October 9, 1992

Docket No. 52-001

APPLICANT: GE Nuclear Energy (GE)

PROJECT: Advanced Boiling Water Reactor (ABWR)

SUBJECT: SUMMARY OF MEETING WITH GE ON SEPTEMBER 21-22, 1992

A public meeting was held between the Nuclear Regulatory Commission (NRC) staff, GE Nuclear Energy (GE), and the Nuclear Materials Resources Council (NUMARC) at the offices of GE in San Jose, California, on September 21-22, 1992. The purpose of this meeting was to discuss issues related to the industry and staff review of the ABWR inspections, tests, analyses, and acceptance criteria. Enclosure 1 is a list of those who attended.

Enclosure 2 contains the agenda for the meeting and the viewgraphs presented at the meeting. The agenda items on the review of the revised high pressure core flooder system and the reactor building heating ventilation, and air conditioning (HVAC) system were not discussed due to time constraints.

NUMARC opened the meeting on September 21 by presenting a short summary of the status of the NUMARC/industry review. The results of the review were illustrated by discussion of the changes to the Tier 1 material for the standby liquid control system. GE then presented the remote shutdown system and HVAC emergency cooling water system for discussion by the industry group. The staff clarified its comments on the Tier 1 material provided to GE in a letter dated August 12, 1992. On September 22, the design acceptance criteria for the human factors engineering and instrumentation and controls aspects of the ABWR were discussed.

The nature of the changes to the Tier 1 material were discussed; however, no conclusions were reached on the material. The staff will evaluate the changes when GE provides a revised Tier 1 submittal to the NRC. GE will address the staff's comments of August 12 when it resubmits the Tier 1 material for staff review.

Original Signed By:

Thomas H. Boyce, Project Manager
Standardization Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation

Enclosures:
1. Attendees List
2. Meeting Agenda

cc w/enclosures:
See next page

140033

DISTRIBUTION:

Docket File	PDST R/F	TMurley/FMiraglia	DCrutchfield
NRC PDR	RPierson	JNWilson	CPoslusny
RNease	PShea	JMoore, 15B18	WTravers
EJordan, MNBB3701	ACRS (10)	GGrant, EDO	THiltz
TBoyce	WBurton, 8D1	WRussell, 12G18	RPerch, 8H7
JStewart, 8H7	CGoodman, 10D24	WBeckner, 10E4	OGC

OFC:	LA:PDST:ADAR	PM:PDST:ADAR	SC:PDST:ADAR
NAME:	PShea	TBoyce:tz	JNWilson
DATE:	10/6 /92	10/6 /92	10/9 /92

OFFICIAL RECORD COPY: DOCUMENT NAME: MTGSM921.TB

D103

cc: Mr. Patrick W. Marriott, Manager
Licensing & Consulting Services
GE Nuclear Energy
175 Curtner Avenue
San Jose, California 95125

Mr. Robert Mitchell
General Electric Company
175 Curtner Avenue
San Jose, California 95114

Mr. L. Gifford, Program Manager
Regulatory Programs
GE Nuclear Energy
12300 Twinbrook Parkway
Suite 315
Rockville, Maryland 20852

Director, Criteria & Standards Division
Office of Radiation Programs
U. S. Environmental Protection Agency
401 M Street, S.W.
Washington, D.C. 20460

Mr. Daniel F. Giessing
U. S. Department of Energy
NE-42
Washington, D.C. 20585

Mr. Steve Goldberg
Budget Examiner
725 17th Street, N.W.
Room 8002
Washington, D.C. 20503

Mr. Frank A. Ross
U.S. Department of Energy, NE-42
Office of LWR Safety and Technology
19901 Germantown Road
Germantown, Maryland 20874

Mr. Raymond Ng
1776 Eye Street, N.W.
Suite 300
Washington, D.C. 20006

Marcus A. Rowden, Esq.
Fried, Frank, Harris, Shriver & Jacobson
1001 Pennsylvania Avenue, N.W.
Suite 800
Washington, D.C. 20004

Jay M. Gutierrez, Esq.
Newman & Holtzinger, P.C.
1615 L Street, N.W.
Suite 1000
Washington, D.C. 20036

Mr. Mark McCabe
U.S. Dept. of Justice/EAG
555 4th Street, N.W.
Room 11-809
Washington, D.C. 20001

Mr. Joseph Quirk
GE Nuclear Energy
Mail Code 782
General Electric Company
175 Curtner Avenue
San Jose, California 95125

Enclosure 1

MEETING ATTENDEES

SEPTEMBER 21-22, 1992

NAME	AFFILIATION
T. Boyce	NRC
W. Burton	NRC
W. Russell	NRC
R. Perch	NRC
R. Pierson	NRC
J. Stewart	NRC
C. Goodman	NRC
W. Beckner	NRC
W. Zimmerman	AEPSC/Nuclear Safety
D. Wilson	EPRI/NMPC
H. Messer	Duke Power Co.
B. Brown	GE/Diagnostic Testing
S. Frantz	Newman & Holtzinger (GE)
R. Louison	GE
M. Ross	GE
P. Billig	GE
T. O'Neil	GE
B. Cockrell	INPO
A. Heymer	NUMARC
B. Rasin	NUMARC
T. McDonnell	Bechtel
N. Kaushal	Commonwealth Edison
A. Sterdis	Westinghouse
C. Brinkman	ABB-CE
J. Rec	ABB-CE
N. Fletcher	DOE/ALWR
K. Mali	DOE/SF

ABWR DESIGN CERTIFICATION

Enclosure 2

GE/NRC/NUMARC TIER 1/ITAAC
REVIEW 9/21 - 9/22/92

AGENDA

TOPIC	LEAD
MONDAY 8:00 AM - ALL DAY	
o SUMMARY OF NUMARC/UTILITY REVIEW RESULTS	GE/NUMARC (JAMES/HEYMER)
o REVIEW OF REVISED SLCS	NUMARC (HEYMER)
o REVIEW OF REVISED HPCF	GE (JAMES)
o CONTINUATION OF GROUP REVIEW	ALL
RSS	O'NEIL
HVAC CW (N+E)	MILLER
REACTOR BUILDING HVAC	MUNSON
TUESDAY 8:00 AM - ALL DAY	
o CONTINUATION OF GROUP REVIEW	ALL
HFE DAC	ROSS
SOFTWARE DAC	SIMON

REVISED SLCS
ITAAC

	ENTRIES
SUBMITTED	6
REVISED	9

Table 2.2.4: Standb, Liquid Control System

Inspections, Tests, Analyses and [illegible]ce Criteria

Certified Design Commitment	Inspections, Tests, Anal[illegible]	Acceptance Criteria
1. The SLCS is capable of insen[illegible]ng the quantity of boron solution to produce an average boron concentration of $\geq$ 1720 ppm in the RPV at rated conditions.	1. A documentation review and [illegible] inspection will be conducted on [illegible] built parameters listed below:	Certified Design Commitment is met provided that:
	a. Storage tank pumpable volume	a. Storage tank pumpable volume range is between 23.1 to 25.7 m^3.
	b. RPV water inventory at 21°C	b. RPV water inventory is $\leq 455 \times 10^3$ kg.
	c. RHR shutdown cooling system water inventory at 21°C	c. RHR shutdown cooling system inventory is $\leq 130 \times 10^3$ kg.
2. A simplified configuration for the SLC system is described in Section 2.2.4.	2. Construction records will be reviewed and visual inspections will be conducted for the configuration of the SLCS.	2. The as-built configuration of the SLCS is in accordance with the description in Section 2.2.4.

Table 2.2.4: Standby Liquid Control System

Inspections, Tests, Analyses and Acceptance Criteria (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. The SLC system delivers at least 378 l/min of solution with both pumps operating against the elevated pressure conditions which can exist in the reactor during events involving SLC System initiation.	3. Using installed controls, power supplies and other auxiliaries, the following system preoperational tests will be conducted of pump and system performance. For each test, demineralized water will be injected from the storage tank into the RPV. a. Using a simulated ATWS signal, the SLCS will automatically inject $\geq$ 378 l/min with both pumps running against a reactor pressure of $\geq$ 88.9 kg/cm^2 a. b. To demonstrate adequate Net Positive Suction Head (NPSH), delivery of $\geq$ 378 l/min will be confirmed by tests conducted at conditions of low level and maximum temperature in the storage tank. c. Manual initiation of each SLCS division will be tested.	3. The Certified Design Commitment is met provided that: a. The SLC system automatically injects $\geq$ 378 l/min into the RPV with both pumps running against a reactor pressure of $\geq$ 88.9 kg/cm^2 a. b. The SLC system injects $\geq$ 378 l/min at conditions of low level and maximum temperature in the storage tank. c. Each SLCS division initiates upon receipt of a manual signal from the control room.
4. The SLC System is designed to permit functional testing during plant operation.	4. Using installed controls, power supplies and other auxiliaries, the following functional tests will be conducted for each SLCS division after system installation: a. Demineralized water will be pumped against a pressure $\geq$ 88.9 kg/cm^2 a in a closed loop on the test tank. b. Demineralized water will be injected from the test tank into the RPV.	4. a. Demineralized water is pumped with a flowrate $\geq$ 189 l/min. b. Demineralized water is injected from the test tank into the RPV.

Table 2.2.4: Standby Liquid Control System

Inspections, Tests, Analyses and Acceptance Criteria (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. The SLC System is powered from Class 1E buses.	5. a. As-built construction records will be reviewed to determine the source of electrical power. b. A test of the components described in the Design Description in Section 2.2.4 will be conducted with power supplied from the permanently installed electric power busses.	5. SLC System receives electrical power from Class 1E buses.
6. Portions of the SLC System are classified as ASME Code class as indicated in Section 2.2.4. They are designed, material tested, fabricated, installed, and inspected in accordance with the ASME Code, Section III.	6. ASME Code Data Reports will be reviewed and inspections of Code stamps will be conducted for ASME components in the SLCS.	6. Those portions of the SLCS identified as ASME Code class in Section 2.2.4 have ASME Code Section III, Code Data reports and Code stamps (or alternative markings permitted by the Code).
7. The ASME portions of the SLCS retain their integrity under internal pressures that will be experienced during service.	7. A hydrostatic test will be conducted on those portions of the SLCS required to be hydrostatically tested by the ASME Code.	7. The results of the hydrostatic test of the ASME portions of the SLCS conform with the requirements in the ASME Code, Section III.
8. The control room features provided for the SLC system are defined in Section 2.2.4.	8. Inspections will be performed to verify the presence of control room features for the SLC system.	8. Features are present in the control room as defined in Section 2.2.4.
9. Each division of the SLC system (Divisions A, B) is electrically independent.	9. Construction records will be reviewed and visual inspections will be performed of the electrical independence of the SLCS divisions.	9. The injection valve, pump, and suction valve within each division of the SLC System (Division A or B) is supplied from only one division of electrical power, and this division of electrical power is different from the division of electrical power supplying the same components within the other division of the SLC System.

COMPARISON OF SUBMITTED AND REVISED SLCS ITAAL TABLE.

	ENTRIES
SUBMITTED	6
REVISED	9

SUBMITTED

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The minimum average poison concentration in the reactor after operation of the SLC System shall be equal to or greater than 850 ppm.	1. Construction records, revisions and plant visual examinations will be undertaken to assess as-built parameters listed below for compatibility with SLC System design calculations. If necessary, an as-built SLC System analysis will be conducted to demonstrate that the acceptance criteria are met. **Critical Parameters:** a. Storage tank pumpable volume b. RPV water inventory at 70°F c. RHR shutdown cooling system water inventory at 70°F	1. It must be shown the SLC System can achieve a poison concentration of 850 ppm or greater, assuming a 25% dilution due to non-uniform mixing in the reactor and accounting for dilution in the RHR shutdown cooling systems. This concentration must be achieved under system design basis conditions. This requires that the SLC System meet the following values: a. Storage tank pumpable volume range 6100-6800 gal. b. RPV water inventory $\leq 1.00 \times 10^8$ lb c. RHR shutdown cooling system inventory $\leq 0.287 \times 10^8$ lb

REVISED

1. The SLCS is capable of inserting the quantity of boron solution to produce an average boron concentration of $\geq$ 1320 ppm in the RPV at rated conditions.	1. A documentation review and visual inspection will be conducted on the as built parameters listed below: a. Storage tank pumpable volume b. RPV water inventory at 21°C c. RHR shutdown cooling system water inventory at 21°C	1. The Certified Design Commitment is met provided that: a. Storage tank pumpable volume range is between 23.1 to 25.7 m^3. b. RPV water inventory is $\leq 455 \times 10^3$ kg. c. RHR shutdown cooling system inventory is $\leq 130 \times 10^3$ kg.

SUBMITTED

2. A simplified system configuration is shown in Figure 2.2.4.	2. Inspections of installation records, together with plant walkdowns, will be conducted to confirm that the installed equipment is in compliance with the design configuration defined in Figure 2.2.4.	2. The system configuration is in accordance with Figure 2.2.4.

REVISED

2. A simplified configuration for the SLC system is described in Section 2.2.4.	2. Construction records will be reviewed and visual inspections will be conducted for the configuration of the SLCS.	2. The as-built configuration of the SLCS is in accordance with the description in Section 2.2.4.

SUBMITTED

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. The SLC System shall be capable of delivering 100 gpm of solution with both pumps operating against the elevated pressure conditions which can exist in the reactor during events involving SLC System initiation.	3. System preoperation tests will be conducted to demonstrate acceptable pump and system performance. These tests will involve establishing test conditions that simulate conditions which will exist during an SLC System design basis event. To demonstrate adequate Net Positive Suction Head (NPSH), delivery of rated flow will be confirmed by tests conducted at conditions of low level and maximum temperature in the storage tank, and the water will be injected from the storage tank to the RPV.	3. It must be shown that the SLC System can automatically inject 100 gpm (both pumps running) against a reactor pressure of 1250 psig with simulated ATWS conditions. It must also be shown that the SLC System pumps can pump the entire storage tank pumpable volume.

REVISED

3. The SLC system delivers at least 378 l/min of solution with both pumps operating against the elevated pressure conditions which can exist in the reactor during events involving SLC System initiation.	3. Using installed controls, power supplies and other auxiliaries, the following system preoperational tests will be conducted of pump and system performance. For each test, demineralized water will be injected from the storage tank into the RPV. a. Using a simulated ATWS signal, the SLCS will automatically inject $\geq$ 378 l/min with both pumps running against a reactor pressure of $\geq$ 88.9 kg/cm^2 a. b. To demonstrate adequate Net Positive Suction Head (NPSH), delivery of $\geq$ 378 l/min will be confirmed by tests conducted at conditions of low level and maximum temperature in the storage tank. c. Manual initiation of each SLCS division will be tested.	3. The Certified Design Commitment is met provided that: a. The SLC system automatically injects $\geq$ 378 l/min into the RPV with both pumps running against a reactor pressure of $\geq$ 88.9 kg/cm^2 a. b. The SLC system injects $\geq$ 378 l/min at conditions of low level and maximum temperature in the storage tank. c. Each SLCS division initiates upon receipt of a manual signal from the control room.

SUBMITTED

4. The system is designed to permit in-service functional testing of the SLC System.	4. Field tests will be conducted after system installation to confirm that in-service system testing can be performed.	4. Using normally installed controls, power supplies and other auxiliaries, the system has the capability to perform: a. Pump tests in a closed loop on the test tank. b. RPV injection tests using demineralized water from the test tank.

REVISED

4. The SLC System is designed to permit functional testing during plant operation.	4. Using installed controls, power supplies and other auxiliaries, the following functional tests will be conducted for each SLCS division after system installation: a. Demineralizeo water will be pumped against a pressure $\geq$ 88.9 kg/cm^2 a in a closed loop on the test tank. b. Demineralized water will be injected from the test tank into the RPV.	4. a. Demineralized water is pumped with a flowrate $\geq$ 189 l/min. b. Demineralized water is injected from the test tank into the RPV.

SUBMITTED

5. The pump, heater, valves and controls can be powered from the standby AC power supply as described in Section 2.2.4.	5. System tests will be conducted after installation to confirm that the electrical power supply configurations are in compliance with design commitments.	5. The installed equipment can be powered from the standby AC power supply.

REVISED

5. The SLC System is powered from Class 1E buses.	5. a. As-built construction records will be reviewed to determine the source of electrical power. b. A test of the components described in the Design Description in Section 2.2.4 will be conducted with power supplied from the permanently installed electric power busses.	5. SLC System receives electrical power from Class 1E buses.

SUBMITTED

6. SLC System components which are required for the injection of the neutron absorber into the reactor are classified Seismic Category I and qualified for appropriate environment for locations where installed.	6. See Generic Equipment Qualification verification activities (ITA).	6. See Generic Equipment Qualification Acceptance Criteria (AC).

REVISED

NO ENTRY.

SUBMITTED

ISSUES NOT ADDRESSED

REVISED

6. Portions of the SLC System are classified as ASME Code class as indicated in Section 2.2.4. They are designed, material tested, fabricated, installed, and inspected in accordance with the ASME Code, Section III.	6. ASME Code Data Reports will be reviewed and inspections of Code stamps will be conducted for ASME components in the SLCS.	6. Those portions of the SLCS identified as ASME Code class in Section 2.2.4 have ASME Code Section III, Code Data reports and Code stamps (or alternative markings permitted by the Code).
7. The ASME portions of the SLCS retain their integrity under internal pressures that will be experienced during service.	7. A hydrostatic test will be conducted on those portions of the SLCS required to be hydrostatically tested by the ASME Code.	7. The results of the hydrostatic test of the ASME portions of the SLCS conform with the requirements in the ASME Code, Section III.
8 The control room features provided for the SLC system are defined in Section 2.2.4.	8. inspections will be performed to verify the presence of control room features for the SLC system.	8. Features are present in the control room as defined in Section 2.2.4.
9. Each division of the SLC system (Divisions A, B) is electrically independent.	9. Construction records will be reviewed and visual inspections will be performed of the electrical independence of the SLCS divisions.	9. The injection valve, pump, and suction valve within each division of the SLC System (Division A or B) is supplied from only one division of electrical power, and this division of electrical power is different from the division of electrical power supplying the same components within the other division of the SLC System.

GE Nuclear Energy

ABWR Remote Shutdown System ITAAC

Presentation to NRC and Utility Review Committee

T. J. O'Neil

September 21, 1992

RSS Design Features

The following elements of the RSS design are described in the Tier 1 Design Description. Items followed by "***(ITAAC)***" have a corresponding entry in the ITAAC table.

- **Safety-related features**
  - The RSS is a safety-related system, as it interfaces with nuclear safety-related equipment in other systems
  - The RSS has two divisional panels located in or c remote shutdown station. A physical barrier provides separation between the two panels. ***(ITAAC)***
  - The RSS provides controls and indicators for controlling the following plant systems: ***(ITAAC)***
    1) Residual Heat Removal (RHR) System
    2) High Pressure Core Flooder (HPCF) System
    3) Nuclear Boiler System (NBS)
    4) Reactor Service Water (RSW) System
    5) Reactor Building Cooling Water (RCW) System
    6) Electrical Power Distribution System (EPDS)
    7) Flammability Gas Control System (FCS)

RSS Design Features (cont.)

- **Safety-related features** (cont.)
  - The RSS provides indicators for plant process parameters supplied by the following systems: ***(ITAAC)***
    1) Atmospheric Control (AC) System
    2) Emergency Diesel Generator (D/G)
    3) Suppression Pool Temperature Monitoring System (SPTMS)
    4) Make-up Water Condensate (MUWC) System
  - Control is transferred to the RSS panels through transfer devices which override the controls from the main control room

2.2.6 Remote Shutdown System

Design Description

The Remote Shutdown System (RSS) for the Advanced Boiling Water Reactor (ABWR) provides remote manual control of ~~normal and~~ nuclear safety related AND NON-SAFETY RELATED systems ~~necessary~~ to bring the reactor to cold shutdown conditions ~~in an orderly fashion~~ from outside the main control room.

~~No Loss of Coolant Accident (LOCA), seismic event, or other abnormal plant condition, except loss of off-site power, is assumed to occur coincident with the event requiring the main control room evacuation.~~ The RSS has two divisional panels and associated controls and indicators for ~~monitoring~~ the following INTERFACING WITH ~~interfacing~~ systems:

(1) Residual Heat Removal System (RHR) ~~(Pool cooling and shutdown cooling modes).~~

(2) High Pressure Core Flooder System (HPCF)

(3) Nuclear Boiler System (NBS) ~~Safety Relief Valves~~

(4) Reactor Service Water System (RSW)

(5) Reactor Building Cooling Water System (RCW)

(6) Electrical Power Distribution System (EPDS)

(7) Atmospheric Control System (AC)

(8) Emergency Diesel Generator (D/G)

(9) Make-up Water Condensate System (MUWC)

(10) Flammability Gas Control System (FCS)

(11) Suppression Pool Temperature Monitoring System (SPTMS)

The RSS is classified as a safety-related system because it interfaces with nuclear safety-related equipment from other systems. The two remote shutdown control panels are Seismic Category I and are located in a single remote shutdown station in the Reactor Building. A physical barrier provides separation between the two panels. The RSS provides remote control capability through control and transfer switches in the RSS panels which override the controls from main control room and transfer control to the RSS panels.

Indication for plant parameters is also provided on the remote shutdown panels TO CONDUCT THE PLANT SHUTDOWN ~~to assure a safe and controlled shutdown of the plant.~~ Figure 2.2.6 shows the RSS with the interfacing systems and control and indication functions provided.

Inspections, Tests, Analyses and Acceptance Criteria

Table 2.2.6 provides a definition of the visual inspections, tests and/or analyses, together with associated acceptance criteria, which will be performed for the RSS.

Table 2.2.6: Remote Shutdown System

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. RSS provides ~~a~~ remote manual control ~~of~~ the following interfacing systems to bring the reactor to cold shutdown conditions ~~from~~ DEFINED IN SECTION 2.2.6:	1. ~~Review of as-built documentation and visual~~ inspections of the RSS will be performed ~~Testing of the RSS control functions will be performed.~~ TO VERIFY THE PRESENCE OF CONTROLS AND INDICATORS ON THE RSS PANELS.	1. RSS has the ~~required plant system~~ controls ~~capability~~ AND INDICATORS ON THE PANELS FOR THE SYSTEMS LISTED IN THE CERTIFIED DESIGN COMMITMENT DEFINED IN SECTION 2.2.6.
a. RHR ~~(pool cooling and shutdown cooling modes)~~ b. HPCF c. NBS Safety Relief Valves d. RSW e. RCW f. EPDS ~~g. AC~~ ~~h. D/G~~ ~~i. MUWE~~ g. FCS		
2. The RSS has two divisional panels for 3. monitoring and controlling of the interfacing systems. The panels are ~~physically~~ separated and are located in a remote shutdown station. MECHANICALLY 3. RSS provides indication ~~of~~ plant parameters ~~in RSS~~ panels to monitor a ~~controlled~~ shutdown of the plant. SEE PAGE 3a	2. Visual inspections and documentation 3. review to confirm the ~~appropriate location, isolation, and seismic capabilities of the panels.~~ MECHANICAL SEPARATION 3. Visual inspections and ~~review~~ of as-built documentation ~~relating~~ to RSS monitoring function.	2. The panels ~~conform to their requirements~~ 3. ~~for divisional separation and seismic criteria. They are located in a separate RSS station.~~ ARE MECHANICALLY SEPARATED BY MEANS OF A THREE HOUR FIRE BARRIER 3. The RSS has the ~~required plant~~ monitoring capability.
2. RSS PROVIDES INDICATIONS OF PLANT PROCESSING PARAMETERS DEFINED IN SECTION 2.2.2 FOR THE FOLLOWING SYSTEMS: a. AC b. D/G c. MUWC d. SPTMS	2. INSPECTIONS OF THE RSS WILL BE PERFORMED TO VERIFY THE PRESENCE OF INDICATIONS ON THE RSS PANELS.	2. RSS HAS THE INDICATIONS ON THE PANELS FOR THE SYSTEMS LISTED IN THE CERTIFIED DESIGN COMMITMENT DEFINED IN SECTION 2.2.6.

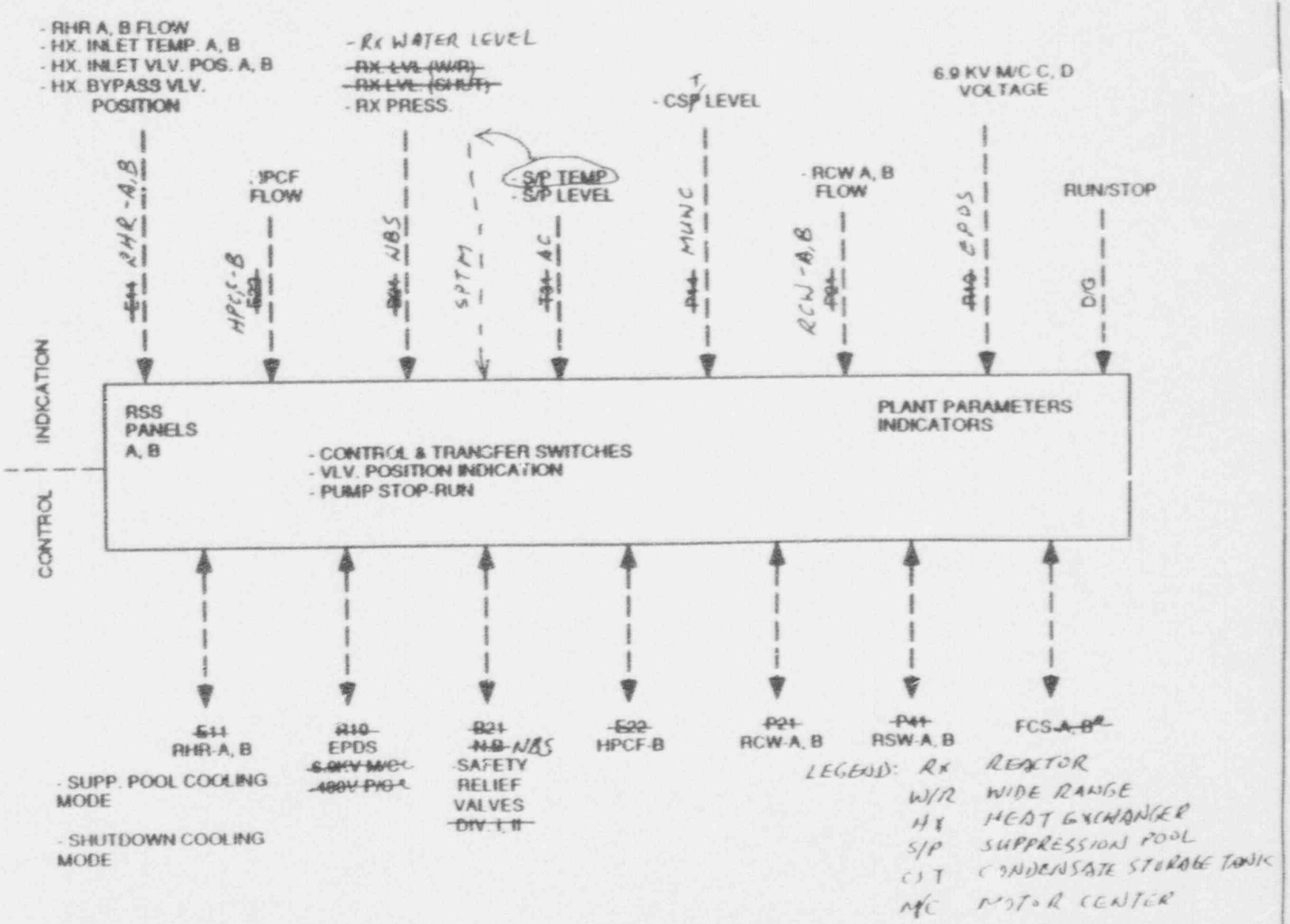


Figure 2.2.6 Rem[illegible] Shutdown System

HVAC EMERGENCY COOLING WATER SYSTEM

2.11.6

KEY SYSTEM FUNCTIONS:

SAFETY COOLING LOADS

IMPORTANT ELEMENTS OF DESIGN:

THREE INDEPENDENT LOOPS POWERED BY EMERGENCY POWER

EACH LOOP DELIVERS CHILLED WATER TO ESSENTIAL ELECTRICAL EQUIPMENT ROOMS AND DIESEL GENERATOR ZONE COOLERS; B AND C LOOPS SERVE MAIN CONTROL ROOM

SEISMIC CATEGORY 1 AND QUALITY GROUP C

REMOVE HEAT WITH ONE OF FOUR CHILLER/PUMPS IN B AND C IN STANDBY

HVAC EMERGENCY COOLING WATER SYSTEM

2.11.6

(CONTINUED)

STANDBY CHILLER/PUMP STARTS AUTOMATICALLY WHEN OPERATING CHILLER/PUMP TRIPS

CHILLER/PUMPS CAN BE CONTROLLED FROM MAIN CONTROL ROOM

ITAAC ENTRIES:

SYSTEM CONFIGURATION CONFIRMED

EACH LOOP MECHANICALLY AND ELECTRICALLY SEPARATED AND POWERED BY INDEPENDENT CLASS 1E SOURCES

STANDBY CHILLERS AND PUMPS START AUTOMATICALLY DURING TEST ON HIGH COOLING WATER TEMPERATURE, OPERATING CHILLER OR PUMP FAILURE AND MAIN CONTROL ROOM SIGNAL

CHILLER HEAT REMOVAL CAPACITY REVIEWED AND LOOP FLOW TESTED

2.11.6 HVAC Emergency Cooling Water System

Design Description

The HVAC Emergency Cooling Water (HECW) System delivers chilled water to the ~~control building~~ IN THE CONTROL BUILDIA essential electrical equipment room coolers, the diesel generator zone coolers, and the main control room coolers during shutdown of the reactor, normal operating modes, and abnormal reactor conditions including LOCA.

The HECW System consists of three mechanically separated divisions (Figure 2.11.6). Each division provides cooling to one control building essential electrical equipment room and one diesel generator zone. Either division "B" or "C" also provides cooling to the main control room. Power is supplied to each division from independent Class 1E sources.

HECW division "A" consists of one pump, one refrigeration unit, instrumentation, and distribution piping and valves to the cooling coils. Divisions "B" and "C" are similar except that two parallel pumps and refrigeration units are used. Surge tanks and condenser coolant flow are provided by the corresponding division of the (RCW) REACTOR BUILDING COOLING WATER system. A chemical addition tank is shared by all HECW divisions.

Makeup water is supplied from the makeup water (Purified) system at the surge tanks. The surge tanks are capable of replacing system water losses for more than 100 days during an emergency.

The refrigeration and pump units are designed to meet the following requirements:

(1) Refrigerator Capacity ~~(BTU/hr)~~ (kCal/hr) ~~2.9x10^6~~ 5.8×10^5

(2) Pump Capacity ~~(gpm)~~ (L/min) ~~256~~ 969

All major system components are located in the control building except for the diesel generator zone cooling coils, which are in the reactor building. There are no primary or secondary containment penetrations within the system. In addition, the system layout is designed to permit periodic in-service inspection of ~~all~~ system components ~~to assure the integrity and capability of the system~~.

Piping and valves for the HECW System, as well as the cooling water lines from the RCW System, are designed to Seismic Category I and ASME Code, Section III, Class 3 and Quality Group C requirements. The classification extends up to and including the block valves for the chemical addition tank. The only non-safety-related portion of the system is the chemical addition tank and the piping from the tank to the block valves.

The HECW System is capable of removing all heat loads with one of the four pump and refrigerator units from division "B" and "C" in standby. The standby refrigerator is equipped with an interlock which automatically starts the unit upon failure of the operating refrigerator. Flow switches prohibit the refrigerators from operating unless there is water flow through the evaporator and condenser. The refrigerator units can be controlled individually from the main control room by a remote manual switch.

The HECW System is designed to perform its required safe reactor shutdown cooling function following a postulated loss-of-coolant accident/loss of offsite power (LOCA/LOOP), assuming a single active failure in any mechanical or electrical division. In case of a failure which disables any one of the three HECW divisions, the other two divisions meet plant safe shutdown requirements.

Inspections, Tests, Analyses and Acceptance Criteria

Table 2.11.6 provides a definition of the inspections, tests, and/or analyses together with associated acceptance criteria which will be undertaken for the HECW System.

Table 2.11.6: HVAC Emergency Cooling Water (HECW) System

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. ~~The system configuration includes key components and flow paths as shown in Figure 2.11.6.~~ SEE 2.11.6 3a	1. ~~Inspection of construction records will be performed. Visual inspection (VI) will be performed based on Figure 2.11.6.~~ SEE 2.11.6 3a	1. ~~The system configuration conforms with Figure 2.11.6.~~ SEE 2.11.6 3a
2. ~~The HECW divisions are mechanically and electrically independent.~~ ~~The HECW divisions are powered by independent Class 1E sources.~~ SEE 2.11.6 3b	2. ~~Tests and VI of the divisions will include independent and coincident operation of the three divisions to demonstrate complete divisional separation. VI will check for independent Class 1E power sources.~~ SEE 2.11.6 3b	2. ~~Plant tests and VI confirm proper independence of each HECW division. VI confirm Class 1E power sources for each HECW division.~~ SEE 2.11.6 3b
3. The standby refrigerator and pump units automatically start ~~upon high~~ AT THE HIGH SET-POINT temperature cooling water or failure of the operating units. The refrigerator units can be controlled individually from the main control room.	3. Tests simulating high temperature cooling water and operating pump failure will be conducted for each refrigerator and pump unit in divisions "B" and "C". Tests simulating main control room switch signals will be conducted for the refrigerator units.	3. Refrigerator and pump units acting as standby units start upon a high temperature cooling water or operating pump failure signal. Refrigerator and pump units ~~are operable from~~ INSERT #1 main control room signals.
4. The HECW cooling capacity is capable of removing the heat loads on the system.	4. Inspections of vendor documentation will include refrigeration and pump capacities. Flow tests will confirm that adequate flow ARE ~~is~~ available to the system. INSERT #2	4. Each refrigeration unit shall have an effective heat removal capacity of $\geq 5.8 \times 10^6$ kCal/hr ~~2.3 x 10^6 Btu/hr~~ at ~~256 gpm~~ ≥969 lpm. Each pump is capable of delivering ~~256 gpm~~ ≥969 lpm to the system.

INSERT #1: OPERATE UPON RECIEPT OF
INSERT #2: AND HEAT REMOVAL

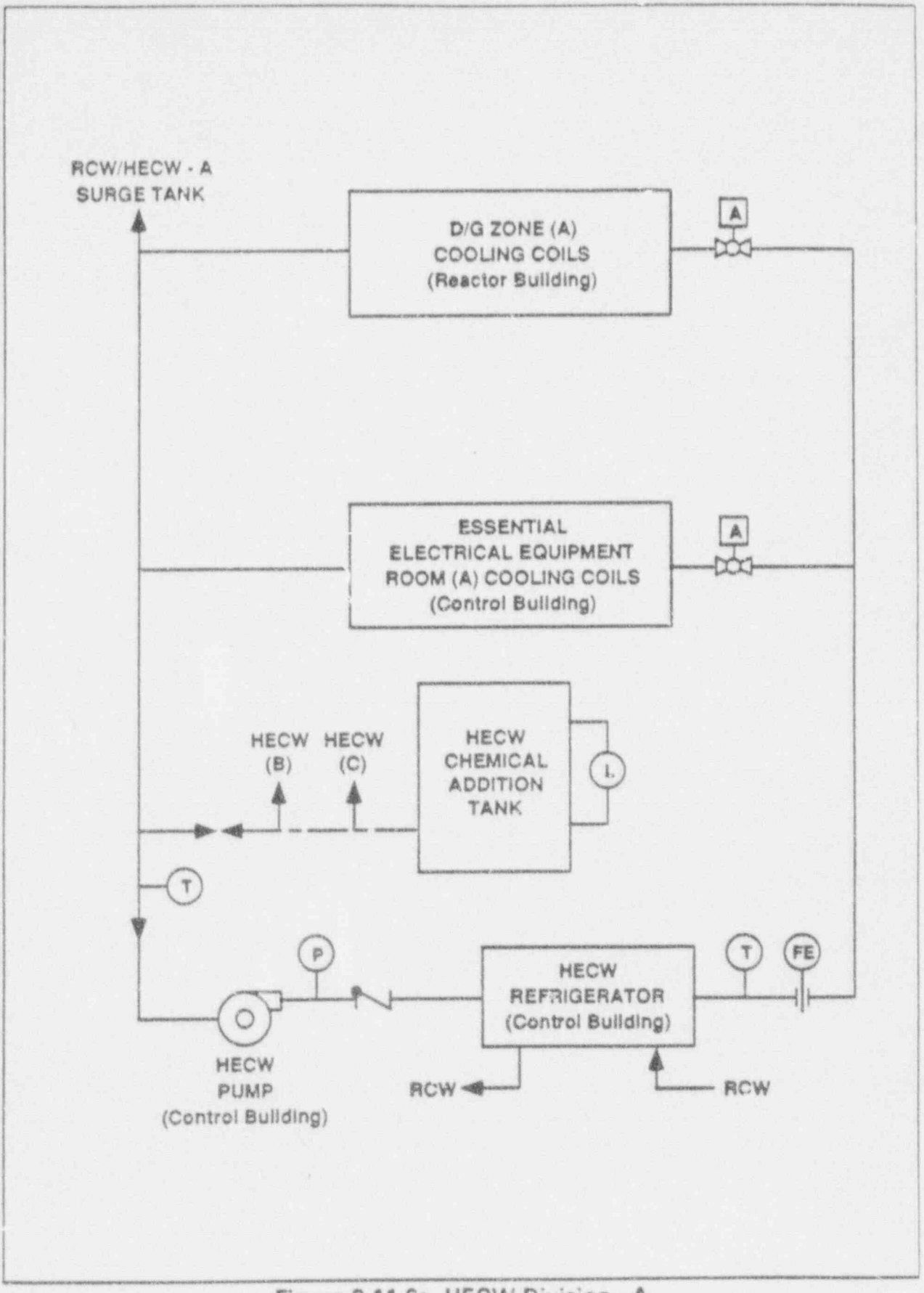


Figure 2.11.6a HECW Division - A

Table 2.11.6: HVAC Emergency Cooling Water (HECW) System

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. ~~The system configuration includes key components and flow paths as shown in Figure 2.11.6.~~ SEE 2.11.6 3a	1. ~~Inspection of construction records will be performed. Visual inspection (VI) will be performed based on Figure 2.11.6.~~ SEE 2.11.6 3a	1. ~~The system configuration conforms with Figure 2.11.6.~~ SEE 2.11.6 3a
2. ~~The HECW divisions are mechanically and electrically independent.~~ ~~The HECW divisions are powered by independent Class 1E sources.~~ SEE 2.11.6 3b	2. ~~Tests and VI of the divisions will include independent and coincident operation of the three divisions to demonstrate complete divisional separation. VI will check for independent Class 1E power sources.~~ SEE 2.11.6 3b	2. ~~Plant tests and VI confirm proper independence of each HECW division. VI confirm Class 1E power sources for each HECW division.~~ SEE 2.11.6 3b
3. The standby refrigerator and pump units automatically start ~~upon high~~ AT THE HIGH SET-POINT temperature cooling water or failure of the operating units. The refrigerator units can be controlled individually from the main control room.	3. Tests simulating high temperature cooling water and operating pump failure will be conducted for each refrigerator and pump unit in divisions "B" and "C". Tests simulating main control room switch signals will be conducted for the refrigerator units.	3. Refrigerator and pump units acting as standby units start upon a high temperature cooling water or operating pump failure signal. Refrigerator and pump units ~~are operable from~~ INSERT #1 main control room signals.
4. The HECW cooling capacity is capable of removing the heat loads on the system.	4. Inspections of vendor documentation will include refrigeration and pump capacities. Flow tests will confirm that adequate flow ARE ~~is~~ available to the system.	4. Each refrigeration unit shall have an effective heat removal capacity of ~~2.3×10^6 Btu/hr at 256 gpm~~ $\leq 5.8 \times 10^6$ kCal/hr at 969 lpm. Each pump is capable of delivering ~~256 gpm~~ ≤ 969 lpm to the system. INSERT #2

INSERT #1: OPERATE UPON RECIEPT OF

INSERT #2: AND HEAT REMOVAL

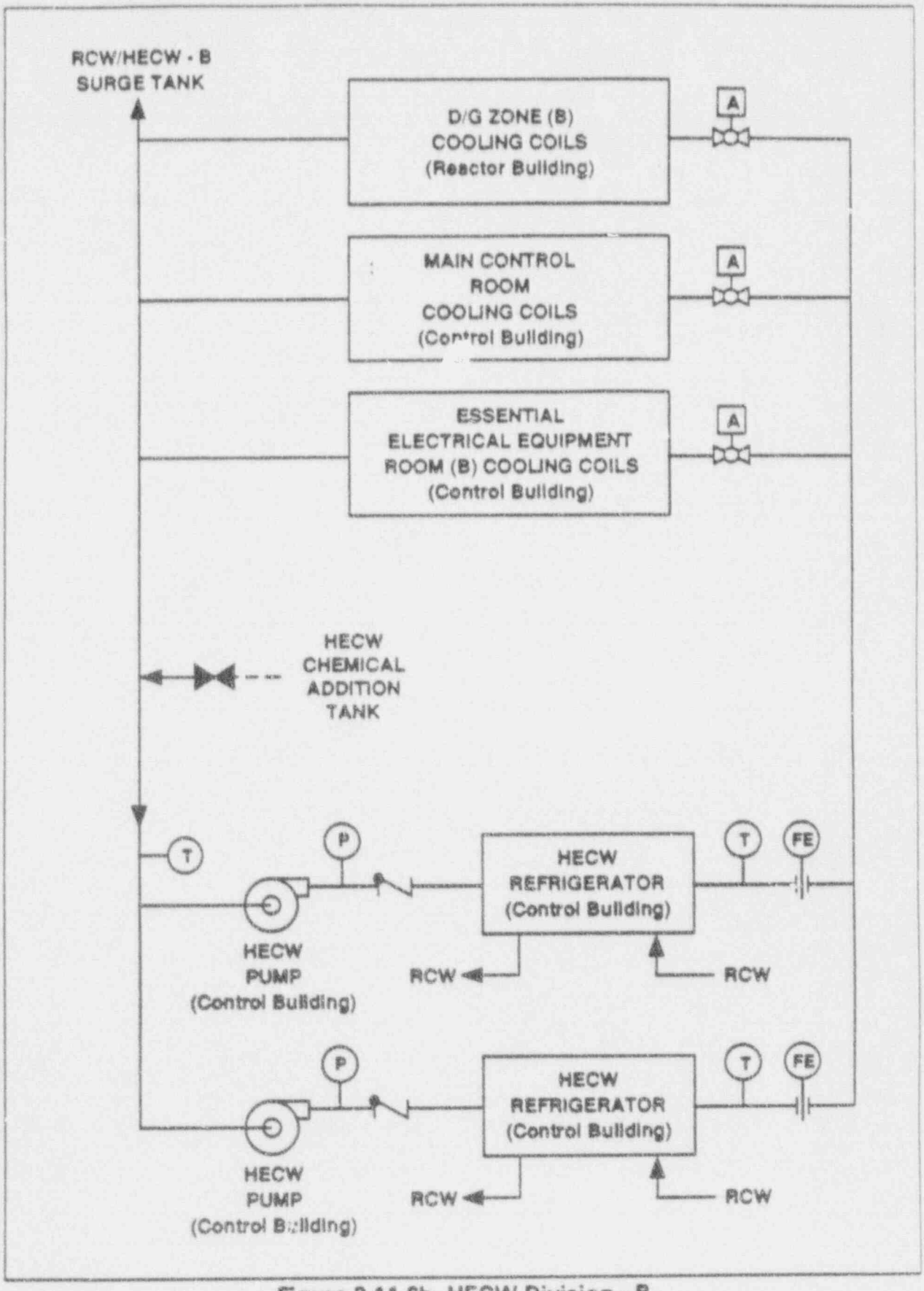


Figure 2.11.6b HECW Division - B

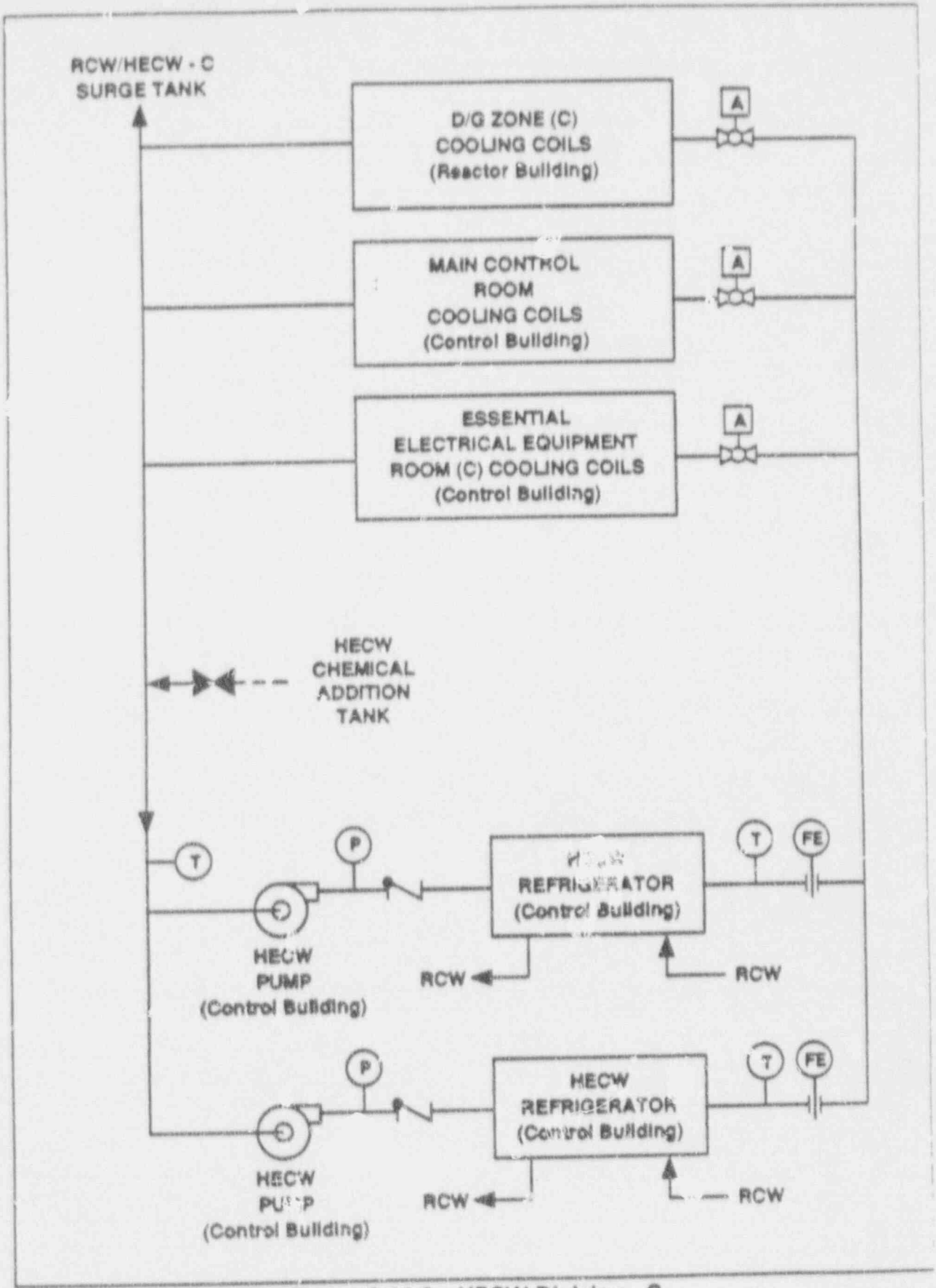


Figure 2.11.6c HECW Division C

2.11.6

ADDENDUM TO 2.11.6

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. A simplified configuration for the HECW System is described in Section 2.11.6.	1. Construction records will be reviewed and visual inspections will be conducted for the configuration of the HECW System.	1. The as-built configuration of the HECW System is in accordance with the description in Section 2.11.6.
Portions of the _____ System are classified as ASME Code class as indicated in Section _____. They are designed, fabricated, installed, and inspected in accordance with the ASME Code, Section III.	ASME Code Data Reports will be reviewed and inspections of Code stamps will be conducted for ASME components in the _____ System.	Those portions of the _____ System identified as ASME Code class in Section _____ have ASME Code Section III, Code Data Reports and Code stamps (or alternative markings permitted by the Code).
The ASME portions of the _____ System retain their integrity under internal pressures that will be experienced during service.	A hydrostatic test of the ASME portions of the _____ System will be conducted.	The results of the hydrostatic test of the ASME portions of the _____ System conform with the requirements in the ASME Code, Section III.
Control room indicators are provided for _____ System parameters defined in Section _____.	Inspections will be performed to verify the presence of control room indicators for the _____ System.	Instrumentation is present in the Control room as defined in Section _____.
The _____ System operates when powered from either normal off-site or emergency on-site sources.	_____ System functional tests shall be performed to demonstrate operation when supplied by either normal off-site power or the emergency diesel generator(s).	_____ System operates when supplied by either normal off-site sources or the emergency diesel generators.

TABLE:T1AAC30

ADDENDUM TO 2.11.6

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2. Each ~~loop~~ DIVISION of the HECW System is mechanically and electrically separate. THE HECW DIVISIONS ARE POWERED BY INDEPENDENT CLASS 1E SOURCES.	2. Construction records will be reviewed and visual inspections will be performed of the mechanical and electrical separations DIVISIONS of the HECW ~~loops~~, AND THEIR POWER SOURCES.	2. Any room outside the primary containment does not contain components from more than one ~~loop~~ DIVISION of the HECW System. Each ~~loop~~ DIVISION of the HECW System is supplied by electrical power from only one division of electrical power, and this division is different from the divisions supplying the other ~~loops~~ DIVISIONS of the HECW System.
The ~~pumps~~ have sufficient NPSH.	An analysis for NPSH will be prepared based upon the as-built data and vendor pump records. This analysis will be based upon - pressure losses for pump inlet piping and components - suppression pool water level at the minimum value - 50% blockage of pump suction strainers - design basis fluid temperature (100°C) - containment pressure of 1.03 kg/cm^2a	The analyzed NPSH exceeds pump NPSH required by the vendor for the pump. THE HECW DIVISIONS ARE POWERED BY INDEPENDENT CLASS 1E SOURCES.

2.11.6 - 3b -

GE Nuclear Energy

Human Factors Engineering ITAAC/DAC

Presentation to

NUMARC/NRC

M. A. Ross
September 22, 1992

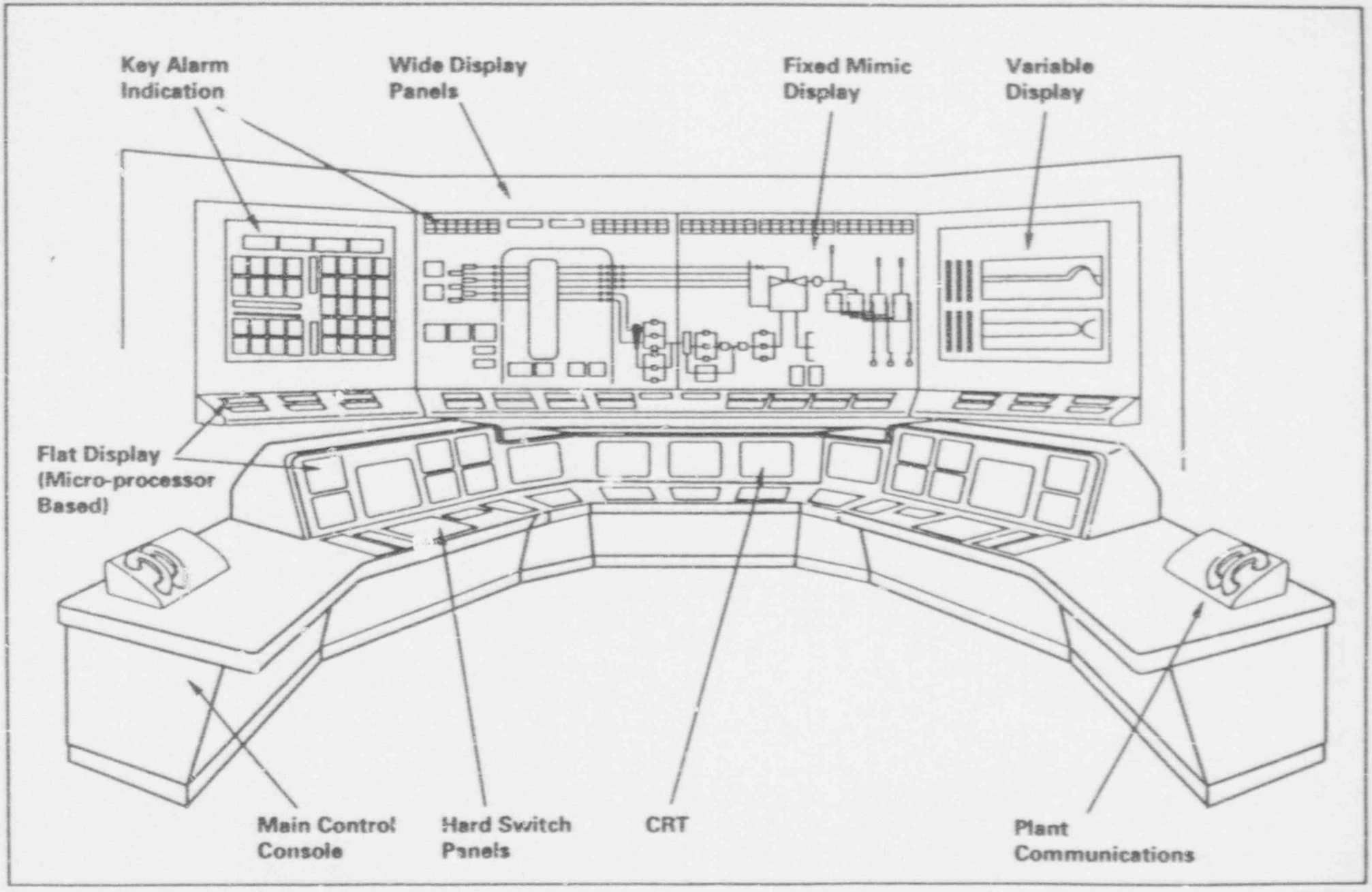
Discussion Material

- Background
  - URD Chapter No. 10 (M-MIS)
  - ABWR Design Certification
- ITAAC/DAC
  - Revised Text
  - NRC Comment Resolutions

Paragraph No.	Requirement	Rev.
2.2	**ALWR M-MIS POLICY STATEMENT**	0
	Policy statements provide overall direction and guidance and form the basis for many of the requirements in the following sections. The policy statements are intended to give the reader a summary view of the direction to be taken in the requirements which follow Section 2.	0
2.2.1	**M-MIS Systems Approach**	0
	The M-MIS will employ modern digital technology to implement the monitoring, control and protection functions for the ALWR. Robust system design, including segmentation of major functions, separation of redundant equipment within a segment, and fault tolerant equipment will be used to achieve high reliability and protection against the propagation of failures. Application of signal validation to selected parameters will be used to assure the operators have data of high quality and reliability. Where it is appropriate and demonstrated, multiplexed data communications will be used for any function, including safety functions, to reduce the cost and complexity of the instrumentation and control cable runs throughout the plant. The high accuracy and drift free operation of the digital systems will reduce the overall maintenance calibration burden. Where appropriate, the use of fiber optic cables for data transmission will be used to provide high data transmission rates with electrical isolation and protection from electromagnetic interference at reduced costs.	0
	Standardization of hardware and software and modularity of design will be used to simplify maintenance and provide protection against obsolescence. Built-in test features are to be provided to perform continuous self-diagnosis of digital hardware and communication paths and annunciate detected failures. Built-in test features will provide computer-aided, periodic functional testing capabilities that automatically verify system functionality once they are manually initiated, locate failures upon detection, and record test results. Most M-MIS equipment is to be located in compartments with controlled environments, maintained by reliable HVAC systems. All M-MIS equipment will be selected to be compatible with its environment under normal conditions and under casualty conditions as appropriate to meet functional requirements.	0

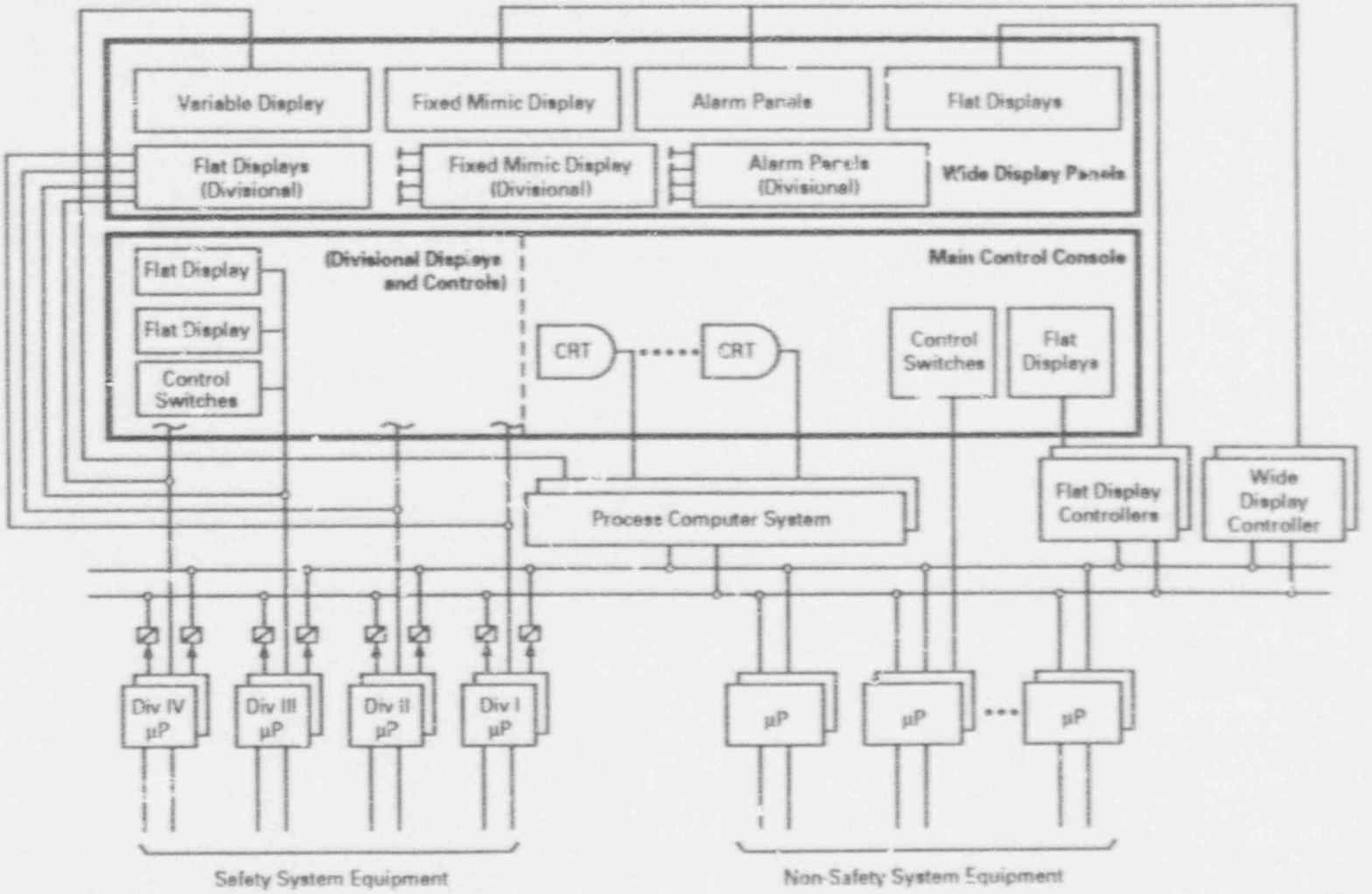
Paragraph No.	Requirement	Rev.
2.2.2	**Design Process**	0
	The M-MIS design process will be directed by a single organization responsible for the entire M-MIS design, will be carried out by a multi-disciplined design team and shall include direct Plant Owner involvement, including engineering and maintenance personnel and operations staff familiar with plant normal, abnormal, and emergency operating procedures. The process forces coordination of the design by ensuring the M-MIS design team and the plant systems designers work together and take into account operation/maintenance inputs. The design process also calls for integration of human factors considerations into the design effort, including the use of mockups and simulations early in the design to evaluate specific design features and choices and support iterative design development and validation. In addition, a continuous verification and validation effort is performed in parallel to the design by an independent team (see Section 3.1.4) particularly in the difficult software area to assure the final product meets the requirements, and is robust and resistant to inadvertent errors. Formal documentation of the M-MIS design is achieved by including it in the plant-wide design documentation and configuration control process.	3
2.2.3	**Reliability Inherent in Design**	0
	The M-MIS design should possess sufficient defense against the propagation of faults through segmentation, independence and other measures so that a failure or upset in one plant control function cannot propagate to other plant control functions and thereby overburden the operators due to complex transient events. Further, the M-MIS design should be sufficiently robust to prevent a single random failure of M-MIS equipment from causing a forced outage. This is expected to require, for example, multiple computers as well as extensive use of distributed microprocessors. The emphasis is to be on assuring that failures are accommodated gracefully, operators will not become over-burdened, and no loss of essential capability results.	1
2.2.4	**Testing of M-MIS**	1
	Significant improvements in the area of system testing are to be provided with the ALWR M-MIS design. Accordingly, the equipment should be designed and configured to readily support in-service testing by incorporating good human factors principles, avoiding the use of undesirable features such as addition of test jumpers or lifting of leads, and providing built-in test features, including self diagnostics for continuous on-line testing and automated functional testing for periodic surveillance testing.	0

Key Feaures of Advanced BWR Control Room Designs



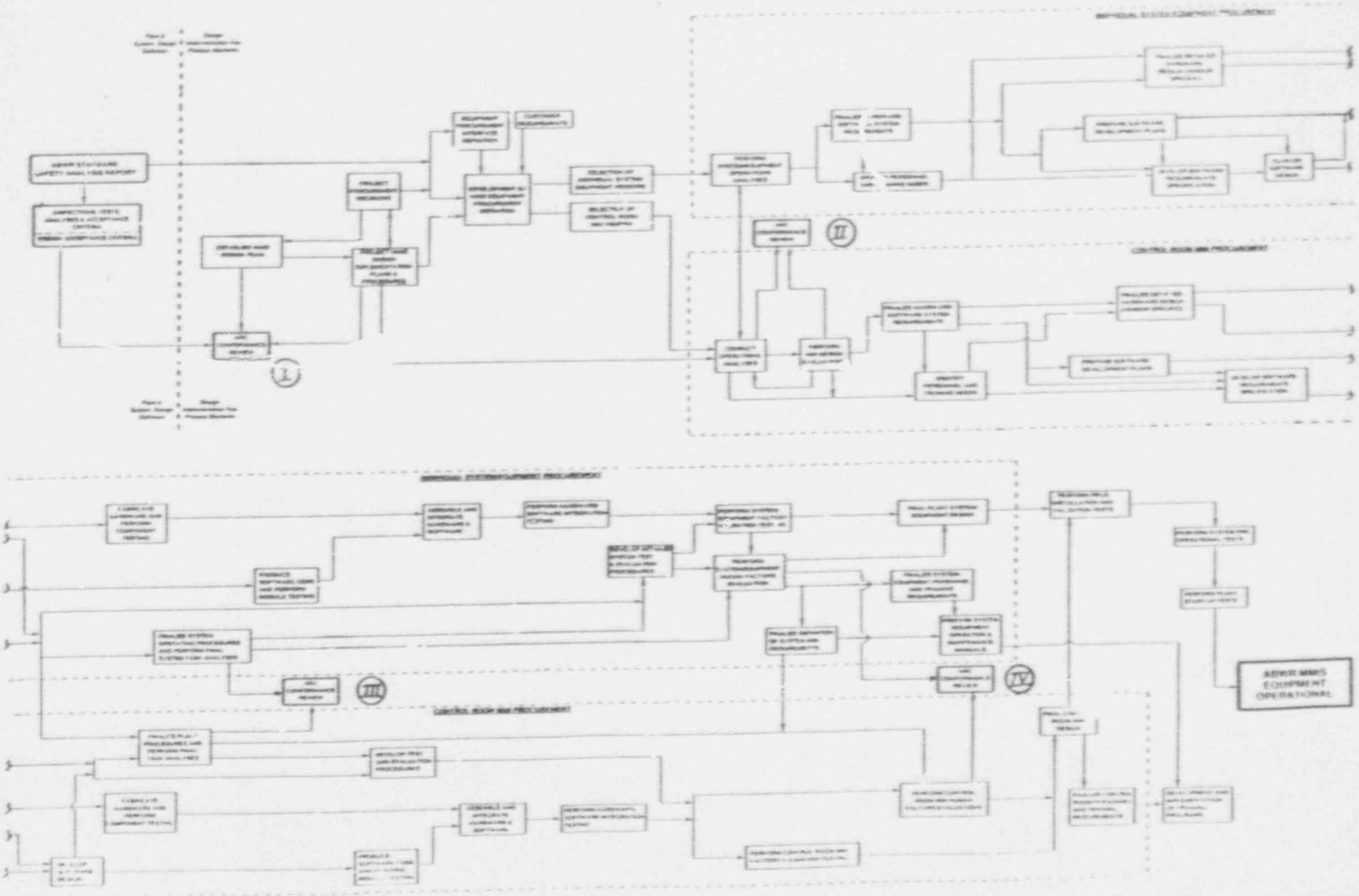
M20252-2

Configuration of Operator Interface System



M20545

ABWR DESIGN IMPLEMENTATION PROCESS (TYPICAL)



Establish the HFE Team and Plans

- (I) First HFE Conformance Review
  - HFE Design Team Composition (1a)
  - HFE Program Plan (1b)
  - System Functional Requirements Analysis Implementation Plan (2a)
  - Allocation of Function Implementation Plan (3a)
  - Task Analysis Implementation Plan (4a)
  - Human-System Interface (HSI) Design Implementation Plan (5a)
  - Plant and Emergency Operating Procedure Development Implementation Plan (6a)
  - Human Factors Verification and Validation (V&V) Implementation Plan (7a)

Implement the Design Per the Plans

- (II) Second HFE Conformance Review
  - Function Requirements Analyses (2b)
  - Function Allocation (3b)
  - Task Analyses (4b)

- (III)Third HFE Conformance Review
  - HSI Design Implementation (5b)
  - Plant and Emergency Operating Procedure Development (6b)

- (IV) Fourth and Final HFE Conformance Review
  - Verification and Validation (7b)

AN HFE PROGRAM PLAN SHALL BE ESTABLISHED BY THE HFE DESIGN TEAM TO ASSURE PROPER DEVELOPMENT, EXECUTION, OVERSIGHT AND DOCUMENTATION OF THE HFE PROGRAM. THE HFE PROGRAM, DEVELOPED BY THE

3.6 Human Factors Engineering

Design Description

The ABWR certified design's primary human-system interfaces (HSI) will be developed, designed, and evaluated based upon a ~~structured top-down~~ human factors systems analysis and shall reflect ~~state-of-the-art~~ human factors principles. The HSI scope will include operations, maintenance, test, and inspection interfaces, operations technical procedures, and training needs of the Main Control Room and Remote Shutdown System functions and equipment.

~~To assure integration of Human Factors Engineering (HFE) into the plant system design,~~ the HSI design effort will be directed by a multi-disciplinary HFE Design Team comprised of personnel with expertise in HFE and in other technical areas relevant to the HSI design, evaluation and operations. ~~The~~ HFE Design Team will establish the methods which will implement the HSI design through the process as shown in Figure 3.6-1. Implementation of that pr. will be as follows:

a. (X) Plant System requirements will be analyzed to identify those functions which must be performed to satisfy the objectives of each functional area. System function analysis shall determine the objective, performance requirements, and constraints of the design; and establish the functions which must be accomplished to meet the objectives and required performance.

b. (X) ~~To facilitate an allocation of functions to the human which capitalize upon areas of human strengths and avoids areas of human limitations, a structured and well documented~~ methodology of allocating functions to personnel, system elements, and personnel-system combinations will be established and implemented.

c. (X) Task analysis will be conducted and used to identify the behavioral requirements of the tasks the personnel subsystem is required to perform in order to achieve the functions allocated to them. A task will be a group of activities that have a common purpose, often occurring in temporal proximity, and which utilize the same displays and controls. The task analysis will be used to maintain human performance requirements within human capabilities; be used as an input for developing personnel skill, personnel training, and system communication requirements and as an input to the evaluation of established plant operations control room staffing levels; and form the basis for specifying the requirements for the displays, data processing and controls needed to carry out tasks.

PLANT PROCEDURES

d (4) Human engineering principles and criteria will be applied in the design definition and evaluation of the Human-System Interface (HSI).

e (5) Plant and emergency operating technical procedures will be developed to support and guide human interaction with plant systems and to support and guide human interactions in the control of plant operations. Human engineering principles and criteria shall be applied in the procedures development.

f (6) Through the human factors verification and validation activities, the HSI design will be evaluated as an integrated system using HFE evaluation procedures, guidelines, standards, and principles.

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.6 provides a definition of the inspections, tests, and/or analyses (together with associated acceptance criteria) which will be performed to demonstrate compliance with the HFE commitments for the certified design.

Table 3.6: Human Factors Engineering

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
1. Human-system interfaces (HSI) shall be developed, designed, and evaluated based upon ~~a structured top-down~~ human factors systems analysis and shall reflect ~~state-of-the-art~~ human factors principles. The HSI shall include operations, maintenance, test, and inspection interfaces, operations technical procedures, and training needs of the main control room and remote shutdown system functions and equipment.	~~1. To assure the integration of HFE into plant system (i.e., system) development:~~ 1.a. A HFE Design Team shall be established; and	1.a. The HFE design team shall ~~include~~ BE COMPRISED OF the following expertise: (1) Technical Project Management (2) Systems Engineering (3) Nuclear Engineering (4) Control and Instrumentation Engineering (5) Architect Engineering (6) Human Factors (7) Plant Operations (8) Computer Systems Engineering (9) Plant Procedure Development (10) Personnel Training
	1.b. A HFE Program Plan shall be established to assure the proper development, execution, oversight, and documentation of the human factors engineering program.	1.b The Human Factors Engineering (HFE) Program Plan shall establish: (1) Human-System Interface (HSI) design and evaluation methods and criteria which are consistent with accepted HFE practices and principles. (2) The primary objectives of the HFE Program shall ~~include, at the minimum, the objective~~ to develop an HSI which makes possible safe, efficient, and reliable operator performance.

TABLE 18.E.2.1 HUMAN FACTORS ENGINEERING DESIGN TEAM AND PLANS

1. (Satisfaction of the requirements presented herein shall result in the creation of a Human Factors Engineering Program Plan which is in full compliance with the Item 1.b. Acceptance Criteria presented in Table 3.6 of the Tier 1 Design Certification material for the GE ABWR design). The Human Factors Engineering (HFE) Program Plan shall establish:

   a. Methods and criteria, for the development and evaluation of the Main Control Room (MCR) and Remote Shutdown System (RSS) HSI which are consistent with accepted HFE practices and principles. Within the defined scope and content of the HFE Program Plan, accepted HFE methods and criteria are presented in the following documents:

      (i) AR 602-1, Human Factors Engineering Program, 1983, (Dept. of Defense)

      (ii) DI-HFAC-80740, Human Engineering Program Plan, 1989, (Dept. of Defense)

      (iii)DOD-HDBK-763, Human Engineering Procedures Guide, Chapters 5-7 and Appendices A and B, 1991, (Dept. of Defense)

      (iv)EPRI NP-3659, Human Factors Guide for Nuclear Power Plant Control Room Development, 1984, (Electric Power Research Institute)

      (v) IEEE Std. 1023-1988, IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations, 1988, (IEEE)

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

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

      (viii)NUREG-0737, Clarification of TMI Action Plan Requirements (Item I.C.5, "Feedback of Operating Experience to Plant Staff"), 1983, (U. S. Nuclear Regulatory Commission)

      (ix)NUREG-0899, Guidelines for the Preparation of Emergency Operating Procedures, 1982, (U. S. Nuclear Regulatory Commission)

      (x) NUREG/CR-3331, A Methodology for Allocating Nuclear Power Plant Control Functions to Human and Automated Control, 1983, (U. S. NRC)

      (xi)TOP 1-2-610, Test Operating Procedure - Part 1, 1990, (Dept. of Defense)

   Note that within the set of documents listed above, differences may exist regarding specific methods and criteria applicable to the HFE Program Plan. In situations that such differences exist, all of the methods and criteria presented within those documents are considered to be equally appropriate and valid and, therefore, any of the above listed documents may be selected as the basis for elements of the HFE Program.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
1. Continued	1.b.Continued	(3) The goals of the HFE Program which shall be ~~stated in "operator-centered" terms and serve as criteria for test and evaluation activities. These "operator-centered" HFE design goals shall include:~~ : (i) The operating team can accomplish ~~all~~ assigned tasks within system defined time and performance criteria. (ii) The system and allocation of functions will provide acceptable workload levels and facilitate operator vigilance. (iii) The system will ~~support a high degree of~~ operating crew "situation awareness." INCREASE (iv) Signal detection and event recognition requirements will be kept within the operators' information processing limits and will ~~minimize~~ the need for operators to mentally transform data in order to be usable REDUCE (v) The system will ~~minimize~~ operator memory ~~load.~~ REDUCE THE NEED FOR (vi) The operator interfaces will ~~minimize~~ the potential for operator error. REDUCE

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
1. Continued	1.b.Continued	(4) HSI design and evaluation scope which consists of the Main Control Room and Remote Shutdown System operations,maintenance, test, and inspection interfaces,operating technical procedures, and identification of personnel training needs. (5) The HFE Design Team as being responsible for: (i) the development of HFE plans and procedures; (ii) the oversight and review of HFE design, development, test, and evaluation activities; (iii) the identification, recommendation, and provision of solutions through designated channels for problems identified in the implementation of the HFE activities; (iv) verification of implementation of ~~team recommendations~~ SOLUTIONS TO PROBLEMS; (v) assurance that all HFE activities comply to the HFE plans and procedures, and (vi) scheduling of activities and milestones.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
1. Continued	1.b.Continued	(6) The HFE Design Team having the authority and organizational freedom to accomplish its responsibilities. The team shall have the authority to determine where its input is required and to access work areas, and design documentation. The Team shall have the authority to control further processing,delivery, installation or use of HFE/HSI products until the disposition of a non-conformance, deficiency or unsatisfactory condition has been achieved.
		(7) An HFE issue tracking system which monitors the identification and closure of human factors issues. The HFE issue tracking system shall document and track human factors engineering issues and concerns, from identification until elimination or reduction to a level acceptable to the HFE Design Team.
		(8) The Design Control procedures through which the results of the iterative design development activities are documented and processed to maintain integration of design activities and assure that the design, design analyses and documentation are consistent and ~~appropriately~~ reflect the details of design implementation decisions.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
2. Plant System requirements shall be analyzed to identify those functions which must be performed to satisfy the objectives of each functional area. System function analysis shall determine the objective, performance requirements, and constraints of the design; and (2) establish the functions which must be accomplished to meet the objectives and required performance.	2.a. A System Functional Requirements Analysis Implementation Plan shall be developed to assure that the analysis is conducted according to accepted HFE principles.	2.a. The System Functional Requirements Analysis Implementation Plan shall establish: (1) Methods and criteria for conducting the System Functional Requirements Analysis which are consistent with accepted HFE practices and principles. (2) That system requirements shall define the system functions and those system functions shall provide the basis for determining the associated HSI performance requirements. (3) That critical functions shall be defined (i.e., those functions required to achieve major system performance requirements; or those functions which, if failed, could pose a safety hazard to plant personnel or to the general public).

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
2. Continued	2.a. Continued	(4) That safety functions shall be identified along with any functional interrelationship those safety functions may have with non-safety systems.
		(5) that functions shall be defined as the most general, yet differentiable means whereby the system requirements are met, discharged, or satisfied. Functions shall be arranged in a logical sequence so that any specified operational usage of the system can be traced in an end-to-end path.
		(6) That functions shall be described initially in graphic form. Function diagramming shall be done starting at a "top level", where major functions are described, and continuing to decompose major functions to lower levels until a specific critical end item requirement emerges, e.g., a piece of equipment, software, or an operator

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
2. Continued	2.a. Continued	6 pf) That detailed narrative descriptions shall be developed for each of the identified functions and for the overall system configuration design itself. Each function shall be identified and described in terms of inputs (observable parameters which will indicate system status) functional processing (control process and performance measures required to achieve the function), functional operations (including detecting signals, measuring information, comparing one measurement with another, processing information, and acting upon decisions to produce a desired condition or result such as a system or component operation actuation or trip) outputs, feedback (how to determine correct discharge of function), and interface requirements from the top down so that subfunctions are recognized as part of larger functional elements.
	2.b. An analysis of system functional requirements shall be conducted in accordance with the System Functional Requirements Analysis Implementation Plan and the findings will be documented in System Functional Require ments Analysis Results Report. The analyses of the system functional requirements shall be reviewed by the HFE Design Team and shall be documented in System Functional Requirements Analysis Evaluation Report.	2.b. The system functional requirements analyses shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the System Functional Requirements Analysis Implementation Plan.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
3. ~~To facilitate an allocation of functions to the human which capitalize upon areas of human strengths and avoid areas of human limitations, a structured and well-documented~~ A methodology of allocating functions to personnel, system elements, and personnel-system combinations shall be established and implemented.	3.a. An Allocation of Function Implementation Plan shall be developed to assure that the allocation of function is conducted according to accepted HFE principles.	3.a. The Allocation of Function Implementation Plan shall establish: (1) The methods and criteria for the execution of function allocation which are consistent with accepted HFE practices and principles. (2) That ~~all~~ aspects of system and functions definition shall be analyzed in terms of resulting human performance requirements based on the expected user population. (3) That the allocation of functions to personnel, system elements, and personnel-system combinations shall reflect: (i) sensitivity, precision, time, and safety requirements, (ii) ~~required~~ reliability of system performance, and (iii) the number and the necessary skills of the personnel required to operate and maintain the system. THAT (4) The allocation criteria, rationale, analyses, and procedures shall be documented.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
3. Continued	3.a. Continued	(5) Analyses shall confirm that the personnel elements can correctly perform tasks allocated to them while maintaining operator situation awareness, acceptable personnel workload, and facilitating personnel vigilance.
	3.b. An analysis of the allocation of function shall be conducted in accordance with the Allocation of Function Implementation Plan and the findings will be documented in an Allocation of Function Analysis Results Report. The analyses of the allocation of function shall be reviewed by the HFE Design Team and the results of that review shall be documented in an Allocation of Function Evaluation Report.	3.b. The function allocation analyses shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the Allocation of Functions Implementation Plan.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
4. Task analysis shall be conducted and used to identify the behavioral requirements of the tasks the personnel subsystem is required to perform in order to achieve the functions allocated to them. A task shall be a group of activities that have a common purpose, often occurring in temporal proximity, and which utilize the same displays and controls. The task analysis shall be used to maintain human performance requirements within human capabilities; be used as an input for developing personnel skill, personnel training, and system communication requirements and as an input to the evaluation of established plant operations control room staffing levels; and form the basis for specifying the require-ments for the displays, data processing and controls needed to carry out tasks.	4.a. A Task Analysis Implementation Plan shall be developed to assure that the analysis is conducted according to accepted HFE principles.	4.a. The Task Analysis Implementation Plan shall establish: (1) The methods and criteria for conduct of the task analyses which are consistent with accepted HFE practices and principles. (2) The scope of the task analysis which shall include ~~all~~ operations performed at the operator interface in the main control room and at the remote shutdown system. The analyses shall be directed to the ~~full~~ range of plant operating modes, including startup, normal operations, abnormal operations, transient conditions, low power and shutdown conditions. The analyses shall also address operator interface operations during periods of maintenance test and inspection of plant systems and equipment and of the HSI equipment. (3) That the analysis shall link the identified and described tasks in operational sequence diagrams. The task descriptions and operational sequence diagrams shall be used to identify which tasks are "critical" in terms of importance for function achievement, potential for human error, and impact of task failure. Human actions which are found to affect plant risk in PRA sensitivity analyses shall also be considered "critical."

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
4. Continued	4.a. Continued	THAT (4) Task analysis shall begin with the development of ~~detailed~~ narrative descriptions of the personnel activities required for successful completion of the tasks. ~~Task analyses~~ AND shall define the input, process, and output required by and of personnel. THAT (5) The task analysis shall be in detail sufficient enough to identify information and control requirements such that requirements for alarms, displays, data processing, and controls for human task accomplishment may be specified. THAT (6) The task analysis results shall be made available as input to the personnel training programs.
	4.b. An analysis of tasks shall be conducted in accordance with the Task Analysis Implementation Plan and the findings will be documented in a Task Analysis Results Report. The task analyses shall be reviewed by the HFE Design Team and the results of that review shall be documented in a Task Analysis Evaluation Report.	4.b. The task analyses shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the Task Analysis Implementation Plan.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
5. Human engineering principles and criteria shall be applied in the design definition and evaluation of the Human-System Interface (HSI).	5.a. A Human-System Interface (HSI) Design Implementation Plan shall be developed to assure that human factors analyses of the HSI Design are conducted according to accepted HFE principles.	5.a. The HSI Design Implementation Plan shall establish: (1) The methods and criteria for HSI equipment design; and evaluation of HSI human performance, equipment design and associated workplace factors; which are consistent with accepted HFE practices and principles. 2) That the HSI design shall implement the information and control requirements developed through the task analyses, including the displays, controls and alarms necessary for the execution of those tasks identified in the task analyses as being critical tasks. (3) The methods ~~which will assure~~ For Assurance that the HSI human performance, equipment design and associated workplace factors are consistent with those modeled and evaluated in the completed task analysis. (4) That the HSI design shall not incorporate ~~any~~ equipment (i.e., hardware or software function)which has not been specifically evaluated in the task analysis.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
5. Continued	5.a Continued	(5) The HSI design criteria and guidance for control room operations during periods of maintenance, test and inspection of control room HSI equipment and of other plant equipment which has control room personnel interface. (6) The test and evaluation methods for resolving HFE/HSI design issues. These test and evaluation methods shall include the criteria to be used in selecting HFE/HSI design and evaluation tools which: (i) may incorporate the use of static mockups and models for evaluating access and workspace related HFE issues, and (ii) shall require dynamic simulations and HSI prototypes for conducting evaluations of the human performance associated with the activities in the critical tasks identified in the task analysis.
	5.b. An analysis of the human system interface design shall be conducted in accordance with the HSI Design Implementation Plan and the findings will be documented in an a HSI Design Implementation Analysis Results Report. The analyses of the HSI Design Implementation shall be reviewed by the HFE Design Team and the results of that review shall be documented in an HSI Design Implementation Evaluation Report.	5.b. The Human System Interface (HSI) Design Analyses shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the HSI Design Implementation Plan.

Table 3.6. Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
6. Plant and Emergency Operating Procedures shall be developed to support and guide human interaction with plant systems and to support and guide human interactions in the control of plant operations. Human engineering principles and criteria shall be applied in the procedures development.	6.a. A Plant and Emergency Operating Procedure Development Implementation Plan shall be developed to assure that the development of the Plant and Emergency Operating Procedures is conducted according to accepted HFE principles.	6.a. The Plant and Emergency Operating Procedure Development Implementation Plan shall establish: (1) That operator actions identified in the task analysis shall be used as the basis for specifying the procedures for operations. (2) That the procedures to be developed shall address normal, abnormal, and emergency plant operations including consideration of plant operations during periods when plant systems/equipment and primary operator interface (i.e., main control room) equipment is undergoing, test, maintenance or inspection. (3) Methods and criteria for development of the operating technicalprocedures which are consistentwith accepted HFE practices and principles. (4) That a Writer's Guide shall be developed which establishes the process for developing the technical procedures for normal plantand system operation, abnormal plant operations, emergency plant operations and for responding to plant alarm conditions. The Writer's Guide shall contain objective criteria which will require that the operations technical procedures developed are consistent in organization, style, content and usage of terms

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
6.a. Continued	6.b. The Plant and Emergency Operating Procedures shall be developed in accordance with the Plant and Emergency Operating Procedure Development Implementation Plan and the results will be documented in a Plant and Emergency Operating Procedure Development Report. The Plant and Emergency Operating procedure development results shall be reviewed by the HFE Design Team and the results of that review shall be documented in a Plant and Emergency Operating Procedure Development Evaluation Report.	6.b. The development of the plant operations technical procedures shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the Plant and Emergency Operating Procedure Development Implementation Plan.
7. The HSI design shall be evaluated as an integrated system using HFE evaluation procedures, guidelines, standards, and principles.	7.a. A Human Factors Verification and Validation Implementation Plan shall be developed to assure that the evaluation of the integrated HSI Design is conducted in accordance with accepted HFE principles.	7.a. The Human Factors Verification and Validation (V&V) Implementation Plan shall establish: (1) Human factors V&V methods and criteria which are consistent with accepted HFE practices and principles. (2) The methods and evaluation criteria ~~which are consistent with accepted HFE practices~~ and principles FOR CONFIRMING THAT THE PERFORMANCE OF THE INTEGRATED HSI MEETS THE HFE DESIGN GOALS AS ESTABLISHED IN THE HFE PROGRAM PLAN.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7.a. Continued	(3) The scope of the evaluations of the integrated HSI shall include: (i) The Human-System Interface (including both the interface of the operator with the HSI equipment hardware and the interface of the operator with the HSI equipment's software driven functions) (ii) The plant and emergency operating technical procedures, and (iii) The overall HSI work environment (4) That static and/or "part-task" mode evaluations of the HSI equipment shall be conducted to confirm that the controls, displays, and data processing functions identified in the task analyses are provided and that those controls, displays and data processing functions are designed in accordance with accepted HFE practices and principles.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7.a. Continued	(5) The integration of HSI equipment with each other, with the operating personnel and with the Operations Technical Procedures shall be evaluated through the conduct of dynamic task performance testing. The dynamic task performance testing and evaluations shall be performed over the full scope of the integrated HSI design using dynamic HSI proto-types (i.e., prototypical HSI equipment which is dynamically driven by real time plant simu-lation computer models), other evaluation tools and/or past dynamic task performance test and evaluation results. The methods for defining the scope and application of the dynamic HSI prototype, past test results and other evaluation tools shall be documented in the implementation plan. The dynamic task performance tests and evaluations shall have as their objectives: (i) Confirmation that the integrated HSI design facilitates achievement of the identified safety functions and critical functions, (ii) Confirmation that the allocation of function and the structure of tasks assigned to personnel is consistent with accepted HFE principles,

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7.a. Continued	(iii) Confirmation of established main control room staffing and the HSI design and configuration provided to support that staff in accomplishing their assigned tasks. (iv) Confirmation that Operations Technical Procedures are complete and accurate, (v) Confirmation that the dynamic aspects of the HSI are sufficient for task accomplishment, and (vi) Confirmation that the integrated HSI design is condusive to ~~eliminating~~ REDUCING the potential for operator errors. (8) That dynamic task performance test evaluations shall be conducted over the ~~full~~ range of operational conditions and upsets, including: (i) Normal plant operations, such as plant startup, shutdown, full power operations, and plant maintenance activities; (ii) Plant system and equipment failures; (iii) HSI equipment failures; (iv) Plant transients, and; (v) Postulated plant accident conditions.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7 a. Continued	(7) The HFE performance measures to be used as the basis for evaluating the dynamic task performance test results. These performance measures shall include: (i) Operating crew primary task performance characteristics, such as task times and procedure violations, (ii) operating crew errors and/or error rates, (iii) operating crew situation awareness, (iv) operating crew workload, (v) operating crew communications and coordination, (vi) anthropometry evaluations.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7.a. Continued	(vii) physical positioning and interactions, and (viii) HSI equipment performance measures (8) The methods to confirm that HFE issues identified and documented in the Human Factors Issue Tracking System have been resolved in the integrated HSI design, and (9) The methods and criteria to be used to confirm that critical human actions, as defined by the task analysis, have been addressed in the integrated HSI design in a manner consistent with accepted HFE practices and principles. (10) The methods and criteria to be used to confirm that the operating technical procedures are correct and can be executed within the realm of accepted human performance capabilities.

Table 3.6: Human Factors Engineering (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Design Acceptance Criteria
7. Continued	7.b. A human factors engineering analysis of the integrated HSI design shall be conducted in accordance with the Human Factors Verification and Validation Implementation Plan and the findings will be documented in Human Factors Verification and Validation Results Report. The analyses of the integrated HSI design shall be reviewed by the HFE Design Team and the results of that review shall be documented in Human Factors Verification and Validation Evaluation Report.	7.b. The human factors verification and validation (V&V) of the human system interface (HSI) design shall be conducted in accordance with the requirements of the Human Factors Engineering Program Plan and the Human Factors V&V Implementation Plan.

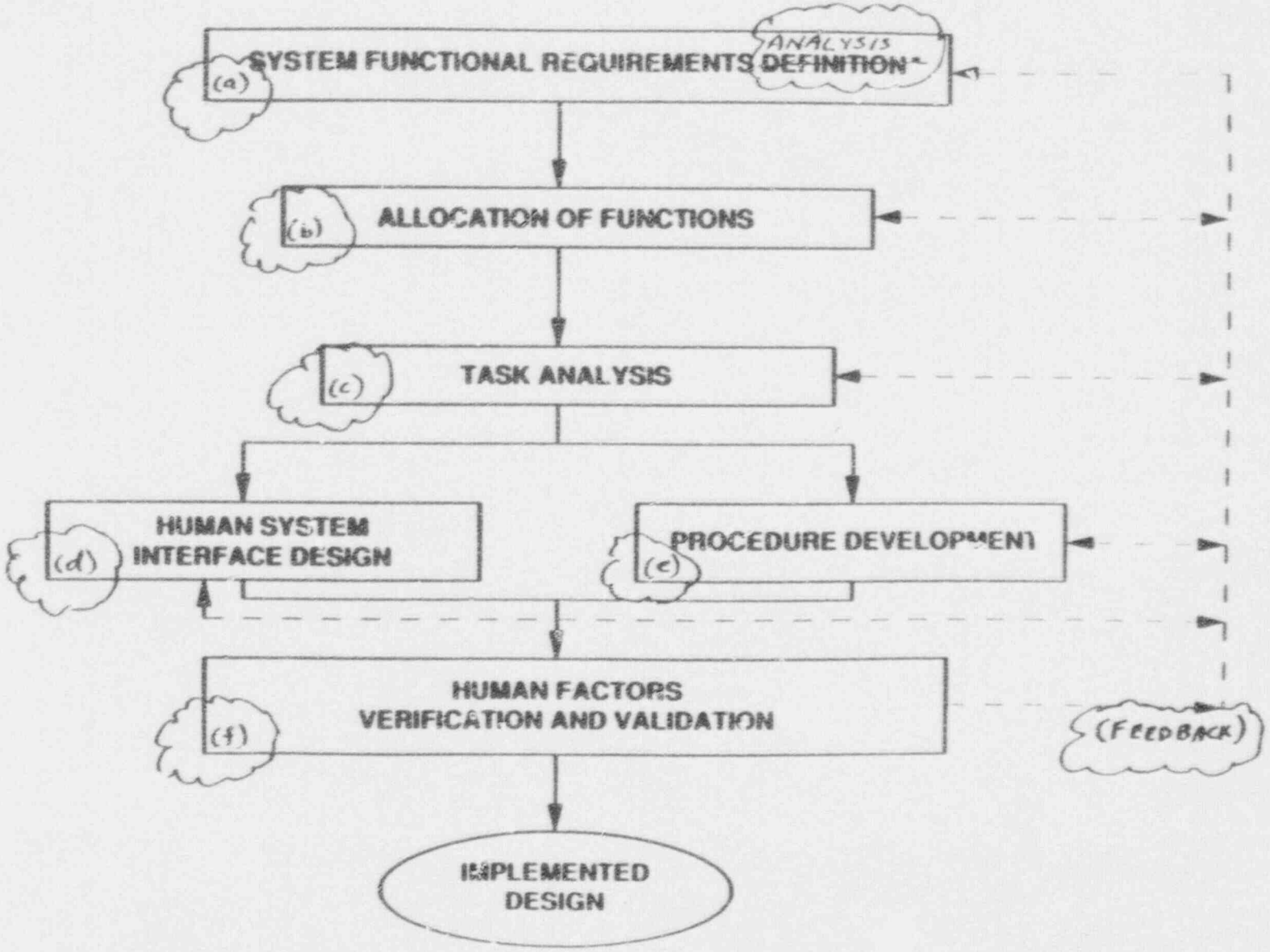


Figure 3.6 Human System Interface Design Implementation Process

The following are LHFB's comments:

95

DISAGREE 1. The numbering scheme should match the numbering scheme in the ITAAC.

O.K. 2. The implementation process described in the "design description" needs to include reference to the HFE Program Plan.

DISAGREE 3. The HFE issues tracking system needs to be referenced in the "design description."

DISAGREE* 4. Sub-titles would help to divide the different concepts discussed in the "design description."

DISAGREE 5. The HFE Review Team and the reports that the HFE Review Team will be responsible for producing must be referenced in the "design description."

DISAGREE 6. Each of the reports that will be generated by the applicant should be listed in the "design description."

a- DISAGREE
b.- O.K. 7. Figure 3.6.1 should be revised to (a) include the Program Plan and (b) "definition" should be replaced with "analysis" in the first box.

O.K. 8. Number 2 under "design commitment" is missing (1).

O.K. 9. Number 7.a.(2) is missing a sentence.

O.K. 10. Number 7.a(7)(ii) should be revised to delete the "or."

O.K. 11. The entire section should be reviewed to correct the typographical errors.

764

3.3-5 Section 3.3, page 3.3 -2 (6/1/92), Table 3.3:

Certified Design Commitment number 1 includes the requirements for ASME Code fatigue analyses. Following subsequent operating experience (e.g., operational transients) the fatigue analyses will require reevaluation and reconciliation to show continued applicability and conservatism. Does GE recommend application of monitoring instrumentation on piping to aid provide confidence in the validity of such reevaluations?

3.4-1 Section 3.4, pages 3.4 -1 thru -16 (6/1/92) -- No Comments
3.5-1 Section 3.5, pages 3.5 -1 thru -18 (6/1/92) -- No Comments

---

3.6-1 Section 3.6, pages 3.6 -1 thru -24 (6/1/92)

The *Design Description* (Page -1) states the HSI scope will include the Remote Shutdown System. The Design Commitment number 1 (Page -3) and the Design Acceptance Criteria number 1(4) (Page -5) are consistent with that scope.

DISAGREE 1. However, in the later steps which are more concerned with implementation of HFE the Remote Shutdown System appears to have been partially omitted from consideration as in Design Acceptance Criteria number 5.a(5) (Page -15) and Design Acceptance Criteria number 6.a(2) (Page -16).

O.K. 2. In Table 3.0, Application of Generic Material to ABWR Systems, the matrix box for applicability of 3.6, Human Factors Engineering, shows no to RSS (2.2.6). (Although I haven't researched this question, I believe NRC and industry standards provide for HFE to be applied to a much wider scope than just the MCR and RSS. In fact, Table 3.0 shows applicability to ARM and PRM as well as the MCR, but to nothing else.)

3.7-1 Section 3.7, pages 3.7 -1 (6/1/92)

The First Sentence of the Second Paragraph of *Design Description* states:

> The plant design provides radiation shielding ... and thus maintains radiation exposures to plant personnel as low as reasonably achievable.

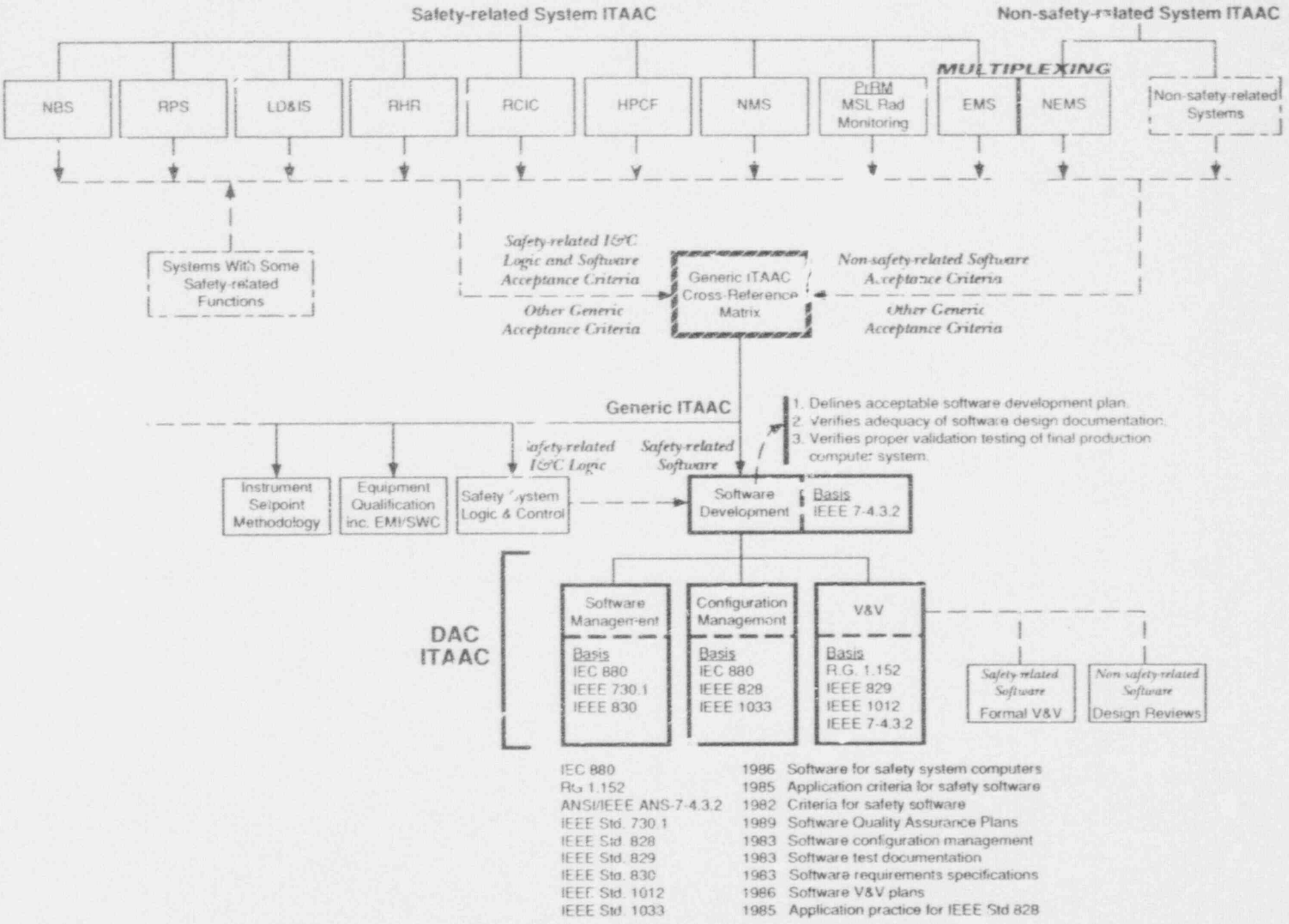
The As Low As Reasonably Achievable (ALARA) goal and practices to achieve it involves far more than a plant design which provides "radiation shielding." For the Tier 1 document for a standardized plant design of potentially widespread future application to imply such a simple situation is very disturbing.

ITAAC SUMMARY

3.5 Software (Computer) Development

- Format
  - Generic ITAAC plus DAC for specific acceptance criteria confirming software development process
  - Not a system ITAAC, but referenced by plant systems using software-based control and monitoring equipment
- Applicability
  - Full ITAAC/DAC process, which specifies a formal verification and validation (V&V) plan, is applicable to development of safety-related software
  - Modified ITAAC/DAC process for non-safety-related software will use design reviews to verify development phases similar to those for safety-related software (EPRI requirement)
- Tier 1 Commitment
  - A plan for developing software shall exist and shall include certain specific elements, as defined in the acceptance criteria, for controlling the development process
  - These elements in turn shall impose acceptance criteria on the planned phases of the development process to determine the acceptability of the design documents produced during each development phase and the adequacy of the V&V process
- Two versions of software ITAAC/DAC exist
  - GE submittal with markups from internal review
  - NRC staff/Lawrence Livermore National Laboratory version developed after NRC review of original GE Phase 2 submittal

GENERIC ITAAC and DAC for SOFTWARE DEVELOPMENT INTERFACE DIAGRAM



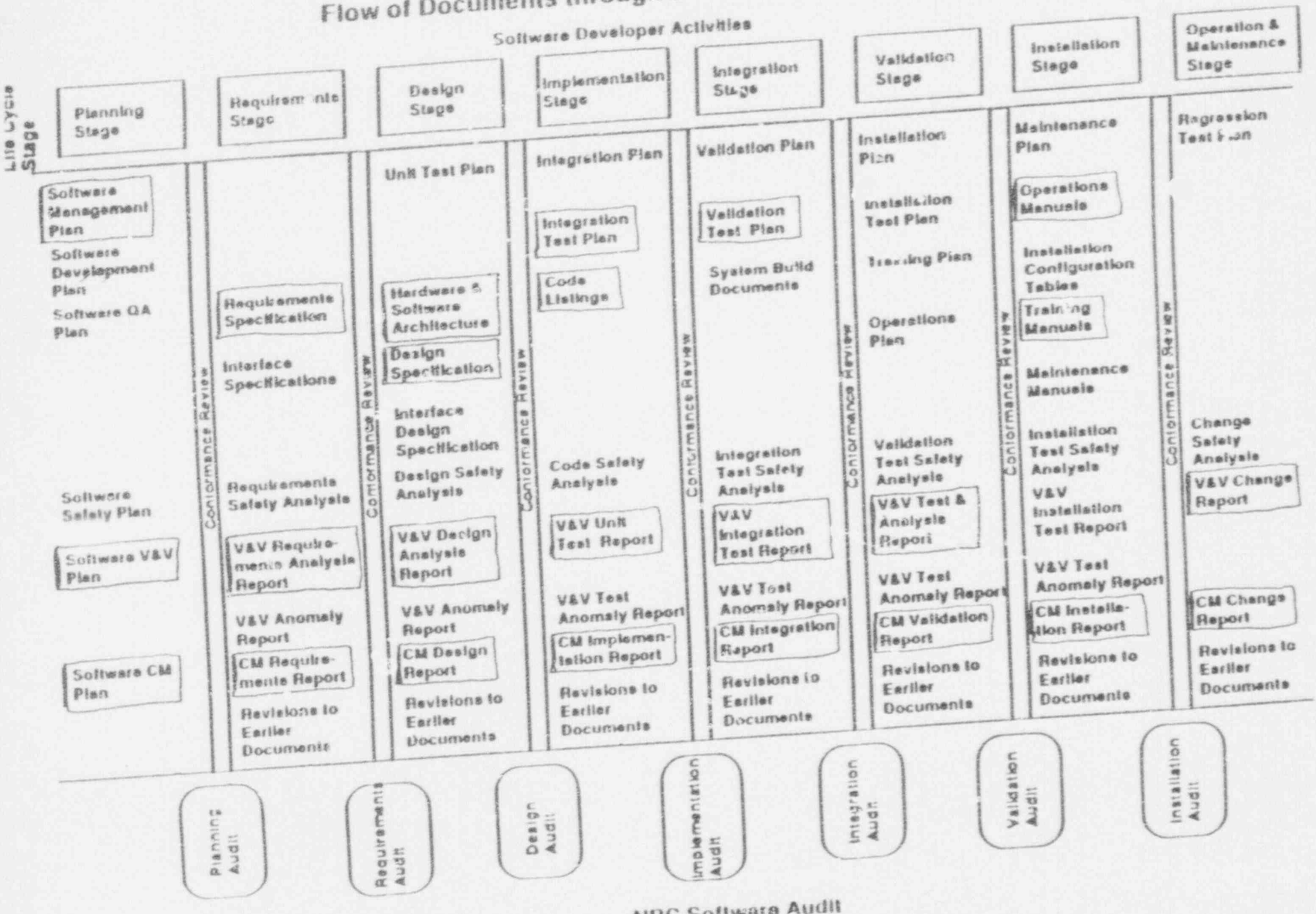
IEC 880	1986	Software for safety system computers
RG 1.152	1985	Application criteria for safety software
ANSI/IEEE ANS-7-4.3.2	1982	Criteria for safety software
IEEE Std. 730.1	1989	Software Quality Assurance Plans
IEEE Std. 828	1983	Software configuration management
IEEE Std. 829	1983	Software test documentation
IEEE Std. 830	1983	Software requirements specifications
IEEE Std. 1012	1986	Software V&V plans
IEEE Std. 1033	1985	Application practice for IEEE Std 828

FIGURE

☐ = GE SOFTWARE DAC COMMITMENT

~~Table~~ 3.5-1

Flow of Documents through the Software Life Cycle



NRC Software Audit

3.5 Software Development

Design Description

The certified design uses microprocessor-based digital equipment to perform selected safety-related functions. Development of the necessary software is dependent upon the as-procured hardware and is thus not part of the certified design. The process to be used for software development and implementation will be in full compliance with the regulatory requirements and industrial standards governing these activities. These requirements will apply to: a) each ABWR safety system that uses the safety-related software functions of the Safety System Logic and Control (SSLC) equipment and b) other safety-related equipment that contains software to perform safety functions.

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.5, together with Appendices A, B, and C, provides a definition of the processes that will be used to demonstrate compliance with the requirements governing development and implementation of software for safety-related functions. This material is structured as follows:

Table 3.5: Generic inspections, tests, analyses, and acceptance criteria (ITAAC) material for the overall software development process. Key elements of this process are a Software Management Plan, Configuration Management Plan, and a Verification and Validation (V&V) Plan.

Appendix A: Design Acceptance Criteria (DAC) for the Software Management Plan

Appendix B: Design Acceptance Criteria (DAC) for the Configuration Management Plan

Appendix C: Design Acceptance Criteria (DAC) for the Verification and Validation (V&V) Plan

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
		1. (Continued) The plan meets the design acceptance criteria described in Appendix B. c. Verification and Validation Plan establishes verification reviews and validation testing procedures with the following components: (1) Independent design verification (2) Baseline reviews (3) Testing (a) Unstructured testing (b) Formal validation testing (4) Firmware issue and validation procedure (5) Procedure for future revisions The plan meets the design acceptance criteria described in Appendix C.
2. The software design documentation shall meet the requirements of each element of the software development plan described in Item 1.	2. Review design documentation: - Hardware/Software System Specification - Software Requirements Specification - Software Design Specification - Hardware Requirements Specification - Hardware Design Specification	2. The documentation complies with the requirements of the software development plan. The design documentation generated by the definition and planning process described in Appendix A allows correlation of the design elements with each specific software requirement as determined by the V&V process described in Appendix C. The computer system hardware documentation identifies the hardware requirements that impact software.

3.5

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix A: Design Acceptance Criteria for Software Management Plan

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The standards, conventions, and design processes to be followed during the design, development, and maintenance of safety-related software shall be established in the software management plan.	1. A review shall be performed of the contents of the software management plan.	1. A software management plan has been issued.
2. The software management plan shall define and document the following major design phases of the software engineering process: a. Definition and Planning b. Product Performance Definition c. High Level Software Design d. Detailed Design/Code/Module Test e. Integration Test f. Validation and Firmware Issue g. Firmware Release	2. A review shall be performed of the contents of the software management plan.	2. The plan contains a description of each ~~specified~~ phase of the software engineering process. ~~A particular design phase shall be verified with respect to the set of documents produced for that phase. These documents are listed in the design commitments in the following sections.~~ See Appendix C for details of, and acceptance criteria for, the verification and validation process.
3. Definition and Planning Phase. This phase comprises the identification of applicable requirements (contractual or from design specifications) and confirmation of suitability of the software planning documents. The documents required to be baselined at the completion of this design phase are: a. Design Requirements b. Software Configuration Management Plan c. Software Management Plan d. Software Verification and Validation Plan e. Baseline Review Record	3. A review shall be performed of the contents of the software management plan. Definition of baseline: A set of documents, assumptions, and open items that reflect the current state of a design phase and define the design input for the next design phase.	3. The plan states that the ~~committed~~ documents are the baseline of the Definition and Planning Phase. The plan also states that ~~all required~~ verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.

6/1/32

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix A: Design Acceptance Criteria for Software Management Plan (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
7. Integration Test: This phase comprises the testing that evaluates performance and adequacy of the software when installed in its destined hardware. The documents required to be baselined at the completion of this design phase are: a. Integration Test Report b. Baseline Review Record	7. A review shall be performed of the contents of the software management plan.	7. The plan states that the ~~commited~~ documents are the baseline of the Integration Test Phase. The plan also states that ~~all required~~ verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.
8. Validation and Firmware Issue: This phase comprises the generation and use of the procedures necessary to perform final testing on a production instrument and to assure the quality of the delivered software. The documents required to be baselined at the completion of this design phase are: a. Validation Test Plan and Procedure b. Validation Test Report c. Firmware Release Description d. Issued Firmware (object code) e. Baseline Review Record	8. A review shall be performed of the contents of the software management plan. Definition of firmware: Object (machine) code contained in non-volatile memory, typically PROM or EPROM.	8. The plan states that the ~~committed~~ documents are the baseline of the Validation and Firmware Issue Phase. The Firmware Release Description contains the following information: a. The means by which the source code was compiled, linked, and located. b. The means by which the master PROMs were generated. c. A record of hardware and software tools used to develop the firmware. The plan also states that ~~all required~~ verification reviews are to be completed before release of the firmware for production, as attested to in the Baseline Review Record.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix B: Design Acceptance Criteria for Configuration Management Plan (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Applicable procedures, such as standards for the designation of software versions, shall be described in the plan or specifically referenced. All software shall be identified such that the version can be verified directly, either embedded in the software if in a non-programmable/ erasable format or permanently inscribed directly on the component.	4. A review shall be performed of the contents of the configuration management plan.	4. The plan describes the procedures for implementation of the plan.
5. The plan shall describe the audits and reviews that are to be performed to verify that the software is being maintained under configuration management. The plan shall describe a procedure for corrective actions if any problems are discovered.	5. A review shall be performed of the contents of the configuration management plan.	5. The plan describes audits and reviews and describes a procedure for corrective actions.
6. The configuration management of tools, techniques, and methodologies shall be specifically delineated. The plan shall address control of development methods to be used (such as formal specification) and tools (such as compilers).	6. A review shall be performed of the contents of the configuration management plan.	6. The plan describes control of tools and methodologies.
7. The plan shall describe the method of records collection and retention.	7. A review shall be performed of the contents of the configuration management plan.	7. The plan describes the record storage plan.
8. The plan shall address control of the final user documentation and the information to be supplied. The method of informing the user of each product of known faults, failures, and changes shall be specifically described.	8. A review shall be performed of the contents of the configuration management plan.	8. The plan identifies the method by which faults, failures, and changes are identified to the affected user.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix C: Design Acceptance Criteria for Verification and Validation Plan

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Verification reviews and validation testing ~~shall be used to assure software quality.~~ The methodology and requirements for ~~these techniques~~ are described in the Verification and Validation (V&V) Plan.	1. A review of ~~this~~ the V&V plan shall be conducted during a product's Definition and Planning design phase (see Appendix A).	1. ~~The review assures the suitability of the plan and notes any needed modifications.~~ The V&V plan will be approved and in place at the beginning of the project.
2. The V&V ~~process shall comprise~~ plan shall describe a combination of the following activities: a. Informal reviews b. Independent design verifications c. Baseline reviews d. Layered testing (unstructured testing and validation testing)	2. A review shall be performed of the contents of the V&V plan.	2. The V&V plan contains a description of the specified ~~committed~~ activities. ~~The activities are defined in the following sections.~~
3. Informal Reviews: Informal reviews ~~shall be used~~ to resolve problems, evaluate alternate approaches, tentatively confirm adequacy of a solution or processing approach, or other design evolution activity.	3. A review shall be performed of the contents of the V&V plan.	3. The V&V plan describes the uses and limitations of informal reviews and their methodology. ~~This activity does not confirm compliance with any external requirements.~~
4. Independent Design Verification: The product assurance process ~~shall provide~~ to provide controlled, independent, documented confirmation that the design meets requirements. The ~~process~~ plan shall address the following aspects of the design as a minimum: a. Quality b. Safety c. Reliability d. Performance	4. A review shall be performed of the contents of the V&V plan.	4. The V&V plan describes the independent design verification process and requires that confirmation of design adequacy is performed by knowledgeable individuals other than those responsible for the design.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix C: Design Acceptance Criteria for Verification and Validation Plan (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
7. Validation Testing: ~~This~~ process confirms ~~that~~ the final version of the software (firmware) loaded in the production (or fully equivalent) hardware, ~~performs all required functions. In addition~~, displays (if any) ~~are confirmed to be consistent~~ with the final version of the User's Manual.	7. A review shall be performed of the contents of the V&V plan.	7. The plan describes the validation testing process. Validation testing is performed as specified in a formal documented procedure which is written by an individual not responsible for software design and is verified against requirements and performance specifications to confirm that all functions are tested. Results of the test are documented, along with a resolution of anomalies, in a Validation Test Report. 3) Validation testing shall be performed by individuals other than the instrument software designers.
8. Firmware Verification and Issue: The final software (firmware) shall be verified prior to issue.	8. A review shall be performed of the contents of the V&V plan.	8. The plan describes the final verification process for firmware. ~~The process~~ includes structured confirmation that the design has been tested or verified by formal review, shows compliance with ~~all~~ requirements, and ~~all~~ testing has been completed and open items resolved.
9. Software Changes: Changes to the software after release shall be handled in accordance with the software management plan and authorized change control provisions.	9. A review shall be performed of the contents of the V&V plan.	9. The plan describes the software change process and required V&V tests. Steps of the V&V process will be repeated as applicable, including repeat of all or part of the Validation Test.

(ITAAC/DAC DEVELOPED BY THE NRC)

8/20/92

3.5 Computer Development

Design Description

The certified design uses microprocessor-based digital equipment to perform many of the safety-related and non-safety-related functions of the instrumentation and control systems. The safety-related software shall be developed in full conformance with these requirements. The non-safety-related software shall be developed using a planned design process similar to the safety-related software. Digital equipment is also used for design and operational support of the on-line systems. The primary focus of this section is on software, however, the implementation of the software includes hardware aspects of the design, such as hardware/software integration, which are not addressed in other sections and are, therefore, included in this section. Examples of equipment for which software performance and quality is necessary for equipment performance and quality includes; programmable logic controllers (PLCs), microprocessors, application specific integrated circuits (ASICs), and computers. These equipment may have a variety of safety related applications including, but not limited to meter and display functions, recording devices, data transmission, control functions and alarms.

Because microprocessor and digital control technology is rapidly evolving it is important that the certified design description (Tier 1) and the ITAAC do not "lock in" a design which would be obsolete at the time of construction. The approach is to "lock in" a design process and specific acceptance criteria (termed design acceptance criteria (DAC)) which if met would result in a design which is acceptable. The DAC will be in the same format as the ITAAC used for other systems in that it

will specify the certified design process commitment and will specify the method of demonstration that the commitment has been met. The method of demonstration will be by inspection, test, or analysis against established acceptance criteria. The functional I&C system requirements are provided in other ITAAC. The software DAC will describe a formal design implementation process with a phased test, analysis, and acceptance criteria (ITAAC). The ITAAC will be inspected by the NRC to verify conformance with the requirements at several phases or stages during the safety related digital control system design process. The documents which demonstrate satisfactory implementation of the ITAAC will be available for inspection at the completion of each of the above stages. The stages or phases are shown in Figure 3.5-1. The COL holder will be required to satisfactorily complete each ITAAC phase prior to proceeding to the next phase of the design development. Failure to successfully complete a phased ITAAC may require repeating an earlier ITAAC and/or changing the system design. The NRC staff will issue an inspection report for each phased ITAAC and identify any open issues which require resolution. Significant open issues which are not resolved could result in the NRC staff concluding that the ITAAC had not been satisfactorily completed. At each phased ITAAC the design development must be verified to be in accordance with the certified design process and that the detailed design developed (through that stage) meets the certified design. Upon completion of each phased ITAAC the COL holder will certify to the NRC that the stage has been completed and the design and construction completed up through that stage is in compliance with the certified design. The COL holder will also provide a description of the next phase of design development and associated testing, analysis and acceptance criteria in enough detail that the NRC staff can determine whether or not the proposed design development and testing is consistent with the certified design process and next ITAAC. This phased process will continue until all ITAAC steps for all the safety-related software are complete.

The certified design description and design development process continue for the lifetime of the plant. Any safety related software that is

changed or added after plant startup is required to either to be developed using the certified design process described in the computer DAC or submit a design process (together with the design bases) that will produce software of the same or higher quality than the certified design process. The COL holder will be required to use an approved Software Change Procedure based upon the certified design development process for the operation stage of the lifecycle. This will be a requirement of the COL and is not included in the design certification DACs.

The Tier 2 commitments described in the SSAR and related (docketed) documents provide methods and descriptions of the implementation of the Tier 1 requirements. The determination that the plant has been constructed in accordance with the design certification will require the use of the information contained in both the Tier 1 and Tier 2 documents. The Tier 2 commitments are based on postulations of how the design will be implemented which may change when detailed design begins; therefore, the Tier 2 commitments may be changed. The Tier 2 commitments that effect the technical design of the I&C systems including the design process, design implementation, and the NRC staff review as described in the final safety evaluation report which are changed must be submitted to the NRC for review prior to implementation.

The process to be used for software development and implementation will be in full compliance with the regulatory requirements and specified industrial standards governing those activities. The requirements of 10CFR Part 50 will be met in addition to the requirements listed in this description and ITAAC/DAC. In particular, the vendor implementation and the NRC evaluation of the software QA program will be accomplished under a 10 CFR Part 50 Appendix B program.

Inspections, Tests, Analyses and Acceptance Criteria (and Design Acceptance Criteria)

The design description, together with the section 3.5 ITAAC/DAC listed below, provides the definition of the processes that will be used to develop the ABWR software. The ITAAC also includes specific steps which describe how the conformance to the requirements will be demonstrated.

Table 3.5.1: Design Acceptance Criteria (DAC) for the Software Management Plan

The Software Management Plan (SMP) shall establish the organization and authority structure for the design, the procedures to be used, and the inter-relationships between major activities. The SMP will describe a Software Lifecycle which describes the method to develop plans and procedures that will guide the design process throughout the lifecycle stages. Those stages shall include:

1. Planning
2. Requirements
3. Design
4. Implementation
5. Integration
6. Validation
7. Installation
8. Operation and Maintenance

Table 3.5.2: Design Acceptance Criteria (DAC) for the Software Development Plan

The Software Development Plan will describe a

development process, tools documentation, and products developed according to the software lifecycle.

Tab;e 3.5.3: Design Acceptance Criteria (DAC) for the Configuration Management Plan

The Software Configuration Management Plan (CMP) shall provide the means to identify software products, control and implement changes, and record and report change implementation status.

Table 3.5.4: Design Acceptance Criteria (DAC) for the Software Verification and Validation Plan

The Software Verification and Validation (V&V) Plan shall describe the method to assure that the requirements of each phase are fully and accurately implemented into the next phase and validated.

Table 3.5.5: Design Acceptance Criteria (DAC) for the Software Safety Plan

The Software Safety Plan describes the safety and hazards analyses that shall be performed.

Tab;e 3.5.6: Design Acceptance Criteria (DAC) for the Operations and Maintenance Plan

The Software Operation and Maintenance Plan shall include the procedures required to assure that the software will be operated correctly and that the quality of the software is maintained as revisions are made.

Table 3.5.7: Design Acceptance Criteria (DAC) for the Software

Conformance Review Plan

The Conformance Review Plan will include descriptions of the documentation and tests which are required for the software developer to demonstrate conformance to the requirements and provide adequate information for the NRC staff to confirm that conformance.

3.5 Software Development

Design Description

The certified design uses microprocessor-based digital equipment to perform selected safety-related functions. Development of the necessary software is dependent upon the as-procured hardware and is thus not part of the certified design. The process to be used for software development and implementation ~~will be in full compliance with the regulatory requirements and industrial standards governing these activities. These requirements~~ will apply to: a) each ABWR safety system that uses the safety-related software functions of the Safety System Logic and Control (SSLC) equipment and b) other safety-related equipment that contains software to perform safety functions.

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.5, together with Appendices A, B, and C, provides a definition of the processes that will be used to demonstrate compliance with the requirements governing development and implementation of software for safety-related functions. This material is structured as follows:

Table 3.5: Generic inspections, tests, analyses, and acceptance criteria (ITAAC) material for the overall software development process. Key elements of this process are a Software Management Plan, Configuration Management Plan, and a Verification and Validation (V&V) Plan.

Appendix A: Design Acceptance Criteria (DAC) for the Software Management Plan

Appendix B: Design Acceptance Criteria (DAC) for the Configuration Management Plan

Appendix C: Design Acceptance Criteria (DAC) for the Verification and Validation (V&V) Plan

3.5

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. A plan shall be developed for software used in microprocessor-based equipment that performs safety-related functions. The plan shall describe the organizational and procedural aspects of software development and shall comprise the following elements: - Software Management Plan - Configuration Management Plan - Verification and Validation (V&V) plan	1. Review: - Software Management Plan - Configuration Management Plan - Verification and Validation Plan	1. The overall development plan documents the requirements and methodology for achieving the software attributes of consistency, accuracy, error tolerance and modularity. The plan includes the methodology for assuring the software is both auditable and testable during the design, implementation and integration phases. Each element of the plan contains the following items as a minimum: a. Software Management Plan establishes standards, conventions and design processes for the design, development, and maintenance of safety-related software. The plan meets the design acceptance criteria described in Appendix A. b. Configuration Management Plan establishes a formal set of standards and procedures to provide visible status and control of software documentation. The following basic elements are addressed: (1) Unique identification of each software documentation item (2) Management of software documentation change control (3) Accounting methods to provide visibility and traceability for all changes to baseline product software (4) Verification steps required to assure proper adherence to software design requirements

-2-

6/92

Table 3.5: Software for Programmable Digital Computers In Safety-related Applications (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
		1. (Continued) The plan meets the design acceptance criteria described in Appendix B. c. Verification and Validation Plan establishes verification reviews and validation testing procedures with the following components: (1) Independent design verification (2) Baseline reviews (3) Testing (a) Unstructured testing (b) Formal validation testing (4) Firmware issue and validation procedure (5) Procedure for future revisions The plan meets the design acceptance criteria described in Appendix C.
2. The software design documentation shall meet the requirements of each element of the software development plan described in Item 1.	2. Review design documentation: - Hardware/Software System Specification - Software Requirements Specification - Software Design Specification - Hardware Requirements Specification - Hardware Design Specification	2. The documentation complies with the requirements of the software development plan. The design documentation generated by the definition and planning process described in Appendix A allows correlation of the design elements with each specific software requirement as determined by the V&V process described in Appendix C. The computer system hardware documentation identifies the hardware requirements that impact software.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. The generation of documentation for (1) software implementation and (2) the integration of hardware and software into the final product shall follow the process described in the elements of the software development plan.	3. Review the software development plan.	3. The documentation for software implementation and hardware/software integration testing meets the requirements of the software development plan, as shown in Appendices A, B, and C.
4. The assembled, final production computer system shall be exercised through static and dynamic simulations of input signals present during normal operation and design basis event conditions requiring computer system action. The validation test plan shall identify the validation tests for each software-based system component of Safety System Logic and Control (SSLC). The plan shall also include tests that validate correct operation for each safety system requirement of the systems that interface with SSLC. The requirements are those stated in the System Design Specification of each interfacing safety system.	4. Review formal (verified) validation test report.	4. The test report summarizes the results of the computer system validation testing and shows how the system is in compliance with the requirements. The test report identifies the validation tests for each computer system and safety system requirement. In addition, the required input signals and their values, the anticipated output signals, and the acceptance criteria are stated. The test report identifies the hardware and software used, test equipment and calibrations, simulation models used, test results, and discrepancies and corrective actions. The test plan was developed, the tests executed, and the test results evaluated by individuals who did not participate in the design or implementation phases.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix A: Design Acceptance Criteria for Software Management Plan

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The standards, conventions, and design processes to be followed during the design, development, and maintenance of safety-related software shall be established in the software management plan.	1. A review shall be performed of the contents of the software management plan.	1. A software management plan has been issued.
2. The software management plan shall define and document the following major design phases of the software engineering process: a. Definition and Planning b. Product Performance Definition c. High Level Software Design d. Detailed Design/Coda/Module Test e. Integration Test f. Validation and Firmware Issue g. Firmware Release	2. A review shall be performed of the contents of the software management plan.	2. The plan contains a description of each ~~specified~~ phase of the software engineering process. ~~A particular design phase shall be verified with respect to the set of documents produced for that phase. These documents are listed in the design commitments in the following sections.~~ See Appendix C for details of, and acceptance criteria for, the verification and validation process.
3. Definition and Planning Phase. This phase comprises the identification of applicable requirements (contractual or from design specifications) and confirmation of suitability of the software planning documents. The documents required to be baselined at the completion of this design phase are: a. Design Requirements b. Software Configuration Management Plan c. Software Management Plan d. Software Verification and Validation Plan e. Baseline Review Record	3. A review shall be performed of the contents of the software management plan. Definition of baseline: A set of documents, assumptions, and open items that reflect the current state of a design phase and define the design input for the next design phase.	3. The plan states that the ~~committed~~ documents are the baseline of the Definition and Planning Phase. The plan also states that ~~all required~~ verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix A: Design Acceptance Criteria for Software Management Plan (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Product Performance Definition: Defines the general product design and the split between hardware and software. The documents required to be baselined at the completion of this design phase are: a. Product Schematic b. Product Performance Specification, including Software Requirements c. Product User's Manual d. Communications Protocols e. Baseline Review Record	4. A review shall be performed of the contents of the software management plan.	4. The plan states that the committed documents are the baseline of the Product Performance Definition Phase. The plan also states that all required verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.
5. High Level Software Design: This phase comprises the design of the software architecture and structure and the determination of general module functions. The documents required to be baselined at the completion of this design phase are: a. Software Design Specification b. Baseline Review Record	5. A review shall be performed of the contents of the software management plan.	5. The plan states that the committed documents are the baseline of the High Level Software Design Phase The plan also states that all required verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.
6. Detailed Design/Code/Module Test: This phase comprises detailed design of the software and testing of individual software modules by the designer. The documents required to be baselined at the completion of this design phase are: a. Source Code b. Module Testing Report c. Baseline Review Record	6. A review shall be performed of the contents of the software management plan. Definition of module: Executable computer code that implements a functional requirement or part of a functional requirement; normally the smallest segment of code controlled by the operating system.	6. The plan states that the committed documents are the baseline of the Detailed Design/Code/Module Test Phase. The plan also states that all required verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record. Someone other than the designer reviews the software modules.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix A: Design Acceptance Criteria for Software Management Plan (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
7. Integration Test: This phase comprises the testing that evaluates performance and adequacy of the software when installed in its destined hardware. The documents required to be baselined at the completion of this design phase are: a. Integration Test Report b. Baseline Review Record	7. A review shall be performed of the contents of the software management plan.	7. The plan states that the ~~committed~~ documents are the baseline of the Integration Test Phase. The plan also states that ~~all required~~ verification reviews are to be completed before the design moves to the next phase, as attested to in the Baseline Review Record.
8. Validation and Firmware Issue: This phase comprises the generation and use of the procedures necessary to perform final testing on a production instrument and to assure the quality of the delivered software. The documents required to be baselined at the completion of this design phase are: a. Validation Test Plan and Procedure b. Validation Test Report c. Firmware Release Description d. Issued Firmware (object code) e. Baseline Review Record	8. A review shall be performed of the contents of the software management plan. Definition of firmware: Object (machine) code contained in non-volatile memory, typically PROM or EPROM.	8. The plan states that the ~~committed~~ documents are the baseline of the Validation and Firmware Issue Phase. The Firmware Release Description contains the following information: a. The means by which the source code was compiled, linked, and located. b. The means by which the master PROMs were generated. c. A record of hardware and software tools used to develop the firmware. The plan also states that ~~all required~~ verification reviews are to be completed before release of the firmware for production, as attested to in the Baseline Review Record.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix B: Design Acceptance Criteria for Configuration Management Plan

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Development of software for the microprocessor-based safety systems shall be controlled according to a configuration management plan	1. A review shall be performed of the contents of the configuration management plan.	1. A configuration management plan has been issued.
2. The configuration management plan will define the purpose and scope of the plan with emphasis on the groups to which it applies and the specific product which is to be developed. The product description shall include both executable and non-executable material.	2. A review shall be performed of the contents of the configuration management plan.	2. The configuration management plan identifies each group which develops and/or maintains software for safety systems. The plan includes both executable and non-executable portions of the design.
3. The configuration management plan shall describe the organizational responsibilities. The organizational independence or dependence of the groups responsible for the software configuration shall be specifically described. The plan shall describe a function independent of the software designers that is responsible for verifying that the software is maintained under this plan. The plan shall detail the relationships of the configuration control with the software QA, development, and other groups.	3. A review shall be performed of the contents of the configuration management plan.	3. The configuration management plan describes the organizational independence and responsibilities.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix B: Design Acceptance Criteria for Configuration Management Plan (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Applicable procedures, such as standards for the designation of software versions, shall be described in the plan or specifically referenced. All software shall be identified such that the version can be verified directly, either embedded in the software if in a non-programmable/ erasable format or permanently inscribed directly on the component.	4. A review shall be performed of the contents of the configuration management plan.	4. The plan describes the procedures for implementation of the plan.
5. The plan shall describe the audits and reviews that are to be performed to verify that the software is being maintained under configuration management. The plan shall describe a procedure for corrective actions if any problems are discovered.	5. A review shall be performed of the contents of the configuration management plan.	5. The plan describes audits and reviews and describes a procedure for corrective actions.
6. The configuration management of tools, techniques, and methodologies shall be specifically delineated. The plan shall address control of development methods to be used (such as formal specification) and tools (such as compilers).	6. A review shall be performed of the contents of the configuration management plan.	6. The plan describes control of tools and methodologies.
7. The plan shall describe the method of records collection and retention.	7. A review shall be performed of the contents of the configuration management plan.	7. The plan describes the record storage plan.
8. The plan shall address control of the final user documentation and the information to be supplied. The method of informing the user of each product of known faults, failures, and changes shall be specifically described.	8. A review shall be performed of the contents of the configuration management plan.	8. The plan identifies the method by which faults, failures, and changes are identified to the affected user.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix B: Design Acceptance Criteria for Configuration Management Plan (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
9. The configuration management plan shall be in place and approved by the implementor prior to the first concept development phases of software development.	9. A review of the configuration management plan shall be conducted during a product's Definition and Planning design phase (see Appendix A).	9. The configuration management plan is to be approved and in place at the beginning of the project.
10. The configuration management plan shall require that the design documents (such as software requirements specifications) shall provide specific reference to the applicable configuration management plan. The plan shall define procedures for change control, including change request, evaluation, approval, and implementation.	10. A review shall be performed of the contents of the configuration management plan.	10. The plan requires that the design documents reference the configuration management plan.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix C: Design Acceptance Criteria for Verification and Validation Plan

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Verification reviews and validation testing ~~shall be used to assure software quality.~~ The methodology and requirements for ~~these techniques~~ are described in the Verification and Validation (V&V) Plan.	1. A review of ~~this~~ the V+V plan shall be conducted during a product's Definition and Planning design phase (see Appendix A).	1. ~~The review assures the suitability of the plan and notes any needed modifications.~~ The V&V plan will be approved and in place at the beginning of the project.
2. The V&V ~~process shall comprise~~ plan shall describe a combination of the following activities: a. Informal reviews b. Independent design verifications c. Baseline reviews d. Layered testing (unstructured testing and validation testing)	2. A review shall be performed of the contents of the V&V plan.	2. The V+V plan contains a description of the ~~committed~~ specified activities. ~~The activities are defined in the following sections.~~
3. Informal Reviews: Informal reviews ~~shall be used~~ The V+V plan shall describe a process for to resolve problems, evaluate alternate approaches, tentatively confirm adequacy of a solution or processing approach, or other design evolution activity.	3. A review shall be performed of the contents of the V&V plan.	3. The V+V plan describes the uses and limitations of informal reviews and their methodology. ~~This activity does not confirm compliance with any external requirements.~~
4. Independent Design Verification: The product assurance process ~~shall provide~~ V+V plan shall describe a to provide controlled, independent and documented confirmation that the design meets requirements. The ~~process~~ plan shall address the following aspects of the design as a minimum: a. Quality b. Safety c. Reliability d. Performance	4. A review shall be performed of the contents of the V&V plan.	4. The V+V plan describes the independent design verification process and requires that confirmation of design adequacy is performed by knowledgeable individuals other than those responsible for the design.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix C: Design Acceptance Criteria for Verification and Validation Plan (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. Baseline Reviews: Formal, independent evaluations of the design process, and the effectiveness and completeness of the process to specified points in the design, shall be performed. Baseline reviews are required during the following software development phases: a. Definition and Planning b. Product Performance Definition c. High Level Software Design d. Detailed Design/Code/Module Test e Integration Test f. Validation and Firmware Issue g. Firmware Release	5. A review shall be performed of the contents of the V&V plan.	5. The plan describes the baseline review process, as a minimum, each reviews of evaluates the following areas: a. Adequacy of documentation b. Adequacy of design process c. Adequacy of test methods d. Adherence to software management plan, configuration management plan and V&V plan Baseline reviews are performed by knowledgeable individuals other than those directly responsible for the design.
6. Unstructured Testing: No formal test plan or procedure shall be required. The following unstructured tests shall be performed during the design process: a. Exploratory testing evaluates implementation ideas of the designer. b. Module testing confirms the performance of individual software modules via emulation of hardware components c. Integration testing is performed on prototype hardware and confirms that all instrument functions, including self-test (if applicable), work properly	6. A review shall be performed of the contents of the V&V plan.	6. The plan describes the testing processes, which are documented as follows: a. Exploratory testing requires no formal certification, but may be documented by design notes. b. Module testing is documented in the Module Test Report. c. Integration test results are documented in the Integration Test Report. Concurrence on test adequacy is achieved during the Integration Test Baseline Review.

Table 3.5: Software for Programmable Digital Computers in Safety-related Applications

Appendix C: Design Acceptance Criteria for Verification and Validation Plan (Continued)

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	Inspections, Tests, Analyses and Acceptance Criteria	
7. Validation Testing: ~~This~~ process confirms ~~that~~ the final version of the software (firmware) loaded in the production (or fully equivalent) hardware, ~~performs all required functions, in addition~~, displays (if any) ~~are confirmed to be consistent~~ with the final version of the User's Manual.	7. A review shall be performed of the contents of the V&V plan.	7. The plan describes the validation testing process. Validation testing is performed as specified in a formal documented procedure which is written by an individual not responsible for software design and is verified against requirements and performance specifications to confirm that all functions are tested. Results of the test are documented, along with a resolution of anomalies, in a Validation Test Report. 3) Validation testing shall be performed by individuals other than the instrument software designers.
8. Firmware Verification and Issue: The final software (firmware) shall be verified prior to issue.	8. A review shall be performed of the contents of the V&V plan.	8. The plan describes the final verification process for firmware. ~~The process~~ includes structured confirmation that the design has been tested or verified by formal review, shows compliance with all requirements, and ~~all~~ testing has been completed and open items resolved.
9. Software Changes: Changes to the software after release shall be handled in accordance with the software management plan and authorized change control provisions.	9. A review shall be performed of the contents of the V&V plan.	9. The plan describes the software change process and required V&V tests. Steps of the V&V process will be repeated as applicable, including repeat of all or part of the Validation Test.