHS¹**

Critical Safety Functions	Safety-Related		Nonsafety-Related	
	AP600	Reference Plant	AP600	Reference Plant
1. Subcriticality	<ul style="list-style-type: none"> - Reactor trip (PMS via trip breakers) - CMT boration 	<ul style="list-style-type: none"> - Reactor trip (Solid State Protection System SSPS via trip breakers) - High head safety injection 	<ul style="list-style-type: none"> - Reactor trip (DAS via motor generator (MG) set) - Ride out (PRHR actuation and turbine trip from DAS)² - Control rod insertion - CVS boration 	<ul style="list-style-type: none"> - Ride out (Auxiliary Feedwater System (AFW) actuation and turbine trip from AMSAC)² - Control rod insertion - CVS boration
2. Core Cooling	<ul style="list-style-type: none"> - PRHR - Automatic RCS feed and bleed (CMT / accum / IRWST / recirculation ADS) - Manual RCS feed and bleed (accum / IRWST / recirculation / ADS) - Refueling cavity inventory (refueling) 	<ul style="list-style-type: none"> - Auxiliary feedwater - RHR closed loop cooling (shutdown) - Refueling cavity inventory (refueling) 	<ul style="list-style-type: none"> - Main feedwater - Startup feedwater - Manual RCS feed and bleed (CMT / accum / RNS injection / IRWST / recirculation / partial ADS) - RNS closed loop cooling (shutdown) - Spent fuel pool cooling system (SFS) refueling cavity cooling (refueling) 	<ul style="list-style-type: none"> - Main feedwater - Manual RCS feed and bleed (pressurizer power-operated relief valve (PORV) / high head SI pump)

TABLE 2
SUCCESS PATHS (Cont.)

Critical Safety Functions	Safety-Related		Nonsafety-Related	
	AP600	Reference Plant	AP600	Reference Plant
3. Heat Sink	<ul style="list-style-type: none"> - PCS drain / air cooling - Air cooling w/o PCS drain 	<ul style="list-style-type: none"> - SG safety valves - Component cooling water system (CCS) / essential service water / cooling tower fans (shutdown) 	<ul style="list-style-type: none"> - Steam dumps / circ water - SG PORVs - SG safety valves - RNS closed-loop cooling of IRWST - Fan coolers / chilled water / CCS / service water / cooling tower fans - Fire protection drain / air cooling - CCS / service water / cooling tower fan (shutdown) 	<ul style="list-style-type: none"> - Steam dumps / circ water - SG PORVs - CCS / service water / cooling tower
4. Integrity ³	<ul style="list-style-type: none"> - PRHR isolation - Steam generator (SG) PORV and block valve closure - Steam dump closure - Main steamline isolation valve (MSIV) and bypass closure - CMT isolation - Accum isolation - ADS - Reactor vessel (RV) head vent 	<ul style="list-style-type: none"> - Auxiliary feedwater control / SG PORV closure - SG PORV and block valve closure - Steam dump closure - MSIV and bypass valve closure - High head safety injection isolation - Accum isolation - RHR cooling control - RV head vent 	<ul style="list-style-type: none"> - SG PORV control - Steam dumps control - Main feedwater control - Startup feedwater control - RNS cooling control - CVS makeup / letdown control - Pressurizer heaters / spray - Pressurizer auxiliary spray 	<ul style="list-style-type: none"> - Steam dumps control - Main feedwater control - CVS makeup / letdown control - Pressurizer heaters / spray - Pressurizer auxiliary spray

TABLE 2
SUCCESS PATHS (Cont.)

Critical Safety Functions	Safety-Related		Nonsafety-Related	
	AP600	Reference Plant	AP600	Reference Plant
5. Containment	Containment Heat Removal - PCS drain - PCS drain w/o air flow - Air cooling w/o drain Containment Isolation - Isolation valves (1 inside reactor containment (IRC) / 1 outside reactor containment (ORC)) - Containment can be open (shutdown) LOCA Outside Containment - RNS (3 barriers)	Containment Heat Removal - Fan Coolers - Containment spray Containment Isolation - Isolation valves (1 IRC / 1 ORC) LOCA Outside Containment - RHR (2 barriers)	Containment Heat Removal - Fan coolers - Fire protection drain - Fire protection drain w/o air cooling LOCA Outside Containment - Higher RNS design pressure (no rupture)	

TABLE 2
SUCCESS PATHS (Cont.)

Critical Safety Functions	Safety-Related		Nonsafety-Related	
	AP600	Reference Plant	AP600	Reference Plant
6. Inventory	High-Pressure Injection - CMT injection - Accum and IRWST injection / ADS Low-Pressure Injection - Accum / ADS - IRWST / ADS Long-Term Recirculation - Containment recirculation / ADS Refueling - Refueling cavity inventory	High-Pressure Injection - High head safety injection Low-Pressure Injection - Accum injection - Low head safety injection Long-Term Recirculation - Low head safety injection (supplying high head safety injection pumps) Refueling - Refueling cavity inventory - SFS makeup	High-Pressure Injection - CVS makeup pumps - Accum / RNS injection / partial ADS Low-Pressure Injection - RNS injection / IRWST / partial ADS Long-Term Recirculation - RNS recirculation / partial ADS - Containment makeup Refueling - SFS makeup	High-Pressure Injection - CVS makeup pumps

NOTES for TABLE 3

¹ The definitions for each column are as follows:

Unchanged	<i>This category is selected for an AP600 success path where there are no operationally significant changes in either the SSC design or function allocation from the equivalent success path in current plants.</i>
Modified	<i>This category is selected for an AP600 success path where either the SSC design or its function allocation may be similar to the success path operation in typical Westinghouse PWRs, but where there are also some significant operational differences that must be considered for the functional requirements analysis.</i>
New	<i>This category is selected for an AP600 success path that may have a functional equivalent in current plants, but where a new system design feature is employed to perform specific functions in mitigating the consequences of an event. For example, the CMTs employ passive processes to provide high pressure injection that is provided by high head safety injection pumps in current plants.</i>

As discussed in subsection 2.1.3, two aspects are considered in determining whether an AP600 success path is unchanged, modified, or new. The first aspect relates to the overall system design configuration or system arrangement. This is represented in Table 3 by the letter "D" for "design."

The second aspect relates to whether there are any differences in person-machine function allocation. The set of SSCs associated with an AP600 success path may be the same as for the generic Westinghouse PWR reference plant but there may be changes in the level of automation. This second aspect of the comparison between the AP600 success paths and the corresponding success paths for the reference plant is represented in Table 3 by the letter "A" for "allocation."

The notes in the last column of Table 3 provide a brief summary description where there are differences between the AP600 and reference plant for the SSCs in the various success paths.

The abbreviations "SR" indicates "safety-related" SSCs and "NSR" indicates "nonsafety-related" SSCs. A list of abbreviations is provided at the beginning of this document.

² Referenced "Items" refer to other entries in this table.

**TABLE 3 (Subsection 2.1.3)
SUCCESS PATH DIFFERENCES**

Critical Safety Function	Unchanged ¹	Modified ¹	New ¹	Notes ²
1. Subcriticality				
1.a Reactor trip (PMS)	A	D		The SR reactor trip functions are equivalent to those on the reference plant, but they are provided by the protection and safety monitoring system with a design architecture based on advanced, digital instrumentation and control hardware and software that is different from the solid state protection system design in the reference plant. The digital instrumentation and control architecture has been licensed to provide process control reactor trip inputs to the SSPS in the reference plant.
1.b Reactor trip (DAS)		D	A	<p>The NSR DAS provides a diverse, automatic, and manual trip capability that was added based on the AP600 PRA evaluation recommendations.</p> <p>DAS provides actuation functions provided by I&C system hardware and architecture that is diverse from the PMS and PLS designs to protect against common-cause malfunctions.</p> <p>Although the DAS trip function is a new function, it is fundamentally an extension of the original <u>W</u> AMSAC actuation capabilities for ATWS mitigation (only AFW actuation and turbine trip) and is performed using an improved system design.</p> <p>(Additional automatic and manual functions beyond these three basic AP600 ATWS functions were added to this system, based on PRA recommendations.)</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
1.c Control rod insertion (rod control system)	A	D		<p>The NSR rod control system performs equivalent functions to the same system on the reference plant, but the AP600 architecture now uses advanced, digital instrumentation and control hardware and software that is different from those in the reference plant. The digital I&C architecture has been licensed to provide process control applications in the reference plant.</p> <p>Some of the types of power generation and distribution components, such as the motor-generator sets and the electrical breakers, are used for both the AP600 and the reference plant.</p>
1.d Rideout	A	D		<p>Rideout is a design capability of the plant, given that the operator is unable to initiate a reactor trip, but that turbine trip and heat removal have been actuated. The automatic actuation is performed by the AMSAC in the reference plant.</p> <p>The automatic actuation of these two functions is unchanged from the reference plant, but the DAS design is new, as discussed in Item 1.b, and the PRHR now performs the heat removal function performed by the AFW in the reference plant.</p>
1.e CVS boration	A	D		See Item 6.a.
1.f CMT boration			D, A	This is one of the SR passive design features that provides an equivalent boration function to that provided by the high head safety injection pumps in the reference plant.

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
2. Core Cooling				
2.a Main feedwater	D, A			
2.b Startup feedwater	D	A		<p>This system has an unchanged design and is functionally similar to the AFW system in the reference plant, but has been enhanced by providing automatic SG level control instead of manual control as on the reference plant.</p> <p>Therefore, the AP600 does not require post-event operator action to throttle back feedwater flow to prevent SG overfill and/or RCS overcooling, as required on the reference plant AFW system.</p> <p>This NSR design feature can also support the heat removal function, in conjunction with SG venting via the SG safety valves, steam dumps, or SG PORVs in Items 3.a and 3.b.</p>
2.c PRHR			D, A	<p>This is one of the SR passive design features that provides an equivalent heat removal function to that provided by the SR AFW and SG safety valves in the reference plant.</p> <p>This SR design feature provides design basis heat removal, in conjunction with heat sink support in Items 3.d to 3.i.</p>
2.d CMT injection			D, A	<p>This is one of the SR passive design features that provides an equivalent high-pressure safety injection function to that provided by the high head safety injection pumps in the reference plant.</p> <p>This SR design feature provides a defense-in-depth heat removal function, in conjunction with ADS venting.</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
2.e Accumulator injection	D,A			<p>This is one of the SR passive design features that provide intermediate pressure safety injection and is identical to the accumulators used in the reference plant.</p> <p>This SR design feature provides a defense-in-depth heat removal function, in conjunction with ADS venting.</p>
2.f IRWST heat removal and injection			D, A	<p>This is one of the SR passive design features that provides an equivalent post-depressurization safety injection function to that provided by the low head safety injection pumps in the reference plant.</p> <p>This SR design feature provides a defense-in-depth heat removal function, in conjunction with ADS venting.</p>
2.g Recirculation			D, A	<p>This is one of the SR passive design features that provides an equivalent post-depressurization safety recirculation function (after the IRWST empties) to that provided by the low head safety recirculation arrangement in the reference plant.</p> <p>This SR design feature provides a defense-in-depth heat removal function, in conjunction with ADS venting.</p>
2.h ADS			D, A	<p>This is one of the SR passive design features that provides an RCS depressurization (venting) function to provide the transition between the various passive injection sources. Only a manual depressurization capability (using pressurizer PORVs) is provided in the reference plant.</p> <p>This SR design feature provides a defense-in-depth heat removal function, in conjunction with the various passive and active injection sources.</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
2.i RNS injection	D	A		<p>The design of the RNS is essentially the same as the SR RHR system in current plants, except that the AP600 RNS is an NSR, defense-in-depth system that is not automatically actuated following an event.</p> <p>The RNS provides an NSR, defense-in-depth injection capability that must be manually aligned and actuated following an event, in conjunction with Items 3.f and 3.g. The SR RHR system in the reference plant provides the automatically actuated, design basis low-pressure safety injection capability.</p> <p>This NSR design feature provides a defense-in-depth heat removal function, in conjunction with ADS venting.</p>
2.j RNS closed loop cooling (shutdown)	D, A			
2.k SFS cooling of refueling cavity (refueling)	D, A			
2.l Refueling cavity cooling (refueling)	D, A			
3. Heat Sink				
3.a Steam dumps	D, A			<p>This NSR design feature provides the same defense-in-depth, heat sink function, in conjunction with main or startup feedwater to the SGs in Items 2.a and 2.b, as provided in the reference plant.</p> <p>This NSR design feature provides a heat sink function in conjunction with the operation of circulating water in Item 3.b.</p>
3.b Circulating water	D, A			<p>This NSR design feature provides the same defense-in-depth, heat sink function in conjunction with the operation of steam dumps in Item 3.a, as provided in the reference plant.</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
3.c SG PORVS	D, A			<p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with main or startup feedwater to the SGs in Items 2.a and 2.b.</p> <p>This component was also NSR (to open) in the reference plant, providing the NSR defense-in-depth heat sink function.</p>
3.d Fan coolers	D	A		<p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with cooling water support in Items 3.e to 3.h. The fan coolers do not automatically actuate on a safety injection signal as they do in the reference plant since they provide NSR defense-in-depth functions.</p> <p>This component was SR in the reference plant and provided the SR design basis heat removal function.</p>
3.e Chilled water	D, A			<p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with cooling water support in Items 3.f to 3.h.</p> <p>This component was SR in the reference plant and provided the SR design basis heat removal function.</p>
3.f Component cooling water	D, A			<p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with cooling water support in Items 3.g and 3.h.</p> <p>This component was SR in the reference plant and provided the SR design basis heat removal function.</p>
3.g Service water	D, A			<p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with heat sink support in Item 3.h.</p> <p>This component was SR in the reference plant and provided the SR design basis heat removal function.</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
3.h Service water cooling tower and fan	D, A			<p>This NSR design feature provides a defense-in-depth, heat sink function.</p> <p>This component was SR in the reference plant and provided the SR design basis heat removal function.</p>
3.i SG safety valves	D, A			
3.j RNS closed-loop cooling of the IRWST / PRHR	D, A			<p>This NSR RNS can be used to remove heat from the IRWST. The manually actuated, closed-loop cooling of the IRWST is not operationally significant from the normal operation of RHR in the reference plant to support closed-loop RCS cooling (except that a different volume of water is being cooled).</p>
3.k PCS water drain			D, A	<p>This is one of the SR passive design features that provides an equivalent containment heat sink function to that provided by the fan cooler and support heat sink success path in the reference plant.</p> <p>The SR design feature functions in conjunction with Item 3.l to provide SR design basis protection.</p>
3.l Containment air cooling (external)			D, A	<p>This is one of the SR passive design features that provides an equivalent containment heat sink function to that provided by the fan cooler and support heat sink success path in the reference plant.</p> <p>The SR design feature functions in conjunction with Item 3.k to provide SR design basis protection. It can also function in conjunction with Item 3.m or alone to provide NSR defense-in-depth protection.</p>
3.m Fire protection water drain			D, A	<p>The NSR design feature functions in conjunction with Item 3.l to provide NSR defense-in-depth protection.</p>

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
4. Integrity				
4.a Steam dumps				See Item 3.a
4.b SG PORVs				See Item 3.c
4.c PRHR				See Item 2.c
4.d MSIVs and bypasses	D, A			
4.e Main feedwater				See Item 2.a
4.f Startup feedwater				See Item 2.b
4.g RNS				See Items 2.i and 2.j.
4.h Pressurizer heaters	D, A			
4.i Pressurizer spray	D, A			
4.j Pressurizer auxiliary spray	D, A			
4.k ADS				See Item 2.h
4.l CVS makeup				See Items 1.e and 6.a
4.m CMT injection				See Item 2.d
4.n Accum injection				See Item 2.e
4.o CVS letdown				See Item 2.e and 6.a
4.p RV head vent letdown	D, A			

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes¹
5. Containment				
5.a Fan coolers				See Item 3.d
5.b Chilled water				See Item 3.e
5.c Component cooling water				See Item 3.f
5.d Service water				See Item 3.g
5.e Service water cooling tower and fan				See Item 3.h
5.f PCS water drain				See Item 3.k
5.g Containment air cooling (external)				See Item 3.l
5.h Fire protection water drain				See Item 3.m

TABLE 3
SUCCESS PATH DIFFERENCES (Cont.)

Critical Safety Function	Unchanged	Modified	New	Notes ¹
6. Inventory				
6.a CVS injection		D, A		<p>The CVS performs equivalent functions to the CVS on the reference plant, but the AP600 CVS makeup and letdown are not required to continuously operate for two reasons. Canned rotor RCPs are installed that eliminated the seal and associated continuous seal leakage in the reference plant design. Also, the AP600 purification subsystem uses RCP differential pressure to drive purification flow, which is different from the reference plant. RCS makeup is automatically actuated, but boration must be manually actuated. See Item 1.e for additional CVS information.</p> <p>Although many of the operational features of the CVS are similar to the reference plant, some additional automatic actuation functions were added or changed as a result of these design differences.</p>
6.b CMT				See Item 2.d
6.c Accumulator				See Item 2.e
6.d IRWST				See Item 2.f
6.e Recirculation				See Item 2.g
6.f ADS				See Item 2.h
6.g RNS injection				See Item 2.i
6.h Containment makeup	A	D		This SR makeup water piping flowpath allows manual addition of water to containment for long-term cooling using transportable equipment and available water sources.
6.i SFS makeup (refueling)	D, A			

NOTES for TABLE 4

- ¹ The actuation, control, continuing operation, and operator monitoring of the various SSCs for the critical function success paths require operation of both I&C systems and electrical power systems. Following a loss of electrical power, the NSR emergency diesel-generators automatically start and load the appropriate front-line and support NSR defense-in-depth systems and also provide electrical power to both dc and UPS systems to provide power for actuation, control, and monitoring instrumentation. These SR and NSR SSCs are included in the following AP600 systems:

Instrumentation and Control Systems

SR Protection and Safety Monitoring System

NSR Plant Control System

NSR Diverse Actuation System

Electrical Power Systems

NSR Main ac Power System

NSR Onsite Standby Power System (includes the NSR emergency diesel-generators)

SR Class 1E dc and UPS System

NSR Non Class 1E dc and UPS System

- ² Main feedwater is normally operating and does not automatically start, but automatically aligns to the startup feedwater discharge header. The startup feedwater flow control valves automatically throttle both main feedwater pump flow and startup feedwater pump flow in the startup feedwater supply header.
- ³ The RNS includes automatic temperature control of the inlet flow to the HX, but the operator manually controls the operating temperature for the automatic control circuitry.
- ⁴ Referenced "Items" refer to other entries in this table. A list of abbreviations is provided at the beginning of the document.
- ⁵ The actuation and control implementation schemes are discussed in subsection 3.2 and identified in this table. The appropriate codes are listed under the "actuation" and "control" columns. When automatic schemes exist with some type of manual actuation or control, "x" is included in the manual column to indicate the manual capability.
- If only manual control exists (and no automatic actuation or control function, as appropriate), then that scheme is indicated with "Man" in the actuation or control column instead of an "x."
- ⁶ Normally the operation of this component is passively controlled, but limited manual control is possible under certain special conditions. The first stage ADS valves are provided with the capability to be manually throttled, if an ADS actuation signal is not present. The PRHR discharge flow control valves are provided with the capability to be modulated, if a PRHR actuation signal is not present.

TABLE 4 (Subsection 3.2)
SUCCESS PATH SSC ALLOCATIONS

Critical Safety Function ¹	Actuation ⁵		Control ⁵		Comments ^{3,4}
	Auto	Man	Auto	Man	
1. Subcriticality					
1.a PMS reactor trip	Para	x			SR PMS actuates reactor trip breakers. These SSCs provide the SR design basis event response for reactor trip following all events.
1.b DAS reactor trip	Para	x			NSR DAS diversely de-energizes the MG set output. These SSCs provide NSR defense-in-depth event response for beyond-design-basis SR component failures.
1.c Control rod insertion (rod control system)		Man			NSR rod control circuits can be manually de-energized using remotely-operated motor control center (MCC) supply breakers from the main control room or manually-operated local MCC or rod control system MG set breakers. These SSCs provide NSR defense-in-depth event response for beyond-design-basis SR component failures.
1.d CVS boration		Man	Comp Comp	x x	NSR CVS makeup is normally aligned to automatically actuate and maintain programmed pressurizer level. CVS will automatically maintain the manually set boration parameters, but boration must be manually actuated for protection during events such as ATWS where pressurizer level is not expected to decrease. The boration process may also require manually initiating letdown to maintain RCS inventory. - Boron concentration These SSCs provide NSR defense-in-depth event response for beyond-design-basis SR component failures.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
1.e CMT boration	Para	x	Pass		<p>SR CMT injection / boration is automatically actuated. CMT injection passively controls the RCS boration flow by natural processes that depend on conditions such as the existing RCS inventory, flow, and voiding.</p> <p>These SSCs provide SR defense-in-depth event response for beyond-design-basis SR component failures.</p>
1.f Rideout	Para	x	Pass		<p>Rideout requires automatic or manual actuation of turbine trip and PRHR. NSR DAS automatically initiates diverse reactor trip and turbine trip, along with PRHR actuation. (Rideout capability is enhanced by both design (larger pressurizer, more negative MTC, RCS pressure relief) and defense-in-depth (startup feedwater / PRHR, CVS boration / CMT boration.)</p> <p>These SSCs provide SR and NSR defense-in-depth event response for beyond-design-basis SR and NSR component failures.</p>
2. Core Cooling					
2.a Main feedwater	Sel ²	x	Sel	x	<p>NSR main feedwater is manually aligned and actuated on plant startup, normally operates during power operation, and automatically aligns to the startup feedwater automatic flow control valves following a reactor trip, to provide heat removal. It is designed to actuate before the SR PRHR and provide heat removal.</p> <p>These SSCs provide the expected NSR defense-in-depth event response for non-LOCA events. This would be used in conjunction with Items 3.a (steam dumps) or 3.b (SG PORVs).</p>

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
2.b Startup feedwater	Sel	x	Sel	x	<p>NSR startup feedwater automatically starts and controls SG level following an event and automatically starts the standby pump if the operating pump fails. It is designed to actuate before the SR PRHR and provide heat removal.</p> <p>This system is enhanced by providing automatic SG level control (in addition to automatic actuation), which does not require operator action to throttle back feedwater flow to prevent SG overfill and/or RCS overcooling, as required on current plant AFW systems.</p> <p>These SSCs provide NSR defense-in-depth event response for non-LOCA events. This would be used in conjunction with Item 3.a (Steam dumps) or 3.b (SG PORVs).</p>
2.c PRHR	Para	x	Pass	x ⁶	<p>SR PRHR is automatically actuated and normally operates with discharge isolation valves fully open, with heat removal controlled by natural processes that depend upon conditions such as RCS decay heat and flow and the IRWST conditions. The HX discharge isolation valves can be manually throttled under certain conditions. Automatic actuation is designed to allow sufficient time for either main or startup feedwater to establish and maintain SG level control, if they are available.</p> <p>These SSCs provide the SR design basis event response for non-LOCA events.</p>

TABLE 4
SUCCESS PATH SSC ACTUATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
2.d CMT / Accum / RNS injection / IRWST / Recirculation / Partial ADS (Manual RCS feed and bleed operation)	Para	x	Pass		1. SR CMTs actuate automatically and control RCS inventory by natural processes that depend on conditions such as the existing RCS inventory, flow, and voiding.
	Pass		Pass		2. SR accumulators are automatically actuated by operation of the discharge check valves that open based on RCS pressure. Injection is also automatically controlled by natural processes that depend upon the same conditions such as RCS pressure.
		Man			3. NSR RNS must be manually aligned and actuated, but it requires no operator control to provide RCS injection from the SR IRWST or containment recirculation when the RCS is partially depressurized.
	Sel	x			- RNS suction is manually aligned to the IRWST / recirculation flowpath
	Para	x		Man	- Automatic restart of operating pump on loss of power - Automatic pump shutoff on high containment radiation - Manual control of pump combinations and flow throttling
	Para	x	Pass	x ⁶	4. Automatic SR ADS actuation based on CMT-level and manual system- and component-level ADS valve actuation. ADS vent flow is controlled by natural processes that depend on conditions such as RCS pressure and discharge backpressure.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
					These SSCs provide SR and NSR defense-in-depth event response for beyond-design-basis SR and NSR component failures. This event response sequence requires manual actions to initiate NSR RNS and maintain RCS inventory, thereby preventing significant steaming to containment and opening fourth-stage ADS valves, prior to automatic actuation of the backup SR design basis event response sequence in Item 2.e. Only partial ADS is required to decrease RCS pressure to within the pressure capability of the RNS.
2.e CMT / Accum /IRWST /Recirculation / Full ADS (Automatic and manual RCS feed and bleed operation)	Para	x	Pass		1. SR CMTs actuate automatically on low-pressurizer level or safety injection (SI) signal to automatically maintain RCS inventory w/o operator control.
	Pass		Pass		2. SR accumulators are automatically actuated by operation of the discharge check valves that open based on RCS pressure. Injection is also automatically controlled by natural processes that depend upon the same conditions such as RCS pressure.
	Para	x	Pass		3. SR IRWST injection automatically actuates and is controlled by the physical conditions within the RCS and containment.
	Para	x	Pass		4. SR containment recirculation automatically actuates and is controlled by the physical conditions within the RCS and containment.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
	Para	x	Pass	x ⁶	5 Automatic SR ADS actuation is based on CMT level. Manual system- and component-level ADS valve control is also available. ADS vent flow is controlled by natural processes that depend on conditions such as RCS pressure and discharge backpressure.
					These SSCs provide SR defense-in-depth event response for beyond-design-basis SR and NSR component failures.
2.f Accum / RNS Injection / IRWST / Recirculation / Partial ADS	Pass		Pass		1. SR accumulators are automatically actuated by operation of the discharge check valves that open based on RCS pressure. Injection is also automatically controlled by natural processes that depend upon the same conditions such as RCS pressure.
		Man			2. NSR RNS must be manually aligned and actuated, but it requires no operator control to provide RCS injection from the SR IRWST or containment recirculation when the RCS is partially depressurized.
		Man			- RNS suction is manually aligned to the IRWST / recirculation flowpath
	Sel	x			- Automatic restart of operating pump on loss-of-power
	Para	x			- Automatic pump shutoff on high containment radiation
				Man	- Manual control of pump combinations and flow throttling

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
		Man	Pass	x ⁶	3. Manual SR ADS actuation is required since CMTs are not available to provide automatic actuation. ADS vent flow is controlled by natural processes that depend on conditions such as RCS pressure and discharge backpressure.
					These SSCs provide SR and NSR defense-in-depth event response for beyond-design-basis SR and NSR component failures. This event response sequence requires manual actions to initiate NSR RNS and maintain RCS inventory and is similar to the NSR manual RCS feed and bleed Item 2.d, except that beyond-design-basis failure of all CMTs occurs, thereby preventing automatic actuation of ADS. The same RNS actuation and control capabilities exist as in Item 2.d. Only partial ADS is required to decrease RCS pressure to within the pressure capability of the RNS.
2.g Accum / IRWST / Recirculation ADS	Pass		Pass		1. SR accumulators are automatically actuated by operation of the discharge check valves that open based on RCS pressure. Injection is also automatically controlled by natural processes that depend upon the same conditions such as RCS pressure.
	Para	x	Pass		2. SR IRWST injection automatically actuates and is controlled by the physical conditions within the RCS and containment.
	Para	x	Pass		3. SR containment recirculation automatically actuates and is controlled by the physical conditions within the RCS and containment.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
		Man	Pass	x ⁶	4. Manual SR ADS actuation is required since CMTs are not available to provide automatic actuation. ADS vent flow is controlled by natural processes that depend on conditions such as RCS pressure and discharge backpressure.
					These SSCs provide SR defense-in-depth event response for beyond-design-basis SR and NSR component failures. This event response is similar to the SR event response of Item 2.e except that beyond-design-basis failure of all CMTs occurs, thereby preventing automatic actuation of ADS. Therefore, manual ADS is required and subsequent automatic actuation of the other SR components occurs.
2.h RNS closed loop cooling (shutdown)	Sel Para	x x	Comp ³	x ³ Man	NSR RNS is manually aligned and actuated to provide closed-loop RCS cooling and some manual control of the cooling process is possible. - Automatic restart of operating pump on loss of power - Automatic pump shutoff on high containment radiation - Automatic control of RNS HX inlet (RCS) temperature by throttling CCS flow to the RNS HX - Manual control of pump combinations and flow throttling

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
					These SSCs provide the expected NSR defense-in-depth event response during shutdown conditions. This NSR shutdown cooling mode operates in conjunction with the heat sink described in Item 3.i (CCS/SW) and does not require ADS venting for heat removal as required in Items 2.d or 2.f, where RNS is providing RCS injection.
2.i SFS cooling of refueling cavity (refueling)		Man		x	NSR SFS is manually aligned and actuated to provide refueling cavity cooling and automatically starts the standby pump if the operating pump fails. Some manual control of the cooling process is possible.
				Man	- Manual control of pump combinations
					These SSCs provide the NSR defense-in-depth event response for beyond-design-basis NSR component failures during shutdown conditions. This NSR shutdown cooling mode operates in conjunction with the heat sink described in Item 3.i (CCS/SWS).
2.j Refueling cavity cooling (refueling)	Pass		Pass	Man	SR refueling cavity cooling is automatically available during shutdown modes when the reactor vessel head is removed and the refueling cavity is flooded up. The heat capacity of this large volume of refueling cavity water provides a heat sink with heatup to boiling, controlled by natural processes that depend on conditions such as the core decay heat load and water circulation in the RV and refueling pool. - Makeup water can be manually re-supplied as refueling cavity water boils off.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
2.k IRWST injection / venting (shutdown)	Para	x	Pass		<p>These SSCs provide the SR design basis event response for multiple NSR component failures during shutdown conditions.</p> <p>SR IRWST automatically actuates to provide RCS injection when the RCS is fully depressurized and the ADS valves are required to be open or the RCS is opened to provide sufficient steam venting area. Injection and RCS heat removal are controlled by natural processes that depend on conditions such as core decay heat levels and IRWST level.</p> <p>These SSCs provide SR design basis or defense-in-depth event response, depending on the specific event.</p>
3. Heat Sink					
3.a Steam dumps / circulating water	Sel / Comp	x	Comp	x	<p>1. NSR steam dumps automatically actuate and automatically maintain the programmed Tave following an event. Following a reactor trip, operation is manually selected to a mode where the steam dumps automatically control the SG pressure at a value selected by the operator.</p>
		Man			<p>2. NSR circulating water system is manually aligned and actuated on plant startup, normally operates during power operation, and no actions are expected to be needed or taken to maintain this system as a post-accident heat sink except to manually restart a pump following power recovery after a loss of site power.</p>

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
3.b SG PORVs	Comp	x	Comp	x	<p>1. NSR SG PORVs automatically actuate and automatically maintain the SG pressure at a value selected by the operator.</p> <p>This NSR design feature provides a defense-in-depth, heat sink function, in conjunction with main or startup feedwater to the SGs in Items 2.a (main feedwater) and 2.b (startup feedwater).</p>
3.c Fan coolers / chilled water / component cooling water / service water / SW cooling tower fan	Sel	x	Comp	x	<p>1. NSR fan coolers are manually aligned and actuated on plant startup, normally operate during power operation, automatically start the standby fan coolers, and automatically maintain preset discharge temperatures during power operation.</p>
	Sel	x	Comp	<p>x</p> <p>Man</p>	<p>- Automatic start of standby fan cooler</p> <p>- Automatic control of discharge air temperature by throttling chilled water flow to the cooling coils</p> <p>- Manual control of fan cooler combinations and flow throttling</p>

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
	Sel	x			2. Both NSR chilled water systems are manually aligned and actuated on plant startup, normally operate during power operation, automatically start the standby chiller unit if the operating unit fails, automatically maintain chilled water outlet temperature, and automatically control individual cooler bypass valves to maintain associated heating, ventilation and air-conditioning (HVAC) system discharge air temperature.
	Sel	x			- Automatic re-start following loss of power
	Sel	x		Man	- Automatic start of standby unit and shutdown of faulted chiller - Manual control of chiller combinations and flow throttling
					3. See Item 3.i for discussion of NSR component cooling water operation.
					4. See Item 3.i for discussion of NSR service water operation.
					These SSCs provide the expected NSR defense-in-depth event response.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
3.d SG safety valves	Passive	x			<p>SR SG safety valves automatically open at the high-pressure relief set point to discharge steam from the SG to remove decay heat. The safety valves automatically re-close when SG pressure is subsequently reduced. These valves provide a backup to the SG PORVs since the safety valve relief set point is above the SG PORV operating set point.</p> <p>- Safety valves can be manually gagged.</p> <p>These SSCs provide the expected NSR defense-in-depth event response for non-LOCA events. This would be used in conjunction with Item 2.a (main feedwater) or 3.b (AFW).</p>
3.e RNS closed- loop cooling of IRWST	Sel Para	x x			<p>NSR RNS is manually aligned and actuated to provide closed-loop IRWST cooling and some manual control of the cooling process is possible.</p> <p>- Automatic restart of operating pump on loss of power</p> <p>- Automatic pump shutoff on high containment radiation</p>
			Comp ³	x ³ Man	<p>- Automatic control of RNS HX inlet (IRWST) temperature by throttling CCS flow to the RNS HX</p> <p>- Manual control of pump combinations and flow throttling</p>

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
					These SSCs provide NSR defense in-depth event response following beyond-design-basis NSR component failures. This event response can prevent steaming to containment when IRWST heating occurs, such as following PRHR or ADS actuation, but no other containment steaming source such as a LOCA or steam break event has occurred. This NSR heat sink mode operates in conjunction with the heat sink described in Item 3.i (CCS/SW).
3.f PCS drain / air cooling	Par	x	Pass		1. SR PCS automatically actuates water drain on the containment shell, with convective / evaporative heat transfer controlled by natural processes that depend on conditions such as containment temperature, PCS storage tank level, and water coverage.
	Pass		Pass		2. SR natural convection air flow on the outside of the containment shell continuously exists and the convective / evaporative heat transfer is controlled by natural processes that depend on conditions such as containment temperature and ambient air temperature. These SSCs provide the SR design basis event response.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
3.g Fire protection drain / air cooling		Man	Comp	x	1. The NSR fire protection system can be manually aligned and actuated to provide water to either the PCS storage tank or directly to the water distribution bucket above the containment shell. The water flow to the PCS is automatically controlled by fire protection system design conditions such as system flow characteristics. The water flow to the distribution bucket is manually controlled by the fire protection system alignment (flowpath to tank or distribution bucket). The convective / evaporative heat transfer is controlled by natural processes that depend on conditions such as containment temperature, PCS storage tank level, and water coverage.
	Sel	x			- Automatic start of standby pump
	Pass		Pass		2. SR natural convection air flow on the outside of the containment shell continuously exists and the convective / evaporative heat transfer is controlled by natural processes that depend on conditions such as containment temperature and ambient air temperature.
					These SSCs provide SR and NSR defense-in-depth event responses for beyond-design-basis SR and NSR component failures.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
3.h Air cooling w/o PCS or fire protection drain	Pass		Pass		SR natural convection air flow on the outside of the containment shell continuously exists and the convective / evaporative heat transfer is controlled by natural processes that depend on conditions such as containment temperature and ambient air temperature. Air flow can provide containment heat removal even in the event that water drain is unavailable. These SSCs provide SR defense-in-depth event response for beyond-design-basis SR and NSR component failures.
3.i Component cooling water / service water / SW cooling tower fan (shutdown)	Sel	x			1. Component cooling water is manually aligned and actuated on plant startup, normally operates during power and shutdown operation, and automatically starts the standby pump if the operating pump fails.
	Sel	x	Comp ³	x ³	- Automatic start of standby pump - Automatic control of CCS flow to the RNS HX based on RNS HX inlet (RCS) temperature
				Man	- Manual control of pump combinations
	Sel	x			2. Service water is manually aligned and actuated on plant startup, normally operates during power operation, and automatically starts the standby pump if the operating pump fails.
	Sel	x			- Automatic start of standby pump.
	Sel	x	Sel	x	- Automatic operation of cooling tower fans to control system temperature

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
					These SSCs provide the expected NSR defense-in-depth event response. These NSR systems are manually aligned and actuated on plant startup, normally operate during power operation, and automatically operate as indicated to support plant operation and defense-in-depth event mitigation.
4. Integrity					
4.a Stop excessive RCS cooldown. - SG PORVs - Steam dumps - PRHR - MSIVs - Main/startup feedwater - RNS	Sel	x	Sel	x	The identified NSR SSCs are verified for proper operation and manually controlled as necessary to stop any excessive RCS cooldown, which could lead to pressurized thermal shock or cold overpressurization. The excessive cooldown could be due to the consequences of the event, the subsequent actuation of the associated SSCs, or the actuation or control failures for the associated SSCs.
	Para	x	Pass	x ⁶	The identified SR SSCs are actuated and controlled as follows: - PRHR (See Item 2.c for additional information.) - MSIVs
	Para	x			
					These SSCs provide the expected SR and NSR defense-in-depth event response.
4.b Stop excessive RCS pressurization. Pressure control SSCs: - Pressurizer heaters - Pressurizer spray - Pressurizer aux spray - ADS	Sel	x	Sel	x	The identified NSR SSCs are verified for proper operation and manually controlled as necessary to stop any excessive RCS overpressurization, which could lead to pressurized thermal shock or cold overpressurization. The overpressurization could be due to the consequences of the event, the subsequent actuation of the associated SSCs, or the actuation or control failures for the associated SSCs.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
Inventory control SSCs: - CVS makeup - CMT injection - Accum injection - CVS letdown - RV head vent letdown	Para	x	Pass		The identified SR SSCs are actuated and controlled as follows: - CMT injection - ADS
	Para	x	Pass	x ⁶	
	Pass	Man	Pass		- Accumulator injection - RV head vent letdown
					These SSCs provide the expected SR and NSR defense-in-depth event response.
5. Containment					The same design features that satisfy the heat sink CSF are also used to satisfy the containment CSF.
5.a Fan coolers / chilled water / component cooling water / service water / SWS cooling tower fan					See Item 3.c
5.b PCS drain / air cooling					See Item 3.f
5.c Fire protection drain / air cooling					See Item 3.g
5.d Air cooling w/o PCS or fire protection drain					See Item 3.h
6. Inventory					With the exception of the Items 6.a, 6.f, and 6.g, the same design features that satisfy the core cooling CSF are also used to satisfy the inventory CSF.

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3,4}
	Auto	Man	Auto	Man	
6.a CVS injection	Sel	x			NSR CVS makeup pumps are manually aligned for periodic automatic actuation during power operation and following any event where RCS inventory decreases. It is designed to actuate and provide RCS makeup before automatic actuation of SR injection sources following events where RCS inventory is lost.
			Comp	x Man	<ul style="list-style-type: none"> - RCS makeup flow rate and boron concentration - Manual control of pump combinations
					These SSCs provide the expected NSR defense-in-depth event response for RCS leak. This NSR RCS injection source operates in conjunction with the heat sink described in Item 3.i (CCS/SWS)
6.b CMT / accum / RNS injection / IRWST / Recirculation / Partial ADS					See Item 2.d
6.c CMT / accum / IRWST / Recirculation / Full ADS					See Item 2.e
6.d Accum / RNS injection / IRWST / Recirculation / Partial ADS					See Item 2.f
6.e Accum / IRWST / Full ADS					See Item 2.g

TABLE 4
SUCCESS PATH SSC ALLOCATIONS (Cont.)

Critical Safety Function ¹	Actuation		Control		Comments ^{3, 4}
	Auto	Man	Auto	Man	
6.f IRWST injection / venting (shutdown)	Para	x Man	Pass	Man	<p>SR IRWST automatically actuates to provide RCS injection when the RCS is fully depressurized and the ADS valves are required to be open or the RCS is opened and can provide sufficient vent area. Injection and RCS heat removal are controlled by natural processes that depend on conditions such as core decay heat levels and IRWST level.</p> <p>SR IRWST gravity injection to the RCS can also be manually aligned and controlled through the RNS when the RNS is aligned to the RCS.</p> <p>These SSCs provide SR design basis or defense-in-depth event response, depending on the specific event.</p>
6.g Containment makeup		Man		Man	<p>NSR long-term (after 72 hours) makeup water is provided to containment through an SR piping connection in the RNS.</p> <p>These SSCs provide NSR defense-in-depth event response for beyond-design-basis SR and NSR component failures.</p>
6.h Spent Fuel Pool Cooling System (SFS) makeup (refueling)		Man		Man	<p>NSR SFS is manually aligned and actuated to provide RCS / refueling cavity makeup when the RCS is fully depressurized and open for refueling. Requires operator control to maintain the required spent fuel pool inventory.</p> <p>- Manual control of pump combinations</p> <p>These SSCs provide NSR defense-in-depth event response for beyond-design-basis SR and NSR component failures.</p>

TABLE 5 (Subsection 3.3)

FUNCTION ALLOCATION BASIS CODES (Paths in Figure 1 shown in parenthesis)

Automatic

- A1 The operator is NOT able to perform the required task due to human limitations. (1b, 2,10)
- A2 Automation is necessary due to regulatory design requirements. (1c, 2, 10)
- A3 Automation is necessary due to utility design requirements. (1c, 2, 10)
- A4 Automation provides a safety benefit as identified in the PRA. (5a, 5b(2), 10)
- A5 Automation is preferred based on operating experience. (5a, 5b(1), 10)
- A6 Automation is preferred due to concerns for operator overload. (5a, 5b(4), 10)
- A7 Automation is inherent in the passive design. (5a, 5b(3), 10)
- A8 Tasks are not well suited to human performance and are better suited to automation. (7a-f, 10)

Manual

- M1 Human performance is required because automation is not technically feasible. (3a, 4, 11)
- M2 Human performance is required by design recommendations or requirements. (3b, 4, 11)
- M3 Human performance is preferred because of consideration of safety requirements, task complexity, cost/benefit considerations to implement automation, and the value of human judgement. (6a, 11)

NOTES:

- ¹ Referenced "Items" refer to other entries in this table. A list of abbreviations is provided at the beginning of this document.

TABLE 5 (Subsection 3.3)
FUNCTION ALLOCATION BASIS

Critical Safety Function	Success Path(s) in Table 4	Function Allocation Basis Code	Automated on the Reference Plant	Notes¹
1. Subcriticality				
a. Reactor trip (PMS)	1.a	A2	x	
b. Reactor trip (DAS)	1.b	A4		
c. Control rod insertion (rod control system)	1.c	M3		Manual insertion is a backup to multiple beyond-design-basis failures of automatic PMS and DAS reactor trips in Items 1.a and 1.b.
d. Rideout	1.f	A2	x	
e. CVS boration	1.d, 4.b, 6.a	M3, A3		The URD only requires automatic CVS makeup based on maintaining programmed pressurizer level. Automatic boration can occur for certain events as a result of automatic boron dilution protection that isolates makeup water.
f. CMT boration	1.e	A2		
2. Core Cooling				
a. Main feedwater	2.a, 4.a	A6	x	
b. Startup feedwater	2.b, 4.a	A3, A6	x	
c. PRHR	2.c, 4.a	A2		
d. CMT injection	2.d, 2.e, 4.b, 6.b, 6.c	A2		
e. Accumulator injection	2.d, 2.e, 2.f, 2.g, 4.b, 6.b, 6.c, 6.d, 6.e	A7	x	

TABLE 5
FUNCTION ALLOCATION BASIS (Cont.)

Critical Safety Function	Success Path(s) in Table 4	Function Allocation Basis Code	Automated on the Reference Plant	Notes ²
2. Core Cooling (cont.)				
f. IRWST heat removal and injection	2.d, 2.e, 2.f, 2.g, 2.k, 6.b, 6.c, 6.d, 6.e, 6.f	A2		
g. Recirculation	2.d, 2.e, 2.f, 2.g, 6.b, 6.c, 6.d	A2	x	
h. ADS	2.d, 2.e, 2.f, 2.g, 2.k, 4.b, 6.b, 6.c, 6.d, 6.e, 6.f	A2		
i. RNS injection	2.d, 2.f, 4.a, 6.b, 6.d	M3, A4		
j. RNS closed loop cooling (shutdown)	2.h, 4.a	M3, A4		
k. SFS cooling of refueling cavity (refueling)	2.i	M3		
l. Refueling cavity cooling (refueling)	2.j	A7	x	
3. Heat Sink				
a. Steam dumps	3.a, 4.a	A3	x	
b. Circulating water	3.a	M3	x	
c. SG PORVS	3.a, 4.a	A3	x	
d. Fan coolers	3.c, 5.a	A3	x	
e. Chilled water	3.c, 5.a	A3	x	

TABLE 5
FUNCTION ALLOCATION BASIS (Cont.)

Critical Safety Function	Success Path(s) in Table 4	Function Allocation Basis Code	Automated on the Reference Plant	Notes ²
3. Heat Sink (cont.)				
f. Component cooling water	3.c, 3.i, 5.a	A3	x	
g. Service water	3.c, 3.i, 5.a	A3	x	
h. SG safety valves	3.d	A2	x	
i. Service water cooling tower and fan	3.c, 3.i, 5.a	A3	x	
j. RNS closed-loop cooling of the IRWST/PRHR	3.e, 4.a	M3, A6		
k. PCS water drain	3.f, 5.b, 5.e	A3		
l. Containment air cooling (external)	3.f, 3.g, 3.h, 5.b, 5.c, 5.d	A7		
m. Fire protection water drain	3.g, 5.c, 5.f	M3	x	
4. Integrity				
a. Steam dumps				See Item 3.a
b. SG PORVs				See Item 3.c
c. PRHR				See Item 2.c
d. MSIVs and bypasses	4.a	A2	x	
e. Main feedwater				See Item 2.a
f. Startup feedwater				See Item 2.b
g. RNS				See Items 2.i and 2.j.

TABLE 5
FUNCTION ALLOCATION BASIS (Cont.)

Critical Safety Function	Success Path(s) in Table 4	Function Allocation Basis Code	Automated on the Reference Plant	Notes ²
4. Integrity (cont.)				
h. Pressurizer heaters	4.b	A5	x	
i. Pressurizer spray	4.b	A5	x	
j. Pressurizer auxiliary spray	4.b	M3		
k. ADS				See Item 2.h
l. CVS injection				See Items 1.d and 6.a
m. CMT injection				See Item 2.d
n. Accum injection				See Item 2.e
o. CVS letdown				See Item 1.d and 6.a
p. RV head vent letdown	4.b	M3		
5. Containment				
a. Fan coolers				See Item 3.d
b. Chilled water				See Item 3.e
c. Component cooling water				See Item 3.f
d. Service water				See Item 3.g
e. Service water cooling tower and fan				See Item 3.h
f. PCS water drain				See Item 3.k
g. Containment air cooling (external)				See Item 3.l

TABLE 5
FUNCTION ALLOCATION BASIS (Cont.)

Critical Safety Function	Success Path(s) in Table 4	Function Allocation Basis Code	Automated on the Reference Plant	Notes ²
5. Containment (cont.)				
h. Fire protection water drain				See Item 3.m
6. Inventory				
a. CVS injection	1.d, 4.b, 6.a	A3	x	
b. CMT				See Item 2.d
c. Accumulator				See Item 2.e
d. IRWST				See Item 2.f
e. Recirculation				See Item 2.g
f. ADS				See Item 2.h
g. RNS injection				See Item 2.i
h. Containment makeup	6.g	M1		
i. SFS makeup (refueling)	6.h	M3		

TABLE 6
FUNCTION ALLOCATION QUESTIONS

1. Is automation mandatory?
<ul style="list-style-type: none"> a. Are working conditions hostile to humans? b. Are tasks included that humans cannot perform? (consider speed, complexity, strength, computation, etc.) c. Is automation required by regulatory or utility requirements? (one of the following documents: URD)
2. Is automation technically feasible?
Consider availability of technology, cost, development and implementation, and scheduling issues.
3. Is human performance mandatory?
<ul style="list-style-type: none"> a. Is automation not technically feasible? b. Is operator involvement required by design requirements? (regulatory, utility, or design requirements)
4. Is human performance a feasible solution?
<ul style="list-style-type: none"> a. Can humans perform the specified tasks? b. Will operator workload be manageable?
5. Is automation clearly preferable to human operators?
<ul style="list-style-type: none"> a. Can automation technology be effectively implemented? b. Is human performance clearly less satisfactory for one of the following reasons? <ul style="list-style-type: none"> - Does operating experience suggest a need for automation? - Does PRA analysis suggest a need for automation? - Does an effective AP600 design require automation? - Are operator tasks likely to lead to overload if allocated to human performance?
6. Is human performance clearly preferable to automation?
<ul style="list-style-type: none"> a. Is human performance regarded as clearly necessary, or superior to automation? (Consider operating experience, safety significance, need for human judgement, special human capabilities, cost, barriers to the development and implementation of automation, and scheduling issues.)
7. Is the segment a suitable candidate for automation?
<ul style="list-style-type: none"> 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 response? 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?

**TABLE 6 (Cont.)
FUNCTION ALLOCATION QUESTIONS**

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 operator's 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)

9. 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

10. Consider the residual role of the human operator in support of the automated function.

(see text for guiding principles)

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

(see text for guiding principles)

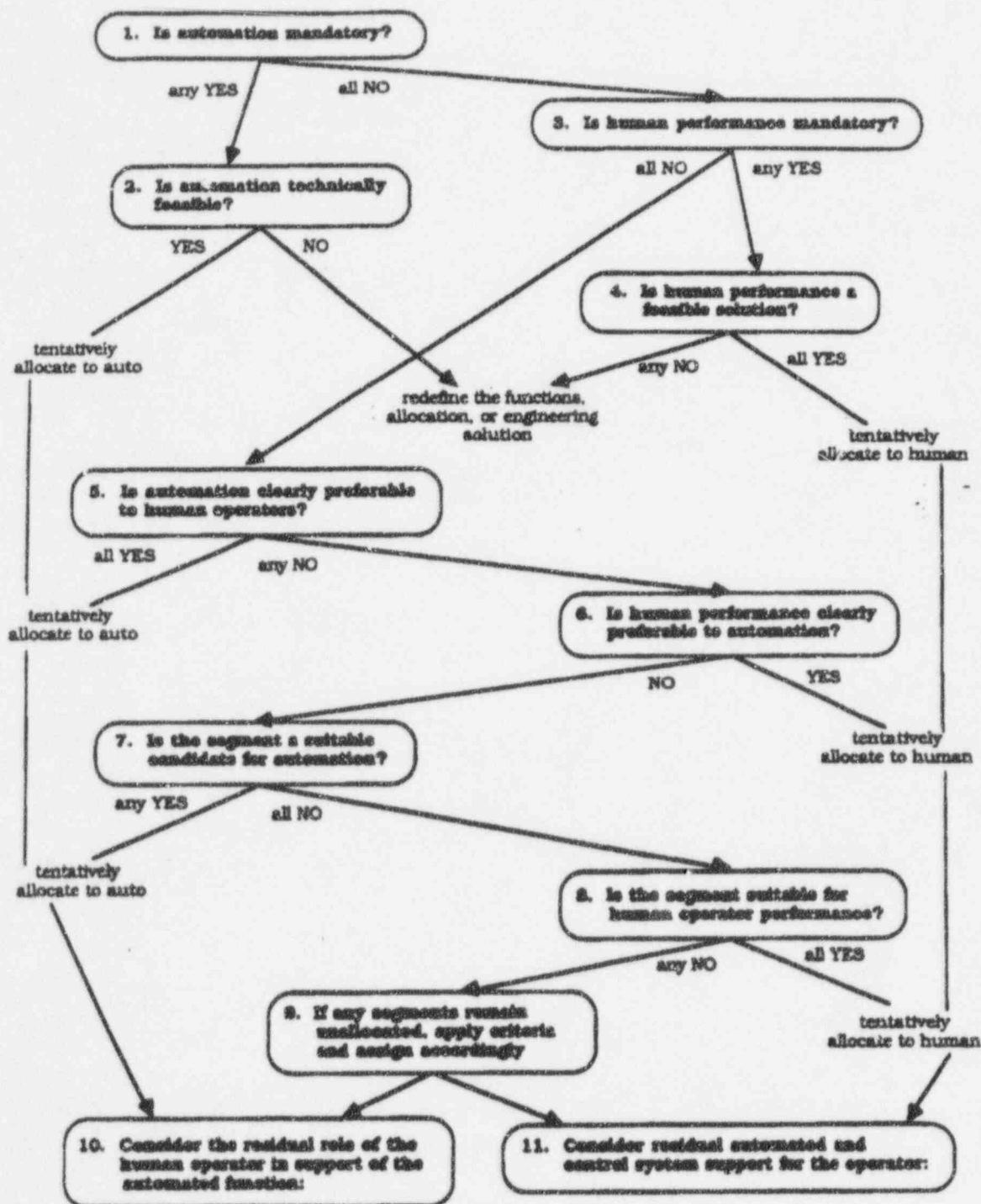


Figure 1. Function Allocation Decision Process