ABB

October 12, 1994
LD-94-061

Docket No. 52-002

Attn: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Subject: System 80+™ Design Control Document

Dear Sirs:

This letter transmits ABB-CE's input to the Design Control Document (DCD). Attachment 1 transmits markups identifying conceptual design material in brackets and a summary table which will be included in the introduction section of the DCD. Attachment 2 provides bracketed material identifying COL information items and a summary table for section 1.10 of the DCD Approved Design Material. Attachment 3 presents markups with Tier 2* material bracketed. In the actual DCD, this bracketed material will also be printed in italics. Summary tables for the introduction of the DCD are also included.

Attachment 4 provides pages from Nuplex 80+ design documents (which have already been reviewed by NRC staff) to identify Tier 2* material in those documents. Please note that the Tier 2* material in Attachment 4 is submitted conditionally, based on our understanding that changes to Tier 2* material do not necessarily constitute an Unreviewed Safety Question nor automatically provide the opportunity for a public hearing.

Attachment 5 transmits markups to Chapters 5, 6, 17, and 19 which resulted from the removal of PRA methods and results.

Please note that during the preparation of the material in Attachments 1 - 5, editorial and minor technical changes were discussed with NRC staff and included in the corresponding attachment.

200017

ABB Combustion Engineering Nuclear Power

Combustion Engineering, Inc. P.O. Box 500 Telephone (203) 688-1911
1000 Prospect Hill Rd. Fax (203) 285-5203
Windsor, CT 06095

9410210016 941012
PDR ADOCK 05200002
A PDR

D032

If you have any questions, please call me or Mr. Stan Ritterbusch at (203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

S. E. Ritterbusch for

C. B. Brinkman
Director
Nuclear Systems Licensing

SER/lw

cc: P. Lang (DOE)
J. Santucci (EPRI)
T. Wambach (NRC)

ATTACHMENT 1

Table 1-1: Index of Conceptual Design Information

Conceptual Design Item	Reference ADM Section
Administration Building	1.2.1.4.1.1
Personnel Access Portal	1.2.1.4.1.2
Switchyard	8.2.1.2
Warehouse	1.2.1.4.1.3
Emergency Operations Facility	13.3.3.2.1; 13.3.3.2.2
Compressed Gas Systems	1.2.11.18; 9.5.10.2; 9.5.10.2.1; 9.5.10.5
Station Service Water Pump Structure	3.8.4.1.3; 9.2.1.2.1.2; 9.2.1.2.1.4
Ultimate Heat Sink, Including SSWS Intake/Discharge	9.2.5.2; 9.2.5.4; 9.2.5.5
Potable and Sanitary Water System Structure	9.2.4
Condenser Circulating Water System	10.4.5.1.1; 10.4.5.2; 10.4.5.5
Offsite Power System	8.1.1; 8.2.1.1; 8.2.1.6
Potable and Sanitary Water System	9.2.4; 9.2.4.2; 9.2.4.2.1; 9.2.4.2.2; 9.2.4.5
Security System	13.6.1
Service Water Pump Structure Ventilation System	9.4.8.2; 9.4.8.5
Layout and Equipment for the Laboratory Facilities	13.3.3.4.1
Layout and Equipment for the Onsite Decontamination Facilities	13.3.3.6.1
Offsite Communications	9.5.2.2.5

1.2.1.4.1 Site-Specific Structures Description and Interface Requirements

Some structures which house non-safety related and certain safety-related systems and components are supplied by the licensee and are not included in the System 80+ design certification. To ensure that the design of such structures is compatible with the System 80+™ Standard Design, certain interface requirements must be met by the applicant (owner/operator). The following sections present the interface requirements and conceptual descriptions for the Administration Building, Personnel Access Portal and Warehouse. In addition to lists of interface requirements, the word "shall" is used to identify interface requirements in descriptive text. The remainder of the description is conceptual and it is not intended to be binding on the COL holder.

Interface requirements for structures which are related to a specific mechanical or electrical system are covered in the appropriate CESSAR-DC chapter, e.g. the Station Service Water Pump Structure is covered in Section 9.2.1, Station Service Water System. Section 1.9 contains an index of all interface requirements contained in CESSAR-DC.

1.2.1.4.1.1 Administration Building

An Administration Building shall be provided by the licensee. [This building provides office and support space for station administration and management personnel who have no need to be located within the Protected Area.]

[A typical Administration Building is designed as non-safety related, non-seismic structure with the following conceptual features. The building is a steel-framed structure with a steel deck roof covered by non-combustible roofing. Walls are insulated metal siding or masonry. Roof drainage and clean floor drainage are discharged to the storm and waste water system. The building is located immediately outside the Protected Area fence at the entrance to the plant, near the Personnel Access Portal building. Air conditioning and heating is provided to meet normal office environment conditions.]

1.2.1.4.1.2 Personnel Access Portal

The Personnel Access Portal (PAP) shall be provided by the licensee, and shall be designed to provide the following functions:

A. Serve as access point through the Protected Area Boundary.

B. Provide facilities to search, badge, and permit access to the Protected Area.

C. Provide the Secondary Alarm Stations.

D. Provide the required bullet-resistant features to support security force functions.

[A typical PAP building is a masonry building with non-combustible roofing on a metal deck. The PAP building is located along the Protected Area fence at the entrance to the plant, near the Administration Building. A PAP building ventilation system is provided to maintain the building within design temperature limits.]

1.2.1.4.1.3 Warehouse

The licensee shall provide a warehouse to accommodate the following:

A. Material access to the Protected Area incorporating the Vehicle (and Cargo) Access Portal (VAP).

B. Loading docks, search areas, QA inspection and QA Hold Areas, along with systems and fixtures to provide bulk storage of QA and non QA parts and supplies.

C. A material issue area to control dispensing of materials for maintenance.

[A typical warehouse is founded at grade on a reinforced concrete foundation. The warehouse is typically a metal enclosed building with a structural steel frame and non-combustible roofing. The warehouse ventilation system is designed to meet the appropriate requirements of ANSI/ASME NQA-2 Part 2.2.]

1.2.2 SYSTEM 80+ STANDARD DESIGN - SCOPE AND DESCRIPTION

The scope of the System 80+ Standard Design (see Section 1.1.1) covers an essentially complete nuclear power plant and includes all structures, systems, and components that can significantly affect safe operation. The primary design characteristics are summarized in the subsections below and improvements based on operating experience are summarized in Table 1.2-1. The seismic category, safety classification, and quality assurance requirement of structures, systems, and components are listed in Table 3.2-1.

Building and to protect the diesel generator units from flooding caused by a major pipe rupture.

A description of this system is provided in Section 9.5.9.

1.2.11.18 Compressed Gas Systems

[The compressed gas supply systems are provided to supply various gases for equipment and instrumentation cooling, purging, diluting, inerting, and welding. The major items of equipment are the high pressure gas cylinders and pressure regulators to control the pressure and distribution of the various gases used throughout the plant. These compressed gas supply systems are non-safety-related and any failure does not jeopardize the operation of any safety-related components or systems.]

A description of these systems is provided in Section 9.5.10.

1.2.11.19 Potable and Sanitary Water Systems

Those portions of the Potable and Sanitary Water Systems (PSWS) that are within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are within the scope of the Certified Design. Those portions of the PSWS that are not within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are not within the scope of the Certified Design. Out of scope portions of the system are licensee supplied and are site specific.

These systems process water for general plant use. These systems serve no safety functions and any malfunction has no adverse effect on any safety-related system. The requirements of General Design Criterion 60 are met as related to design provisions provided to control the release of liquid effluents containing radioactive material from contaminating the PSWS.

These systems are described in Section 9.2.4.

1.2.11.20 Demineralized Water Makeup System

The Demineralized Water Makeup System supplies filtered, demineralized water to the Condensate Storage System for makeup and to other systems throughout the plant that require high quality, non-safety-related, makeup water. This system, therefore, serves no safe shutdown or accident mitigation function, and has no safety design bases.

The Demineralized Water Makeup System Demineralizer trains are located in the Station Services Building. A description of the Demineralized Water Makeup System is presented in 9.2.3.

3.8.4.1.3 Station Service Water Pump Structure

The Service Water Pump Structure is classified as a Seismic Category I structure and is not included in the scope of design certification due to its specific site design requirements. The Station Service Water Pump Structure interface requirements are described in Section 9.2.1.1.4.

[The building includes a mat type foundation and a reinforced concrete superstructure with rigid walls.] The service water pump room and its supporting elements will be protected against flooding.

The Service Water Pump Structure shall be designed to the same criteria (Section 3.8.4.5) as other Seismic Category I structures as well as including consideration of slosh effects using the guidelines of Reference 19. The design shall also consider wave action due to the maximum hurricane flood.

3.8.4.1.4 Diesel Fuel Storage Structures

Each of the two Diesel Fuel Storage Structures is classified as a Seismic Category I, reinforced concrete structure containing two bays. Each bay encloses a diesel fuel oil tank, a tank vent, a sump with a sump pump, and necessary piping. The bays are separated from each other and from the adjacent equipment room by two-hour rated fire barriers. The building arrangement for the Diesel Fuel Storage Structure is shown on Figure 1.2.-24. An unloading pad is provided to retain any spills during the fuel oil deliveries.

The adjacent equipment room is a Seismic Category II steel framed structure with insulated metal siding and metal deck roof. The equipment room is designed for the SSE using Seismic Category I criteria.

The Diesel Fuel Storage Structures are not connected to the Nuclear Island Structures except by underground fuel transfer piping.

3.8.4.1.5 Component Cooling Water Heat Exchanger Structure

The Component Cooling Water (CCW) Heat Exchanger Structure arrangement is shown on Figure 1.2-25. The structure is one of two reinforced concrete buildings classified as Seismic Category I which house the CCW heat exchangers. The two structures provide complete physical separation between the two divisions of the CCW and station service water (SSW) systems. Each structure contains two CCW heat exchangers, CCW and SSW piping and associated valves, sumps and sump pumps. A division of the CCW piping enters the structure through a separate Seismic Category I, reinforced concrete pipe tunnel which runs below grade to the nuclear annex.

8.0 ELECTRIC POWER

8.1 INTRODUCTION

An offsite power system and an onsite power system are provided to supply the unit auxiliaries during normal operation and the Reactor Protection System and Engineered Safety Feature Systems during abnormal and accident conditions.

8.1.1 OFFSITE POWER SYSTEM

[The typical offsite power transmission system grid may consist of interconnected hydro plants, fossil-fueled plants, combustion turbine units, and nuclear plants supplying energy to the service area at various voltages.]

The unit is connected to a switchyard and to the transmission system via a transmission line. The switchyard is connected to the onsite generator circuit breaker through the unit main transformer, which allows this line not only to supply power to the transmission system during normal operation, but also to serve as an immediately available source of preferred power. Another separate transmission line is connected to the preferred switchyard interface II via the switchyard and two reserve auxiliary transformers, to provide an independent second immediate available source of offsite power to the onsite power distribution system for safety, non-safety and permanent non-safety loads.

A description of a representative offsite power system is provided in Section 8.2.

8.1.2 ONSITE POWER SYSTEMS

The onsite power system for the unit, as depicted on Figures 8.3.1-1 and 8.3.1-2, consists of the main generator, the generator circuit breaker, unit main transformer, the unit auxiliary transformers, reserve auxiliary transformers, the diesel generators, an alternate AC source, the batteries, and the auxiliary power system. Under normal operating conditions, the main generator supplies power through an isolated phase bus and generator circuit breaker to the unit main and unit auxiliary transformers. The unit auxiliary transformers are connected to the bus between the generator circuit breaker and the unit main transformer. During normal operation, station auxiliary power is supplied from the main generator through these unit auxiliary transformers. During startup and shutdown, the generator circuit breaker is open, and station auxiliary power is supplied from the transmission system through the unit main and unit auxiliary power transformers.

8.2 OFFSITE POWER SYSTEM

8.2.1 SYSTEM DESCRIPTIONS

The utility grid system and switchyard(s) are out of scope and site specific items which shall be provided by the license applicant. The following sections contain a description of a typical grid system and switchyard and interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements which are mandatory from the text that is purely descriptive.

8.2.1.1 Utility Grid System

[The utility grid system, which is not within the scope of the System 80+ Standard Design, may consist of interconnected hydro, fossil fueled and nuclear plants supplying energy to the service area at various voltages. The grid transmission system is also a source of reliable and stable power for the onsite power distribution system.] The grid system design shall include at least two preferred power circuits, each having sufficient capacity, be continuously energized, and available to supply power to the plant safety-related systems within a few seconds following a loss of coolant accident (LOCA) to assure that core cooling, containment integrity, and other vital safety functions are maintained. The offsite transmision circuits shall be sized to supply their load requirements, during all design modes, of their respective Class 1E divisions and Non-Class 1E loads.

8.2.1.2 Utility Grid and Switchyard Interconnections

[The switchyards are connected to the primary transmission system by overhead transmission lines. Figures 8.2-1 and 8.2-2 depict typical interconnections of the switchyards and onsite power.]

The two designated offsite power transmission lines (Preferred I and II) shall be designed and routed to minimize, to the extent practical, the likelihood of their simultaneous failure. These transmission lines shall originate at separate switching stations. No other lines shall cross above these two circuits. These circuits shall be routed to ensure that no single event, such as a tower falling or a line breaking can simultaneously affect both circuits in such a way that neither can be returned to service in time to prevent fuel design limits or design conditions of the reactor coolant pressure boundary from being exceeded. The two designated offsite power circuits shall terminate at two switchyards that are physically separate and electrically independent to the extent practicable.

8.2.1.3 Station Switchyard

A transmission line from the primary transmission system shall terminate in the preferred switchyard interface I with provisions for additional lines to be added in the future. The Unit

as a minimum, all tests outlined in Appendix A, Subsection B.2, to SRP Section 8.2.

After the unit generator has been brought to rated speed and its field applied, the unit generator shall be then connected to the system by closing the generator circuit breaker. Automatic and manual synchronization are provided and supervised by synchronizing relays.

8.2.1.5.1 Offsite Power System Protective Relaying

The offsite power system protective relaying system shall be designed to remove from service with precision and accuracy any element of the offsite power system subjected to an abnormal condition that may prove detrimental to the effective operation or integrity of the unit.

8.2.1.6 Reliability Considerations

The transmission system shall be designed to conform to the reliability criteria established by the owner's appropriate electric reliability council. Typically, transmission systems are designed to avoid system cascading upon the occurrence of any one of the following:

A. Loss of Generation

1. Sudden loss of entire generating capability of the largest operating or worst case unit on the electrical grid.

B. Loss of Load

1. Sudden loss of largest load or major load center.

C. Loss of Transmission

1. The outage of the most critical transmission line caused by a three-phase fault during the outage of any other critical transmission line, or

2. Sudden loss of all lines on a common right-of-way, or

3. Sudden loss of a substation (limited to a single voltage level within the substation plus transformation from the voltage level), including any generating capacity connected thereto, or

4. Delayed clearing of a three-phase fault at any point on the system due to failure of a breaker to open.

In addition to the transmission system design, the switching arrangement in the switchyard and the redundant relaying that is provided minimizes the probability of losing offsite power.

8.2.2 ANALYSIS

8.2.2.1 Grid Stability and Availability Analysis

Grid stability and availability analyses involving interconnections with the primary transmission system shall be performed by the site operator. These analyses shall demonstrate that the 13,800V non-safety load buses do not subject the reactor coolant pumps to sustained frequency decays of greater than 3 Hz/sec.

Voltage variations of the transmission system shall not cause voltage variations at the loads of more than +/- 10% of the loads' nominal voltage rating.

The normal steady-state frequency of the offsite system shall be within +/- 2 Hertz during recoverable periods of system instability.

8.2.2.2 Offsite and Switchyard Power Systems Single Failure Analysis

The design of the offsite power system shall be consistent with failure modes and effects analysis in Tables 8.2-1 and 8.2-2.

The pump motors are connected to their associated 4160 volt Class 1E Auxiliary Power System. In the event offsite power is lost, the pumps are stopped and restarted in accordance with the diesel generator's load sequencing.

The sizing of the station service water pumps is based on the following operating mode requirements:

Normal power operation	- 1	pump per division operating
Normal shutdown (24 hours)	- 4	pumps operating
Safety-grade shutdown (24 hours)	- 2	pumps required, in a single division
Post-LOCA	- 1	pump required, (corresponding with the operating CCW heat exchanger)

During normal power operation as cooling requirements increase, the additional pump in a division may be needed.

The station service water pumps are provided with at least 7% margin in head at the pump design point. The head versus flow curve is continuously rising from the design point to shut-off.

The minimum available NPSH is the smaller of (1) 25 percent greater than, or (2) 10 feet greater than the required NPSH specified by the pump vendor.

The available NPSH is calculated at the highest expected operating temperature and flow, at the normal water elevations, and assuming the travelling screens are 50% clogged. The available NPSH exceeds the required NPSH for worst case UHS water elevations for all operation, flow, and temperature conditions. (Note: For worst case UHS water elevation, the margins previously specified need not apply.)

9.2.1.2.1.2 SSWS Pump Structure

[The pump structure is a Seismic Category I design.

The UHS inlet to the station service water pumps is equipped with a safety grade screen system (see Section 9.2.1.2.1.4).]

The COL applicant will provide a detailed description of the SSWS pump structure.

9.2.1.2.1.3 Piping, Valves, and Fittings

Piping to and from the CCW heat exchangers is corrosion resistant. Materials are to be selected on a site-specific basis to be compatible with the ultimate heat sink makeup water

chemistry and water treatment. All safety-related piping, valves, and fittings are supplied in accordance with ASME Code Section III, Class 3.

All material exposed to the raw water will be tested at typical operating temperatures with similar station service water chemistry to evaluate the adequacy of the materials.

The supply and return piping to and from system components in a division is physically separated from the supply and return lines in the redundant division.

The nominal flow velocity in the SSWS piping does not exceed 12 ft/sec nor is less than 8 ft/sec for nominal operating conditions.

Vents are installed at all high points, and drains are installed at all low points in the SSWS.

Vents are located to reduce the chances for water hammer after pump startups. Valve opening and closing times are selected to minimize water hammer effects.

9.2.1.2.1.4 SSWS Pump Structure Screens

[A safety grade traveling screen with a screen wash system is provided for each pump structure. The traveling screens are located prior to station service water pump inlets. The screen mesh size is selected to prevent flow blockage of the pump inlets and to limit ingestion of biofouling, organics and debris.]

9.2.1.2.1.5 Station Service Water System Strainers

Each station service water pump is provided with a station service water strainer which is located at the pump discharge. This is to prevent clogging of the downstream heat exchangers. The strainers are of the automatic backwash type. The strainers backwash with station service water from their corresponding pumps. The strainers are designed to retain particles greater than 1/16 inch in diameter and to be consistent with the fouling design limits of the component cooling water heat exchangers.

9.2.1.2.1.6 Station Service Water System Sump Pumps

Each division has two station service water sump pumps, two for SSW Sump 1 and two for SSW Sump 2. During maintenance, station service water from the component cooling water heat exchangers is drained to these sumps. The sump water is returned to the UHS by the sump pumps.

9.2.4 POTABLE AND SANITARY WATER SYSTEMS

Those portions of the PSWS that are within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are within the scope of the Certified Design. Those portions of the PSWS that are not within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are not within the scope of the Certified Design. Out of scope portions of the system are licensee supplied and are site specific.

[Water from the Filtered Water System is processed by the PSWS for general plant use. Potential sources for the Filtered Water System include lakes, rivers, wells, and municipal water supplies. A backflow preventer is provided between the Potable Water System supply and the Filtered Water System Supply to other plant systems.]

Section 9.2.4.1 provides the interface requirements which must be met by the licensee supplied design. Subsequent sections of Section 9.2.4 contain descriptive information concerning a conceptual design for the Potable and Sanitary Water Systems.

9.2.4.1 Interface Requirements

The PSWS shall be designed to meet the requirements of General Design Criterion 60 of 10 CFR 50 Appendix A, as related to provisions to control the release of liquid effluents containing radioactive material from contaminating the PSWS. The following specific requirements shall be met:

A. There shall be no interconnections between the Potable and Sanitary Water Systems and systems having the potential for containing radioactive material.

B. The Potable Water System shall be protected by an air gap, where necessary.

The licensee shall ensure that the sewage treatment facility design complies with applicable state and local regulations. Adequate treatment facility capacity shall be provided to accommodate the maximum number of personnel assigned to the site, with provisions for expansion as necessary.

9.2.4.2 System Description

[The Potable and Sanitary Water Systems consist of a Potable Water System and a Sanitary Drainage System. The Potable and Sanitary Water Systems are shown in Figure 9.2.4-1. The systems include all components and piping from the Filtered Water System to all points of discharge to sewage facilities.]

The COL applicant will provide information on the potable and sanitary water systems design.

9.2.4.2.1 Potable Water System

[Water for drinking and sanitary services is supplied by the Potable Water System. Filtered water from the Filtered Water System is pumped to the potable water storage tank by two potable water pumps. The potable water chlorination pumps take suction from the hypochlorite day tank and chlorinate the potable water to the required chlorine residual. The potable water storage tank and distribution headers are kept pressurized by compressed air from the Station Air System so that water can be provided throughout the plant as needed. A branch sends potable water to a heater and to a hot water distribution system where it is distributed throughout the plant.]

9.2.4.2.2 Sanitary Drainage System

[The Sanitary Drainage System collects liquid wastes and conveys them to the sewage treatment system. This system is installed in accordance with all applicable state and local codes.]

9.2.4.3 Safety Evaluation

The Potable and Sanitary Water Systems do not perform any safety functions and any malfunction has no adverse effect on any safety related system.

9.2.4.4 Inspection and Testing Requirements

Prior to startup all piping is hydrostatically tested and flushed in accordance with applicable codes and standards. Operability of the Potable and Sanitary Water Systems is verified by placing these systems into operation prior to fuel loading. Potable water quality and treatment are monitored in accordance with the requirements of state and local departments of health and environmental control.

9.2.4.5 Instrumentation Requirements

[Sufficient instrumentation is provided to monitor system performance and to control the system automatically or manually under all operating conditions.]

2. Non-current site related events, including transportation accidents, oil spills and fires.

3. Credible single failures of man-made structures.

4. Sabotage

E. In order to ensure the normal cooldown (two division cooldown) performance requirements given in Section 5.4.7.1.2.F.1 the Ultimate Heat Sink temperature at the SSWS inlet must remain at or below 95°F throughout the cooldown. One percent exceedance meteorologic conditions can be utilized in showing acceptability, since this is a performance requirement and not a safety requirement.

F. For sites with severe winters, where ice formation of the Ultimate Heat Sink could occur, an analysis shall be provided showing the function of the Ultimate Heat Sink is not impaired during winter months. Where required, the intake structures shall be provided with a means of deicing, such as warm water recirculation, to prevent flow blockage of the SSW pump inlets.

G. The site water chemistry for the Ultimate Heat Sink shall be analyzed to determine if a water treatment system is required to minimize corrosion and fouling of the SSWS.

H. Water boundaries that form part of the protected area boundary shall be avoided, if at all possible.

9.2.5.2 System Description

[The Ultimate Heat Sink described here consists of a single passive independent cooling water pond connected to the SSWS through intake and discharge paths. However, it is recognized that site-specific conditions may require the use of two ponds to meet Regulatory Guide 1.27. The design brackets alternative Ultimate Heat Sinks which may be specified for a particular site if environmental restrictions limit the use of a cooling pond or if an alternative water supply is more reliable. Acceptable alternate ultimate heat sinks are an ocean, a large lake, a large river, a lake and a cooling pond, a river and a cooling pond, or a cooling tower and cooling pond.

The cooling water pond is provided with makeup water pumps to maintain level. Water chemistry is maintained by a site-specific water treatment system (i.e., chemical injection). Salinity buildup in a pond is limited by blowdown.

The Ultimate Heat Sink will operate for the required nominal 30 days following a postulated LOCA without requiring any makeup water to the source, and without requiring any blowdown from the pond for salinity control.]

9.2.5.3 Safety Evaluation

The Ultimate Heat Sink meets the intent of Regulatory Guide 1.27. The cooling water pond is Seismic Category I and of sufficient volume to provide the required nominal 30-day cooling capacity without makeup and under worst case meteorological conditions.

Ultimate Heat Sink temperature will not exceed the maximum allowable temperature required for cooling any safety-grade component through the component cooling water heat exchangers during a design basis accident concurrent with a loss of offsite power.

The function of the Ultimate Heat Sink is not lost during or after any of the following events:

A. Natural phenomena, including SSE, tornado, flood, and drought.

B. Non-concurrent site-related events, including transportation accidents, oil spills, and fires.

C. Credible single failures of man-made structures.

D. Sabotage.

9.2.5.4 Inspection and Testing Requirements

The COL applicant will provide site-specific aspects regarding the resolution of Generic Safety Issue 51, including maintenance and inspection programs.

[Samples of water and substrate will be collected annually to determine if biological fouling organisms have populated the water source. Upon the detection of biological fouling organisms, appropriate corrective action, such as the modification of the chemical treatment program, should be taken. However, consideration must be given to environmental regulations.]

9.2.5.5 Instrumentation Requirements

[The level of each cooling water pond is monitored and controlled. Alarms are provided in the main control room which actuate if the level of the pond approaches minimum allowable value, or the temperature approaches the maximum allowable value.]

9.2.6 CONDENSATE STORAGE SYSTEM

9.2.6.1 Design Bases

9.2.6.1.1 Overall Design Bases

A. The Condensate Storage System provides demineralized water for initial fill of the condensate and feedwater systems. As

G. The Station Service Water Pump Structure Ventilation System shall be controlled from the main control room. Instrumentation and controls shall be provided in accordance with ANSI/ANS 59.2 and be designed such that the following operational criteria are met:

1. Fans shall be automatically started whenever a pump associated with that particular division is started.

2. Fans shall always be stopped manually.

3. A manual start shall be provided for fans for use during testing and maintenance.

H. If required by the historical site weather conditions, non-safety heating shall be provided to maintain the temperature within the station service water pump structure greater than 40°F.

9.4.8.2 System Description

[The Station Service Water Pump Structure Ventilation System consists of two 100% capacity essential vane-axial supply fans with associated dampers, ductwork, supports and control systems per pump compartment. A non-safety related vane-axial fan is provided to supply ventilation air to the pool area below the pumps when maintenance or inspection is performed in this area.

The ventilation fans are automatically activated in response to temperature. A low temperature control will deactivate the fans when the temperature is below 40°F.

Each safety-related fan is provided with a check damper on the fan discharge to prevent backflow through the fan on standby.]

9.4.8.3 Safety Evaluation

The Station Service Water Pump Structure Ventilation System is an engineered safety feature. The two 100% capacity fans in each pump compartment are powered from separate trains of the onsite power system. This assures the integrity and availability of the ventilation system in the event of a loss of offsite power or any single active failure.

9.4.8.4 Inspection and Testing Requirements

The Station Service Water Pump Structure Ventilation System operates as required to limit temperature in the pump structure and is accessible for periodic inspection. Safety-related electrical components, switchcovers, and starting controls are tested during preoperational tests.

9.4.8.5 Instrumentation Application

[Instrumentation is provided to provide automatic or manual operation of the system, both from local and/or remote locations and permit verification that the system is operating satisfactorily.

Indication of the fan operating status is provided in the control room. Failure of a running fan is alarmed in the control room.

Space temperature indication for the pump structure is provided in the control room along with alarm indication of high and low temperatures.]

9.4.9 NUCLEAR ANNEX VENTILATION SYSTEM

9.4.9.1 Design Basis

The Nuclear Annex Ventilation System consists of a general supply and exhaust ventilation system that performs heat removal and air exchange functions. The ventilation system is supplemented by individual cooling units and ventilation fans of the Normal Chilled Water System (NCWS) and Essential Chilled Water System (ECWS) discussed in Section 9.2.9 that serve essential and non-essential mechanical equipment areas. The Nuclear Annex Ventilation System serves all areas of the Nuclear Annex Building. The Nuclear Annex structure is designed to Seismic Category I standards as noted in Table 3.2-1.

The safety-related mechanical equipment room ECWS cooling systems are designed to maintain the space temperatures below 100°F at times when the served equipment must operate. At least one train of essential mechanical equipment rooms is maintained below 100°F assuming a single failure of an active component concurrent with a loss of offsite power.

The safety-related mechanical equipment room ECWS cooling systems perform the required safety function following a safe shutdown earthquake, and are able to withstand the effects of appropriate natural phenomena such as tornadoes, floods, and hurricanes (GDC 2).

The safety-related mechanical equipment room ECWS cooling systems are protected from the effects of internally generated missiles, pipe break effects, and water spray (GDC 4).

The Nuclear Annex Ventilation System is designed to provide ventilation and heat removal for personnel access to non-essential areas of the building. The design temperature range for the non-essential building areas is 60°F to 100°F.

The Nuclear Annex building is maintained at a slight negative pressure with respect to the environment to assure that all potentially radioactive releases are monitored prior to atmospheric discharge. As an ALARA consideration, design air flow patterns within the building are generally from clean areas to potentially contaminated areas.

9.5.2.2.4 Intraplant Sound-Powered Telephone Systems

Intraplant sound-powered telephone systems, independent of the PABX and PA systems, are provided for normal and abnormal/accident conditions. These sound-powered systems include, but are not limited to, the following:

A. Maintenance Circuit consists of phone jacks located throughout the plant which can be patched together to establish communications between areas as necessary.

B. Refueling Circuit consists of phone jacks located in areas required for refueling operations.

C. Emergency Circuit consists of phone jacks connecting specific areas of the plant for the purpose of communication during auxiliary shutdown operations.

9.5.2.2.5 Offsite Communications

[Normal offsite communications is provided by public telephone lines and the utility private network which is connected to the PABX telephone switch.]

[Emergency offsite communications, independent of the PABX telephone switch, is provided by public telephone lines and the utility private network lines connected directly to specific telephones located in critical areas of the plant and support facilities.] Emergency telephones are color-coded to distinguish them from the intraplant telephone system. The emergency telephones include, but are not limited to, the following:

A. Emergency Notification System (ENS)

   Provides a communications link with the Nuclear Regulatory Commission (NRC).

B. Health Physics Network (HPN)

   Provides a communications link with the NRC's health physics personnel.

C. Ringdown Phone System

   Provides communications link with local and state agencies.

9.5.10 COMPRESSED GAS SYSTEMS

9.5.10.1 Design Bases

9.5.10.1.1 Overall Design Bases

The compressed gas supply systems are provided to supply various gases for equipment and instrumentation cooling, purging, diluting, inerting, and welding. [The major items of equipment are the high pressure gas cylinders and pressure regulators to control the pressure and distribution of the various gases used throughout the plant. These compressed gas supply systems are non-safety-related and any failure does not jeopardize the operation of any safety-related components or systems.]

9.5.10.1.2 Interface Requirements

Bulk storage of high pressure gas cylinders is an out of scope item which shall be provided by the applicant. The licensee shall verify that the following interface requirements are met to ensure adequacy with the System 80+™ Standard Design:

A. Bulk storage of gas cylinders shall be located in areas which contain no safety-related equipment such that rupture of a cylinder does not adversely affect the operability of any safety-related component or system.

B. Storage of flammable and combustible gases shall be located in accordance with applicable requirements of local, state, and Federal regulations and the NFPA Fire Code.

C. Hazardous gases shall not be stored in close proximity to any HVAC system fresh air in-take, the control room, or the compressed air system in-takes.

D. Bulk storage of gas cylinders shall be located away from high traffic areas to the maximum extent practical and outside the turbine missile path.

E. Storage locations shall provide adequate protection of high pressure gas cylinders from the environment.

9.5.10.2 System Description

[The compressed gas systems are arranged into the following separate and isolated subsystems:

A. N_2 System

High pressure Bulk Storage cylinders and High usage LN_2 evaporators.

B. H_2 System

High pressure cylinders. H_2 Leak Detection system required.

C. O_2 System

High pressure cylinders. All distribution hardware shall be oil free with no combustibles and specifically rated for O_2 service.

D. CO_2 System

High pressure cylinders. CO_2 Leak Detection system required.

E. Argon/Methane

High pressure cylinders for use in radiation detection equipment.

F. Acetylene System

High pressure cylinders for use in welding service applications.

G. Argon System

High pressure cylinders for use in inert welding service applications.

9.5.10.2.1 Valves

All valves specified for compressed gas service are designed and rated specifically for gas service with resilient materials used for sealing surfaces. Valves are packless and utilize either diaphragm or bellows stem seals to prevent or minimize potential gas leakage.]

9.5.10.3 Safety Evaluation

The compressed gas supply systems serve no safety function.

The following System 80+ interface requirements are met:

A. Steam Generator

Nitrogen is used to maintain a pressure of 5 psig in the steam generator during shutdown. This nitrogen overpressure

No single failure allows the compressed nitrogen system delivery pressure to exceed 700 psig.

9.5.10.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation and as a result of normal usage. Equipment not in continuous use is subject to periodic testing and visual inspection.

9.5.10.5 Instrumentation Application

An "on-demand" manual selection capability is provided to remotely monitor the various gas systems operation status. This includes a multichannel control room monitor for the following:

A. Manifold pressures

B. Manifold temperatures

C. Flow rates of flammable or toxic gases

A low pressure annunciator is provided to alarm the control room when bottled gas supplies are nearly depleted. A high flowrate annunciator is provided to alarm the control room when flammable or toxic gas flowrates exceed this normal operating range.

Vaporizers for LN_2 and other areas stored in liquid form have fail-safe controls to prevent cryogenic liquid from reaching the serviced component in case of vaporizer failure or loss of power. Alarms for vaporizer functions failure are provided.

Acceptance criteria are that the TBV open on receipt of the signal simulating turbine bypass.

10.4.4.5 Instrumentation Application

The control system for the Turbine Bypass System is described in Section 7.7.1.1.5 (Steam Bypass Control System).

Refer to Section 7.7.1.1.12 for a description of the Process-Component Control System which provides applicable non-safety remote monitoring and controls from the main control room.

10.4.5 CONDENSER CIRCULATING WATER SYSTEM

10.4.5.1 Design Bases

10.4.5.1.1 Overall Design Basis

The Condenser Circulating Water System (shown in Figure 10.4.5-1) is a non-safety interface system that provides cooling water for the turbine condensers and rejects heat to the environment via the normal heat sink. **NOTE:** Cooling towers are specified for the reference plant; however, other alternate heat sinks can be utilized for specific sites as long as they also meet the interface requirements given in Section 10.4.5.1.2. These shall be discussed in the site-specific SAR supplement. [The tower is capable of supporting full reactor thermal output at site 0% exceedance atmospheric conditions. Pump head, piping size, and cooling tower height are optimized based on capital and pumping cost. Pumps are sized such that full load can be maintained with one pump down except during the three hottest summer months of the year.

Estimated circulating water system operating parameters based on a natural draft cooling tower site and bounding meteorological conditions are presented in Table 10.4.5-1.] The actual design and operating parameters will be determined on a site specific basis.

10.4.5.1.2 Interface Requirements

Although the majority of the condenser Circulating Water System is an out of scope system provided by the applicant, the parts of the system that are in the Turbine Building are within the certified design scope. These portions are indicated in Figure 10.4.5-1 for the reference plant by the location code "TB".

A reference circulating water system is discussed in the sections immediately following 10.4.5.2. The licensee shall verify that the interface requirements listed in this section are met to ensure adequacy with the System 80+™ Standard Design.

F. To measure individual circulating pump flow and total flow to the main condenser, access ports shall be provided to allow temporary flow meters to be installed in the main circulating water piping.

G. Where forced draft towers are used, valving and controls shall be provided such that each cooling tower can be isolated during normal power operation.

H. Valving and controls shall be provided such that each of the condenser circulating water pumps can be isolated during normal operation.

I. Valving and controls shall be provided such that the condenser waterbox sections can be isolated and the unit operated at partial load.

J. An interlock shall be provided to prohibit a condenser circulating water pump from starting should it be in reverse rotation or its discharge valve open.

K. The instrumentation and controlled equipment shall be designed to interface with the Process Component Control System, described in Section 7.7.1.1.12, if necessary for remote monitoring or control from the main control room.

10.4.5.2 System Description

The condenser circulating water pumps circulate cooling tower basin water through the turbine condensers. Water chemistry is maintained by blowdown and chemical addition. Basin level is maintained with makeup water.

The towers may be natural or mechanical draft for a particular site. (A single natural draft tower may be used where prescribed maintenance can be accomplished during the specified refueling time period.) **NOTE:** A single natural draft tower is specified for the reference plant. Valving is provided such that each tower can be isolated during normal power operation. The tower contains no wooden components exposed to circulating water. Tower design allows complete drainage, silt removal, and good access to the fans (if applicable) for inspection and maintenance. Tower icing during subfreezing conditions is prevented by a fill bypass system which diverts a portion of the total hot water flow to the basin, louvers to restrict air flow, an ice prevention ring which distributes a portion of the total hot water flow across tower inlet air, and a fill zoning subsystem which diverts water to limited locations in the tower.

Four condenser circulating water pumps are motor-driven, high flow, low head pumps. Valving is provided such that each pump can be isolated during normal operation. Suction screens prevent debris ingestion. Pump material selection is based on compatibility with circulating water chemistry and tested for

acceptability. Pump location is such that the available NPSH exceeds the required NPSH by at least 10 feet, and flooding of one pump will not affect any of the other pumps. Seal water for the pumps is maintained within the temperature and purity limits established by the manufacturer. High quality cooling water for the pump bearings is provided in sufficient quantity to maintain bearing temperatures within manufacturers limits under full pump output during the hottest days of the year. Separate flow paths, each with their own pressure control, are provided for each pump support system requiring cooling water (e.g., thrust bearing cooling, seal water cooling, wear ring flushing).

The Main Condenser waterbox is divided into sections. To prevent the introduction of non-condensate quality water into the condensate and feedwater system, conductivity monitors in each main condenser hotwell shell are used to detect leakage of circulating water, as described in Section 10.4.1.5.

The reference plant condenser incorporates a three zone, multi-pressure condenser (3 condenser shells). Each condenser shell consists of two parallel tube bundles to permit maintenance and cleaning of the circulating water system water boxes and condenser tube bundles during operation. Valving is provided such that each of the two condenser waterbox flowpaths can be isolated and the unit operated at partial load. Means are provided for entry into the waterboxes and circulating water piping for repair and cleaning. Entry provisions allow cleaning within one eight-hour shift. Drains are available such that the circulating water system can be drained within eight hours.

The condenser circulating water system (CWS) is designed to minimize the potential for water hammer by providing adequate filling and high point venting. Valve opening/closing times are selected to minimize water hammer effects. All CWS piping and components are designed to meet the requirements of ANSI/ASME B31.1.

Blowdown is provided to control the concentration factor of cooling tower solids. A throttling valve allows regulation of the blowdown flow.

Acid is injected in the cooling tower inlet header. Biocide and scale inhibitor are injected into the basins. Water treatment for the circulating water system is based on site makeup water chemistry, blowdown requirements, environmental regulations, and system materials. Consideration is given to the need for biogrowth control, pH control, and scale buildup. Water treatment follows the options in EPRI report CS-2276 (Reference 1).

Makeup flow to the cooling tower basin is regulated by a throttling valve. The tower is provided with two 100% capacity makeup pumps. Trash racks and traveling screens at tne makeup intake structure prevent debris from entering the pumps. The makeup pump discharge strainers additionally remove debris which might enter the circulating water system. Warm water from the condenser outlet is used to prevent icing of the intakc structure during winter months. The intake structure is separated from the discharge structure to minimize the potential for recirculation.

An automatic condenser cleaning system is provided.]

10.4.5.3 Safety Evaluation

The Condenser Circulating Water System does not perform any safety functions. Thus reliance on this system was not assumed in the safety analysis.

10.4.5.4 Tests and Inspections

Prior to startup, all piping is hydrostatically tested and flushed to applicable codes and standards. A full power performance test is performed immediately following installation. Condenser inlet/outlet temperature, cooling tower inlet/outlet temperature, cooling water flow, circulating pump suction/discharge pressure, ambient weather conditions (dry bulb, wet bulb, wind speed), and the position of all valves are recorded. The cooling tower is tested in accordance with Cooling Tower Institute Standard ATC-105.

After startup, the circulating water pumps, valves, and motor operators are inspected and maintained on a routine basis.

10.4.5.5 Instrumentation Applications

[Pressure is measured at each circulating water pump suction and discharge. Differential pressure is also monitored across each pump. Temperature is measured at the condenser inlet and outlet for each tube bundle. The circulating water is also monitored for pH and conductivity. Permanent flow meters measure individual circulating pump flow and total flow to the main condenser. Access ports allow temporary flow meters to be installed in the main circulating water piping. Cooling tower basin level is monitored and used to control makeup flow. Blowdown flow is manually adjusted as required to maintain desired water chemistry.]

Refer to Section 7.7.1.1.12 for a description of the Process-Component Control System which provides applicable non-safety remote monitoring and controls from the main control room.

A. Plant systems variables.

B. In-plant radiological variables.

C. Meteorological information.

D. Offsite radiological information.

Trend information display and time-history display capability is provided in the TSC to give the TSC personnel a dynamic view of the plant status during abnormal operating conditions. The TSC displays are designed so that callup, manipulation, and presentation of data is easily performed. The TSC data display format presents information that is easily understood by the TSC personnel performing analyses.

The Data Processing System (DPS) data set associated with plant safety status is displayed in the TSC. This duplication will improve the exchange of information between the control room and the TSC. The total TSC data system reliability is designed to achieve an operational unavailability goal of 0.01 during all plant conditions above cold shutdown. Operational unavailability is defined as DOWN TIME divided by OPERATING TIME. E

13.3.3.1.9 Records Availability

The TSC includes provisions for a complete and up-to-date repository of plant records and procedures at the disposal of TSC personnel to aid in their technical analysis and evaluation of emergency conditions.

13.3.3.2 Emergency Operations Facility

The Emergency Operations Facility (EOF) is an out of scope item which shall be provided by the license applicant and is site specific. The following sections contain a description of a typical EOF and interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive. J

13.3.3.2.1 Summary Description

[The Emergency Operations Facility (EOF) is a nearsite support facility for the management of overall licensee emergency response (including coordination with Federal, State, and local officials), coordination of radiological and environmental assessments, and determination of recommended public protective actions.] The EOF has appropriate technical data displays and plant records as discussed in the site-specific SAR. E

[When the EOF is activated, the functions of providing overall emergency response management, monitoring and assessing radiological effluent and the environs, making offsite dose projections, providing recommendations to State and local officials, and coordinating with Federal officials shift to the EOF in accordance with site procedures.] Transfer of emergency response functions from the control room to the EOF under the various emergency classes shall be accomplished as outlined in Table 13.3.3-1. The EOF shall be designed to the habitability criteria given in Table 13.3.3-2.

13.3.3.2.2 Functions

The EOF is a licensee controlled and operated offsite support center. The EOF shall have facilities for:

A. Management of overall licensee emergency response.

B. Coordination of radiological and environmental assessment.

C. Determination of recommended public protective actions.

D. Coordination of emergency response activities with Federal, State, and local agencies.

[When the EOF is activated, it is staffed by licensee, Federal, State, local and other emergency personnel designated by the emergency plan to perform these functions. It is the location where the licensee provides overall management of licensee resources in response to an emergency having actual or potential environmental consequences.]

Facilities shall be provided in the EOF for the acquisition, display, and evaluation of all radiological, meteorological, and plant system data pertinent to determine offsite protective measures. These facilities are used to evaluate the magnitude and effects of actual or potential radioactive releases from the plant and to determine offsite dose projections. Facilities used in performing essential EOF functions shall be located within the EOF complex; however, supplemental calculations and analytical support of EOF evaluations may be provided from facilities outside the EOF. The licensee also may use the EOF as the post-accident recovery management center.

[The EOF allows the licensee to coordinate emergency response activities with local, State, and Federal agencies, including the NRC. Licensee personnel in the EOF use the evaluations of offsite effects to make protective action recommendations for the public to State and local emergency response agencies.

State and local agencies are responsible for implementing emergency response actions involving the general public. The State and local agencies may operate from the EOF or from their own control centers at other locations, dependent upon the site-specific provisions of the emergency plan at each plant. E J

13.3.3.2.3 Staffing and Training E

The licensee shall address all staffing and training issues. J

13.3.3.2.4 Size E

The EOF building or building complex shall be large enough to provide the following: J

A. Working space for the personnel assigned to the EOF as specified in the licensee's emergency plan, including State and local agency personnel, at the maximum level of occupancy without crowding (minimum size of working space provided is approximately 75 sq ft/person).

   The EOF working space is sized for at least 35 persons, including 25 persons designated by the licensee, 9 persons from NRC, and 1 person from FEMA. This minimum size is increased if the maximum staffing levels specified in the licensee's emergency plan, including representatives from State and local agencies, exceed 25 persons. E

B. Space for EOF data system equipment needed to transmit data to other locations.

C. Sufficient space to perform repair, maintenance, and service of equipment, displays, and instrumentation.

D. Space for ready access to communications equipment by all EOF personnel who need communications capabilities to perform their functions.

E. Space for ready access to functional displays of EOF data.

F. Space for storage of plant records and historical data or space for means to readily acquire and display those records.

G. Separate office space to accommodate at least five NRC personnel during periods that the EOF is activated for emergencies.

13.3.3.4 Laboratory Facilities

13.3.3.4.1 Summary Description

The Laboratory Facilities are out of scope items which shall be provided by the license applicant. [Consistent with the requirements stated in NUREG-0654, II.H.9 and NUREG-0737, II.B.3, the System 80+ Standard Plant design makes provisions for inclusion of both hot and conventional Laboratory Facilities. Hot facilities are currently located in the Nuclear Annex; additional hot facilities should be located in a Radwaste Building. Space for a large conventional laboratory should be provided in the Station Services Building. Locations for other, smaller lab facilities are allocated at various places throughout the plant.] The facilities themselves shall be designed according to particular owner preference, but they shall support efforts to monitor plant systems and environmental samples for compliance with technical specifications. Complete descriptions of the facilities shall be provided by the licensee.

The following sections contain interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive.

13.3.3.4.2 Function

The laboratory facilities shall provide for the following primary functions: J

A. to provide plant support services for routine analyses required for personnel protection, surveys, and related health physics functions.

B. to provide normal and post-accident cold chemical analyses on required plant chemistry samples.

C. to provide routine and post-accident counting on all plant radioactivity samples.

D. to provide grab sample analyses used as a check on the accuracy of the continuous on-line process monitoring instrumentation.

E. to provide a facility to store and secure radioactive calibration and check sources and instruments undergoing calibration, maintenance, or repair.

13.3.3.6 Onsite Decontamination Facilities

13.3.3.6.1 Summary Description

The Onsite Decontamination Facilities (ODF), located in the Nuclear Annex (el. 91+9) and in the Radwaste Facility, are out of scope items which shall be provided by the license applicant. These facilities shall be provided to remove or reduce radioactive contaminants from plant equipment, protective clothing, and personnel. These facilities shall be designed according to particular owner preference, but shall be supplied by the major decontamination equipment, including various spray nozzle assemblies, chemical and/or abrasive supply systems, collection and storage tanks, high pressure pumps, filters, demineralizers and piping connections to waste processors. Complete descriptions of the facilities shall be provided by the licensee.

The following sections contain a description of a typical ODF and interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive.

The ODF shall include the hot laundry facilities, hose washdown stations, personnel decontamination fixtures, hot shower, radiation detection equipment and personnel decontamination supplies. Also equipment necessary to decontaminate small tools and instruments as well as larger tools and pieces of equipment shall be provided. J

These facilities shall be designed to meet the requirements as stated in 10 CFR 50 Appendix E, IV.E.3; and 10 CFR 50.47 (b) (8). The role(s) of the Onsite Decontamination Facilities in the event of a plant emergency shall be described in the emergency planning documents provided by the licensee.

13.3.3.6.2 Function

The Onsite Decontamination Facilities shall provide for the following functions:

A. To facilitate equipment disposal by reducing contamination and radiation levels to releasable limits.

B. To facilitate equipment repair by reducing contamination and radiation levels consistent with ALARA guidelines.

ATTACHMENT 2

TABLE 1.10-1

(Sheet 1 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
1-1		1.8	Applicable editions of industry codes and standards
1-2		1.9	Design interfaces
2-1	2.0-1	2.0	Site Parameters
2-2	2.1-1	2.1	Geography and Demography Information
2-3	2.2-1	2.2	Industrial, Transportation and Military Hazards
2-4	2.3-1	2.3	Meteorology Information
2-5	2.4-1	2.4	Hydrologic Information
2-6	2.5-1	2.5	Geology, Seismology and Geotechnical Information
3-1	3.4-1	3.4	Flood Analysis
3-2	3.5-1	3.5	Missile Protection
3-3	3.6-1	3.6	Final Piping Design Information
3-4	3.7-1	3.7	Site and Plant-Specific Seismic Design Information
3-5	3.8-1	3.8	Site and Plant-Specific Structural Design Information
3-6	3.9-1	3.9	Site and Plant-Specific Information for Mechanical System and Components Design
3-7	3.10-1	3.10	Seismic and Dynamic Qualification Program Details
3-8	3.11-1	3.11	Environmental Qualification Program Details
4-1	4.2.7-1	4.2.3.2.10.K	Online fuel failure monitoring and post-irradiation surveillance
4-2	4.4.4-1	7.2.1.1.2.5	CPC/CEAC software testing and change control
5-1	5.2.1.1-1	5.2.1.1	ASME Code edition, Addenda and Code cases for construction of the reactor coolant pressure boundary components
5-2	5.2.2.2-1, 5.2.2.3-1, 5.3.1-1, 5.3.2-1	5.2.2.10.2.2, 5.2.3.1, 5.3.2, 5.4.14.3	Verification of the material properties and end-of-life fluence and resulting P-T limits and LTOP temperatures

TABLE 1.10-1

(Sheet 2 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
5-3	5.2.4-1, 6.6-1	5.2.4, 6.6	PSI and ISI program plans for NRC staff review
5-4	5.4-1	5.4.2.5	Steam Generator tube inservice inspection program
5-5	5F-1	5.6.3 (App. 5F)	Leakage monitoring program
6-1	6.1.1-1, 6.1.1-2, 6.1.1-3, 6.1.1-4	6.1.1.1~~5~~, ~~6.1.1.1.5~~	Engineered Safety Feature Systems materials selection and fabrication
6-2	6.3.7-1	6.3.4.1	Periodic testing of the safety injection system
6-3	6.4-2	6.4.1.2, 6.4.2.2	Protection against the effects of toxic substance releases (including TMI III.D.3.4)
6-4	6.4-3	6.4.1.1	~~Licensing basis for the~~ Control room habitability system
6-~~6~~	6.5-1	6.5.4.1	Containment spray system operability
6-~~7~~	6.2.4-1	~~6.2.4.2~~ Table 6.2.4-1	~~CIV location and pipe size~~ Containment Isolation Details
6-~~8~~		6.8.2.2.1	IRWST screen area margin analysis
7-1		7.1.2.7	Integrated response time for protection system
7-2		7.4.1.1.8.2	Operating procedures for SCS
7-3		7.3.1.1.10	Procedures for removing ESFAS signals during plant testing
7-4		7.3.2.1	Procedures for ESFAS Reset
7-5		7.3.2.3.2	ESFAS setpoint analyses
7-6		7.4.2.5.2	Cold shutdown procedures
7-~~7~~		7.5.2.5.10	Administrative controls associated with PAMI
8-1	8.3.1-1	8.1.4.5	~~Immediate and alternate modes associated with offsite power~~
~~8-2~~		~~8.1.4.5~~	Electrical power systems testing, calibration and maintenance
9-1		9.1.2.2.2, 9.1.4.2.1.2, 9.1.4.4, 9.1.4.6	Administrative controls and procedures associated with fuel storage and handling systems
6-5		6.4.1.2	Pump seal leakage procedure

TABLE 1.10-1

(Sheet 3 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
9-2	9.2.1-1	9.2.1.1.4, 9.2.1.4, 9.2.5.4	Organic fouling and inorganic buildup in the SSWS (including GS-151) GSI-51
9-3	9.2.1-2	9.2.1.2.1.2	Station service water system pump structure
9-4	9.2.4-1	9.2.4.2	Potable and sanitary water systems
9-5		9.3.4.1.4	Structures housing boric acid storage tank, reactor makeup water tank, and holdup tank
~~9-6~~	~~9.5.1-1~~	~~9.5.1~~	~~Safety grade provisions for the fire protection systems~~
9-76	9.5.1.5-1	9.5.1.11 19.15.3.2	Administrative controls for BTP CMEB 9.5-1 conformance and fire brigade
9-87	9.5.1.5-1	9.5.1.12	Fire Hazards Analysis
9-98	9.5.2-1, 9.5.2-2, 9.5.2-3	9.5.2.2.5, 9.5.2.1, 9.5.2.2.6	Communications systems
9-109		9.5.3.2.2	Security lighting system
9-1110	9.5.4.1-1	8.3.1.1.4.11	Diesel operator training
9-1211	9.5.4.1-2, 9.5.4.2-1, 9.5.5-1, 9.5.5-2, 9.5.6-1, 9.5.6-2, 9.5.7-1, 9.5.8-1, 9.5.9-1	9.5.4.2.1, 9.5.5.2, 9.5.4, 9.5.6.5, 9.5.6.2.2, 9.5.7.2, 9.5.8.2.1, 9.5.9.2, 9.5.9.4, 9.5.9.5	Diesel generator auxiliary support systems
9-1312	9.2.5-1	9.2.5.1.3	Protected area perimeter abutting or crossing a body of water
9-1413	9.5.1.2.1.2-1	9.5.1.2	Procedures and training for using transfer switches
10-1	10.2-1	10.2.1	Turbine valve closing time
10-2	10.3-1	10.3.2.2	Steam hammer prevention
10-3	10.4.4-1	10.4.4.2.4.1	Pressure drops between the steam generator nozzles and each system valve

TABLE 1.10-1

(Sheet 4 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
10-4	10.4.7-2, 10.4.9-2	10.4.7.2.5, 10.4.9.1.2	Avoidance of water hammer in the condensate, feedwater, and emergency feedwater systems
10-5	10.4.9-3	10.4.9.5.2	Steam binding in the emergency feedwater pump
11-1	11.1-1, 11.5-1	11.1, 11.5.1.1	Conformance with Appendix B to 10 CFR 20, Appendix I to 10 CFR 50, ANSI N13.1, R.G. 1.21 and R.G. 4.15
11-2	11.4-1	11.4.1.1	Site-specific solid waste management system operating procedures
11-3	11.5-2	11.5.1.4	Procedures in accordance with Position C of R.G. 4.15
11-4	11.2.1-1	11.2.5	Setpoints for radiation monitors
11-5	11.5.1-1	11.5.2.6	Operation and maintenance manual for monitoring and sampling liquid and gaseous process and effluent streams
12-1	12.1.1-1	12.1.1.2	Operational ALARA policy
12-2	12.1.2-1	12.2.3 12.3.2.2	Shielding analysis (including TMI II.B.2)
12-3	12.1.3-1	~~12.1.3~~	New Regulatory Guides
~~12-4~~		~~12.2.2.1~~	~~Radiation protection design acceptance criteria~~
12-84	12.3.1-1	12.3.1.8	List of vital areas
12-85	12.3.4-1	12.3.4	Area radiation monitor location
12-76	12.3.4-2	12.3.4	Portable airborne iodine monitor (TMI III.D.3.3)
12-87	12.4.5-1	12.4.5	Dose assessment
12-88	12.5-1	12.5	Health physics ~~organization~~ program
13-1	13.1-1	13.1	Organizational structure of the site operator ~~(including TMI I.A.1.4, II.J.3.1)~~
13-2	13.3-1	13.3.2	Site-specific emergency planning
13-3		13.3.3.1.7	TSC communication equipment

12.1.2.1
12.2.2.1

no section in CESSAR-DC } use smaller font size

TABLE 1.10-1

(Sheet 5 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
13-4	13.3-2	13.3.3.2, ~~13.3.3.2.3,~~ ~~13.3.3.2.6,~~ 13.3.3.4, 13.3.3.6, ~~13.3.3.6.5~~	TMI III.A.1.2, "Upgrade Licensee Emergency Support Facilities"
13-5	13.4-1	13.4	Review and audit
13-6	13.5-1	13.5	Plant procedures (TMI I.C.1, I.C.5, & I.C.9)
13-7		1.2.13, 13.6	Site security and sabotage protection
13-8	13.2-1	13.2	Training [TMI I.A.4.2, I.A.4.1(2), II.K.1(26)]
13-9	13.5-2	13.5.2	Administrative Control Procedures TMI II.J.4.1, II.K.1(10)
14-1		14.2.2.1	Organization and Staffing
14-2	14.2.3-1, 14.2.3-2, 14.2.3-3, 14.2.3-4, 14.2.4-1, 14.2.10-1, 14.2.11-1	14.2.1.1, 14.2.3, 14.2.4, 14.2.10, 14.2.11	Testing program procedures and schedules including scoping documents, startup administrative manual, test conditions, test methodologies data collection and reduction, reconciliation methods, and initial fuel load and criticality procedures
14-3	14.2.6-1	14.2.6	Retention of Test Records
14-4	14.2.9-1	14.2.9	Trial use of plant operating and emergency procedures
14-5	14.2.12.2-1	14.2.7.1.3	Testing of personnel monitors and radiation survey instruments test
14-6	14.2.13-1	14.2.7.5	Security system detailed description, ~~tests,~~ and acceptance criteria
~~14-7~~		~~14.3~~	~~ITAAC for site-specific design features~~
15-1		15.7.3.4	Liquid tank failure minimum dilution flow
15-2	15.A.3.2-1	6.1.2.2	Quantity of electrical cable insulation
17-1	17.1-1, 17.2-1	17.1, 17.2	Construction and Operation QA (including TMI I.F.2, II.J.3.1)

TABLE 1.10-1

(Sheet 6 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
17-2	17.3.1-1, 17.3.5-1	17.3.1, 17.3.5, ~~17.3.7~~ 17.3.13	D-RAP completion
17-3	17.3.9-1, 17.7	17.3.7, 17.3.9, 17.3.10, 17.3.13 Table 19.15-1	Operations reliability assurance process implementation
18-1		18.9.3.2	Validation of operating ensemble
18-2	18.6.1.3.4-1	13.2	Operator training on "Plant Safety Parameter Display Console"
19-1	19.1, 19.1.2.2.2-1	19.15.3.1	Vulnerability of the intake structure due to tornado-generated debris
19-2	19.1.2.2.3-1	19.7.5.3	Elements of the plant affecting the performance of systems in seismic events
19-3	19.1.2.4-4, 19.5, 19.6, 19.7	19.15 ~~20.2.56~~	Details of the layout of the critical components for fire and flood, interaction of internal flood sources, and effects of fire suppression systems on other systems
19-4	19.8	19.7.5.3 Table 19.15-1	Development of detailed seismic walkdown procedures to verify as-built SSC HCLPFs
19-5	19-10, 19-11	~~19.11.3.8~~ 6.5.5, 19.15	Calculation of specific flow rate and consideration of shielding requirements for local operator actions for the emergency containment spray backup system
19-6	19.1.2.2.6-1, 19.1.4-1, 19.1.2.4-1, 19.1.2.4-2, 19.1.2.4-3, 19.12	19.7.5.3, 19.15, ~~Chapter 20~~ 20.2.105	Update of PRA to include final design detail and site-specific information including examination of all external event hazards and analysis using site-specific spectra
19-7	19.14	19.15.6 Table 19.15-1	List of risk significant SSCs for D-RAP and operations reliability assurance process
19-8	19.15, 19-16, 19.19	19.15.6	Consideration of risk important operator actions in developing procedures, training and human reliability related programs, and systems to address in severe accident management and aligning the alternate AC source (AAC) procedures

TABLE 1.10-1

(Sheet 7 of 7)

COL LICENSE INFORMATION

COL No.	FSER No.	Section	Subject
19-9	19.3.6-1, 19.3.8-1, 19.3.8-2, 19.17, 19.18	19.8.1.2, 19.8A	Establishment of administrative controls, outage management, procedures and training for control of fire and flood barriers, containment closure capability and alternate equipment during shutdown operations
19-10	19.9	19.7.5.1	Use of seismically rugged electrical equipment

1.8 REGULATORY COMPLIANCE, INDUSTRY CODES AND STANDARDS

System 80+ compliance with U.S. NRC Regulatory Guides, Generic Letters, Bulletins, and elements of the Standard Review Plan is documented in this section. Regulatory Guides, the guide date or revision, and System 80+ compliance with applicable Guides are summarized in Table 1.8-1.

Operational experience information highlighted in Regulatory Bulletins and Letters has been incorporated into the System 80+ design. Generic Letters and NRC Bulletins from 1980 through December, 1993 are identified in Tables 1.8-2 and 1.8-3. The applicability of each Generic Letter or Bulletin to System 80+ is assessed, with additional information for applicable issues provided in the referenced sections of this report.

System 80+ deviations from the U.S. NRC Standard Review Plan, NUREG-0800 [LWR Edition, June 1987], are listed in Table 1.8-4. Specific sections are also identified where further details relevant to each SRP deviation are discussed. Site-specific compliance with individual Standard Review Plan sections is provided in Table 1.8-5.

Table 1.8-6 identifies the industrial Codes and Standards, and code editions, invoked for certification of the System 80+ Standard Design. [Where a particular structure, system, or component requires a code edition different from that listed in Table 1.8-6, an explanation of such difference is provided in the appropriate text.] Other Codes and Standards that are utilized but not invoked as essential for design certification are incorporated into the individual chapters of this Safety Analysis Report. Revisions to accepted industry codes applied to System 80+ will be evaluated on a case-by-case basis. [The applicability of code editions will be confirmed by the Combined Operating License applicant in the site-specific Safety Analysis Report.]]

ASME Section III, Division 1 Code Cases applicable to System 80+ are identified in Table 1.8-7. Except for N-122-1, these Code Cases are consistent with those identified in Regulatory Guide 1.84, Revision 29, for design and fabrication, or Regulatory Guide 1.85, Revision 29, for materials and testing, that were in effect on July 31, 1993.

Cross-references to subsections of this report discussing Unresolved and Generic Safety Issues, the Three Mile Island Rule [10 CFR 50.34 (f)], and new NRC policy issues (SECY-93-087) are provided in Tables 1.8-8, 1.8-9, and 1.8-10.

1.9 SYSTEM 80+ STANDARD DESIGN INTERFACES

This section provides a listing of the interfaces as used in 10 CFR 52.47(a). The System 80+ Standard Design includes an essentially complete nuclear plant, except for structures, systems and components which require site-specific design. These structures, systems and components are not included in the System 80+ design certification and shall be provided by the applicant (owner/operator) during site specific engineering. To ensure that the design of these items is compatible with the System 80+ Standard Design, interface requirements must be satisfied by the applicant. In general, interface requirements for applicant-supplied structures, systems and components that relate to a specific mechanical or electrical system are covered in the appropriate CESSAR-DC chapter (The word "shall" is used to identify interface requirements included in descriptive text). Interface requirements which have sufficient significance to safety are specified in the Certified Design Material. Table 1.9-1 provides an index to all sections of this report containing interface requirements.

1-2

Site-specific assumptions on which the System 80+ Standard Design is based are presented in Section 1.2.1, Principal Site Characteristics, and Chapter 2.0, Site Envelope Characteristics. The applicant (owner/operator) shall verify that the chosen site is enveloped by the characteristics given in Sections 1.2.1 and 2.0. These site-specific characteristics must be compatible with the System 80+ design envelopes, but they are not considered interface requirements as used in 10 CFR 52.47(a).

2.0 SITE ENVELOPE CHARACTERISTICS

The System 80+ Standard Design is designed on the basis of a set of assumed site-related parameters. These parameters were selected to envelope most potential nuclear power plant sites in the United States. A summary of the assumed parameters is provided in Table 2.0-1.

Detailed site characteristics will be provided by the COL applicant referencing the System 80+ Standard Design for any specific application. These characteristics will be reviewed and compared to the enveloping assumptions of Table 2.0-1. Should specific site parameters or characteristics be outside the envelope of assumptions established by Table 2.0-1, the applicant will demonstrate that the design satisfies the requirements imposed by the specific site parameters and conforms to all design commitments and acceptance criteria described in this report. 2-1

The remainder of this chapter identifies specific assumptions related to site characteristics that are employed in the evaluation of the System 80+ Standard Design.

2.1 GEOGRAPHY AND DEMOGRAPHY

Site-specific information on geography and demography will be provided by the COL applicant referencing the System 80+ design. 2-2

2.1.1 SITE LOCATION AND DESCRIPTION

No specific assumptions were employed in the evaluation of the System 80+ Standard Design. Site-specific information will include site and location description.

2.1.1.1 Site Location

Considerations of site location for the System 80+ plants are made for the purpose of minimizing the risk significance of site-dependent characteristics on plant design. Sections 2.2 through 2.5 discuss System 80+ plant siting considerations for site-dependent design parameters. Chapters 3, 9, and 13 also discuss System 80+ design features incorporated to mitigate the consequences of site-dependent and site-independent parameters.

2.1.1.2 Site Area Map

The site area map is site-specific and will be provided with other site-dependent information.

2.1.1.3 Boundaries for Establishing Effluent Release Limits

Boundary distances have been selected for an exclusion area and a low population zone as defined in 10 CFR 100.11. These distances are employed in Sections 2.3.4 and 2.3.5 to calculate estimates for diffusion of radiological releases. A site specific application will address the combined influences of site characteristics and local meteorology on diffusion of releases.

2.1.2 EXCLUSION AREA AUTHORITY AND CONTROL

No specific assumptions were employed in the evaluation of the System 80+ Standard Design. Site-specific information will include exclusion area authority and control.

2.1.3 POPULATION DISTRIBUTION

No specific assumptions were employed in the evaluation of the System 80+ Standard Design. Site-specific information will include population distribution.

2.2 NEARBY INDUSTRIAL, TRANSPORTATION AND MILITARY FACILITIES

Industrial, transportation and military hazards are discussed below. [Site-specific information on industrial, transportation, and military hazards will be provided by the COL applicant referencing the System 80+ design.] 2-3

2.2.1 AIRCRAFT HAZARDS

A site is acceptable for the System 80+™ without further review if the distances from the plant meet the following requirements:

A. The plant-to-airport distance D is between 5 and 10 statute miles, and the projected annual number of operations is less than 500 D^2, or the plant-to-airport distance D is greater than 10 statute miles, and the projected annual number of operations is less than 1000 D^2.

B. The plant is at least 5 statute miles from the edge of military training routes, including low-level training routes, except for those associated with a usage greater than 1000 flights per year, or where activities (such as practice bombing) may create an unusual stress situation.

C. The plant is at least 2 statute miles beyond the nearest edge of a federal airway, holding pattern, or airport.

If the above site proximity acceptance criteria are not met, or if sufficiently hazardous military activities are identified, a detailed review of the aircraft hazards must be performed to qualify a specific site for the System 80+™ plant.

2.2.2 TRANSPORTATION

Site-specific information will include hazards related to transportation.

The ultimate heat sink, which is not included in the System 80+ scope for design certification, provides the source of cooling water for all safety-related plant systems and components during all modes of operation. Interface requirements (Section 9.2.5.1.3) are identified to eliminate the potential impacts on plant operations from boat or barge accident events.

2.2.3 OTHER INDUSTRIAL HAZARDS ON AND OFF SITE

Site-specific information will include onsite and offsite industrial hazards.

2.3 METEOROLOGY

Meteorology parameters are as specified in Table 2.0-1. Site-specific meteorology information will be provided by the COL applicant referencing the System 80+ design. 2-4

2.3.1 REGIONAL CLIMATOLOGY

Site-specific information will include regional climatology.

2.3.1.1 Low Temperature Effects

The effects on the plant from low temperature events, such as frost, snow fall, and ice cover, are considered in the design process. Structures are designed to withstand loadings in excess of the loads generated from combinations of snow, ice, and rain.

Ventilation paths are designed and reviewed to verify that they are free from snow blockage.

2.3.2 LOCAL METEOROLOGY

No specific assumptions were employed in the evaluation of the System 80+ Standard Design other than the assumptions in Sections 2.3.4 and 2.3.6 that establish the values of relative concentrations for the offsite accident analyses and control room operator dose analysis as presented in Chapter 15 and Section 6.4, respectively.

As indicated in Table 2.0-1, pressure effects and missile spectra associated with the design tornado are considered to be controlling. Site-specific information will include an evaluation to assure that this assumption is not violated for the specific site selected or will include analysis results for any potential hazards that are more limiting than the parameters given in Table 2.0-1.

2.3.2.1 Tornados

Tornado characteristics are as specified in Table 2.0-1.

Tornado-generated missiles are considered in the System 80+ Standard Design (See Section 3.5).

Structures housing safety-related equipment are designed to withstand the loadings generated by 330 mph winds.

Tornados that occur at the plant site, causing extensive damage to the switchyard and a prolonged loss of offsite power, are quantitatively evaluated.

2.4 HYDROLOGIC ENGINEERING

Hydrologic engineering parameters are as specified in Table 2.0-1. Site-specific hydrologic information will be provided by the COL applicant referencing the System 80+ Standard Design. This information will include the following considerations as appropriate for the specific site: external floods; probable maximum flood on streams and rivers; potential dam failures; probable maximum surge and seiche flooding; probable maximum tsunami loading; ice effects; cooling water canals and reservoirs; channel diversions; flood protection requirements; cooling water supply; groundwater; potential accidental release of liquid effluents in ground and surface water, and technical specifications and operation requirements. 2-5

2.4.1 EXTERNAL FLOODS

The site-specific flooding projections will consider severe precipitation, snow melt, flooding due to ice cover, river flooding, ocean flooding, tsunami flooding, seiche effects, wave and storm surge effects, hurricane effects, high lake levels and any other effects appropriate for the specific site.

Intake structures will be designed to preclude the potential for debris blockage caused by wind, wave, and other effects.

2.4.2 INTERNAL FLOODS

See Section 3.4.

2.5 GEOLOGY, SEISMOLOGY, AND GEOTECHNICAL ENGINEERING

Site-specific geology, seismology, and geotechnical engineering information and characteristics of the site and region surrounding the site, including site acceptance criteria, will be provided by the COL applicant referencing the System 80+ Standard Design. 26

To cover a range of possible site conditions where System 80+ may be constructed, a range of generic site conditions was selected for geologic and seismologic evaluation (Figure 2.5-1). The System 80+ is a standard plant design to be built on a suitable site. The basis for selecting any particular site is documented in the site-specific Safety Analysis Report (SAR). Site geologic features, seismological features, liquefaction potential, site instability, ground rupture and man-made conditions are included in the site-specific SAR. Site-specific investigations, including borings, are conducted in accordance with 10 CFR 50 and 100 (Reference 2) and Standard Review Plan 2.5 (Reference 3). Any deviations from Reference 3 are identified and justified in the site-specific SAR.

The total depth to bedrock for each site condition and the dynamic soil properties (in terms of maximum shear wave velocities and their variation with depth, and in terms of the variations of modulus and damping with strain) were established to cover a wide range of sites and to provide reasonably conservative results. Using these site conditions and the variations of maximum shear wave velocities, 13 cases were developed; 12 soil cases and one rock outcrop case. For analysis of the superstructure, the rock outcrop case was further broken into two subcategories. One subcategory covers the case where the structure is sitting on rock, with its embedded portion not restrained. The second subcategory covers cases where the backfill material has rock type characteristics. Further discussions on the rock outcrop case is provided in Appendix 3.7-B. The cases selected are summarized in Section 2.5.2, and more details for each case are included in Appendix 2A.

For the System 80+ seismic design, three control motions were developed which, when combined cover the majority of potential sites in the continental U.S. The twelve generic soil sites and one rock site were evaluated for each of the control motions.

To cover sites with deep soil deposits, a control motion with a Regulatory Guide 1.60 spectral shape is used as the input motion to the ground surface of each site. To cover shallow soil sites, two rock motions applied at a hypothetical rock outcrop are used. The selection of the two rock outcrop motions was performed using low frequency content consistent with industry-wide accepted response spectra, and high frequency content that exceeds the current industry practice. The enrichment of the rock outcrop motions with high frequency content is consistent with recent studies on Eastern North America seismicity and is a proactive measure of the System 80+ design in anticipation of future trends

3.4 WATER LEVEL (FLOOD) DESIGN

All Seismic Category I structures, components and equipment are designed for applicable loadings caused by postulated floods. Section 2.4 of the site-specific SAR describes, in detail, the relationship of the site-specific flood levels to safety-related buildings and facilities.

The COL applicant referencing the System 80+ Standard Design will provide a site-specific flood analysis to demonstrate safe shutdown of the plant. This analysis will include a site description and elevations of safety-related structures and equipment; evaluations of penetrations in Seismic Category I structures; and effects of flooding due to postulated pipe breaks. 3-1

3.4.1 FLOOD ELEVATIONS

The elevation level for floods at the reactor site is determined in accordance with Regulatory Guide 1.59, "Design Basis Floods for Nuclear Power Plants," and ANSI/ANS 2.8, "Determining Design Basis Flooding at Power Reactor Sites." The design basis level for the System 80+ Standard Design is 1 foot below plant finished yard grade. Flood level values in excess of this 1 foot level are site-specific and protection measures for that flood level are described in Section 2.4 of the site-specific SAR.

3.4.2 PHENOMENA CONSIDERED IN DESIGN LOAD CALCULATION

All Seismic Category I structures are designed to withstand the static and dynamic forces of the design basis flood level.

Site-specific information will include a specific description of the site and elevation for all safety-related structures, exterior accesses, equipment and systems.

3.4.3 FLOOD FORCE APPLICATION

The design flood is used in determining the applicable water level for design of all Seismic Category I structures in accordance with the load combinations discussed in Section 3.8.4. The forces acting on those structures are determined on the basis of full external hydrostatic pressure corresponding to that flood level. All Seismic Category I structures will be in a stable condition due to both moment and uplift forces resulting from the proper load combinations, including design basis flood levels.

3.4.4 FLOOD PROTECTION

3.4.4.1 Flood Protection Measures for Seismic Category I Structures

The flood protection measures for Seismic Category I structures, systems and components are designed in accordance with Regulatory Guide 1.102, "Flood Protection for Nuclear Power Plants."

Seismic Category I structures identified in Table 3.2-1 are designed for flood protection.

3.5 MISSILE PROTECTION

The missile protection design for Seismic Category I structures, systems and components is described in this section.

Missile protection or redundancy is provided for Seismic Category I equipment and components such that internal and external missiles will not cause the release of significant amounts of radioactivity or prevent the safe and orderly shutdown of the reactor.

The protection of essential structures, systems and components will be accomplished by one or more of the following:

A. Reducing the potential for sources of missiles by equipment design features that prevent missile generation.

B. Orientation or physical separation of potential missile sources away from safety-related equipment and components.

C. Containment of potential missiles through the use of protective shields and barriers near the source.

D. Hardening of safety-related equipment and components to withstand missile impact, where such impacts cannot be reasonably avoided by the methods above.

Site and plant specific missile protection information regarding potential missiles and protection thereof will be provided by the COL applicant referencing the System 80+ design. Information will include site proximity missiles, probabilistic evaluations for turbine missiles, and as-built conditions and evaluations. 3-2

3.5.1 MISSILE SELECTION AND DESCRIPTION

Potential missiles are identified and characterized by type and source and their probability of occurrence, retention and impact. For equipment with energy sources capable of creating a missile, the selection is based on the application of a single-failure criterion to the retention features of the component. Where sufficient retention redundancy is provided in the event of a failure, no missile is postulated.

Internally generated missiles can be generated potentially from two types of equipment: rotating components and pressurized components. Rotating components include turbine wheels, fans, auxiliary pumps and their associated motors. Pressurized components include valves, heat exchangers, vessels and their associated components.

3.6 PROTECTION AGAINST DYNAMIC EFFECTS ASSOCIATED WITH THE POSTULATED RUPTURE OF PIPING

The COL applicant referencing the System 80+ Standard Design will provide final designs of high and moderate energy fluid systems. Information provided will include documentation of radiographic examination of welds, verification of leak-before-break (LBB) analyses, a pipe break analysis report, and a LBB evaluation report. 3-3

High-energy piping systems not approved for LBB are subject to postulated pressure boundary failures. The resultant consequences of these postulated breaks are assessed for their effect on maintenance of plant safe shutdown capability, containment integrity and offsite dose consequence. Consideration is given to the effects of pipe whip, jet impingement and the environmental impact of release of system contents. Provisions of physical separation, system redundancy, component strength, and, as necessary, mitigating hardware, are utilized to protect against the effects associated with postulated pipe breaks.

Protection of vital equipment is achieved primarily by separation of redundant safe shutdown systems and by separation of high-energy pipe lines from safe shutdown systems, which are required to be functional following specific pipe rupture events. This redundancy and separation results in a design which requires very few special protective features (such as whip restraints and jet deflectors) to ensure safe shutdown capability following a postulated high-energy line break.

Separation is maintained by barriers such as the containment secondary shield wall, refueling cavity wall and certain Nuclear Annex walls and tunnels or by physical distance. Loadings and jet zones of influence are calculated using methodology described in Section 3.6.2.

Supplemental information on design for protection against dynamic effects of postulated pipe breaks is given in Appendix 3.6A.

3.6.1 POSTULATED PIPING FAILURES IN FLUID SYSTEMS

3.6.1.1 Design Basis

Most systems and components outside Containment required for safe plant shutdown are located in the Reactor Building Subsphere. The Reactor Building Subsphere and Nuclear Annex are divided by a structural wall which serves as a barrier between redundant trains of safe shutdown systems and components. Each half of the Reactor Building Subsphere is compartmentalized to separate redundant safe shutdown components to the extent practical. High-energy piping systems located in the Nuclear Annex, which

3.7 SEISMIC DESIGN

The COL applicant referencing the System 80+ Standard Design will provide site and plant-specific seismic design information which will include evaluation of interactions between Seismic Category I and non-Seismic Category I structures, systems, and components; procedures for pre-earthquake planning and post-earthquake actions; and site-specific confirmatory analyses, as required. 3-4

3.7.1 SEISMIC INPUT

This section discusses the seismic design parameters and methodologies being used for the design of those systems and subsystems important to safety and classified as Seismic Category I in Section 3.2.

3.7.1.1 Design Response Spectra

The System 80+ Standard Design as defined by CESSAR-DC is not based on a specific site. The design response spectra which define the free field design ground motion or control motion specified either at the site soil surface or on a hypothetical rock outcrop are shown in Figure 2.5-5. Generic site conditions were selected to cover a range of possible conditions for the System 80+ sites. For the Nuclear Island, sets of representative cases from each of four generic site categories were evaluated. Ground surface and foundation level spectra which correspond to the design response spectra of control motions CMS1, CMS2 and CMS3 for rock and soil cases are shown in Section 2.5. Out of 12 soil cases analyzed in Section 2.5.2, ten are used in the soil structure interaction (SSI) analyses. The two cases eliminated in the SSI analysis (B3 and D1) were non-governing cases whose soil response levels were enveloped by other cases. See Section 2.5.2 for details of this analysis phase. Two rock cases were analyzed, one with no backfill (fixed base at bottom of basemat) and one with concrete backfill (fixed base at all subsurface elevations). The ten soil cases and the two rock cases were analyzed for all three control motions (CMS1, CMS2, and CMS3).

A sensitivicy study was performed to demonstrate that the selected motions and the soil profiles provide a conservative design envelope for the System 80+ structures. In this study, a simplified analytical model of the 3D NI structure was developed and analyzed with five soil profiles and the CMS2 control motion. Three of the soil profiles were part of the 12 profiles selected for the System 80+ 3D SSI analyses (B-1, B-1.5, B-2). The remaining two soil profiles were developed to serve as "test" profiles. The two new profiles were chosen such that they have low strain soil properties that are in-between the soil properties of cases B-1, B-1.5 and B-2. Hence, they were named B-1.25 and B-1.75. Response parameters such as maximum in-structure acceleration, maximum base shear and maximum base

3.8 DESIGN OF CATEGORY I STRUCTURES

The COL applicant referencing the System 80+ Standard Design will provide site and plant-specific structural design information. Information provided will include:

- Site related design parameters,
- Foundation mat construction procedures,
- Allowable loads for designated laydown areas,
- Final electrical layout drawings to verify load allowances for cable trays,
- Procedures for quality control inspections,
- Documentation of radiographic examination of welds,
- Site-specific design specifications, including expansion anchors,
- A steel containment vessel as-built structural analysis report, and
- A Seismic Category I structural analysis report.

3-5

3.8.1 CONCRETE CONTAINMENT

This section is not applicable to the System 80+ Standard Design. For a description of the containment, see Section 3.8.2. For a description of the containment shield building, see Section 3.8.4.

3.8.2 STEEL CONTAINMENT

3.8.2.1 Description of the Containment

3.8.2.1.1 General

The containment is a spherical welded steel structure supported by embedding a lower segment between the containment internal structures concrete and the reactor building subsphere concrete. There is no structural connection between the free standing portion of containment and the adjacent structures other than penetrations and their supports. The lateral loads due to seismic and other forces are transferred to the foundation concrete by shear bars, friction and bearing. The diameter of containment is 200 ft. The plate nominal thickness is 1.75 inches. The transition region, where the free standing portion of the steel containment vessel enters the concrete, has a plate thickness of 2 inches. The containment is shown on the plans and elevations of Figures 1.2-2, 1.2-3, 1.2-5, 1.2-6, 1.2-7 and 1.2-9.

The arrangement of the Nuclear Island structures, which includes containment and defines critical dimensions, flood barriers, and fire barriers, is shown in Figure 3.8-5.

The spherical shell plate segments will be shop fabricated and field welded. These plates will be approximately 25 feet long and 13 feet wide and can weigh as much as ten tons each; however,

3.9 MECHANICAL SYSTEMS AND COMPONENTS

The COL applicant referencing the System 80+ Standard Design will develop and/or provide site and plant-specific information on mechanical systems and components design. Information will include:

- Verification of computer codes that are not precertified,
- Reconciliation of as-built with as-designed piping configurations,
- Documentation of pressurizer safety valve adjustments,
- Documentation of radiographic examination of welds,
- Identification of safety-related components which utilize snubbers,
- Description of energy absorbing and/or non-linear piping restraints, if used, and
- Qualification and preoperational testing of safety-related pumps and valves and a detailed pump and valve inservice testing (IST) program.

3-6

3.9.1 SPECIAL TOPICS FOR MECHANICAL COMPONENTS

3.9.1.1 Design Transients

The following information identifies the transients used in the design and fatigue analysis of ASME Code Class 1 components, reactor internals and component supports. Cyclic data for the design of ASME Code Class 2 and 3 components, as applicable, are discussed in Section 3.9.3. All transients are classified with respect to the component operating condition categories identified as Level A (Normal), B (Upset), C (Emergency) and D (Faulted) and testing as defined in the ASME Code, Section III. The transients specified below represent conservative estimates for design purposes only and do not purport to be accurate representations of actual transients, or necessarily reflect actual operating procedures; nevertheless, all envisaged actual transients are accounted for, and the number and severity of the design transients exceeds those which may be anticipated during the life of the plant.

Pressure and temperature fluctuations resulting from the normal, test, upset, emergency and faulted transients are computed by means of computer simulations of the reactor coolant system, pressurizer, and steam generators. Design transients are detailed in the equipment specifications. The component designer then uses the specification curves as the basis for design and fatigue analysis.

In support of the design of each Code Class 1 and CS component, a fatigue analysis of the combined effects of mechanical and thermal loads is performed in accordance with the requirements of Section III of the ASME Code. The purpose of the analysis is to

3.10 SEISMIC AND DYNAMIC QUALIFICATION OF MECHANICAL AND ELECTRICAL EQUIPMENT

This section describes the tests, analyses, procedures, and acceptance criteria applied to two categories of mechanical and electrical equipment to assure operability and structural integrity under the full range of normal, transient, seismic and accident loadings.

The two categories are safety related (Seismic Category I) equipment and non-safety related equipment whose failure can prevent the satisfactory accomplishment of safety functions (Seismic Category II). The safety related equipment are those necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures in excess of 10 CFR 100 guidelines. Non-safety related equipment whose failure could reduce the performance of safety related equipment is designated as Seismic Category II.

Examples of mechanical and electrical equipment included in these two categories are pumps, valves, fans, valve operators, valve operator motors, solenoid valves, pump and fan motors, compressors, chillers, air handlers, blowers, fuel rod assemblies, control rod drive mechanisms, battery and instrument racks, control consoles, cabinets, panels, pressure switches, level transmitters, and electrical penetrations.

The licensee at the time of COL will make the specific details of the plant-specific seismic and dynamic qualification program available for NRC evaluation. This includes a description of administrative control procedures; equipment qualification reports and records; results of in-plant tests; and, if used, documentation on qualification by experience.

3-7

3.10.1 SEISMIC QUALIFICATION CRITERIA

3.10.1.1 Requirements

The seismic and dynamic qualification program ensures that equipment classified as Seismic Category I can meet functional performance requirements, as defined in the equipment's design specification, during and after the dynamic loadings due to normal operating, transient, seismic and accident conditions. For Seismic Category II equipment it is demonstrated that structural integrity is maintained under normal operating, transient, seismic and accident loads and therefore this equipment will not be a missile hazard or in some other manner damage nearby safety-related equipment.

The seismic and dynamic qualification program conforms to the requirements of Regulatory Guide 1.100, Rev. 2 and IEEE Std. 344-1987. The seismic and dynamic testing portion of the qualification program is performed in a sequence consistent with the requirements of Section 6 of IEEE Standard 323-1974.

required to be functional. If more than one type of radiation is significant, each type may be considered separately.

The COL applicant will make the specific details of the plant specific environment qualification program available for NRC evaluation. This includes a detailed maintenance/surveillance program and documentation of test reports and analyses. 3-8

3.11.1 EQUIPMENT IDENTIFICATION AND ENVIRONMENTAL CONDITIONS

Appendix 3.11B lists the equipment required to mitigate a DBA or to attain a safe shutdown. Specific equipment for each system is discussed in the appropriate section of the Safety Analysis Report as referenced in Appendix 3.11B. The major component categories, such as motor-operated valves, pump motors, instrumentation and pressure boundary equipment and their location by area are also provided.

3.11.2 QUALIFICATION TESTS AND ANALYSES

Qualification of electrical equipment for System 80+ will comply with 10 CFR 50.49 as described below:

A. Environmental qualification of electrical equipment located in harsh environments within Combustion Engineering's scope of supply will be in accordance with the methodologies outlined in CENPD-255-A, Rev. 3 (Reference 1). Reference 1 has been reviewed and approved by the NRC staff as an acceptable methodology for environmental qualification of nuclear steam supply system safety-related electrical equipment. The NRC's approval of Reference 1 includes references to Amendment 9 of CESSAR-F. The development of CESSAR-DC necessitated a review of Reference 1 which resulted in a review of Section 3.11 of CESSAR-F, Section 3.11 and appendix J of supplement No. 3 to NUREG-0852 (Safety Evaluation Report for CESSAR System 80), and the NRC's approval letter (the NRC approval letter is included as an integral part of Reference 1). As a result of these reviews, ABB-CE has determined that there is no basis for including references to Amendment 9 of CESSAR-F in the review of CESSAR-DC. Therefore, the intent of CESSAR-DC is to utilize CENPD-255-A, Rev. 3, independent of reference to Amendment 9 of CESSAR-F. In instances where CESSAR-DC and CENPD-255-A, Rev. 3 differ, CESSAR-DC takes precedence.

B. Environmental qualification of electrical equipment located in mild environments within Combustion Engineering's scope of supply will be in accordance with the methodologies outlined in NPX80-IC-QG790-00, Qualification Guidelines for Instrumentation and Controls Equipment for Nuplex 80+ (Reference 2).

C-E/KWU in Obrigheim and Petten. In the Petten test, a single unpressurized fuel rod was power cycled between 9 kW/ft and 17 kW/ft at a power change rate of about 3 kW/ft/min. The fuel rod successfully completed 400 cycles and achieved a burnup of 8000 MWd/MTU. Power cycling tests were then conducted in Obrigheim on eight short pressurized and unpressurized fuel rods. The test fuel rods were attached to a control rod drive mechanism and driven from the low power to a high power position on a nominal cycle. Power changes from 50% to 100% at rates of 20% per minute for 880 cycles were included. After successfully completing the experiment, the test rods achieved a peak burnup of 30,000 MWd/MTU without substantial cladding deformation or fuel rod perforation. More recent information has been published in Reference 77.

K. Fuel Surveillance Programs

C-E has conducted a number of fuel surveillance programs on fuel in operating plants. Thus far, a total of thirty-eight poolside fuel inspection programs of varying detail have been performed by C-E (see Table 4.2-3). A large number of assemblies have been visually examined, and dimensional measurements have been obtained on a large number of these assemblies. Fuel bundle disassembly operations have been conducted either to obtain information on particular performance aspects or as part of test assembly surveillance programs. A listing of these programs and a summary of the results is provided in Reference 70. The results of the C-E poolside inspection program have been used to verify fuel assembly operation and provide data in support of design. A poolside fuel surveillance program is being conducted at Palo Verde-1 for C-E's System 80 fuel (see Section 4.2.1.5.1).

The COL applicant will perform on-line fuel failure monitoring and post-irradiation surveillance to detect anomalies. 4-1

4.2.3.2.11 Temperature Transient Effects Analysis

4.2.3.2.11.1 Waterlogged Fuel

The potential for a fuel rod to become waterlogged during normal operation is discussed in Section 4.2.3.2.9. In the event that a fuel rod does become waterlogged at low or zero power, it is possible that a subsequent power increase could cause a buildup of hydrostatic pressure. It is unlikely that the pressure would build up to a level that could cause cladding rupture because a fuel pin with the potential for rupture requires the combination of a very small defect together with a long period of operation at low or zero power.

The reactor coolant pump speed measurement system is designed, manufactured, tested, and installed to the identical design, quality assurance, and testing criteria as the remainder of the signal generation and processing equipment for signals utilized by the RPS.

7.2.1.1.2.5 Core Protection Calculators

Four independent Trip Logic Calculators (TLCs) are provided, one in each Core Protection Calculator (CPC) channel. Calculation of DNBR and local power density is performed in each TLC, utilizing the input signals described below. The DNBR and local power density so calculated are compared with trip setpoints for initiation of a low DNBR trip (Section 7.2.1.1.1.4) and the high local power density trip (Section 7.2.1.1.1.3). A trip signal from a TLC in each channel is sent to the local coincidence processors in all four protective channels. The TLC also provides pre-trip output signals.

Two independent CEA Calculators are provided as part of the CPC to calculate individual CEA deviations from the position of the other CEAs in their subgroup. The software design of the CPCs and CEACs is described in detail in Reference 1 and 2 and References 4 through 8, and has been reviewed and approved by the NRC in References 7 through 13. The algorithms described and approved in these references are applicable to System 80+. The System 80+ software also includes new algorithms for the following functions:

1. A combined low pressure/low DNBR trip described in Section 7.2.1.1.1.4.

2. Control and protective actions for CEA deviation events described in Section 7.2.1.1.2.2.2.B

References 14 and 15 described the procedure which must be followed to incorporate changes to the algorithms, data base constants and data block constants for the CPCs and CEACs. Any changes to these procedures will be conducted in accordance with Reference 16. 4-2

As shown in Figure 7.2-10, each TLC receives the following inputs:

A. Core inlet and outlet temperature.

B. Pressurizer pressure.

C. Reactor coolant pump speed.

D. Ex-core nuclear instrumentation flux power (each subchannel from the safety channel).

Outputs of each TLC are:

A. DNBR trip and pre-trip.

B. DNBR margin (to DIAS and DPS for control board indication).

C. Local power density trip and pre-trip.

D. Local power density margin (to DIAS and DPS for control board indication).

E. Calibrated neutron flux power (to DIAS and DPS for control board indication).

F. High pressurizer pressure pre-trip to CEDM Control System CWP logic.

G. CEA inward deviation cutback demand to Reactor Power Cutback System.

H. CEA deviation motion inhibit to CEDM Control System.

I. RCP speeds and other TLC measurement channel parameters to Data Processing System.

J. RPC Demand Signal to RPCS logic.

K. CMI Signal to CEDM Control System CMI logic.

Each calculator is mounted in cabinets located in separate channelized equipment rooms with an operator's display and control module located in the main control room. From the four modules an operator can monitor all calculators, including specific inputs or calculated functions. Changes to CPC constants by the operator are controlled by administrative procedures.

STFT

STFT

STFT

STFT

4-2

7.2.1.1.2.6 Bistable Trip Generation

The bistable proccesors compare input signals from the process measurement instrumentation to either fixed or variable setpoints. The PLC design Bistable Processors (two per channel) initiate a channel-trip, whenever any monitored parameter exceeds the trip setpoint. Each bistable processor is assigned process measurements for comparison basesd on a transient versus mitigating process analysis. When two process measurements are available for mitigating a transient, they are assigned to different bistable processors. Refer to Table 7.2-4 for identification of trip parameters vs. type setpoints. The trip outputs of the bistable processors are sent to the local coincidence processors. Each bistable processor trip output in each channel is input to each of the four protective channels - Figure 7.2-11. A pre-trip output is also provided as part of the bistable logic.

5.2 INTEGRITY OF REACTOR COOLANT PRESSURE BOUNDARY

This section discusses the measures employed to provide and maintain the integrity of the Reactor Coolant Pressure Boundary (RCPB) throughout the facility's design lifetime. The RCPB is defined in accordance with ANSI/ANS 51.1-1983. Included are all pressure containing components such as pressure vessels, piping, pumps, and valves which are:

A. Part of the Reactor Coolant System, or

B. Connected to the Reactor Coolant System, up to and including the following:

   1. The outermost containment isolation valve in piping which penetrates the containment;

   2. The second of two valves normally closed during reactor operation in piping which does not penetrate the containment.

5.2.1 COMPLIANCE WITH CODES AND CODE CASES

5.2.1.1 Compliance with 10 CFR 50.55a

The codes and component classifications are listed in Table 5.2-1 and are in accordance with the provisions of 10 CFR 50.55a. The ASME Code Edition and Addenda used in the design and construction of the reactor coolant pressure boundary components are specified in Table 1.8-6 and discussed in Section 1.8. If ASME Code Editions and Addenda other than those specified in Table 1.8-6 and Section 1.8 are used they will be identified to the Commission by the COL applicant and shall have been endorsed by 10 CFR 50.55a. 5-1

5.2.1.2 Applicable Code Cases

Reactor Coolant Pressure Boundary components are fabricated in accordance with the ASME Code, Section III.

The applicable ASME Code cases listed in Table 1.8-7 are utilized in the plant design and manufacturing.

If code cases other than those specified in Table 1.8-7 are used they will be identified to the Commission by the COL applicant and shall have been endorsed by Regulatory Guides 1.84, 1.85 or 1.147 as applicable. Code cases not endorsed by the above Regulatory Guides may be used with specific authorization from the Commission under 10 CFR 50.55a.

controls to require that the technical specification P-T Limits not be exceeded above the BTP defined LTOP enable and disable temperatures.

The Combined Operating License applicant must verify that the site-specific material properties used in the reactor vessel beltline and the as-deposited welds are consistent with the material specifications set forth in Section 5.2.3.1. If not, new plant-specific pressure-temperature limit curves must be derived and used in a reevaluation of the LTOP enable and disable temperatures. 5-2

5.2.2.10.2.3 Equipment Parameters

The SCS relief valves (SI-179, SI-189), used to provide LTOP, are spring-loaded liquid relief valves with sufficient capacity to mitigate the most limiting overpressurization event. Pertinent valve parameters are as follows:

Parameter	Value
Nominal Setpoint	545 psia*
Accumulation	10%
Capacity	5000 gpm (@10% acc)

Since each SCS relief valve is a self actuating spring-loaded liquid relief valve, control circuitry is not required. The valve will open when RCS pressure exceeds its setpoint.

The SCS relief valves are sized, based on an inadvertent safety injection actuation signal (SIAS) with full pressurizer heaters operating from a water-solid condition. The analysis assumes simultaneous operation of four SIS pumps and one charging pump with letdown isolated. The resulting flow capacity requirement for water is 5000 gpm. The analysis in Section 5.2.2.10.2.1 assumed that either SCS relief valve relieved water at this rate.

The design relief capacity of each of two SCS relief valves (shown in P&ID Figure 6.3.2-1C) as supplied by the valve manufacturer meets the minimum required relief capacity of 5000 gpm which contains sufficient margin in relieving capacity for even the worst transient. The SCS relief valves SI-179 and SI-189 are Safety Class 2, designed to Section III of the ASME Code. Testing of valve relieving capacity and set pressure are discussed in Section 5.4.7.4.

* Pressure measured at the valve inlet.

5.2.3 REACTOR COOLANT PRESSURE BOUNDARY MATERIALS

5.2.3.1 Material Specification

A list of specifications for the principal ferritic materials, austenitic stainless steels, bolting and weld materials, which are part of the reactor coolant pressure boundary is given in Table 5.2-2.

All carbon and low alloy steel materials including weld materials used within the reactor coolant pressure boundary will be limited to a maximum sulfur (S) content of ≤ 0.010% by weight.

Studies, as referenced by Regulatory Guide 1.99, Revision 02, have shown that the irradiation induced mechanical property changes of SA-533B and SA-508 materials can depend significantly upon the amount of residual elements present in the compositions, namely; copper, nickel, phosphorous, and vanadium. It has also been found that residual sulfur affects the initial toughness of SA-533B and SA-508 materials. Specific controls are placed on the residual chemistry of reactor vessel materials and the as-deposited welds used to join these materials to limit the maximum predicted increase in the reference temperature (RT_{NDT}, which is discussed in Sections 5.3.1.6 and 5.3.2.1.1) and to limit the extent of the reactor vessel beltline. The beltline is defined by Appendix G of 10 CFR 50.

Materials used in the reactor vessel beltline and the as-deposited welds contain no greater than the following weight percentages of residual elements:

Copper (in welds)	0.03		
Copper (in forgings)	0.03	Phosphorous	0.012
Nickel (in forgings)	1.00	Sulfur	0.010
Nickel (in welds)	0.10	Vanadium	0.030

The COL applicant will verify that the plant-specific material properties are within the limits assumed in the CESSAR-DC and the information will be provided in the site-specific SAR. 5-2

5.2.3.2 Compatibility with Reactor Coolant

5.2.3.2.1 Reactor Coolant Chemistry

Controlled water chemistry is maintained within the RCS. Control of the reactor coolant chemistry is the function of the CVCS which is described in Section 9.3.4. Water chemistry limits applicable to the RCS are given in Section 9.3.4.

discussion concerning prediction of irradiation effects and the material surveillance program.

Testing and measuring equipment for fracture toughness tests for the reactor vessel, steam generators, pressurizer, piping and reactor coolant pumps are calibrated in accordance with Subarticle NB2360 of the ASME Code, Section III.

5.2.3.3.2 Control of Welding

5.2.3.3.2.1 Avoidance of Cold Cracking

C-E complies with the recommendations of Regulatory Guide 1.50, Control of Preheat Temperature for Welding of Low Alloy Steel, May 1973, as discussed below.

Paragraph C.1.b implies that the qualification materials are an infinite heat sink that would instantaneously dissipate the heat input from the welding process. The qualification procedure consists of starting the welding at the minimum preheat temperature. Welding is continued until the maximum interpass temperature is reached. At this time, the test material is permitted to cool to the minimum preheat temperature and the welding is restarted. Preheat temperatures utilized for low alloy steel are in accordance with Section III of the ASME Code. The maximum interpass temperature utilized is 500°F.

6-1

[The paragraph C.2 recommendation is considered an unnecessary extension of procedures which apply to low-alloy steel welds, meeting ASME Code Sections III and IX requirements. The recommendations of Regulatory Guide 1.50 are met by complying with paragraph C.4. The soundness of all welds is verified by ASME Code acceptable examination procedures.]

FSER COL Item 6.1.1-4

With regard to Regulatory Guide 1.43, major components are fabricated with corrosion resistant cladding on internal surfaces exposed to reactor coolant. The major portion of the material protected by cladding from exposure to reactor coolant is SA-533B Class 1 or SA-508, Class 2 or 3. Cladding of SA-508, Class 2 forging material is performed using low-heat-input welding processes controlled to minimize heating of the base metal. Low-heat-input welding processes are not known to induce underclad cracking.

5.2.3.3.2.2 Regulatory Guide 1.34

Regulatory Guide 1.34 recommends controls to be applied during welding using the electroslag process. The electroslag process is not used in the fabrication of any RCPB components. Therefore, the recommendations of this guide are not applicable.

C-E specifies the use of a manganese phosphate coating on threads of studs, nuts and washers to improve anti-galling properties and resistance to corrosion. In addition, a nickel-based high purity anti-seize lubricant is specified to be added to threads and bearing surfaces at installation to further enhance anti-galling properties. Laboratory testing and field experience to date have shown no evidence of deleterious breakdown of either phosphate coating or lubricant.

5.3.2 PRESSURE-TEMPERATURE LIMITS

All components in the Reactor Coolant System (RCS) are designed to withstand the effects of cyclic loads due to RCS temperature and pressure changes. These cyclic loads are introduced by normal unit load transients, reactor trips, and startup and shutdown operation.

The design number of cycles for heatup and cooldown is based on a rate of 100°F/hr. During unit startup and shutdown, the rate of temperature change is limited to less than 100°F/hr by administrative procedure.

The maximum allowable RCS pressure at the corresponding minimum allowable temperature is based upon the stress limitations for brittle fracture. These limitations are derived using linear elastic fracture mechanics (LEFM) principles, the procedures prescribed by Appendix G to Section III of the ASME Code, "Protection Against Nonductile Fracture," Appendix G to 10 CFR 50, "Fracture Toughness Requirements," NRC Regulatory Guide 1.99, "Radiation Embrittlement of Reactor Vessel Materials," and the procedures recommended by Welding Research Council (WRC) Bulletin 175, "PVRC Recommendations on Toughness Requirements for Ferritic Materials." Compliance with Appendix H to 10 CFR 50, "Reactor Vessel Material Surveillance Program Requirements," is discussed in Section 5.3.1.6.

The COL applicant will verify that the plant-specific materials are consistent with the material specifications set forth in Section 5.2.3.1. If not, the applicant will submit the plant specific material fracture toughness data and resulting pressure-temperature curves. 5-2

During pre-operational testing of the Reactor Coolant System, the support displacements will be monitored for concurrence with calculated displacements and/or clearances. Subsequent inspections of supports which are integral with Reactor Coolant System components will be in accordance with Section XI of the ASME Code.

The COL applicant will verify that the as-built support materials properties and 60 year neutron fluence are consistent with the following: 5-2

- Maximum phosphorous, 0.012 percent per heat and 0.018 percent per product analysis
- Maximum copper, 0.15 percent per heat and per product analysis
- Other chemical compositions consistent with SA508 chemistry
- 60 year neutron fluence of 3.0×10^{18} neutrons per square centimeter ($E > 1.0$ MeV)

If not, revised fracture mechanics analysis shall be performed.

3. Regulatory Guide 1.71

Regulatory Guide 1.71 is discussed in Section 5.2.3.3.2.3.

5.2.4 INSERVICE INSPECTION AND TESTING OF REACTOR COOLANT PRESSURE BOUNDARY

An Inservice Inspection (ISI) program will be provided for the examination of the Reactor Coolant Pressure Boundary (RCPB) components and supports defined as Code Class 1. The program will reflect the principles and intent embodied in the ASME Boiler and Pressure Vessel Code, Section XI. Specific Code Editions and addenda required by 10 CFR 50.55a are referenced in the Preservice Inspection (PSI) and ISI programs, however, the PSI program will meet all requirements for Section XI of the same edition as the ASME Code used for construction, and the ISI program will meet the ASME Code Section XI in effect in accordance with 10 CFR 50.55a(g). The purpose of the inservice inspection program is to periodically monitor the systems or components requiring Inservice Inspection in order to identify and to repair those indications which do not meet acceptance standards.

The ISI Program consists of three subprograms as follows:

A. The Component Inspection Program, which includes piping system welds, hangers, supports, internal inspection of pump and valve bodies and bolting. This includes ultrasonic testing in accordance with Appendix VIII of ASME Section XI, Edition and Addenda required by 10 CFR 50.55a.

B. The Pump and Valve Inservice Test (IST) Program, which requires operability testing of selected pumps and valves, and

C. The Hydrostatic Test Program.

The development of the PSI and ISI program plans is the responsibility of the COL applicant and will be based on the ASME Code Section XI, Edition and Addenda specified in accordance with 10 CFR 50.55a. For design certification, the NSSS designer is responsible for designing the reactor coolant pressure boundary for accessibility to perform the preservice and inservice inspections. Responsibility for designing other components for preservice and inservice inspection is the responsibility of the COL applicant. The COL applicant is also responsible for specifying the Edition of the ASME Code Section XI to be used, based on the procurement date of the component per 10 CFR 50.55a. ASME Boiler and Pressure Vessel Code, Section XI, Subsection IWH has not been formally approved and issued for use by the nuclear industry. After approval and prior to implementation of the System 80+ pre-service inspection and in-service inspection programs, the COL applicant shall review the B&PV Code Subsection IWH to ensure appropriate compliance of these inspection programs. The provisions of 10 CFR 50.55a(a)(3)(i) and (ii) shall apply in cases where the System 80+ design does not practically accommodate full adherence to Subsection IWH. 5-3

of the ASME Code Section XI to be used, based on the procurement dates of Class 2 and 3 components, per 10 CFR 50.55a. ASME Boiler and Pressure Vessel Code, Section XI, Subsection IWH has not been formally approved and issued for use by the nuclear industry. After approval and prior to implementation of the System 80+ pre-service inspection and in-service inspection programs, the COL applicant shall review the B&PV Code Subsection IWH to ensure appropriate compliance of these inspection programs. The provisions of 10 CFR 50.55a(a)(3)(i) and (ii) shall apply in cases where the System 80+ design does not practically accommodate full adherence to Subsection IWH. 53

6.6.2 ACCESSIBILITY AND INSPECTABILITY

Accessibility to equipment for maintenance, testing, and inspection is a basic element of the System 80+ design process, as indicated in Table 1.2-1 (Item A.2). Provisions have been made in the design and layout of Code Class 2 and 3 Systems to allow for compliance with the inservice inspection requirements contained in ASME Code Section XI, Articles IWC-2000 and IWD-2000, and as defined in the inservice inspection program. Code Class 2 and 3 components requiring inspection will be designed for and be provided with access to enable the performance of Section XI inspections onsite. Systems and components are designed such that design, materials, and geometry do not restrict inspections required by Section XI of the ASME Code.

Welds and other areas requiring periodic inspection are made accessible. Reinforcing pads, supports, piping and equipment have been located not to obstruct welds. Insulating materials are removable to provide accessibility for the required in-service inspection.

6.6.3 EXAMINATION TECHNIQUES AND PROCEDURES

The examination techniques to be used for inservice inspection will include radiographic, ultrasonic, magnetic particle, liquid penetrant, eddy current, and visual examination methods. For all examinations, both remote and manual, specific procedures will be prepared describing the equipment, inspection technique, operator qualifications calibration standards, flaw evaluation, and records. These techniques and procedures will meet the requirements of Articles IWC-2000 and IWD-2000 in the ASME Code, Section XI edition in effect as stated in Section 6.6.1. Pre-service Inspection (PSI) and subsequent Inservice Inspection (ISI) will be conducted with equivalent equipment and techniques.

For the preservice inspection, all of the items selected for inservice inspection shall be performed once in accordance with the ASME Code Section XI, Subsections IWC-2200 and IWD-2200, with the exception of the examinations specifically excluded by ASME Section XI from preservice requirements, such as the VT-2 examinations for Category C-H.

5.4.2.5 Tests and Inspections

Prior to, during and after fabrication of the steam generator, nondestructive tests based upon Section III of the ASME Code are performed.

Initial hydrostatic tests of the primary and secondary sides of the steam generator are conducted in accordance with ASME Code, Section III. Leak tests are also performed. Following satisfactory performance of the hydrostatic tests, magnetic-particle inspections are made on all accessible welds.

Inservice inspection of the steam generator will be performed in accordance with ASME Code, Section XI.

The COL applicant will establish and submit for NRC staff review, a surveillance program for inservice inspection of steam generator tubes. 5-4

on one steam line leaving each steam generator. In the event of a tube rupture, the alarm will initiate and then may clear as reactor power decays due to the reactor trip. Therefore, when a N-16 radiation monitor detects the high gamma radiation condition, the alarm will be latched. Acknowledging the alarm does not reset the latch, the alarm latch must be reset separately by the operator. This logic is presented by Figure 5F-96.

5.6.3 Primary-to-Secondary Leakage Monitoring Program

The instrumentation described above will be incorporated by the COL applicant into a primary-to-secondary leakage monitoring program that addresses three specific scenarios:

a. Low Level and/or Slowly Increasing Primary-to-Secondary Leakage,

b. Rapidly Increasing Primary-to-Secondary Leakage (as described in IN-91-43 and IN-88-99), and

c. Steam Generator Tube Rupture (No Leak Before Break)

5-5

The program will also address instrumentation setpoints and methodology for equipment (including N-16 monitors) used to detect steam generator tube leakage and ruptures commensurate with the above scenarios.

5.7 REACTOR COOLANT GAS VENT SYSTEM

5.7.1 DESCRIPTION

The System 80+ design includes a safety grade Reactor Coolant Gas Vent System (RCGVS) used to vent non-condensible gases and steam from the reactor vessel upper head and the pressurizer steam space. The system is comprised to two independent piping trains, one from the reactor vessel and one from the pressurizer each with parallel valve paths in each train allowing for single failure operation. The parallel path from the pressurizer and the reactor vessel upper head contains two isolation valves in series. The pipe trains are routed to the IRWST and the Reactor Drain Tank (RDT). The valves are remote manually controlled.

5.7.2 OPERATION

The RCGVS is designed to be operable during all design basis events. In the event a void forms in either the reactor vessel upper head, the RCGVS may be used to depressurize the RCS and remove the void in the upper head. In the pressurizer if pressurizer spray is not available, the operator manually opens the RCGVS valves to vent steam and depressurize the reactor coolant system.

5.7.3 INSTRUMENTATION

Pressure indication is provided between the isolation valves in each RCGVS train which alarms and provides the operator with indication that a valve did not reseat or the valve leaks. Temperature indication is provided downstream of RCGVS isolation valves to monitor leakage from the reactor coolant pressure boundary.

6.1 ENGINEERED SAFETY FEATURE MATERIALS

6.1.1 METALLIC MATERIALS

6.1.1.1 Materials Selection and Fabrication

6.1.1.1.1 Specifications for Principal ESF Pressure Retaining Materials

Principal ESF pressure retaining materials are listed in Table 6.1-1.

6.1.1.1.2 Engineered Safety Feature Construction Materials

Materials located inside containment that are exposed to the containment spray solution are indicated on Table 6.1-2. These materials are chosen to be compatible with these chemical solutions.

Materials used in ESF component construction are reviewed for acceptability by C-E prior to release for material procurement.

Corrosion of materials within the containment is minimized by restricting the use of zinc, aluminum, and mercury.

The problems associated with these metals are:

A. Aluminum is attacked by alkaline solutions which may result in the loss of structural integrity and the generation of gaseous hydrogen. The amount of aluminum present inside the containment is the lowest practicable amount.

B. Boric acid spray reacts with zinc, oxidizing it and liberating hydrogen gas. The use of zinc in the containment is kept to a minimum to avoid the generation of hydrogen.

C. The use of mercury and mercuric compounds is prohibited for components inside the containment. These materials react with aluminum, stainless steel, NiCrFe alloy 600, and alloys - containing copper.

6.1.1.1.3 Integrity of ESF Components During Manufacture and Construction

6.1.1.1.3.1 Control of Sensitized Stainless Steel

The NSSS ESF components comply with the recommendations of Regulatory Guide 1.44 in the following manner. 6-1

All raw austenitic stainless steel, both wrought and cast, used to fabricate pressure retaining components of the engineered safety features, is supplied in the annealed condition as specified in the pertinent ASME Specification (i.e., 1900-2050°F for 0.5 to 1.0 hour per inch of thickness and rapidly cooled below 700°F). The time at temperature is determined by the size and type of component. Vendor fabrication procedures will be audited to ensure that unstabilized austenitic stainless steel with a carbon content greater than 0.03% is not exposed to the temperature range of 430°C to 820°C (800°F to 1500°F) other than during welding.

Duplex, austenitic stainless steels, containing greater than 5FN delta ferrite (weld metal, cast metal, weld deposit overlay), are not considered unstabilized, since these alloys do not sensitize; i.e., form a continuous network of chromium-iron carbides. Specifically, alloys in this category are:

CF 8M CF 8	Cast stainless steels (delta ferrite controlled to 5FN to 30FN, 8FN to 20FN for normal operating temperatures above 500°F)
Type 308 Type 309 Type 312 Type 316	Singly and combined stainless steel weld filler metals (delta ferrite controlled to 5FN to 15FN deposited)

In duplex austenitic/ferritic alloys, chromium-iron carbides are precipitated preferentially at the ferrite/austenite interface during exposure to temperatures ranging from 800 to 1500°F. This precipitate morphology precludes intergranular penetrations associated with sensitized Type 300 series stainless steels exposed to oxygenated or otherwise faulted environments.

6.1.1.1.3.2 Cleaning and Contamination Protection Procedures

Specific requirements for cleanliness and contamination protection are provided for NSSS components which provide contamination control during fabrication, shipment, and storage as recommended in Regulatory Guide 1.37.

Contamination of Type 300 series austenitic stainless steels by compounds that can alter the physical or metallurgical structure and/or properties of the material is avoided during all stages of fabrication. Painting of Type 300 series stainless steels is prohibited. Grinding will be performed with resin or rubber bonded aluminum oxide or silicon carbide wheels that have not previously been used on any materials other than Type 300 series stainless alloys. Grinding wheels bonded with rubber compositions that include halides or sulfur will not be used on austenitic stainless steels.

Internal surfaces of completed components are cleaned to produce an item that is clean to the extent that grit, scale, corrosion products, grease, oil, wax, gum, adhered or embedded dirt, or extraneous material are not visible to the unaided eye.

Degreasing solvents, acetone or isopropyl alcohol, may be used on metallic surfaces. Water used for cleaning is inhibited with 30-100 ppm hydrazine.

The specification for water quality is:

Halides

Chloride, ppm	<0.60
Fluoride, ppm	<0.40
Conductivity, μmhos/cm	<5.0
pH	6.0-8.0
Visual clarity	No turbidity, oil or sediment

6.1

6.1.1-3

[To prevent halide-induced intergranular corrosion which could occur in an aqueous environment with significant quantities of dissolved oxygen, flushing water is inhibited via additions of hydrazine.] Many experiments conducted by C-E have proven this inhibitor to be effective.

Onsite and pre-operational cleaning of ESF components is in accordance with the recommendations of Regulatory Guide 1.37.

6.1.1.1.3.3 Cold-Worked Stainless Steel

Cold-worked austenitic stainless steel is not utilized for components of the ESF.

6.1.1.1.3.4 Non-Metallic Insulation

All non-metallic insulation materials installed on stainless steel piping and equipment of the ESF are made of calcium silicate, expanded pearlite, fiberglass fiber, or similar materials (ASTM C533, C547, C553, C610, C612) and are consistent with the recommendations of Regulatory Guide 1.36.

(Paints) for Light Water Nuclear Reactor Containment Facilities," and recommendations of Regulatory Guide 1.54, "Quality Assurance Requirements for Protective Coatings Applied to Water-Cooled Nuclear Power Plants." In addition, the selection of coatings are based on ASTM Standards D3842-86, "Standard Guide for Selection of Test Methods for Coatings for use in Light Water Nuclear Power Plants", ASTM D3911-89, "Standard Test Method for Evaluating Coatings used in Light Water Nuclear Power Plants at Simulated Design Basis Accident (DBA) Conditions", and ASTM D3843-89, "Standard Practice for Quality Assurance for Protective Coatings Applied to Nuclear Facilities". Any particulate debris of appreciable size that does occur will either settle to the bottom of the Holdup Volume Tank or will be trapped by the filter screen at the bottom of the in-containment refueling water storage tank (IRWST). The screen size is smaller than the line piping diameter, the shutdown cooling heat exchanger tube diameter, the containment spray heat exchanger tube diameter, and the spray nozzle openings so that particles that could potentially block the system are filtered out. A list of surface coatings used inside containment and their applicable conditions is given in Table 6.1-3.

6.1.2.2 Other Materials

A listing of other materials in the containment is included in Table 6.1-4. The materials listed are not protective coatings applied to surfaces of nuclear facilities.

The COL applicant will ensure that the total amount of cable insulation is less than or equal to the amount listed in Table 6.1-4. 15-2

established based on system considerations, but all valves should stroke to their designated position as soon as practicable upon actuation. An upper limit of 60 seconds shall be utilized in stroke time determination.

I. Valve operators and power sources are selected for containment isolation valves consistent with their required safety function.

J. Instrumentation and control sensing lines which penetrate the containment are provided with containment isolation provisions which meet the intent of Regulatory Guide. 1.11.

K. All containment penetrations not used for accident mitigation or safe shutdown are automatically isolated by a Containment Isolation Actuation Signal (CIAS) unless:

1. The valves are normally locked closed

2. The penetrations are normally sealed (i.e., fuel transfer tube)

3. The lines are needed for RCP operation (RCP seal injection and component cooling water to RCP seal coolers, motors, and lube oil coolers)

The exception for RCP operation allows the RCPs to be available for accident mitigation or safe shutdown if offsite power and non-essential support systems are available. These lines are continuously monitored for radiation and can be manually isolated from the control room.

L. The induced stresses in the pressure retaining components of the CIVs, due to an internal containment pressure of less than or equal to 120 psig, are within the ASME Code Section III Service Level C stress limits.

6.2.4.2 System Description

No single piping and instrumentation diagram shows all of the containment penetrations; however, they are shown on appropriate piping and instrumentation diagrams for systems. Containment isolation provisions are tabulated in Table 6.2.4-1. The appropriate valve arrangements are illustrated in Figure 6.2.4-1.

All valves that receive an engineered safety features actuation signal are designed and tested with closing time appropriate to the function performed. The sequencing system for loading the onsite emergency electrical generators is designed to close all valves receiving an engineered safety features actuation signal within seconds of the time the shift to emergency onsite electrical power signal is accomplished.

TABLE 6.2.4-1 (Cont'd)

(Sheet 13 of 15)

CONTAINMENT ISOLATION VALVE AND ACTUATOR DATA

Item No.	Service	Valve No.	Figure No.	(Note 16) Valve Type	Location Relative to Containment	Flow Direction Relative to Containment	(Note 1) Valve Arrangement (GDC)	(Note 5) Valve Position Normal	Fail Safe	Shutdown	Accident	(Note 4) Actuator Type	(Note 2) Actuation Signal	(Note 3) Type	Vent and Drain for Type-A Test	(Note 6) Type-C Test	Justification for Not Testing	(Note 17) Essential/ Nonessential
99	Steam Generator Wet Layup Recirculation Return to Steam Generator #1	-	-	Gate	Outside	In	9	LC	-	O/C	LC	HW	-	M	No	No	Note 7	Nonessential
		-		Check	Inside		(57)	C	-	O/C	C	-	-	-				
100	Steam Generator Wet Layup Recirculation Return to Steam Generator #2	-	-	Gate	Outside	In	9	LC	-	O/C	LC	HW	-	M	No	No	Note 7	Nonessential
		-		Check	Inside		(57)	C	-	O/C	C	-	-	-				

NOTES: 1. Valve arrangements are shown in Figure 6.2.4-1. The COL Applicant is to provide penetration pipe sizes and distances of isolation valve from containment.

2. Definition of Actuation Signals

CIAS - Containment Isolation Actuation Signal
CSAS - Containment Spray Actuation Signal
MSIS - Main Steam Isolation Signal
EFAS - Emergency Feedwater Actuation Signal
AFAS - Alternate Feedwater Actuation Signal
HRAS - High Radiation Actuation Signal
HHAS - High Humidity Actuation Signal
SIAS - Safety Injection Actuation Signal
CCWLLSTAS - Component Cooling Water Low-Low Surge Tank Actuation Signal

All of these signals are Engineered Safety Features Actuation Signals, except HRAS, HHAS, CCWLLSTAS, and AFAS. Valves receiving ESF signals are classified as ESF valves.

6.3.4 INSPECTION AND TESTING REQUIREMENTS

During fabrication of the SIS components, tests and inspections are performed and documented in accordance with code requirements to assure high quality construction. As necessary, performance tests of components are performed in the vendor facilities. The SIS is designed and installed to permit in-service inspections and tests in accordance with the ASME Code, Section XI.

6.3.4.1 SIS Performance Tests

Prior to initial plant startup, a comprehensive series of system flow tests, as detailed in Section 14.2, will be performed to verify that the design performance of the system and individual components is attained.

Preoperational tests and analyses will be performed to confirm that the as-built SIS fulfills operability requirements and provides a level of performance that satisfies safety analyses. 6-2

6.3.4.1.1 Flow Testing

Each installed SI train will be tested to measure SI pump developed differential pressure at miniflow, measure runout flow through the DVI lines and, for SI pumps 3 and 4, measure runout flow through the hot leg injection lines. Runout flow testing will be conducted with the RCS at atmospheric pressure conditions. Test results will be used to confirm SI pump performance characteristics over the operating range of the pump and to confirm system resistance characteristics. Test conditions, including fluid temperature, suction and discharge side fluid elevations, and potential instrument uncertainties will be taken into account in performing an analysis. The analysis will use test results, with adjustments made for test conditions, to determine system performance during postulated accident conditions. The calculated system performance shall be within the limits used to perform safety analyses in Section 6.3.3 and Chapter 15.

Testing will be performed to confirm that the SI pump miniflow rate in the installed system meets or exceeds the pump vendor's minimum flow requirements. The pump vendor will perform a type test with fluid conditions representative of those during a natural circulation cooldown to generate data that verifies the SI pumps' ability to operate continuously within the design limits at minimum flow for the mission time. The pump type test will monitor the normal pump qualification test parameters and will use the following as acceptance criteria: 6-2

- Bearing oil equilibrium temperature: The testing will demonstrate that its temperature will not exceed the maximum safe limit for lubrication (typically, vendors have endorsed a limit of 180°F for bearing oil temperature),

- Pump shaft seal leakage temperature: The testing will demonstrate that the temperature will not exceed the maximum safe limit for the seals (typically, vendors have endorsed a limit of 175°F for the shaft seal cooling water),

- Pump bearing housing vibration: Pump bearing housing vibration will be measured in accordance with ISTB 4.6.4 from the ASME OM Code. Testing will demonstrate that vibrations are within the criteria established in Figure ISTB 5.2 from the ASME OM Code, and

- Pump inspection: After completion of the test, the SI pump will be disassembled and the internals inspected with the conditions of the parts being evaluated for excessive wear as a result of degradation during the pump test.

The duration of the test, or mission time, is either eight hours or until the bearing oil temperature, the pump shaft seal leakage temperature and the pump bearing housing vibration stabilize, whichever is longer. Eight hours represents the maximum time the SI pumps are required to operate at minimum flow as discussed in Appendix 5D for a natural circulation cooldown.

Testing will be performed to confirm that the SI pump return line to the IRWST allows each SI pump to be operated at a flow rate equal to or greater than design flow during inservice testing. 6-2

The available NPSH to the SI pumps will be determined based on the as-built elevations, piping arrangements, and system performance parameters measured during testing. Measured pump suction pressures and flow rates will be used in an analysis to demonstrate that adequate available NPSH is provided to each SI pump assuming the following post-accident conditions:

- minimum IRWST level during an accident;

- saturated IRWST fluid conditions;

- as-built pressure losses for pump inlet piping and components.

The calculated minimum available NPSH shall exceed the NPSH required by the pump vendor.

6.3.4.1.2 Safety Injection Tank Testing

A test will be conducted to demonstrate that the SITs can be depressurized by venting for entry into shutdown cooling. During the test, each SIT will be pressurized and its isolation valve shut. The test will confirm that each SIT vent valve can be opened from the control room and that SIT pressure decreases while each SIT is being vented. 6-2

Each SIT will be tested to measure changes in SIT pressure and level during SIT blowdown. The test results will be used in an analysis to demonstrate that the as-built resistance coefficient of each tank's discharge line is within the limits used to perform safety analyses in Section 6.3.3 and Chapter 15. 6-2

6.3.4.2 Reliability Tests and Inspections

6.3.4.2.1 System Level Tests

After the plant is brought into operation, periodic tests and inspections of the SIS components and subsystems are performed to ensure proper operation in the event of an accident. The scheduled tests and inspections are necessary to verify system operability, since during normal plant operation, SIS components are aligned for emergency operation and serve no other function. The tests defined permit a complete checkout at the subsystem and component level during normal plant operation. Satisfactory operability of the complete system can be verified during normally scheduled refueling shutdown. The complete schedule of SIS tests and inspections is detailed in Chapter 16. 6-2

6.3.4.2.2 Component Testing

In addition to the system level tests described in Section 6.3.4.1, tests to verify proper operation of the SIS components are also conducted. These tests supplement the system level tests by verifying acceptable performance of each active component in the SIS. Pumps and automatic valves will be tested in accordance with the ASME Code, Section XI. 6-2

6.3.5 INSTRUMENTATION REQUIREMENTS

6.3.5.1 Design Criteria

The instrumentation and controls for the SIS are designed in accordance with the applicable portions of the IEEE standards as delineated in Section 7.1.2. The controls automatically provide the sequence of operations required to initiate SIS operation. The instrumentation and controls which actuate and control the SIS are designed on the following basis:

E. Fire protection for the control room is provided by alarm systems and portable fire extinguishers. The Fire Protection System is discussed in Section 9.5.1.

F. The intent of "housekeeping requirements" set out by Regulatory Guide 1.39 are met.

G. The quantities and uses of onsite and offsite hazardous chemicals will be controlled by administrative procedures.

H. The control room boundary pressurization system will be periodically tested (every 18 months) to verify that the make up air required to maintain a minimum of 1/8" w.g. pressure inside the control room boundary with respect to the adjacent areas does not exceed 10% of the design value.

The COL applicant will verify that the control room habitability system is consistent with the licensing basis documentation. 6-4

6.4.1.2 Interface Requirements

The COL applicant shall verify that the following interface requirements are met to ensure adequacy with the System 80+ Standard Design:

A. The toxic chemical release analysis will be performed on a site specific bases since location of toxic chemicals is site dependent. 6-3

B. The COL applicant shall develop a procedure for management of the maximum amount of seal leakage that could occur, for the specific pumps procured, during a design basis accident (It is expected that the maximum leakage would be that from one safety injection pump and one containment spray pump during the long-term cooling portions of a loss of coolant accident). 6-5

6.4.2 SYSTEM DESCRIPTION

6.4.2.1 General

The Control Complex Ventilation System description is provided in Section 9.4.1. Component descriptions are also provided in Section 9.4.1.

Climatic conditions in the control room are maintained by cooling and heating units that automatically control the temperature and limit the humidity within the comfort zone for operating personnel. In doing so, the climatic conditions required for the equipment located in the control room are also satisfied.

The following passive safety features are available in System 80+ design to cope with the closure of both intakes due to high concentration of toxic gas at both intakes.

In case of closure of both intakes due to high level of concentration of toxic gas at both intakes, the operator will shut down the control room air conditioning and filtration systems. This will eliminate leakage caused by the pressure differentials created by the fans. The control room temperature will be allowed to rise to pressurize the control room. The operators will don themselves with face masks connected to a storage reservoir before the control room temperature rise exceeds 10°F. The air released from the face masks will travel away from the occupants as it mixes with the control room environment and create slight pressurization to minimize inleakage to the habitability zone. The face masks are at locations accessible to the operators. The storage reservoir provides six hour supply of breathing air. After the operators start using the breathing air, the air conditioning units will be started to keep the control room temperature from rising. [Detailed operating procedure to cope with the toxic gas accident will be prepared by the COL applicant.] The exact location and detailed design of the storage reservoir will be provided by the COL applicant. 6-3

The COL applicant will develop an operating procedure to cope with closure of both intakes due to high concentration of smoke at both intakes.

6.4.3 SAFETY EVALUATION

Analytical evaluations have been performed of the systems required to be operational to ensure control room habitability following a postulated design basis accident. The Control Room data used for these evaluations is provided in Table 15A-10. The parameters associated with the accident releases are provided in the corresponding sections of Chapter 15. Control room shielding design, based on the most limiting design basis loss of coolant accident fission product release, is discussed in Chapter 12. As shown in the Table 6.4-1 radiation exposures to control room personnel resulting from design basis accidents do not exceed the dose limits specified in General Design Criterion 19 and clarified in SRP 6.4; i.e., 30 Rem thyroid, 5 Rem whole body gamma and 30 Rem beta skin (or 75 Rem beta skin if the applicant commits to the use of protective clothing).

The Control Complex Ventilation System is evaluated in detail in Section 9.4.1. Control Complex Ventilation System design prohibits unfiltered intake of air at radioactivity levels above those allowed in 10 CFR 20.

During a LOCA, the reactor cavity will not be flooded as was assumed in determining the minimum water level of 75.5 feet. Because of this, an additional volume of water will be available to raise the minimum water level in the IRWST by approximately 2 feet, thereby increasing the available NPSH.

Prevention of the entrance of debris into the IRWST and SI and CS pump suction lines is described in Section 6.8.

6.5.4 TESTING AND INSPECTION

6.5.4.1 Pre-operational Testing

Pre-operational tests are conducted to verify proper operation of the CSS. The operational tests include calibration of instrumentation, verification of adequate pump performance, verification of the operability of all associated valves, and verification that the spray headers and spray nozzles are free of obstructions. In addition, a pre-operational hot functional performance test is made on the installed CSS heat exchangers as part of the precore hot functional test program.

The CSS also undergoes a series of pre-operational hydrostatic tests conducted in accordance with Section III of the ASME Boiler and Pressure Vessel Code.

Tests of individual components or the complete Containment Spray System will be controlled to ensure that plant safety is not jeopardized and that undesirable transients do not occur.

Pre-operational test results will be used to perform analyses that confirm the as-built CSS fulfills operability requirements and provides a level of performance that satisfies safety analyses.

6.5.4.1.1 Flow Testing

Each installed CS train will be tested to measure CS pump developed differential pressure at a flow rate equal to or greater than the pump design flow rate. An analysis will be performed to convert the test results to determine pump performance at design conditions after an accident. The calculated performance shall be within the limits used to perform safety analyses.

An inspection of the as-built spray header will be performed. The results will be combined with the tested performance characteristics of each CSS pump to perform an analysis to determine the maximum expected CS pump flow rate. The calculated maximum flow rate shall be less than or equal to the maximum allowable flow rate specified by the pump vendor.

also minimizes the entrance of any debris into the IRWST. Screens located at the entrance to the pump suction lines provide assurance that no debris will enter the system. The screen design meets the requirements of Regulatory Guide 1.82, and considers the effects of all types of insulation that may exist in containment on screen blockage. A description of the IRWST screen design is provided in Appendix 19.8A, Section 2.9.

The COL applicant will submit an analysis, consistent with Regulatory Guide 1.82, of the suction inlet screen area based on the insulation type and quantity. This analysis will show that the System 80+ screen area has a margin of at least three over that indicated by Regulatory Guide 1.82. This is a DRAP item; see Section 17.3. 6-7 6-8

6.8.2.2.2 Holdup Volume Tank (HVT)

The HVT is located between the primary shield wall and the IRWST inner wall.

Any leakage from components or piping not routed to the RDT or spills inside containment, will drain to the HVT. This prevents direct contamination of the water in the IRWST.

A sump in the HVT collects any leakage. Pumps located in this sump transfer water to the Liquid Waste Management System (LWMS) during normal operation.

During accidents, water from breaks and containment sprays drains to and collects in the HVT (Figure 6.8-2). This water collects in the HVT until the water level in the HVT reaches the IRWST spillways at which point water flows back into the IRWST.

The HVT provides a delay to cavity flooding following the actuation of the CFS to allow control room operators time to abort cavity flooding, if desired.

6.8.2.2.3 Cavity Flooding System (CFS)

The function of the CFS is to flood the reactor cavity in the event of a severe accident for the purpose of covering core debris in the reactor cavity with water. This facilitates the cooling and stabilization of the debris.

The CFS is shown in Figure 6.8-2. It is comprised of four, 12-inch diameter HVT spillways, two 10-inch diameter reactor cavity spillways, the corresponding spillway valves, motor operators and controls.

The HVT spillways consist of stainless steel pipe within circular conduits in the concrete wall separating the IRWST and HVT. The reactor cavity spillways are similarly constructed in the primary shield wall separating the HVT and the reactor cavity.

7.1.2.3 Conformance to IEEE 308-1980

Descriptions of electrical components, equipment and systems which are vital to safe operation are described in Chapter 8. Conformance to IEEE 308-1980, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," as criteria in the design of these systems is also discussed in Chapter 8.

7.1.2.4 Conformance to IEEE 317-1983

Electrical penetrations and their conformance to IEEE 317-1983, "Electrical Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations," is discussed in Chapter 8.

7.1.2.5 Conformance to IEEE 323-1974, as Augmented by Regulatory Guide 1.89

Compliance with IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," for instrumentation is discussed in Combustion Engineering Topical Report CENPD-255-A, "Qualification of Combustion Engineering Class 1E Instrumentation" (Reference 1). The basic qualification requirements are discussed in Section 3.11.

7.1.2.6 Conformance to IEEE 336-1985, as Augmented by Regulatory Guide 1.30

Conformance with IEEE 336-1985, "Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations," is discussed in Section 1.8.

7.1.2.7 Conformance to IEEE 338-1977, as Augmented by Regulatory Guide 1.118

The PPS and ESF-CCS, as well as the RTSS, are designed so that they can be periodically tested in accordance with the criteria of IEEE 338-1977, "Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems." Combustion Engineering supplies the response times of instrumentation and control components as a result of factory tests to the site operator. [It is the site operator's responsibility to test the integrated response time of each protection system after installation.] Testing criteria are specified in Sections 7.2.2.3.3 and 7.3.2.3.3. Minimum testing frequency requirements are provided in the Technical Specifications (Chapter 16). 7-1

Control board process indication and status instrumentation are provided to enable the operator to determine system status, evaluate system performance, and detect malfunctions. Control panel hand switches and valve position limit indication lights are provided for the isolation valves and the heat exchanger inlet, outlet, and bypass valves. Indication is provided for low Shutdown Cooling System pump discharge pressure and temperature, heat exchanger outlet temperature, and shutdown cooling system flow and pressure. SCS pump operating status is also indicated on the control board.

7.4.1.1.8.2 Interlocks, Sequencing and Bypasses

The SCS has overpressure protection interlocks as discussed in Section 7.6.

[The system sequencing will be in approved operating procedures provided by the site operator for the manually controlled equipment.] There are no bypasses in the SCS instrumentation that would jeopardize the protection afforded by the interlocks. 7-2

7.4.1.1.8.3 Redundancy and Diversity

Each of the two SCS trains has sufficient instrumentation to assure adequate monitoring during all modes of operation. The isolation valves are discussed in Section 7.6.

7.4.1.1.8.4 Supporting Systems

The SCS trains A and B have independent Class 1E power sources for their actuated equipment (e.g., pumps, valves). The SCS isolation valve interlocks are implemented via the ESF-CCS using a redundant channel configuration such that a single failure will not cause loss of shutdown cooling nor spuriously actuate it.

7.4.1.1.9 Safety Injection System (SIS)

Boron addition via the SIS may be used if the CVCS is not available for the hot and cold shutdown processes. The CVCS is discussed in Section 9.3.4. The SIS instrumentation and controls that are utilized to achieve cold shutdown are described below. The SIS logic and piping are provided in Section 7.3 and Figures 6.3.2-1A through 6.3.2-1F.

7.3.1.1.9 Vital Instrument Power Supply

The vital instrument power supply requirements are discussed in Section 7.1.3, and in Chapter 8.

7.3.1.1.10 Actuated Systems

The ESF Systems are maintained in a standby mode during normal operations. Actuating signals, generated by the ESFAS are provided to assure that the ESF Systems provide the required protective actions. The following descriptions of the instrumentation and controls of the ESF Systems is applicable to each ESF System. Table 7.3-2 presents the Design Basis Events (DBE) which require specific ESF System action. Table 7.3-3 presents the monitored variables required for ESF System actuation. The variables and their ranges are shown on Table 7.3-6.

7.3.1.1.10.1 Containment Isolation System

Section 6.2.4 contains a description of the Containment Isolation System (CIS). The actuation system is composed of redundant trains A and B. The instrumentation and controls of the two trains are physically and electrically separate and independent as discussed above such that the loss of one train will not impair the safety function.

The Containment Isolation System instrumentation and controls are designed for operation during all phases of plant operation. However, the system is removed from service prior to containment leak checking at refueling intervals in order to prevent undesired system actuation. The removal from service is accomplished in accordance with procedures prepared by the site operator. 7-3

The Containment Isolation System is automatically actuated by a CIAS from the ESFAS.

7.3.1.1.10.2 Containment Spray System

Refer to Section 6.5, "Containment Spray System," for a description of the Containment Spray System (CSS). The CSS is actuated by a CSAS. Containment spray pumps are also actuated by an SIAS. When used in the containment spray configuration, the shutdown cooling pumps are actuated by an SIAS or CSAS. The Annulus Ventilation System described in Section 6.2.3 is also activated by CSAS.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of each train are physically and electrically separate and independent. Each train is a 100% capacity system, therefore, the CSS can sustain the loss of an

entire train and still provide its required protective action. The CSS instrumentation and controls are designed to operate under all plant conditions.

The CSAS is removed from service prior to the containment leak test at refueling intervals in order to prevent undesired system actuation. The removal from service is accomplished in accordance with procedures prepared by the site operator. 7-3

The ESF-CCS design accommodates realignment of a spray pump for use as a shutdown cooling pump and vice versa.

7.3.1.1.10.3 Main Steam Isolation System

Refer to Section 10.3, "Main Steam Supply System," for a description of the Main Steam Isolation System. Refer to Section 10.4.7, "Condensate and Feedwater System," for a description of the Main Feedwater Isolation System. Refer to Section 10.4.8, "Steam Generator Blowdown System," for a description of the Blowdown Isolation System.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of the valves in train A are physically and electrically separate and independent of the instrumentation and control of the valves of train B. The separation and independence are such that a failure of one train will not impair the protective action.

The Main Steam Isolation Valves (MSIVs), MSIV Bypass Valves, Main Feedwater Isolation Valves (MFIV) and the isolation valves for the blowdown lines are actuated by an MSIS.

These valves effectively isolate the steam generators from the rest of the main steam and feed systems.

A variable steam generator pressure setpoint is implemented to allow controlled pressure reductions, such as shutdown depressurization, without initiating an MSIS. The pressure setpoint will track the pressure up until it reaches its normal setpoint value.

7.3.1.1.10.4 Safety Injection System

Refer to Section 6.3, "Safety Injection System," for a description of the Safety Injection System (SIS). The SIS is actuated by an SIAS.

The actuation system is composed of redundant trains A, B, C and D. The instrumentation and controls of each train are physically and electrically separate and independent. The SIS

can sustain the loss of an entire train and still provide its required protective action. The SIS instrumentation and controls are designed to operate under all plant conditions.

The low pressurizer pressure setpoint can be decreased as described in Section 7.2.1.1.1.6 to avoid inadvertent operation during startup and shutdown. As pressurizer pressure increases, the setpoint will follow up to its normal value. The SIAS is removed from service during containment leak checking at refueling intervals to prevent undesired system operation. The removal from service is accomplished in accordance with procedures prepared by the site operator. 7-3

7.3.1.1.10.5 Emergency Feedwater System

Refer to Section 10.4.9, "Emergency Feedwater System," for a description of the Emergency Feedwater System (EFWS). The EFWS is actuated by an EFAS-1 for Steam Generator 1 and an EFAS-2 for Steam Generator 2. The EFWS is also actuated by the Alternate Protection System (APS), described in Section 7.7.

The actuation system is composed of redundant trains A, B, C, and D. The instrumentation and controls of each train are physically and electrically separate and independent. The EFWS can sustain the loss of an entire train and still provide its required protective action. The EFWS instrumentation and controls are designed to operate under all plant conditions.

On a low steam generator level, the EFAS signal starts the EFW pumps and opens the EFW isolation valves and flow control valves causing full flow system actuation. The actuation signal which opens the valves will clear automatically when normal steam generator level is restored. Upon clearing of the actuation signal, the valves will remain in their open position, however the plant operator can manually control (i.e., reduce flow) as defined in Section 10.4.9, otherwise, maximum flow will continue. If steam generator water level again falls below the low steam generator water level setpoint after the actuation signal clears, the EFAS signal will reactuate again causing full flow system actuation.

To prevent steam generator overfill, a high steam generator level interlock is provided by the FSF-CCS to automatically close the isolation valves. This interlock is active only when EFAS actuation is not active. This interlock also protects against steam generator overfill due to erroneous operation of the EFW system by the operator or the APS.

7.3.1.3 System Drawings

The typical MCBDs, functional logics and typical control circuits are shown in the figures following this section.

7.3.1.4 ESFAS Supporting Systems

The systems required to support the ESFAS are discussed in Section 7.4. The electrical power distribution is discussed in Section 8.3.

7.3.2 ANALYSIS

7.3.2.1 Introduction

The ESFAS is designed to provide protection against the Design Basis Events listed on Table 7.3-2. The ESF Systems that are actuated are discussed in Chapter 6, along with their design bases and evaluations. The ESFAS is addressed in the Chapter 15 Safety Analysis.

The sensor signals which will cause each ESF actuation signal are listed on Table 7.3-3. The bases are discussed in Section 7.3.1.2. The trip setpoints are given on Table 7.3-5. Most ESF actuation signals are based on fixed setpoint trips. The trip setpoints that do not fall into this category are:

A. Low pressurizer pressure - can be decreased to 400 psi below the existing pressurizer pressure by the operator.

B. Low steam generator pressure - can be decreased to 200 psi below the existing steam generator pressure by the operator.

These resets are controlled by administrative procedures provided by the site operator. 7-K

Additionally, several ESF actuation signals can be actuated by more than one parameter. That is, different parameters can cause the same ESF actuation signal. The ESF signals which fall into this category are:

A. SIAS by either low pressurizer pressure or high containment pressure.

B. CIAS by receiving the SIAS for that channel so that it actuates on low pressurizer pressure or high containment pressure.

Criterion 23 - Protection System Failure Modes:

Refer to Section 3.1.19 for compliance.

Criterion 24 - Separation of Protection and Control Systems:

Refer to Section 3.1.20 for compliance.

Criteria 34, 35, 37, 38, 40, 41, 43, 44 and 46:

Refer to Sections 3.1.30, 31, 33, 34, 36, 37, 39, 40 and 42 for compliance.

The ESFAS provides the actuation which meets the requirements of IEEE Std. 279-1971 and IEEE Std. 338-1977. The single failure criterion is met for all ESFAS. The ESFAS is fully testable. Those components which cannot be tested during power operations are tested when the plant is shutdown.

7.3.2.3.2 Equipment Design Criteria

Many of the design criteria for protection systems are discussed in Section 7.1.2. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," establishes minimum requirements for safety-related functional performance and reliability of the ESFAS. This section describes how the requirements of Section 4 of IEEE Std. 279-1971 are satisfied. The following heading numbers correspond to the Section numbers of IEEE Std. 279-1971.

A. General Functional Requirements (Section 4.1):

The ESFAS is designed to actuate the appropriate ESF Systems, when required, to mitigate the consequences of the specified Design Basis Events. Instrument performance characteristics, response times, and accuracies are selected for compatibility with, and adequacy for, the particular function. Actuation setpoints are established by analysis of the RCS parameters, steam generator parameters and containment pressure. Factors such as instrument inaccuracies, bistable trip delay times, valve travel times and pump starting times, are considered in establishing the margin between the actuation setpoints and the safety limits. In addition, the possible loss of AC power and the time required to start standby power and to sequence loads must also be considered. The final determination of all of these times is the site operator's responsibility. The time response of the sensors or protection systems are evaluated for abnormal conditions. Since all uncertainty factors are

75

7.4.2.4.3 Plant Load Rejection, Turbine Trip, and Loss of Offsite Power

In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the onsite emergency power system. The standby diesel generators will provide power for operation of pumps and valves; the batteries and standby generators via the battery chargers will provide power for operation of instrumentation and control systems required to actuate and control essential components.

7.4.2.5 Emergency Shutdown from Outside the Control Room

Equipment and arrangements discussed in Section 7.4.1 are in response to GDC 19 which requires certain functional capabilities outside of the control room as discussed below.

7.4.2.5.1 Design Capability for Prompt Hot Standby and to Maintain Hot Standby

Should the control room become uninhabitable, the reactor may be manually tripped from the control room, as it is being evacuated, or from the Reactor Trip Switchgear System (RTSS).

Hot standby conditions can be maintained from outside the control room as described in Section 7.4.1.1.10 by control of pressurizer pressure and level, feedwater flow, and atmospheric steam dump. Hot standby, as used here, means the reactor is subcritical at normal operating pressure and temperature.

7.4.2.5.2 Cold Shutdown

Cold shutdown of the reactor without access to the control room is possible by use of instrumentation and controls described in Section 7.4.1.1.10 and suitable procedures prepared by the site operator.

system. The transmission of signals for other non-safety related use from safety-related PAMI channels is also provided through isolation devices.

Category 3: No specific provisions are required. Therefore, these parameters are interfaced without isolation devices.

7.5.2.5.10 Servicing, Testing and Calibration

Categories 1, 2, and 3: The design permits the administrative control of access to all sensor adjustments, module calibration adjustments, and test points. Periodic checking, testing, calibration, and verification will be done in accordance with intent of Regulatory Guide 1.118 pertaining to testing of sensor channels.

Means are provided for removing DIAS processing units and displays from service. Administrative control of these actions will be developed by the site operator. Changes to constants, alarm setpoints and calibration must be made off-line and will be similarly controlled. Redundant processing units will assure continuous display or availability of Regulatory Guide 1.97 variables during adjustments. Administrative controls will also be required for the DPS. The display systems are designed to allow control of access to constants, alarm setpoints, calibration and test points. The DPS continuously checks the validated DIAS data against its own and alarms any deviations. Isolation devices are located outside containment so that they may be accessed by personnel for maintenance during accident conditions.

7-7

7.5.2.5.11 Human Factors

Categories 1, 2 and 3: The DIAS allows repair, adjustment or replacement of the display and processing system. The DPS is also designed to facilitate repair, replacement and adjustment of processing modules and CRTs.

Functional task analysis is used to determine the type and location of all displays in the Nuplex 80+ control room, including the Regulatory Guide

Voltage tap setting calculations for all transformers in the plant electrical distribution system will be performed in order to optimize the voltage levels in the plant.

Relay and timer settings for the first and second level of undervoltage protection provided for the Class 1E and permanent nonsafety switchgear are calculated to be in compliance with Branch Technical Position PSB-1.

G. Branch Technical Position PSB-2 (SRP 8.1) "Criteria for Alarms and Indications Associated with Diesel-Generator Unit Bypassed and Inoperable Status"

The provisions of Branch Technical Position PSB-2 (SRP 8.1), in conjunction with Regulatory Guide 1.47, regarding availability of the Emergency Diesel Generators, are described in Section 8.3.1.1.4.5.

8.1.4.5 COL Action Items

A. The COL applicant will specify the immediate and alternate sources of offsite power for the 4.16 kv ESF buses. This will be decided based on site reliability analysis.

B. The COL applicant will specify all items with periodic testing commitments not covered by the technical specifications.

C. The COL applicant will periodically test relay sensors such as current transformers and potential transformers before installing them and periodically thereafter.

D. The COL applicant will provide a process for periodically verifying and calibrating relay trip setpoints.

E. The COL applicant shall establish a reliability based maintenance program for plant electrical power systems.

F. The COL applicant shall develop a program for maintaining markings and labeling of safety-related components and cabling.

G. The COL applicant will provide provisions and procedures to test the status and operability of protection circuits which are bypassed during accident conditions.

8.3.1.1.4.7 Lube Oil System

Reference Section 9.5.7 for a description of the Diesel Generator Engine Lube Oil system.

8.3.1.1.4.8 Fuel Oil System

Reference Section 9.5.4 for a description of the Diesel Generator Engine Fuel Oil System.

8.3.1.1.4.9 Cooling System

Reference Section 9.5.5 for a description of the Diesel Generator Engine Cooling System.

8.3.1.1.4.10 Emergency Diesel Generator Proven Technology

The emergency diesel generators are of proven technology that has been applied successfully for several years in existing LWRs.

8.3.1.1.4.11 Preoperational and Periodic Testing

In addition to the factory tests, the following preoperational onsite acceptance tests and periodic tests are conducted on each diesel generator and its associated auxiliary systems.

A. Preoperational Testing

Preoperational acceptance tests meet the intent of the following:

1. IEEE Standard 387-1984, Sections 6.4 and 6.5.
2. Regulatory Guide 1.9, Section C.3 and C.4.
3. Regulatory Guide 1.41, Section C.
4. Regulatory Guide 1.68, Appendix A, Section 1.g.3.
5. Regulatory Guide 1.108, Sections C.2.a and C.2.b.
6. Regulatory Guide 1.137, Section C.1.c.
7. ANSI N195, 1976, Section 6.1.

These preoperational tests conform with the provisions of Regulatory Guide 1.108, C.2.a and C.2.b regarding tests to be performed on emergency diesel generators.

B. Periodic Testing

Periodic testing of the emergency diesel generator meets the intent of Regulatory Guide 1.108 and NRC Generic Letter 84-15. Testing is performed by manually synchronizing the diesel generators with the offsite power system. This synchronization is supervised by a synchronism check relay.

~~9-11~~ 9-10

The emergency diesel generator (EDG) is removed from service in accordance with approved procedures. Any maintenance work on the diesels is performed and inspected by qualified personnel in accordance with approved procedures. The COL Applicant will provide diesel operator training to operations and maintenance personnel.

A root-cause analysis maintenance program shall be implemented to track and to resolve repetitive failures of EDG components, including replacement of components with acceptable substitutes, if warranted. Upon completion of maintenance work, appropriate tests are completed to assure operability of the diesel generator. Upon completion of testing, appropriate operating procedures restore the diesels to standby readiness. [After periods of operating the EDG in unloaded condition, the EDG will be run loaded per manufacturer's recommendation to clean any deposits from cylinders, etc.] 9-11 9-12 (COL 9.5.5-2)

8.3.1.1.4.12 125V DC Emergency Diesel Control Power

125V DC control power for each emergency diesel generator is provided by the Class 1E 125V DC Power System batteries as described in Section 8.3.2.1.2.

8.3.1.1.4.13 Operational Requirements

The COL applicant shall provide a complete training program for all mechanical and electrical maintenance, quality control, and operating personnel, including supervisors who are responsible for maintenance and availability of the diesel generators. The depth and quality of training shall be at least equivalent to that provided by the diesel generator manufacturer.

The COL applicant shall establish a preventative maintenance program which encompasses investigative testing of components which have a history of repeated repair and replacement of those components with other products of proven reliability.

8.3.1.1.5 Non-Class 1E Alternate AC Source Standby Power Supply

The Alternate AC Source (AAC) is a non-Class 1E combustion turbine power source provided to cope with Loss of Offsite Power (LOOP) and Station Blackout (SBO) scenarios. This standby unit is independent and diverse from the Class 1E standby emergency diesel generators.

The combustion turbine-generator and supporting auxiliaries are non-safety related, and are provided as a packaged unit, mounted in a self contained metal enclosure. The AAC facility is located within the plant protected area, outside of the turbine missile impact zone, and is surrounded by a perimeter security fence and intrusion alarm system. The security fence is locked, and monitored in the site security office. The combustion turbine fuel tank is surrounded by a dike, sized to retain the entire contents of the tank. Additional details of the combustion turbine-generator and fuel storage structures are provided in Section 1.2.16.2. The location and arrangement of the AAC components/structures is shown on Figure 1.2-1. The AAC is sized with sufficient capacity to accommodate either of the following load configurations:

compatible with fuel assembly materials and the spent fuel borated water environment.

The spent fuel is stored in two regions of the pool. Region I provides core off-load capability for approximately 363 spent fuel assemblies (equivalent to one and one-half cores). This is achieved with 50% density storage in a checkerboard array using "L" inserts in the usable cells (Figure 9.1-2). The "L" insert is a non-poisoned stainless steel insert which provides the needed flux trap water gap. Region II provides 75% density storage for approximately 544 spent fuel assemblies. The cells that are not used are blocked to prevent improper storage. A total of approximately 907 usable spaces for spent fuel storage is thus provided.

If new fuel assemblies are placed in the spent fuel pool in preparation for a refueling outage, they are located in Region I. Space in Region I is also provided for the storage of failed fuel assemblies.

The two regions permit increased spent fuel storage by the use of a denser fuel storage array for full burnup fuel assemblies. This allows increased storage capacity within the pool without the use of neutron poison inserts.

Both Region I and II storage areas are designed to accommodate fuel assemblies with initial enrichment up to 5 weight percent U-235. Region I has no restriction on burnup history of stored fuel assemblies. Region II is restricted for storage of fuel having a minimum cumulative burnup which is dependent on the initial enrichment for each fuel assembly. This restriction on fuel storage in Region II will be imposed by administrative controls developed and implemented by the COL Applicant. 9-4

The division of the spent fuel storage area into two regions provides an increased storage capacity (75% density vs. 50% density) without the use of poison inserts while at the same time providing a large storage capability for spent fuel assemblies with no restrictions on their burnup history.

Total Spent Fuel storage capacity represents approximately 376% of a full core. Region II represents approximately 226% of a full core.

New fuel assemblies placed in the spent fuel pool in preparation for a refueling outage are located in Region I. Region I also includes space for storage of failed fuel assemblies.

The structural design of the spent fuel rack and pool includes provisions for accepting loads associated with 100% storage with neutron poison inserts in order to meet future expansion potential.

The COL applicant will prepare and implement administrative controls to restrict operation of the fuel transfer tube valve during fuel handling operations. 9-4

9.1.4.2.1.3 Spent Fuel Handling Machine

The spent fuel handling machine will be a refueling machine adapted for use in the spent fuel pool area. It will contain the same interlock features as described in Section 9.1.4.2.1.1, except as noted below for the Spent Fuel Handling Machine Translation Zone Interlock:

A. Zone interlocks protect against running the load into walls or the gate of the storage area.

B. If these interlocks fail, the spent fuel handling machine mast will protect the fuel assembly from damage in the event of wall or gate contact.

9.1.4.2.1.4 New Fuel Elevator

The following identifies and describes the functions of the interlocks that are part of the new fuel elevator. The new fuel elevator controls are located on the spent fuel handling machine control console.

A. New Fuel Elevator Hoist Cable-Slack Interlock

Stops the elevator motor should the cable become slack.

If this interlock fails, the operator can stop the elevator motion from the spent fuel handling machine console.

B. New Fuel Elevator Hoist Lock-Out Interlock

Prevents raising of the elevator with a fuel assembly in the elevator box. This interlock is a backup for the administrative control, which prohibits the placement of a spent fuel assembly in the new fuel elevator.

C. New Fuel Elevator Hoist Limit Interlock

Interrupts hoisting when "up" or "down" limits are reached.

9.1.4.2.1.5 CEA Elevator

The following identifies and describes the functions of the interlocks that are part of the CEA elevator.

During these tests, the various operating parameters such as motor speed, voltage, and current, hydraulic system pressures and load measuring accuracy and setpoints are recorded. At the completion of these tests the equipment is checked for cleanliness, and the locking of fasteners by lockwire or other means is verified.

Equipment installation and testing at the plant site are controlled by approved installation procedures and preoperational test procedures designed to verify conformance with procurement specifications. Each component is inspected and cleaned prior to installation into the system. Recommended maintenance, including any necessary adjustments and calibration, is performed prior to equipment operation. Preoperational tests also include checks of all control circuits including interlocks and alarm functions.

The following testing and inspections will be used for both the reactor building polar crane and nuclear annex overhead hoists related to fuel handling.

A. Hoists and cable will be load tested at 125% of the rated load.

B. The equipment will be assembled and checked for proper functional and running operation at the shop and prior to using the equipment.

C. Inspection and maintenance will be performed in accordance with plant maintenance procedures.

The COL Applicant will provide plant operating procedures that specify detailed preoperational checkouts that must be performed prior to equipment use to insure that equipment is in proper working order. These checkouts include, but are not limited to, the following: interlocks, brakes, hoisting cable, control circuitry, lubrication, and load testing. 9-1

9.1.4.5 Instrumentation Requirements

The refueling system instrumentation and controls are described in Section 9.1.4.2. No credit is taken for instrumentation or interlocks on components of the fuel handling equipment to either prevent or mitigate the consequences of the postulated accident. Thus, safety-related interlocks are not provided.

9.1.4.6 Operating Procedure Guidelines

Site-specific guidelines will be established for component handling procedures and plant operating procedures. Component handling procedure guidelines will require the COL Applicant to establish the safe load path for lifting heavy loads and to perform special handling component inspections prior to lift.

Plant operating procedure guidelines will require appropriate operation training and crane inspections. [The guidelines will also require the COL applicant to prepare operating procedures for preoperational load testing and checkouts of interlocks, brakes, hoisting cables, control circuitry and lubrication of fuel handling equipment.] 9-1

H. The SSWS is designated as a vital system. The SSWS pump structure and all SSWS piping and cabling shall be located within the protected area that is common to the main plant.

The COL applicant will take appropriate measures to prevent organic fouling and inorganic buildup, and will provide site-specific aspects regarding the resolution of GSI 51 (See Sections 9.2.1.4 and 9.2.5.4). 9-2

9.2.1.2 System Description

The SSWS consists of two separate, redundant, open loop, safety-related divisions. Each division cools one of two divisions of the CCWS, which in turn cools 100% of the safety-related loads. The SSWS operates at a lower pressure than the CCWS to prevent contamination of the CCWS with raw water.

Each division of the SSWS consists of two pumps, two strainers, two sump pumps, and associated piping, valves, controls and instrumentation. The station service water pumps circulate cooling water to the component cooling water heat exchanger and back to the ultimate heat sink. Provisions are made to ensure a continuous flow of cooling water under normal and accident conditions. Valves SW-120, SW-121, SW-122, SW-123, SW-220, SW-221, SW-222, and SW-223 provide station service water flow isolation/initiation for the component cooling water heat exchangers. These valves are provided with electric motor operators and can be remotely operated from the control room.

9.2.1.2.1 Components Description

Table 9.2.1-2 lists component design parameters. Each component is also described in the following sections. Table 9.2.1-3 lists the active valves for the SSWS. These valves are described in Section 9.2.1.2.1.8.

9.2.1.2.1.1 SSWS Pumps

Four identical station service water pumps are provided, two pumps per division. Manual start and stop actuation of the station service water pumps is provided from the control room to override automatic actuation. Each pump provides 100% of the required flow for post-LOCA conditions. Typically, during normal operation only one pump per division is operating. The second pump in the respective division will automatically start on a low pump discharge pressure signal. This is indicative of a failure of the operating pump.

The pumps are of the vertical centrifugal type and are installed in the station service water pump structure. The station service water pump motor coolers receive cooling water from their respective station service water pump discharge at all times while the pump is in operation. The pump motors and all other electrical equipment in the pump structure are located above the maximum flood elevation.

The pump motors are connected to their associated 4160 volt Class 1E Auxiliary Power System. In the event offsite power is lost, the pumps are stopped and restarted in accordance with the diesel generator's load sequencing.

The sizing of the station service water pumps is based on the following operating mode requirements:

Normal power operation	- 1	pump per division operating
Normal shutdown (24 hours)	- 4	pumps operating
Safety-grade shutdown (24 hours)	- 2	pumps required, in a single division
Post-LOCA	- 1	pump required, (corresponding with the operating CCW heat exchanger)

During normal power operation as cooling requirements increase, the additional pump in a division may be needed.

The station service water pumps are provided with at least 7% margin in head at the pump design point. The head versus flow curve is continuously rising from the design point to shut-off.

The minimum available NPSH is the smaller of (1) 25 percent greater than, or (2) 10 feet greater than the required NPSH specified by the pump vendor.

The available NPSH is calculated at the highest expected operating temperature and flow, at the normal water elevations, and assuming the travelling screens are 50% clogged. The available NPSH exceeds the required NPSH for worst case UHS water elevations for all operation, flow, and temperature conditions. (Note: For worst case UHS water elevation, the margins previously specified need not apply.)

9.2.1.2.1.2 SSWS Pump Structure

The pump structure is a Seismic Category I design.

The UHS inlet to the station service water pumps is equipped with a safety grade screen system (see Section 9.2.1.2.1.4).

The COL applicant will provide a detailed description of the SSWS pump structure. 9-3

9.2.1.2.1.3 Piping, Valves, and Fittings

Piping to and from the CCW heat exchangers is corrosion resistant. Materials are to be selected on a site-specific basis to be compatible with the ultimate heat sink makeup water

J. To prevent damage to components and piping, the system is designed to minimize the potential for water hammer by providing adequate filling and high point venting.

9.2.1.4 Inspection and Testing Requirements

The COL applicant will provide site-specific aspects regarding the resolution of Generic Safety Issue 51, including maintenance and inspection programs. 9-2

During fabrication of the SSW components, tests and inspections are performed and documented in accordance with code requirements to assure high quality construction. As necessary, performance tests of components are performed at the vendor's facility. The SSWS is designed and installed to permit inservice inspection and tests in accordance with ASME Code Section XI. Buried SSWS piping is inspected by means of a leakage test that determines the rate of pressure loss or a test of differential flow between the ends of buried piping.

9.2.1.4.1 SSWS Performance Tests

Prior to initial plant startup, a comprehensive performance test as detailed in Section 14.2 will be performed to verify that the design performance of the system and individual components is attained.

9.2.1.4.2 Reliability Tests and Inspections

A. System Level Tests

After the plant is brought into operation, periodic tests and inspections of the SSW components and subsystems are performed to ensure proper operation. Scheduled tests and inspections are necessary to verify system operability. A complete schedule of tests and inspections of the SSWS is detailed in Chapter 16, Technical Specifications.

B. Component Testing

In addition to the system level tests, tests to verify proper operation of the SSW components are also conducted. These tests supplement the system level tests by verifying acceptable performance of each active component in the SSWS.

Pumps and valves are tested in accordance with ASME Section XI. Various flow rate testing up to and including the design point of the SSW pumps can be performed using the system loop.

The station service water intake will be visually inspected, once per refueling cycle, for macroscopic biological fouling organisms, sediment, and corrosion. Inspections should be performed either by scuba divers or by dewatering the intake structure or by comparable methods. Any fouling accumulations should be removed.

9.2.4 POTABLE AND SANITARY WATER SYSTEMS

Those portions of the PSWS that are within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are within the scope of the Certified Design. Those portions of the PSWS that are not within the Reactor Building, Nuclear Annex, Turbine Building, Radwaste Building, and Service Building are not within the scope of the Certified Design. Out of scope portions of the system are licensee supplied and are site specific.

Water from the Filtered Water System is processed by the PSWS for general plant use. Potential sources for the Filtered Water System include lakes, rivers, wells, and municipal water supplies. A backflow preventer is provided between the Potable Water System supply and the Filtered Water System Supply to other plant systems.

Section 9.2.4.1 provides the interface requirements which must be met by the licensee supplied design. Subsequent sections of Section 9.2.4 contain descriptive information concerning a conceptual design for the Potable and Sanitary Water Systems.

9.2.4.1 Interface Requirements

The PSWS shall be designed to meet the requirements of General Design Criterion 60 of 10 CFR 50 Appendix A, as related to provisions to control the release of liquid effluents containing radioactive material from contaminating the PSWS. The following specific requirements shall be met:

A. There shall be no interconnections between the Potable and Sanitary Water Systems and systems having the potential for containing radioactive material.

B. The Potable Water System shall be protected by an air gap, where necessary.

The licensee shall ensure that the sewage treatment facility design complies with applicable state and local regulations. Adequate treatment facility capacity shall be provided to accommodate the maximum number of personnel assigned to the site, with provisions for expansion as necessary.

9.2.4.2 System Description

The Potable and Sanitary Water Systems consist of a Potable Water System and a Sanitary Drainage System. The Potable and Sanitary Water Systems are shown in Figure 9.2.4-1. The systems include all components and piping from the Filtered Water System to all points of discharge to sewage facilities.

The COL applicant will provide information on the potable and sanitary water systems design. 9.4

2. Non-current site related events, including transportation accidents, oil spills and fires.

3. Credible single failures of man-made structures.

4. Sabotage

E. In order to ensure the normal cooldown (two division cooldown) performance requirements given in Section 5.4.7.1.2.F.1 the Ultimate Heat Sink temperature at the SSWS inlet must remain at or below 95°F throughout the cooldown. One percent exceedance meteorologic conditions can be utilized in showing acceptability, since this is a performance requirement and not a safety requirement.

F. For sites with severe winters, where ice formation of the Ultimate Heat Sink could occur, an analysis shall be provided showing the function of the Ultimate Heat Sink is not impaired during winter months. Where required, the intake structures shall be provided with a means of deicing, such as warm water recirculation, to prevent flow blockage of the SSW pump inlets.

G. The site water chemistry for the Ultimate Heat Sink shall be analyzed to determine if a water treatment system is required to minimize corrosion and fouling of the SSWS.

H. Water boundaries that form part of the protected area boundary shall be avoided, if at all possible. 9-13

9.2.5.2 System Description

The Ultimate Heat Sink described here consists of a single passive independent cooling water pond connected to the SSWS through intake and discharge paths. However, it is recognized that site-specific conditions may require the use of two ponds to meet Regulatory Guide 1.27. The design brackets alternative Ultimate Heat Sinks which may be specified for a particular site if environmental restrictions limit the use of a cooling pond or if an alternative water supply is more reliable. Acceptable alternate ultimate heat sinks are an ocean, a large lake, a large river, a lake and a cooling pond, a river and a cooling pond, or a cooling tower and cooling pond.

The cooling water pond is provided with makeup water pumps to maintain level. Water chemistry is maintained by a site-specific water treatment system (i.e., chemical injection). Salinity buildup in a pond is limited by blowdown.

The Ultimate Heat Sink will operate for the required nominal 30 days following a postulated LOCA without requiring any makeup water to the source, and without requiring any blowdown from the pond for salinity control.

9.2.5.3 Safety Evaluation

The Ultimate Heat Sink meets the intent of Regulatory Guide 1.27. The cooling water pond is Seismic Category I and of sufficient volume to provide the required nominal 30-day cooling capacity without makeup and under worst case meteorological conditions.

Ultimate Heat Sink temperature will not exceed the maximum allowable temperature required for cooling any safety-grade component through the component cooling water heat exchangers during a design basis accident concurrent with a loss of offsite power.

The function of the Ultimate Heat Sink is not lost during or after any of the following events:

A. Natural phenomena, including SSE, tornado, flood, and drought.

B. Non-concurrent site-related events, including transportation accidents, oil spills, and fires.

C. Credible single failures of man-made structures.

D. Sabotage.

9.2.5.4 Inspection and Testing Requirements

The COL applicant will provide site-specific aspects regarding the resolution of Generic Safety Issue 51, including maintenance and inspection programs. 9.2

Samples of water and substrate will be collected annually to determine if biological fouling organisms have populated the water source. Upon the detection of biological fouling organisms, appropriate corrective action, such as the modification of the chemical treatment program, should be taken. However, consideration must be given to environmental regulations.

9.2.5.5 Instrumentation Requirements

The level of each cooling water pond is monitored and controlled. Alarms are provided in the main control room which actuate if the level of the pond approaches minimum allowable value, or the temperature approaches the maximum allowable value.

9.2.6 CONDENSATE STORAGE SYSTEM

9.2.6.1 Design Bases

9.2.6.1.1 Overall Design Bases

A. The Condensate Storage System provides demineralized water for initial fill of the condensate and feedwater systems. As

chemistry conditions, approaching low steady state values within approximately 200 days. A high pH minimizes corrosion product release and assists in the rapid development of the passive oxide film. Most of the film is established during pre-core operations within seven days at hot, high pH conditions.

To aid in maintaining the pH during system passivation, lithium in the form of lithium hydroxide, is added to the coolant and maintained within a 1-2 ppm lithium-7 range.

At power, oxygen concentration is limited by maintaining excess dissolved hydrogen gas in the coolant. The excess hydrogen forces the water decomposition/synthesis reaction in the reactor core toward water synthesis, rather than hydrogen and oxygen formation. Oxygen added via makeup water is removed in this way.

In order to minimize the effect of crud deposition on the reactor core heat transfer surfaces, lithium-7 hydroxide additions are made. Lithium-7 hydroxide produces pH conditions within the reactor coolant at operating temperatures that reduce the corrosion product solubility and, hence, the dissolved crud inventory in the circulating reactor coolant. The elevated pH promotes conditions within the coolant for selective deposition of corrosion products on cooler surfaces (steam generators) rather than hotter surfaces (core). An additional advantage is the formation of a more stable and tenacious passive oxide layer on out-of-core system surfaces. The lithium concentration is maintained within a 0.2-2.2 ppm lithium-7 range during normal operation.

9.3.4.1.3.3 Reactivity Control

Boron concentration is normally controlled by feed-and-bleed. To change concentration, the makeup system supplies either reactor makeup water or boric acid to the VCT, and the letdown stream is diverted to the holdup tank via the pre-holdup ion exchanger and the gas stripper. Toward the end of a fuel cycle, with low boric acid concentration in the coolant, feed-and-bleed to further reduce boron concentration becomes inefficient, and the deborating ion exchanger is used. The deborating ion exchanger contains an anion resin initially in the hydroxyl form, which is converted to a borate form as boron is removed from the reactor coolant.

9.3.4.1.4 Interface Requirements

The structures housing the Boric Acid Storage Tank, the Reactor Makeup Water Tank, and the Holdup Tank are out of scope items which shall be provided by the applicant. The licensee shall 9-5

verify that the structural interface requirements listed in this section are met to ensure adequacy with the System 80+™ Standard Design.

A. The structures housing the tanks shall be designed to meet the requirements of NRC Regulatory Guide 1.143, Design Guidance for Radioactive Waste Management Systems, Structures, and Components Installed in Light-Water-Cooled Nuclear Power Plants. Specifically, the tanks shall be located within a seismically-designed dike or retention pond of sufficient height/size capable of preventing runoff in the event of tank overflow/rupture.

B. All three tanks may be located within a common structure designed to contain the maximum combined liquid inventory in the tanks. 95

C. The licensee shall ensure that the structure/dike design complies with applicable state and local regulations.

9.3.4.2 System Description

9.3.4.2.1 System

The normal reactor coolant flow path through the CVCS is indicated by the heavy lines on the flow diagrams (Figure 9.3.4-1, Sheets 1 through 4). Design parameters for the major components are shown in Table 9.3.4-4. Normal operating parameters for the CVCS are listed in Table 9.3.4-5. Process flow data is shown in Table 9.3.4-6.

Letdown flow from the RCS passes through the tube side of the regenerative heat exchanger where an initial temperature reduction takes place via heat transfer to cooler charging fluid on the shell side of the heat exchanger. The regenerative heat exchanger is designed to cool letdown flow to less than 450°F for all normal operations and to heat the charging flow by a minimum of 100°F. A final temperature reduction to the purification subsystem operating temperature is made by the letdown heat exchanger. The letdown heat exchanger is sized to cool inlet water from the maximum regenerative heat exchanger outlet temperature to 120°F (or lower) for most operating conditions. Both the letdown and the regenerative heat exchangers are designed for full RCS pressure and both are located inside containment.

Letdown fluid pressure is reduced from RCS pressure to the operating pressure of the purification subsystem in two stages. The first pressure reduction occurs at the letdown orifices and the second occurs at the letdown control valves located downstream of the orifices. The letdown orifices are located

L. Sufficient fire area compartmentation to preclude the presence of Category 1 risks. A Category 1 risk is defined in the Fire Hazards Assessment as an area where equipment or component damage and electrical faulting are unacceptable. An example would be a location where redundant equipment and components required for safe shutdown are susceptible to damage by a single fire.

M. A fire protection program that complies with NUREG 0800 Standard Review Plan and CMEB 9.5-1, Rev. 2, July 1981: "Guidelines for Fire Protection of Nuclear Power Plants" and SECY Letter 90-16, "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationships to Current Regulatory Requirements." Specific deviations and technical justification are included in the fire hazards analysis.

The Design Basis Goals and Objectives as stated above will mitigate the potential of fire, provide for prompt detection should fire occur, provide automatic suppression and/or manual fire suppression capabilities as determined by the Fire Hazards Analysis, provide fire resistant barriers to mitigate fire propagation, protect redundant safety related trains of equipment from damage due to a common fire exposure, and preclude the potential release of radioactivity to the environment.

9.5.1.2 General Design Guidelines

A. Outside containment redundant divisions of safety related electrical equipment are separated from each other by three-hour fire rated fire barriers. Exceptions are control room and remote shutdown panel room which are physically separated, electrically isolated, and provide redundant shutdown capability. Transfer switches which transfer control from the Control Room to the Remote Shutdown Panel, are located in the control room. Section 7.4.1.1.10 contains a discussion of the transfer of control from the Control Room to the Remote Shutdown Panel. The COL Applicant shall provide procedures and training for transferring control from the Control Room to the Remote Shutdown Panel from either the transfer switches located in the Control Room or from the Maintenance and Test Panels in the ESF-CCS and Process-CCS channelized equipment rooms. 9-13

B. Inside containment: The Fire Protection Safe Shutdown Analysis (which will be maintained as part of the System 80+ design basis) will assure that fire at any specific location inside containment will not affect redundant safe shutdown components. It will also assure that redundant safe shutdown components such as instruments and valves will be separated to the extent practicable as stipulated in

Storage and disposal of anticontamination clothing at radiation control zone (RCZ) step-off pads is recognized as a potentially significant transient combustible fire hazard. Therefore, anticontamination clothing is stored in enclosed storage cabinets. Cabinet doors are normally closed as required by station directives. Used anticontaminated clothing is placed in metal drums which have fusible link actuated or otherwise Listed or Approved covers. Fire protection and detection features are provided for step-off pad areas based on conclusions of the Fire Hazards Analysis.

9.5.1.11 Fire Protection Program

A Fire Protection Program which includes administrative controls shall be provided by the COL applicant. Items of interest under the administrative controls review will include:

A. control of combustible materials such as combustible/flammable liquids and gasses, fire-retardant-treated wood, plastic materials, and dry ion-exchange resins.

B. transient combustible materials and general housekeeping, including health physics materials.

C. open-flame and hot-work permits and cutting and welding operations.

D. quality assurance with respect to fire protection system(s) components, installation, maintenance, and operation.

E. qualification of fire-protection engineering personnel, fire-brigade members, and fire-protection system(s) maintenance and testing personnel.

F. instruction, training, and drills provided to fire-brigade members.

9.5.1.11.1 Fire Prevention

A. Control of Hot Work

Cutting, welding, and grinding operations are governed by a permit system as required by station administrative controls. Each task is reviewed and an adequate number of trained and qualified fire watch patrols established to assure that hot slag or sparks do not ignite nearby in situ combustible material and that transient combustible materials are relocated outside the vicinity. Fire watch is maintained for at least 30 minutes after completion of hot work to assure that residual hot material does not ignite nearby combustible material.

N. The reliabilities of the fire detection and suppression systems are assumed to be at least 80% and 96%, respectively.

O. Although fire brigade action to suppress fires was not modeled in the scoping fire risk evaluation, the capabilities of the plant fire brigade are important to maintaining a low fire risk. The COL applicant should maintian a well trained and prepared fire brigade.

6
9-7

A quantitative assessment of the risk due to internal fires can not be made at this time because detailed design information for cable routing and the fire detection and fire suppression system is not presently available. However, a scoping evaluation is performed to assess the risk due to internal fires in areas of the Nuclear Annex other than the containment or the control room. Two types of fires were considered in the scoping evaluation: (1) a fire in an area which could disable safety-related equipment in that area and which has the potential for initiating a transient, and (2) a fire in an area which by itself could disable safety-related equipment but would require the penetration of a fire barrier in order to initiate a transient. The first type of fire is designated as type "a" and the second type as type "b". The fire ignition sources and frequencies by applicable areas are presented in Table 19.15.3-2.

Although a detailed quantitative analysis of internal fires was not performed at this stage of the System 80+ design, a scoping estimate of the risk due to fire was calculated by using a conservative scoping value (4.6E-02 per year) for fire event frequency and by assuming that the effects on plant systems would be the same as a loss of one division of component cooling water/station service water. Using this approach, the estimated scoping value core damage frequency due to internal fires is 6.1E-08 per year and the sequence of importance involves an internal fire followed by failure of long-term decay heat removal and failure of SDS.

Based on the robust seal design for the RCPs used in the System 80+ design and on the results of tests and operating experience, ABB-CE asserts that the RCP seals will not fail on loss of seal injection and seal cooling. However, in the interests of completeness, an assessment of a postulated fire induced RCP seal LOCA was included as part of the quantitative fire scoping evaluation. The scoping value for core damage frequency associated with the postulated fire induced seal LOCA was calculated to be 5.2E-10 per year. The potential risk due to a postulated fire inside containment was also assessed. The estimated scoping value of core damage frequency due to fire inside containment is 1.3E-09 per year. Thus, the total estimated scoping value of core damage frequency for internal fires is 6.3E-08 per year.

9.5.1.12 Fire Hazards Analysis

A Fire Hazards Analysis is conducted for each room area or zone of the plant. Containing safety related equipment or equipment important to safety. It considers the function of major equipment in the area, location and number of redundant equipment or functions, known and anticipated quantity and configuration of combustible material, ventilation and smoke control, presences of predetermined fire protection features, and consequences of fire with and without fire protection features functioning properly. Where the Fire Hazards Analysis determines that Design Objectives are met in accordance with Section 9.5.1.1, fire protection is considered adequate. The Fire Hazards Analysis is maintained as part of the Plant Design Basis.

7
9.8

The COL Applicant must complete the Fire Hazards Analysis, using the Fire Hazards Assessment as the base document. The Fire Hazards Analysis must demonstrate that the plant will maintain the ability to perform safe shutdown functions and minimize the radioactive releases to the environment in the event of a fire. The Fire Hazards Analysis must be performed by a qualified fire protection engineer and reactor systems engineer to (1) consider potential fire hazards; (2) determine the consequences of fire in any location of the plant on the ability to safely shutdown the reactor or on the ability to minimize and control the release of radioactivity to the environment; and (3) specify measures for fire prevention, fire detection, fire suppression, and fire containment and alternative shutdown capability as required for each fire area containing structures, systems, and components important to safety. The Fire Hazards Analysis should verify that the NRC fire protection regulations have been met. Deviations from NUREG 0800, "Standard Review Plan", Section 9.5.1, "Fire Protection Program", and SECY 90-016, "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements", must be documented in the analysis.

9.5.1.13 Fire Protection Quality Assurance Program

The Fire Protection Quality Assurance Program implements a "graded" approach focusing attention to features that assure that design, procurement, installation, testing, operation, maintenance, and repair are conducted as appropriate. The program assures that systems, equipment, components, and procedures produce the fire protection function as intended. The program complies with the intent of NUREG 0800, Section 9.5.1, "Standard Review Plan."

9.5.2 COMMUNICATIONS SYSTEMS

9.5.2.1 Design Bases

The communications systems are designed to provide effective communications between all areas of the plant and plant site including all vital areas of the plant. In addition, the communications systems are designed to provide an effective means to communicate to plant personnel and offsite utility and regulatory officials during normal conditions and abnormal/accident conditions such as fire, accident, and plant testing.

The Portable, Wireless Communication System is the primary dedicated means of communication for the plant. In addition to the Portable Wireless Communication System, the Private Automatic Business Exchange (PABX) telephone system and the Public Address (PA) system are designed to provide diverse means of communications to all critical areas of the plant. Additionally, sound-powered telephone systems are provided between selected critical areas of the plant for auxiliary shutdown and other required functional purposes. Finally, multiple offsite communications lines, both direct and through the PABX are provided for effective communications during normal and abnormal/accident conditions. All of these diverse communications systems are independent of each other to assure effective communications assuming a single failure.

The COL applicant will provide specific locations for communications equipment. 9-8

9.5.2.2 System Description (was 9-9)

9.5.2.2.1 Intraplant Portable, Wireless Communication System

The Intraplant Portable, Wireless Communication System provides communications capability among control room operators, equipment operators, and maintenance technicians for routine and emergency operations. In addition to portable and wireless transmitter/receivers, this system is supported by appropriate base stations, antennae, amplifiers and/or repeaters to ensure that clear intelligible communication can be achieved from any locations at which operations and maintenance personnel may need to communicate. Appropriate antennae and the associated containment penetrations are provided to ensure adequate communication from areas inside containment or within the control room. A sufficient number of communication channels are provided to accommodate the expected message load based upon network analysis including task requirements in critical or emergency situations plus allowing margin for expansion and contingency. Specialized system portable and wireless transmitter/receivers

9.5.2-1

In addition, a security radio system is provided in accordance with 10 CFR 73.55(f) and a crisis management radio system is provided in accordance with the intent of NUREG-0654.

8 9-8

9.5.2.2.6 System Operation

9.5.2-3

In areas of high noise levels, noise-cancelling devices, sound isolation booths and/or visual alerting are utilized.

8 9-8

9.5.2.3 Inspection and Testing Requirements

All communications systems are inspected, checked, and tested for operability after installation to assure proper operation and coverage. Tests are performed to verify that adequate measures have been taken to control interference between the communications systems and electronic equipment. Normal and continued use of the systems provides the basis for inspections on the systems.

Normal system operation is not affected by the failure or unavailability of a single lighting transformer.

The circuits to the individual lighting fixtures are staggered as much as possible, with the staggered circuits fed from separate electrical divisions, to ensure some lighting is retained in a room in the event of a circuit failure.

9.5.3.2.2 Security Lighting System

The security lighting system is considered part of the permanent non-safety systems and is fed from the Alternate AC (AAC) Source (Combustion Turbine), which is located in a secure vital area for protection. Selected portions of the security lighting system essential to maintaining adequate plant protection are powered from a non-Class 1E battery power source.

The COL Applicant shall provide a security lighting system that will meet CCTV illumination requirements within camera viewing areas to permit prompt assessment of intrusion alarms. 9-9 9-10

The security lighting system is designed to provide a minimum illumination of 0.2 foot-candles when measured horizontally at ground level.

9.5.3.2.3 Emergency Lighting

Emergency lighting is located in vital areas throughout the plant as identified in Emergency Procedures and Hazards Analysis for safe-shutdown of the plant following an accident or hazard. Included in the vital areas will be the Control Room, Technical Support Center, Operations Support Center, the Remote Shutdown Panel Room, the stairway which provides access from the Control Room to the Remote Shutdown Panel room, Sample Room, Hydrogen Recombiner Rooms, Electrical System Areas, Main Steam Valve Houses, the Chemistry Labs, routes for personnel passage and egress, and other areas where operator access is required post-accident or hazard.

The emergency lighting system in the main control room is integrated with the normal lighting system. Emergency lighting in the main control room is provided such that at least two circuits of lighting fixtures are powered from different Class 1E divisions. The emergency lighting system in the main control room maintains minimum illumination levels in the main control room during emergency conditions, including station blackout.

The emergency lighting installations which serve the main control room and other areas of the plant where safe shutdown operations may be performed are designed to remain functional during and after a design basis earthquake.

storage tank, the tank is inoperable. The tank is operable after being restored to operational readiness in accordance with Technical Specification 3.8.3.

Fuel oil amenders are added as necessary to extend oil life by preventing oxidation and stratification. A sample is used to inspect the oil for water content or degradation and if degradation is determined, the oil may be pumped out for disposal. Accumulated water in the fuel oil storage tanks will be removed by the recirculation system through a sample connection provided on the recirculation pump discharge.

The day tank vent and fuel oil storage tank vents and fill connections which are exposed outdoors are constructed using heavy gauge pipe to provide protection against tornado missiles. These vent and fill lines are located above the probable maximum flood level. Each fill connection is provided with a locking dust cap and each vent line is down turned. The storage tanks can be filled and vented through the manway should the fill or vent lines become impaired.

The COL Applicant will provide the specific diesel generator fuel storage and transfer system design criteria. 9-12 9-11

9.5.4.2.2 Component Description

Fuel oil is recirculated by a recirculation pump within each storage facility to prevent deterioration.

The motor-driven fuel oil booster pump is normally isolated, both electrically and mechanically, but may be operated if required during maintenance to deliver fuel oil to the diesel.

9.5.4.3 Safety Evaluation

The Diesel Generator Engine Fuel Oil System is a ANSI Class 3 piping system with the exception of the Fuel Oil Recirculation System and the fuel oil storage tank fill line strainer which are ANSI Class 4 piping systems. The Fuel Oil Recirculation System and the fuel oil storage tank fill line strainer are separated from the essential Diesel Generator Fuel Oil System by normally

During normal operation of the diesel any accumulated sediment in the bottom of the fuel oil storage tanks is prevented from entering the supply line to the day tank since the outlet connection is raised 6 inches above the storage tank floor. During the addition of new fuel oil, degradation or failure of the diesel generator engine due to stirring of sediments is prevented by a two tank system. Two half capacity fuel oil storage tanks per redundant diesel provide the ability to operate the diesel off one tank while isolating and filling the adjacent tank. Prior to the addition of new fuel oil either during an accident or when "topping-off" the fuel oil storage tank, the diesel would be aligned to one tank while the tank to be filled would be isolated through administrative control. After filling the storage tank, a period of not less than 24 hours must be allotted to allow sediment to settle prior to realigning the tank to its respective diesel. In the event of an accident (blackout or LOCA), a sufficient reserve of fuel oil will be maintained to allow the diesel to operate off one storage tank while refilling the adjacent fuel oil storage tank, allowing for a 24 hour settling period.

To minimize the chances of a fire in the fuel oil system, piping is routed such that it is remote from other piping and equipment with potentially hot surfaces and from any source of open flame or sparks. The fuel oil day tank is protected by a fire barrier.

There are no high energy lines within the diesel generator building and all moderate energy lines are properly supported and restrained to prevent damage to safety-related systems, piping and components resulting from line failure.

All fuel oil equipment is located in heated buildings except buried piping which is installed below the frost line to maintain the fuel oil above the cloud point. The buried piping is surrounded by an annulus to collect fuel oil leakage.

9.5.4.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation; thereafter, the system will be tested in accordance with the technical specifications. Buried fuel oil system piping is inspected by means of a visual examination at each end of the buried piping (annulus enclosure) for evidence of leakage.

9-11
9-12

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Fuel Oil System test frequencies.

E. Fuel oil filter

1. High differential pressure alarm - Alerts the operator to take corrective action by manually switching over to the alternate clean filter.

2. Differential pressure indication.

3. Outlet pressure indication.

4. Low fuel oil pressure alarm.

F. Day tank retaining wall

1. High and low level drain valve and lube oil transfer pump control.

2. High-high level alarm.

9-11

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Fuel Oil System calibration frequencies.

~~9.5-12~~

9.5.5 DIESEL GENERATOR ENGINE COOLING WATER SYSTEM

9.5.5.1 Design Bases

The Diesel Generator Engine Cooling Water System is designed to maintain the temperature of the diesel generator engine within an optimum operating range during standby and during full-load operation in order to assure its fast starting and load-accepting capability and to reduce thermal stresses. The system is also designed to supply cooling water to the engine lube oil cooler, the combustion air aftercoolers, and the governor lube oil cooler.

All components and piping are located within a Seismic Category I structure (diesel generator building) and all essential components are fully protected from floods, tornado missile damage, internal missiles, pipe breaks and whip, jet impingement and interaction with non-seismic systems in the vicinity. The Diesel Generator Engine Cooling Water System is designated as a vital system and components of the system are located within the plant's protected area.

9.5.5.2 System Description

The Diesel Generator Engine Cooling Water System is shown in Figure 9.5.5-1.

The COL Applicant will provide information on the plant-specific diesel generator cooling water system. 9-12 9-11

9.5.5.2.1 General

A separate and complete closed-loop cooling water system is provided for each diesel generator engine, receiving makeup water from the Demineralized Water System and uses as it's sink the Component Cooling Water System. A surge tank, the jacket water standpipe located in the diesel generator building, provides positive suction pressure for the circulation pump and for the keep warm pump. The keep warm pump, which is electric motor-driven, operates continuously during engine standby to assure that the system is completely filled with water. When the diesel starts, the circulation pump, which is engine mounted and engine-driven, would operate to circulate cooling water through the closed loop system.

From the circulation pump, the cooling water passes through an Amot type or equivalent three-way thermostatic control valve which regulates the flow of water through the shell side of the jacket water cooler by diverting varying amounts through a bypass line. From the jacket water cooler, the cooling water flows through the tube side of either the lube oil cooler or the combustion air aftercoolers and then through the engine itself,

The periodic testing and maintenance of all diesel engine cooling water system instruments is controlled by a preventative maintenance program. This program insures that instruments are periodically calibrated and tested, assuring reliability.

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Cooling Water System calibration frequencies. ~~9.5-12~~ 9-11

Relief valves on the compressor discharge line and on the air receiver tanks protect the starting air system from overpressurization.

9.5.6.2.2 Component Description

The starting air compressors are powered from a non-Class 1E motor control center. During a loss of offsite power, the starting air compressors are powered from the alternate AC (AAC) power source. Each compressor discharges compressed air and the heat of compression is removed by a water-cooled aftercooler. The component cooling water system provides cooling water on the tube side.

To minimize the accumulation of moisture, the diesel engine starting air system is equipped with a multi-stage drying and filtering unit located in line between the aftercooler and the receiver tank to supply air with a dewpoint at least 10°F lower than the lowest expected ambient temperature. The air is first passed through a cyclone-type moisture separator and is filtered before entering one of two alternating desiccant drying towers (alternating between active and regeneration cycles). The air is then filtered a second time before entering the receiver tank.

To minimize fouling of the starting air valves or filters with contaminants, drip-traps are provided on the cyclone-type moisture separator and the air dryer pre-filter to collect any oil carryover. Drains are also provided on the aftercooler and air receiver tanks. Periodic blowdown of the drip-traps and drain valves will minimize the buildup of contaminants in the starting air system. Strainers are provided upstream of the starting air solenoid valves to prevent rust carryover to the diesels.

Two starting air receiver tanks for each diesel engine provide storage capacity which is sufficient to allow five successful engine starts without the use of the compressor.

The COL Applicant will provide specific diesel generator starting air system interface requirements. 9-12 9-11

9.5.6.3 Safety Evaluation

The Diesel Generator Engine Starting Air System is ANSI Class 4 from the starting air compressor through the desiccant drying towers, and ANSI Class 3 from the starting air receiver tank inlet check valve to the engine connections. The diesel engine and engine mounted components are constructed in accordance with IEEE Standard 387. The starting air aftercooler, which uses component cooling water on its tube side and the starting air receiver tank are designed in accordance with the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Class 3.

The starting air compressor and the starting air dryer are designed in accordance with the requirements of the applicable codes.

9.5.6.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation; thereafter, the system will be tested in accordance with the technical specifications.

Periodic blowdown of the starting air tanks is done to check for moisture. The frequency will be determined based upon operating experience.

Air dryer desiccant is inspected per the manufacturers recommendations (approximately every six months).

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Starting Air System test frequencies. 9-12 9-11

9.5.6.5 Instrumentation Application

Each starting air receiver is equipped with a set of pressure switches which control the operation of the air compressor on its associated train; starting the compressor on low pressure and stopping the compressor on high pressure. Pressure gauges are located on the tanks for local indication. An alarm is provided at the local diesel generator control panel to alert personnel when the air pressure drops below a preset value. A separate pressure switch on the engine control panel alarms if the air receiver tank pressure falls to a low setpoint.

If the starting air pressure to the starting air manifold drops to a specified value with the engine failing to start, an automatic lockout will prevent further start attempts and an alarm alerts the operator to take corrective action. The automatic lockout ensures there will be sufficient reserve for a manual restart.

All starting air system alarms are annunciated separately on the local diesel engine control panel and signal a general diesel trouble alarm in the control room. In addition, open/closed position indication is provided in the control room for the outlet manual isolation valve for each diesel generator engine starting air tank. Alarms are provided in the control room to alert the operator when the valves are not fully open.

The periodic testing and maintenance of all diesel engine starting air system instruments is controlled by a preventative maintenance program. This program insures that instruments are periodically calibrated and tested, assuring reliability.

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Starting Air System calibration frequencies. ~~9.5-12~~ 9-11

9.5.7 DIESEL GENERATOR ENGINE LUBE OIL SYSTEM

9.5.7.1 Design Bases

The Diesel Generator Engine Lube Oil System is designed to deliver clean lubricating oil to the diesel generator engine, its bearings and crankshaft, and other moving parts. By means of heaters, the lube oil system is designed to deliver warmed oil to the engine during standby to assure its fast-starting and load-accepting capability. The system also provides a means by which used oil may be drained from the engine and its components, and replaced with clean oil.

All essential components and piping are located within a Seismic Category I structure (diesel generator building) and all essential components are fully protected from floods, tornado missile damage, internal missiles, pipe breaks and whip, jet impingement and interaction with non-seismic systems in the vicinity. The Diesel Generator Engine Lube Oil System is designated as a vital system and components of the system are located within the plant's protected area.

9.5.7.2 System Description

The Diesel Generator Engine Lube Oil System is shown in Figure 9.5.7-1 (Sheets 1 through 4).

The COL Applicant will provide specific design criteria for the Diesel Generator Engine Lube Oil System. ~~9.5.2~~ 9-11

9.5.7.2.1 General

Each diesel generator unit utilizes the "dry sump" lube oil system, in which the supply of lubricating oil for the engine is stored in a separate sump tank, independent of, and located at a lower elevation than the engine crankcase. As oil accumulates in the crankcase, it drains by gravity into the sump tank. Additions of clean oil are made to the sump tank from a storage tank located outside the diesel generator building, and used oil is removed from the sump tank via a transfer pump to a used oil storage tank. Each diesel generator has a separate and complete clean lube oil and used lube oil transfer system.

The engine-driven lube oil pump takes suction from the sump tank through a built-in suction pipe with foot valve and delivers the oil in sequence from the pump discharge first to the oil pressure regulating valves which limit the maximum pressure on the pump discharge, and then in series through the lube oil cooler, the full-flow lube oil filter and finally to the full-flow lube oil strainer. From the strainer, the oil enters the engine internal circulation system.

During engine standby, the motor-driven prelube oil pump operates continuously to ensure complete filling of the lube oil system.

The used lube oil transfer pump transfers oil from the used lube oil storage tank to a truck or tanker for disposal. The pump is driven by an electric motor.

The clean and used lube oil transfer pump motors are powered from the Station Normal Auxiliary Power Supply.

9.5.7.3 Safety Evaluation

The Diesel Generator Engine Lube Oil System is an ANSI Class 3 piping system with the exception of the Clean and Used Lube Oil Transfer System which is an ANSI Class 4 piping system. The two systems are separated by ANSI Class 3 isolation valves. The diesel engine and engine mounted components are constructed in accordance with IEEE Standard 387. The off engine essential equipment and components and the nonessential (i.e., Clean and Used Lube Oil Transfer System) equipment and components are designed in accordance with the requirements of the applicable codes.

The exterior of carbon steel tanks and other underground carbon steel components is coated. In addition to being coated, the external surfaces of buried metallic piping and tanks are protected from corrosion by an impressed current cathodic protection system in accordance with NACE Standard RP-01-69 or other means as deemed appropriate based on site specific soil conditions. Periodic monitoring, as described by the maintenance procedure, will remove any accumulated moisture from the tanks.

The governor lube oil coolers on the diesel generator engines are located at an elevation below the governor lube oil level, thereby, not affecting the starting reliability of the engines.

The interior of the clean lube oil storage tank is not coated since the presence of lube oil will act as a deterrent to internal corrosion. During the surveillance intervals for sampling the lube oil in the storage tanks, any accumulated water will be removed.

9.5.7.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation; thereafter, the system will be tested in accordance with the technical specifications.

The COL Applicant will make available for NRC review, information on Diesel Generator Lube Oil System test frequencies. 9-12 9-11

9.5.7.5 Instrumentation Application

Each diesel generator engine is provided with sufficient instrumentation and alarms to monitor the operation of the lube oil system. All alarms are separately annunciated on the local diesel engine control panel which also signals a general diesel trouble alarm in the control room. The lube oil system is provided with the following instrumentation and alarms:

The lube oil sump tank is equipped with a local level indicator along with a low level annunciator to alert the operator to take corrective action.

The full flow filters are equipped with locally-mounted pressure gauges. A high differential pressure alarm alerts the operator to manually switchover to the alternate clean filter; there is no filter bypass line.

The engine mounted full flow strainers are equipped with a high differential pressure alarm which alerts the operator to manually switchover to the alternate clean strainer; there is no strainer bypass line.

The diesel generator engine is equipped with both temperature and pressure monitoring systems with separate alarm and trip switches to alert the operator of abnormal operating conditions. During standby, low prelube oil pressure is alarmed to alert operating personnel to take corrective action. If a shutdown setpoint/alarm is exceeded while the engine is operating during the test mode, a diesel trip will automatically shutdown the engine to prevent incurring any damage.

However, if such a shutdown/alarm is received during the emergency mode (i.e., LOOP or LOCA) the trip is locked out and the engine continues to run. The alarms alert the operator to prepare to switch over to the redundant diesel for power. Only a low-low engine lube oil pressure shutdown/alarm will trip the engine regardless of the diesel operating mode.

The engine inlet and outlet lube oil temperatures are also recorded by a multipoint recorder and may be monitored by a multi-channel pyrometer (in the manual mode). Both the recorder and pyrometer are located on the generator control panel in the diesel generator building.

The periodic testing and maintenance of all diesel engine lube oil system instruments is controlled by a preventative maintenance program. This program insures that instruments are periodically calibrated and tested, assuring reliability.

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Lube Oil System calibration frequencies. 9-72 9-11

9.5.8 DIESEL GENERATOR ENGINE AIR INTAKE AND EXHAUST SYSTEM

9.5.8.1 Design Bases

The Diesel Generator Engine Air Intake and Exhaust System is designed to supply clean air for combustion to the diesel generator engine and to dispose of the engines exhaust. The system is housed in a building designed to withstand the effects of natural phenomena and credible missiles.

All components and piping are located within a Seismic Category I structure (diesel generator building) and all essential components are fully protected from floods, tornado missile damage, internal missiles, pipe breaks and whip, jet impingement and interaction with non-seismic systems in the vicinity. The Diesel Generator Engine Air Intake and Exhaust System is designated as a vital system and components of the system are located within the plant's protected area.

9.5.8.2 System Description

The Diesel Generator Engine Air Intake and Exhaust System is shown in Figure 9.5.8-1.

9.5.8.2.1 General

Each diesel generator is provided with a two pipe combustion air intake system. Combustion air is drawn in through in line air filters prior to entering the turbocharger.

Each diesel generator is provided with a two pipe exhaust system. The waterjacketed exhaust manifold discharges directly into the engine-mounted turbochargers. The exhaust piping then joins to pass through a single exhaust silencer and exits the building.

Intake air for each diesel generator engine is part of the air drawn into the diesel generator building by the Diesel Building Ventilation System.

Outside air intakes are located at one end of the building and exhausts (both Diesel and Ventilation System) at the opposite end of the structure. The intake and exhaust structures are separate for each diesel building and are similar in design. Each intake and exhaust structure is served by a floor drain. In addition a sump, formed by the curb at the bottom of the intake and exhaust structures, provides capacity for preventing accumulation of snow, ice, or freezing rain from interfering with emergency diesel generator system operation.

The COL Applicant will specify the diesel generator air flow capacity. 9-12 9-11

9.5.8.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation; thereafter, the system will be tested in accordance with the technical specifications.

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Air Intake and Exhaust System test frequencies. 9.5-72 9-11

9.5.8.5 Instrumentation Application

Each diesel generator engine unit is provided with sufficient instrumentation and alarms to monitor the combustion intake and exhaust system. A multipoint recorder on the local generator control panel records the individual cylinder exhaust temperatures and the inlet and outlet turbocharger exhaust temperatures. A pyrometer, also on the local generator control panel, automatically monitors each cylinder temperature and compares it to the average temperature of the other cylinders. The pyrometer will annunciate a high/low temperature alarm on the local diesel engine control panel and signal a general diesel trouble alarm in the control room if a cylinder temperature exceeds the average temperature differential setpoint, with the pyrometer automatic sequencer stopping to display the out-of-tolerance cylinder. A high or low exhaust temperature will not initiate a trip on the engine. A manual advance is also provided on the pyrometer to allow each individual cylinder to be checked as well as the inlet and outlet turbocharger exhaust temperatures. The turbocharger temperatures do not affect the cylinder temperature averaging circuit.

The COL Applicant will make available for NRC review, information on Diesel Generator Engine Air Intake and Exhaust System calibration frequencies. 9.5-72 9-11

9.5.9.4 Inspection and Testing Requirements

System components and piping are tested to pressures designated by appropriate codes. Inspection and functional testing are performed prior to initial operation; thereafter, equipment not in continuous use is subject to periodic testing and visual inspection.

The COL Applicant will make available for NRC review, information on Diesel Generator Building Sump Pump System test frequencies.

9.5.9.5 Instrument Application

The COL Applicant will make available for NRC review, information on the Diesel Generator Building Sump Pump System calibration frequencies.

9.5.9 DIESEL GENERATOR BUILDING SUMP PUMP SYSTEM

9.5.9.1 Design Bases

The Diesel Generator Building Sump Pump System is designed to remove leakage and equipment drainage from the diesel generator building and to protect the diesel generator units from internal flooding caused by the maximum credible pipe rupture in the Diesel Generator Building.

All components and piping are located within a Seismic Category I structure (diesel generator building) and all essential components are fully protected from floods, tornado missile damage, internal missiles, pipe breaks and whip, jet impingement and interaction with non-seismic systems in the vicinity. The Diesel Generator Building Sump Pump System is designated as a vital system and components of the system are located within the plant's protected area.

9.5.9.2 System Description

The Diesel Generator Building Sump Pump System flow diagram is shown in Figure 9.5.9-1.

Two sump pumps are provided in each diesel generator building. The pumps are located in the pit below the lube oil sump tank.

The sump pumps start automatically on high sump water level and transfer the water to the equipment and floor drain system.

The diesel generator building sumps and sump pumps are designed for a constant inflow rate of 75 gpm with a maximum pump cycle time of three starts per hour (one pump operating with 37.5 gpm inflow). The maximum pumping flowrate with both pumps operating is 150 gpm.

The COL Applicant will assure the adequacy of the system with respect to the maximum leakage or maximum credible pipe rupture. 9-11

9.5.9.3 Safety Evaluation

The Diesel Generator Building Sump Pump System is an ANSI Class 3 piping system and the pumps and system components are designed in accordance with the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Class 3.

Instrumentation associated with sump pump operation is Safety Class 3 and Seismic Category I. The sump pumps are then powered from the diesel generators in the event of loss of offsite power.

10.2 TURBINE GENERATOR

10.2.1 DESIGN BASES

The turbine generator converts the energy of the steam produced in the steam generators into mechanical shaft power and then into electrical energy. The turbine generator is capable of a 30% step load change with a following 2%/min. load gradient in the loading mode of operation and a 15% step load change with a following 1%/min. load gradient in the unloading mode of operation.

Turbine generator functions under normal, upset, emergency, and faulted conditions are monitored and controlled automatically by the turbine control system described in Section 10.2.2. The control system includes redundant mechanical and electrical trip devices to prevent excessive overspeed of the turbine generator. Additional external trips are provided to prevent damage to the turbine generator.

The turbine generator is designed and manufactured in accordance with the manufacturer's design criteria and manufacturing practices, procedures, and processes as well as its Quality Assurance Program. National codes are not included since existing national codes do not apply to nuclear turbine generators.

The moisture separators, steam reheaters and drain tanks are designed and constructed to ASME Section VIII.

The orientation of the turbine and the design of safety-related structures provide protection against turbine missiles as discussed in Section 3.5.

The Megawatt Demand Setter interfaces with the turbine control system to control the loading of the generator as described in Section 7.7.

The COL applicant will ensure that the selection of the turbine valve operation time meets the turbine valves closing/trip criteria. 10-1

10.2.2 SYSTEM DESCRIPTION

The turbine generator consists of a double-flow, high-pressure turbine and three double-flow low pressure turbines driving a direct-coupled generator.

The flow of main steam is directed from the steam generators to the high-pressure turbine through main stop valves and control valves.

dynamic loads and relief valve discharge loads resulting from rapid closure of system valves and safety/relief valve operation without compromising safety functions. [The COL Applicant shall provide operating and maintenance procedures which educate plant personnel on the potential for the occurrence of steam hammer and water entrainment and the means to minimize such occurrences.] 10-2

10.3.2.3 Piping, Valves, I&C, and Insulation

10.3.2.3.1 Piping

A. The main steam piping and its supports and restraints are designed to withstand loads arising from the various operating and design bases events specified in Section 3.9.3, and a water filled line load under static conditions that may be encountered due to steam generator overfill.

B. The attachment of the main steam piping to the steam generators is designed such that the maximum permissible nozzle loadings are not exceeded.

C. Construction materials or protective coatings containing low melting point elements, particularly lead, mercury and sulfur, are not used where these materials may come in contact with the secondary steam system. This is required to reduce to a minimum the potential for stress corrosion cracking of Inconel material in the steam generators.

D. The flow area of the main steam piping is sufficient to keep steam velocity below 150 ft/sec.

E. Main steam piping layouts that result in 90-degree elbows and miters are minimized.

F. The main steam piping material is carbon steel.

G. Provisions are made for conveniently supporting the deadweight loads imposed during hydrostatic test of the main steam piping.

H. Adequate clearances shall be provided for inservice inspection of the ASME Boiler and Pressure Vessel Code Section III, Class 2 portions of the main steam system piping, in accordance with the provisions of Section XI of the ASME Boiler and Pressure Vessel Code.

I. Loop seals are not utilized in safety valve inlets.

10.4.4.2.4.1 System Performance

A. The total Turbine Bypass Valve capacity is 55% of total full power steam flow at normal full power steam generator pressure (1000 psia). This relieving capacity in conjunction with the Steam Bypass Control and Reactor Power Cutback Systems allows a turbine full load rejection without causing a reactor trip or lifting the primary and/or secondary safety valves.

B. No single Turbine Bypass Valve has a maximum capacity greater than 1.9×10^6 lb/hr at 1000 psia.

C. Turbine Bypass Valves are fail-close valves to prevent uncontrolled bypass of steam to the condenser.

D. The Turbine Bypass Valve operating speeds are as follows:

1. The valves stroke from the full closed position to the full open position and from full open position to full closed position in 15 to 20 seconds when a modulation signal is applied to the valve control system.

2. The valves stroke from the full closed position to the full open position in less than 1 second when a quick opening signal is applied to the valve control system.

3. The valves stroke from the full open position to the full closed position within 5 seconds when the permissive gating signal is removed from the valve control system.

E. The Turbine Bypass Valves and their supports are designed to withstand loads arising from the various normal operating and design bases events as specified in Section 3.9.3.

F. The COL Applicant shall provide the as-built pressure drop between the steam generator outlet nozzles and each Turbine Bypass Valve to ABB-CE to evaluate the actual relieving capacity. 10-3

G. During pre-core hot functional testing, the plant must be maintained at hot standby conditions. To accomplish this, at least one Turbine Bypass valve is capable of controlling flow at 63,000 lb/hr at 1100 psia.

H. The Turbine Bypass Valve control circuits are designed, or precautions are taken, such that no single electrical failure results in the opening of more than one valve.

between 0 percent and 100 percent load. In designing the Condensate System and sizing the condenser hotwell, this difference is considered.

I. Plant operation can continue at 100% power with loss of one operating feedwater pump.

J. Plant operation can continue at 100% power with loss of one operating condensate pump.

K. The feedwater and condensate system is designed to avoid erosion damage. The design and layout of piping systems considers the effect on the piping material from fluid velocity, bend location and the location of flash points. The methods outlined in Section 3.6.3.1.2.1 are used to minimize erosion/corrosion degradation.

L. The feedwater system piping and associated supports and restraints are designed so that a single adverse event, such as a ruptured feedwater line or a closed isolation valve can occur without:

1. Initiating a Loss-of-Coolant incident.

2. Causing failure of the other steam generator's safety class steam and feedwater lines, Main Steam Isolation Valves (MSIVs), safety valves, Main Feedwater Isolation Valves (MFIVs), Steam Generator Blowdown Isolation Valves, or Atmospheric Dump Valves (ADVs).

3. Reducing the capability of any of the Engineered Safety Features Actuation Systems or the Plant Protection System.

4. Transmitting excessive loads to the containment pressure boundary.

5. Compromising the function of the plant control room.

6. Precluding an orderly cooldown of the RCS.

M. System operating and maintenance procedures shall be developed with adequate provisions for avoidance of water hammer.

N. The COL applicant will make information on the provisions for avoidance of water hammer in the condensate and feedwater systems available for NRC staff review. 10-K

T. A four-channel control scheme is provided to preclude inadvertent actuation in the event of a single failure. A four-channel design is provided for the initiation logic, actuation logic, and power.

U. The Equipment and Floor Drainage System (Section 9.3.3) provides for collection and detection of EFW system leakage which may originate in each EFW pump room, in each Emergency Feedwater Storage Tank, and areas containing EFW system piping where a moderate- or high-energy pipe rupture is postulated, as defined in Section 3.8. The control room is alerted on detection of excessive leakage.

V. The emergency feedwater system piping and associated supports and restraints shall be designed so that a single adverse event, such as a ruptured emergency feedwater line or a closed isolation valve can occur without:

1. Initiating a Loss-of-Coolant incident.
2. Causing failure of the other steam generator's safety class steam and feedwater lines, Main Steam Isolation Valves (MSIVs), safety valves, Main Feedwater Isolation Valves (MFIVs), Steam Generator Blowdown Isolation Valves, or Atmospheric Dump Valves (ADVs).
3. Reducing the capability of any of the Engineered Safety Features Actuation Systems or the Plant Protection System.
4. Transmitting excessive loads to the containment pressure boundary.
5. Compromising the function of the plant control room.
6. Precluding an orderly cooldown of the RCS.

W. The EFW System is designated as a vital system and components of the system are located within the plant's vital protection area.

The COL applicant will make information on the provisions for avoidance of water hammer in the emergency feedwater piping available for NRC staff review. 10-K

10.4.9.2 System Description

10.4.9.2.1 General Description

The EFW System is shown in Figure 10.4.9-1, Sheets 1 and 2.

The EFW System is configured into two separate mechanical divisions. Each division is aligned to feed its respective steam generator. Each division consists of one Emergency Feedwater Storage Tank (EFWST), one 100% capacity motor-driven pump

10.4.9.5.2 Temperature Instrumentation

A. Steam Generator Isolation Valves Upstream Temperature

The main control room is provided with temperature indication upstream of steam generator isolation valves and an audible high temperature alarm for detection of back leakage and steam voiding.

B. Emergency Feedwater Storage Tanks Temperature

The main control room is provided with EFWST 1 and 2 temperature indication and high and low temperature alarms.

C. Temperature Test Points

Temperature test points are located at the inlet and outlet of each steam-driven EFW pump turbine bearing oil cooler.

D. Emergency Feedwater Pump Turbine Bearing Temperatures

The main control room is provided with EFW pump bearing temperature indication.

10-5

The COL applicant will make information on the provisions for avoidance of steam binding of the emergency feedwater pumps available for NRC staff review.

10.4.9.5.3 Flow Instrumentation

A. Emergency Feedwater Pumps Discharge Flow

Flow indication for the motor-driven EFW pumps 1 and 2 and steam-driven EFW pump 1 and 2 discharge are provided locally, in the main control room, and at the remote shutdown panel. This instrumentation is designed and procured to meet the criteria given in Regulatory Guide 1.97.

B. Emergency Feedwater Pumps Recirculation Flow

Flow indication for the motor-driven EFW pump 1 and 2 and steam-driven EFW pumps 1 and 2 recirculation are provided locally, in the main control room, and at the remote shutdown panel.

11.0 RADIOACTIVE WASTE MANAGEMENT

11.1 SOURCE TERMS

The average quantity of radioactive material released to the environment during normal operation including anticipated operational occurrences is calculated using PWR-GALE Code (Reference 1) and is based on guidance provided in NUREG-0017 (Reference 2). The adequacy of radioactive waste management systems is demonstrated by verifying compliance with 10 CFR 50, Appendix I offsite radiological release objectives using the NUREG-0017 "expected" source term basis.

Design basis "maximum" source terms are used in plant radiation shielding design and accidental offsite release evaluations. The use of design basis "maximum" source terms in shielding and accident calculations allows for short-term increases in reactor coolant concentration above the NUREG-0017 "expected" average concentrations. Design basis "maximum" source terms are addressed in Chapter 12.

The adequacy of radioactive waste management systems is also demonstrated by verifying compliance with the offsite release rate and concentration limits of 10 CFR 20. Source terms based on a 1% failed fuel rate assumption are used to demonstrate compliance with 10 CFR 20 radiological protection criteria.

The COL applicant will ensure it complies with 10 CFR 50, Appendix I, ANSI N13.1 and RGs 1.21 and 4.15. 11-4

11.1.1 ANTICIPATED PRIMARY COOLANT CONCENTRATIONS

Reactor Coolant System (RCS) radionuclide activity concentration source terms for normal reactor operating conditions, including anticipated operational occurrences, are developed as a basis for a) calculating routine radioactive releases in station effluents, b) calculating radionuclide concentrations in radioactive waste management and other plant systems during normal operation, and c) ensuring that occupational radiation exposures are as low as reasonably achievable (ALARA). A description of reactor coolant and plant system radiation sources used as the basis for shield design calculations is provided in Section 12.2.

11.1.1.1 Fission Product Activities

The concentrations of radioactive fission product isotopes in primary coolant under normal reactor operating conditions are calculated by methods developed in NUREG-0017. The parameters used in the coolant fission product source term calculations are summarized in Table 11.1.1-1. The calculated RCS fission product activity concentrations are summarized in Table 11.1.1-2.

For the purposes of demonstrating compliance with 10 CFR 20, Appendix B, Table 2 limiting concentrations for radioactive

B. Radioactive Liquid Effluent Monitor

Prior to release, waste liquid is held in a monitor tank from which a representative sample is taken. Inlet valves on tanks being prepared for release are closed, providing for a batch release. However, all releases are made through an effluent monitor. The effluent monitor set point is adjusted so that it will only alarm on unexpected high activity (relative to batch release sample information). The alarm also automatically terminates the release.

The setpoint for the liquid waste management system discharge radiation monitor is determined by the COL Applicant and provided in the Offsite Dose Calculation Manual to ensure compliance with 10 CFR 20, Appendix B of Sections 20.1001 through 20.2402 effluent concentrations. The radioactive liquid effluent monitor is located downstream of the last possible point of input of radioactive liquid waste. 11-4

High activity is alarmed in the Radwaste Building control room and in the Main Control Room via the Data Processing System (DPS) and the Discrete Indication and ALARM System (DIAS).

The COL Applicant will provide the operational setpoint for the termination of the liquid waste management system containment cooler condensate tank, turbine building drain, steam generator blowdown, and neutralization tank discharges to the environment in the plant-specific offsite dose calculation manual (ODCM). This setpoint ensures that the ratio of instantaneous concentrations of radionuclides in the liquid effluent in unrestricted areas to the corresponding values given in 10 CFR 20, Appendix B of Section 20.1001-20.2402, Table 2, Column 2 summed over the radionuclides in the liquid effluent does not exceed 10.

Prior to release, the regenerant waste water is held in one of the neutralization tanks from which a representative sample is taken. Releases from the neutralization tanks will be batch releases. All releases are made through a process radiation monitor. Upon detection of a radiation signal above the radiation monitor setpoint, the release is terminated automatically. The contents of the neutralization tank would then be sampled by the operator and the flow manually diverted to the Floor Drain Tank in the low level waste subsystem of the LWMS for further processing.

process parameters (such as settling times, drain time, drying time, etc.) to assure that 10 CFR 61 requirements are met. In addition, resin storage tanks and shipping containers will be sampled and surveyed to verify that the solidification or dewatering process is complete in accordance with guidance from Branch Technical Position ETSB 11-3.

G. The SWMS is designed to ensure that the consequences of an accidental release are within 10 CFR 20, Sections 20.1001 through 20.2402 of Appendix B, Table 2, Column 1 and 2 limits.

In the event of a major component failure of the SWMS, the contents would be contained within the Radwaste Building Structure. Refer to Sections 1.2.16.4 and 3.8.4.1.7 for a description of the Radwaste Building. The Radwaste Building will provide a seismic retention basin. Liquids released from the component will be collected and routed to the LWMS for processing. Any gaseous releases would be released to the Radwaste Building and discharged through filters to the environment via the Radwaste Building Ventilation System. Therefore, there will be no uncontrolled liquid or gaseous release to the environment.

H. An analysis shall be performed which evaluates the collection, processing and storage capacity of the Solid Waste Management System (SWMS) based upon as-built plant component characteristics as well as representative industry data such as:

1. frequency, volume and number of ion exchanger spent resin beds to be processed in the SWMS prior to disposal.

2. frequency, volume and number of filter assemblies to be processed in the SWMS for disposal.

3. plant operating procedures that minimize the production of solid waste in the as-built plant.

The sizing of the spent resin subsystem components shall permit at least a 30-day decay of short-lived radionuclides prior to processing in system equipment. Spent resin collection tanks shall have the capacity to hold at least two batches of spent resin from the source of greatest input.

I. Processed radioactive solid waste will be packaged and shipped to a licensed burial site in accordance with regulatory requirements specified in 10 CFR 71, and by U.S. Department of Transportation (DOT) 49 CFR 170 through 189. The COL Applicant will develop procedures to meet these requirements. 11-2

frequency established by the COL Applicant, onsite to the primary chemistry lab and counting room during normal operating and post-accident conditions.

Continuous sampling of all potential post-accident release points is provided by the continuous unit vent sampler. This sampler contains a fixed filter particulate and iodine cartridge which receives continuous flow of sample air from the unit vent duct. This sample cartridge is routinely replaced and taken for detailed onsite laboratory analysis in the primary chemistry laboratory and counting room, where precise assessment of releases is performed for the period during which the cartridge collected the sample. The frequency at which the cartridge is replaced and analyzed is determined by the COL Applicant and specified in the operations and maintenance manual. The sampler is designed to be used during normal operation and post-accident conditions to meet the sampling requirements specified in 10 CFR 50.34 (f) (2) (xvii) and NUREG-0737, Attachment 2, Section II.F.1.

The Process and Effluent Monitoring and Sampling System is designed with a continuous control room interface via the DPS and DIAS systems. Primary indication of radiation levels and status of alarms for post-accident and non-post-accident radiation monitors are processed through the DPS and DIAS systems.

The COL applicant will demonstrate conformance with 10 CFR 50 Appendix I, ANSI N13.1, RG 1.21 and RG 4.15. //-/

The RMS monitors normal and potential paths for release of radioactive materials to provide continuous indication and recording of gaseous and liquid radioactivity levels leaving the plant. As a minimum, continuous representative sampling is provided for airborne particulate and iodine radioactivity in discharge paths. These systems are designed in accordance with ANSI 13.1. The RMS also initiates control actions on certain systems to control or reduce continuous effluent releases or to terminate batch releases.

Station ventilation systems are monitored for airborne radioactivity resulting from equipment or system malfunction or misoperation, or from maintenance activities which could cause radioactivity levels to reach unacceptable levels. A portable airborne monitor is also available for use in areas where work activities or surveillance pose an unusual risk to plant personnel of exposure to airborne activity.

Radiation monitoring equipment is provided to detect primary to secondary system leakage and leakage from the primary system to the containment atmosphere. These monitoring systems are designed to the recommendations of Regulatory Guide 1.45 for

Radiation Monitoring System equipment is checked and inspected on a periodic basis. Setpoint checks are performed on a monthly basis with detector calibrations performed once per refueling cycle. Detectors are also calibrated if an inadequate checksource response indicates a problem or following any other equipment maintenance that could affect the accuracy of the instrument indication.

11.5.1.4 Administrative and Procedural Controls

As specified in Position C of Regulatory Guide 4.15, written procedures will be prepared, reviewed, and approved for sample collection, preparation, and analysis. Procedures will also exist for the use of radioactivity reference standards, detector calibration and checks of the radiation monitor systems, and for reduction, evaluation and reporting of data. The accuracy of sample flow rate devices will be determined on a regularly scheduled basis. Adjustments to the instrumentation will be made as needed to bring performance into specified limits. The frequency of these calibrations will be specified and results will be recorded. Also, collection efficiencies of the samplers used will be documented. 11-3

11.5.2 PROCESS AND EFFLUENT RADIOLOGICAL SAMPLING PROGRAM

11.5.2.1 Program Overview

Periodic sampling is performed to supplement the function of the process and effluent radiation monitors. The sampling programs will be designed in accordance with Regulatory Guide 1.21 and the sampling requirements defined in the Technical Specifications.

All continuous effluents that are potentially radioactive are periodically sampled and analyzed. All stored wastes are sampled and samples analyzed before release of wastes to the environment. Comparisons will be made between gross radioactivity measurements of continuous monitors and analyses of specific radionuclides as required by Regulatory Guide 1.21.

Special provisions are made for post-accident sampling of effluent pathways in accordance with NUREG-0737, 10 CFR 50, and Regulatory Guide 1.97 requirements.

11.5.2.2 Sampling Locations

Sampling locations are chosen to meet the requirements of Regulatory Guide 1.21 and NUREG-0800 (SRP 11.5, Table 1). Sample points and equipment are also provided to meet special post-accident sampling requirements in NUREG-0737 and Regulatory Guide 1.97. Some of these requirements are met by using special features provided for in the Radiation Monitoring System (RMS) while in other cases only sample taps are provided to collect samples with portable instrumentation and equipment.

Effluent ventilation ducts are sampled isokinetically in accordance with ANSI N13.1 for radioactive gases, particulates, and iodines. Iodine samples are collected using special iodine filtering cartridges and taken to the counting room for analysis. Particulate sampling utilizes fixed paper filters for laboratory analysis. Gas sampling utilizes special gas collection canisters which allow easy connection and disconnection from sample taps for transport to the counting room.

11.5.2.5 Analytical Procedures and Sensitivity

Samples of process and effluent gases and liquids are analyzed in the counting room in accordance with station procedures and Regulatory Guide 1.21. Analytical procedures used are based on methodology utilized in general practice in the nuclear industry or in applicable standards and the accuracy and precision of the results are standardized with central or outside laboratories using radioactivity standards traceable to the National Bureau of Standards. Laboratory equipment is provided for the counting room to perform gross beta counting, gross alpha counting, gamma spectrometry, liquid scintillation counting, and radiochemical separations.

11.5.2.6 System Operations and Maintenance Manual

11-5

The COL Applicant will provide an operation and maintenance manual that demonstrates and describes the following:

a. Procedures and/or methods for converting radiation monitor measurement output into radioactivity release rates of gaseous discharge through the unit vent.

b. The sampling technique used to monitor and sample effluent gases to assure that a representative gas sample is taken and that the sampling system provided is capable of near isokinetic conditions during and following an accident as specified in NUREG-0737, Item II.F.1, Clarification 3 of Attachment 2.

c. The collection technique used to extract a representative sample of radioactive iodines and particulates during and following an accident. The information obtained from these samples will be used to quantify the releases for dose calculations and assessments as specified in NUREG-0737, Table II.F.1-2.

d. Calibration frequency and techniques for radiation monitors based on vendor information for the equipment procured.

e. The sampling system is designed to ensure compliance with regulatory shielding requirements for low radiation exposure during post-accident conditions specified in NUREG-0737, Item II.F.1, Clarification 2 of Attachment 2. The equipment design and location specifications are discussed in Section 11.5.1.2.3.

Piping containing radioactive fluids is routed as part of the engineering design effort. This ensures that lines expected to contain significant radiation sources are adequately shielded and properly routed to minimize exposure to personnel.

Onsite inspections will be conducted, as necessary during construction, to ensure that the shielding and piping layout meets established criteria. During construction, visual inspections will be made to ensure that there are no major defects or scattering and streaming paths for radiation in the shield walls as they are placed. During initial power operations, radiation surveys will be conducted to ensure that the shielding meets design requirements during normal operation and maintenance of the plant.

12.1.1.2 Operation Policies

The station ALARA manual will be one of the primary means of officially expressing the operational ALARA policy. This policy is demonstrated in the radiation protection program, the training program, and station procedures, with specific details to be covered by the owner/operator. The ALARA program is established in conformance with the requirements of Regulatory Guides 1.8, 8.8, and 8.10 and discussed in the site-specific SAR section 13.1. Besides describing management's commitment to ALARA, the Radiation Protection section of the Station Manual designates the station personnel who have the responsibility and authority to implement ALARA. The Radiation Protection Manager has the responsibilities for the onsite Radiation Protection Program. The responsibilities and authority of the supervisory positions for the day-to-day operation of the site radiation protection programs are discussed in the site-specific SAR Sections 13.1.2 and 13.1.3.

Prior to startup of the unit, station procedures to be used for work which involves significant personnel radiation exposure will be reviewed to verify that the procedures adhere to the ALARA philosophy. Revisions to station procedures involving significant personnel exposure will also receive an ALARA review. Systems or station modifications affecting personnel radiation exposure will also be reviewed to see that the ALARA concept is applied.

In addition, periodic reviews of the ALARA program, including review of radiation exposure records and operating procedures, are conducted by offsite Radiation Protection personnel. Personnel requiring access to the restricted area and/or radiological controlled areas will receive training as necessary to permit access to these areas. These personnel will be tested to evaluate each worker's knowledge, competency, and understanding relative to the training provided. Retraining and retesting will be conducted.

minimizing corrosion, tanks are designed with sloped bottoms to prevent CRUD buildup. Those components with the potential of exposure from CRUD are provided with flushing capability from either demineralized water or chemical decontamination. Also, equipment is designed that separates highly radioactive portions from lower radiation level portions of a component.

The COL applicant will submit a detailed shielding analysis and will ensure that the final design incorporates lessons learned from previous nuclear power plant designs. 12-2

The personnel inhalation dose and external whole body dose will be maintained within 10 CFR 20.101 limits.

12.2.3 SOURCES USED IN NUREG-0737 POST-ACCIDENT SHIELDING REVIEW

Item II.b.2 of NUREG-0737 clarifies the requirement for ensuring that areas which require post-accident personnel access or contain safety-related equipment are adequately shielded in the vicinity of systems which may contain highly radioactive materials as a result of the Design Basis Accident.

A radiation and shielding design review of the System 80+ Standard Design in accordance with Item II.B.2 of NUREG-0737 amended by the guidance provided in Draft NUREG 1465 relative to post LOCA source terms is performed during the detailed design phase of the plant. The review of systems that, as a result of an accident, contain highly radioactive materials was performed using the same methodology described in Section 12.3.2. 12-2

Initial core releases are used which are equivalent to those recommended in Draft NUREG 1465. The source terms are presented in Table 12.2-20. The sources are characteristic of a depressurized system.

Plant areas requiring post-accident occupation ("vital areas"), and the duration of occupation are identified.

These source terms are used to evaluate the adequacy of shielding in post-accident conditions using shielding codes, discussed in Section 12.3, to verify that:

a. Vital areas are accessible to operators to take the mitigative actions during post-accident conditions,

b. Safety related equipment are qualified for the radiation area in which they are located.

For vital areas requiring irregular access, sufficient shielding will be provided to ensure the whole body dose, or its equivalent, is limited to 5 rem for the duration of the accident in accordance with 10 CFR 50, Appendix A (General Design Criterion 19). For vital areas requiring continuous occupancy, such as the control room, the local radiation levels are limited to 15 mrem/hr averaged over 30 days per NUREG-0737, Section II.B.2.3.

of these isotopes are divided into six discrete energy groups. Group boundaries remain fixed, but the average group energy is calculated for each spectrum of isotopes. This allows reasonably precise selections of energy dependent shield material properties for attenuation properties.

12.3.2.2 Shielding Design

The plant shielding shall be designed to achieve the radiation zones designated in Tables 12.3-2 and 12.3-3 for normal operation and post-accident conditions respectively. Accessible areas that are potentially greater than 100 R/hr are listed in Table 12.3-6.

Transient sources of greater than 100 R/hr are considered in the System 80+ shielding design to ensure adequate shielding is provided. One such source is a spent fuel assembly. During transfer of a spent fuel assembly through the fuel transfer tube, adjacent corridors may experience elevated radiation levels. Streaming from this source up through the joint between the Reactor Building and the Nuclear Annex has been a concern for the current generation of nuclear plants. The System 80+ design utilizes a connected building design to reduce the potential for streaming. In addition, a lead collar is provided around the fuel transfer tube, as well as several feet of additional concrete shielding to maintain adjacent corridors radiation levels ALARA. This permits personnel to perform maintenance and inspection activities in a lower radiation areas and reduces the potential for adverse radiation zones from impacting refueling outage schedules. An inspection area is provided beneath the fuel transfer tube. Access control is ensured by the provision of an alarm on the hatch to sound when the door is open to the spent fuel transfer tube inspection area, as well as a lockable access door to the inspection area. Figure 12.3-17 provides a sectional view of the fuel transfer tube, the shielding provided to the adjacent areas, and the expected radiation zones in these areas during fuel transfer.

The COL Applicant will perrorm a shielding analysis to verify the adequacy of the shielding provided. Sufficient shielding will be provided to ensure that the areas adjacent to the spent fuel transfer tube inspection area are accessible and that the expected radiation zones are consistent with those illustrated in Figure 12.3-17 during transfer of a spent fuel assembly. 12-2

Typically, infrequent access to pipe chases is required. The System 80+ design specifies that location of active components, such as valves, will be avoided whenever possible in pipe chases, to minimize the frequency of access required by plant personnel and personnel exposure. When access is required, radiation protection personnel would conduct a survey of the area to determine the high radiation areas within the pipe chase. Temporary shielding will be utilized, as necessary, to minimize the personnel exposure. For instance if access to the pipe chase

Q ≡ Activity source term for room (μCi-ft^3/ml-hr)

$$Q = L \times PF \times A_0$$

L ≡ Leakage or evaporation rate (ft^3/hr liquid phase basis)

PF ≡ Partition Factor (The ratio of the quantity of a nuclide in the gas phase to the total quantity in both the liquid and gas phases when the liquid and the gas are at equilibrium.)

A_0 ≡ Initial activity of fluid stream source (μCi/ml)

F ≡ Room exhaust flow rate (ft^3/min)

60 ≡ Conversion factor (min/hr)

Credit for decay has been neglected for conservatism. The airborne concentrations in rooms or cubicles accessible to personnel throughout the plant will be maintained within inplant concentrations prescribed in 10 CFR 20. The design acceptance criteria necessary to assure plant design compliance with 10 CFR 20 requirements are specified in the Radiation Protection Design Acceptance Criteria document. The design acceptance criteria specified include: 12.4 12-2

a. Maintain inplant airborne concentrations of radioisotopes within 10 CFR 20, Appendix B of Sections 20.1001-20.2402, Table 1, Column 3 limits for areas requiring infrequent access.

b. Maintain inplant airborne concentrations of radioisotopes well within or a small fraction (i.e., 0.25) of 10 CFR 20, Appendix B of Sections 20.1001-20.2402, Table 1, Column 3 limits for areas requiring continuous or frequent access. Inplant airborne concentrations will be calculated as described in Section 12.2.2.

c. Provide sufficient containment and ventilation capability to prevent the spread of airborne contamination.

d. Provide airborne radiation monitors in areas normally occupied and where a potential of airborne contamination exists. The airborne radiation monitoring system is discussed in Section 11.5.

The COL Applicant will evaluate the plant design in accordance with this Design Acceptance Criteria document to assure airborne concentrations are maintained less than 10 CFR 20.1204 limits.

Continuous access will be provided during post-accident conditions with dose rates less than or equal to 15 mrem/hr to the following Advanced Control Complex vital area:

- Main Control Room
- Technical Support Center
- Remote Shutdown Panel
- Computer system area
- Rooms housing Instrument and Control systems and equipment

Required access to the following vital areas and systems will not exceed 5 rem:

A. Hydrogen Recombiner Rooms

B. Process Control Sampling Panels

C. Primary Chemistry Labs

Generic plant emergency procedures were reviewed and the above areas were identified as vital areas. The following systems were considered for post-accident access; however, they do not constitute vital areas.

A. Annulus Ventilation System

B. Safety Injection System

C. Containment Spray System

D. Shutdown Cooling System

E. Chemical and Volume Control System

F. Post-Accident Sampling

G. Subsphere Ventilation System

A complete list of vital areas will be developed by the Owner Operator based on site specific Emergency Procedures. 12.3-4

The zone limits are summarized for the DBA LOCA in Table 12.3-3. The Radiation Zone designations, as well as the Radiation Zone Maps are shown in Table 12.3-4 and Figures 12.3-9 through 12.3-16, respectively.

contamination to areas of higher potential airborne contamination. For building compartments with the potential for contamination, the exhaust is designed for greater volumetric flow than is supplied to the area to minimize the amount of uncontrolled exfiltration from these areas. These design features ensure that the average concentration of radioactive material in the air for areas normally occupied is well within or a small fraction (i.e., 0.25) of 10 CFR 20, Appendix B, Table 1, Column 3 limits. Therefore, personnel exposure due to inhalation of and immersion in airborne contamination is maintained ALARA.

Airborne radiation monitoring is provided to areas normally occupied with a significant potential to have airborne contamination. These monitors are designed to have the capability to detect the time integrated change of the most limiting particulate and iodine species equivalent to 10 CFR 20, Appendix B of Sections 20.1001 - 20.2402, inplant concentrations in each area within 10 DAC-hours.

Airborne monitors are discussed in further detail in Section 11.5. The approximate location of the process effluent radiation monitors are shown in Figures 6.2.3-1, 9.4-2, 9.4-3, 9.4-5, 9.4-6, 9.4-8 and 9.4-9. The airborne radiation monitors are located upstream of the process filters.

The ventilation systems are discussed in detail in Section 9.4.

12.3.4 AREA RADIATION AND AIRBORNE RADIATION MONITORING INSTRUMENTATION

Area and airborne radiation monitoring instrumentation are discussed in Section 11.5. Area radiation monitors are illustrated in Figures 12.3-9 through 12.3-16 and 12.3-18 through 12.3-21. Radiation monitors will be provided and located in accordance with Regulatory Guide 1.97 and NUREG-0737 recommendations.

Table 12.3-5 lists the area radiation monitors and their approximate locations. Section 11.5 specifies each monitor's range of sensitivity, power supply, and seismic category.

Area monitors are located based on the expected frequency of access, occupancy time, and expected and potential radiation levels in plant work areas.

- Areas which are typically high radiation areas, such as pipe chases, and have little or no accessibility will not be provided with an area radiation monitor.

- Areas which typically have a high frequency of access and are normally low radiation areas but have a potential to be a high radiation area will be provided with an area radiation monitor. In post-accident

12-6
~~12.7~~

The COL Applicant will develop procedures for Radiation Protection to conduct surveys using portable radiation monitors as part of the Radiation Protection program. ~~12.8~~ During post-accident conditions, plant personnel will be evacuated from the RCA. Radiation protection personnel would then conduct surveys using portable radiation monitors to determine the optimal routes to vital areas through the RCA so that personnel exposure is minimized. Radiation protection personnel would typically escort maintenance personnel and operators into the RCA and would continue to monitor the radiation levels using portable radiation monitors. The area monitors located in the plant would provide an audible and visual alarm if high radiation levels were detected.

prevents the loss of equipment in an adjacent division due to a single event. This facilitates recovery by operators from fire or flood events.

b. RCS Depressurization

The use of the Internal Refueling Water Storage Tank (IRWST) enables the operators to depressurize the RCS by relieving the PORVs to the IRWST. This tank allows the dissipation of a significant portion of energy to the IRWST, thus facilitating the recovery from loss of heat sink events.

c. Safety Injection

The provision of a direct header from safety injection, which takes suction from the IRWST, to the reactor vessel reduces the likelihood of a failure to provide safety injection water to the reactor.

d. Safety Related Equipment Power Supply

In the System 80+ design, safety related equipment are supplied directly from offsite power. Since there are less intermediate equipment to fail, the probability of failure to provide power to safety related equipment when offsite power is available is reduced.

These features are further expected to reduce occupational radiation exposures to ALARA levels.

12.4.5 SYSTEM 80+ ESTIMATED DOSE ASSESSMENT

Data from representative PWRs are taken to create a baseline for this estimate. System 80+ ALARA design features are credited for reduction in occupational exposures. The bases for the dose reduction factors in Table 12.4-4 are described in Section 12.4.4.

12-7
12-8

The COL Applicant will perform a formal dose assessment in accordance with Regulatory Guide 8.19 guidance to ensure that personnel exposure is maintained ALARA. This is ensured by demonstrating compliance with the acceptance criteria specified in the Radiation Protection Design Acceptance Criteria document. This document requires compliance with 10 CFR 20 limits and 10 CFR 50, Appendix A (General Design Criteria 19 and 61).

To confirm compliance with 10 CFR 20 limits and 10 CFR 50, Appendix A (General Design Criteria 19 and 61), the following information and analyses must be available to perform the formal dose assessment:

12.5 HEALTH PHYSICS PROGRAM

The health physics program is outside of System 80+ Standard Design scope. Discussion regarding the health physics program will be provided in the site-specific Safety Analysis Report (SAR). I J

12-8

13.0 CONDUCT OF OPERATIONS

13.1 ORGANIZATIONAL STRUCTURE OF SITE OPERATOR

Information concerning the site operator's organizational structure is within the site operator's scope and shall be provided in the site-specific SAR. This will include site-specific information to address the issues in the TMI Action Plan Items I.A.1.4 and II.J.3.1. 13-1

13.2 TRAINING

Information concerning the site operator's training program is within the site operator's scope and shall be provided in the site-specific SAR. This will include site-specific information to address the issues in TMI Action Plan Items I.A.4.1(2), I.A.4.2, and II.K.1(26).

13B

18-2

13.3 EMERGENCY PLANNING

13.3.1 PRELIMINARY PLANNING

See site-specific SAR.

13.3.2 EMERGENCY PLANNING

[See site-specific SAR.] 13-2

13.3.3 BOP INTERFACES

13.3.3.1 Technical Support Center

13.3.3.1.1 Summary Description

The Technical Support Center (TSC) is an onsite facility located adjacent to the control room that provides the capability for plant management and technical support to the reactor operating personnel located in the control room during emergency conditions. The TSC is located within two minutes walking time of the control room. In addition, the TSC design incorporates a viewing gallery which is located so as to permit visibility into the control room. It has technical data displays and plant records available to assist in the detailed analysis and diagnosis of abnormal plant conditions and any significant release of radioactivity to the environment. The TSC is the primary communications center for the plant during an emergency. The TSC assists the control room operators by providing resources and facilities for handling the administrative items, technical evaluations, and contact with offsite activities. E

Until the TSC is activated, all functions of this facility are performed in the control room. When the TSC is functional, emergency response functions, except direct supervision of reactor operations and manipulation of reactor system controls, shift to the TSC. Plant administration, technical support functions, and contact with offsite activities to assist the control room operators are performed in the TSC throughout the course of an accident.

Table 13.3.3-1 outlines the transfer of emergency response functions from the control room to the TSC under the various emergency classes.

The level of staffing of the TSC may vary according to the severity of the emergency condition. The staffing criteria for each emergency class is fully detailed in the licensee's emergency plan. Section 13.3.3.1.5 defines the TSC work space size.

13.3.3.1.6 Habitability

TSC personnel are protected from radiological hazards, including direct radiation and airborne radioactivity from in-plant sources under accident conditions, to the same degree as control room personnel, so far as the maximum permissible radiation exposure is concerned while the TSC is habitable. Applicable criteria are specified in 10 CFR 50 General Design Criterion 19, NRC Standard Review Plan 6.4, and NUREG-0737, "Clarification of TMI Action Plan Requirements," Item II.B.2.

To ensure adequate radiological protection of TSC personnel, radiation monitoring systems are provided in the TSC. These systems continuously indicate radiation dose rates and airborne radioactivity concentrations inside the TSC while it is in use during an emergency. These monitoring systems shall include local alarms with trip levels set to provide early warning to TSC personnel of adverse conditions that may affect the habitability of the TSC. Detectors are able to distinguish the presence or absence of radioiodines at concentrations as low as 10^{-7} microcuries/cc.

If the TSC becomes uninhabitable, the TSC plant management function can be performed in the control room. Reference Section 6.4 TSC for habitability details. Control Building HVAC is discussed in Section 9.4.1.

13.3.3.1.7 Communications

The TSC is the primary onsite communications center for the nuclear power plant during an emergency. It has reliable voice communications to the control room, the OSC, the emergency operations facility (EOF), and the NRC. The primary functions of this voice communication system are plant management communications and the immediate exchange of information on plant status and operations. Provisions for communications with State and local operations centers are provided in the TSC to provide early notification and recommendations to offsite authorities prior to activation of the EOF.

The TSC voice communications facilities includes means for reliable primary and backup communication. The TSC voice communications will include private telephones, commercial telephones, radio networks, and intercommunication systems as appropriate to accomplish the TSC functions during emergency operating conditions. The licensee provides a means for TSC telephone access to commercial telephone common-carrier services that may be susceptible to loss of power during emergencies. The licensee ensures that spare commercial telephone lines to the plant are available for use by the TSC during emergencies. 13-3

A. Plant systems variables.

B. In-plant radiological variables.

C. Meteorological information.

D. Offsite radiological information.

Trend information display and time-history display capability is provided in the TSC to give the TSC personnel a dynamic view of the plant status during abnormal operating conditions. The TSC displays are designed so that callup, manipulation, and presentation of data is easily performed. The TSC data display format presents information that is easily understood by the TSC personnel performing analyses.

The Data Processing System (DPS) data set associated with plant safety status is displayed in the TSC. This duplication will improve the exchange of information between the control room and the TSC. The total TSC data system reliability is designed to achieve an operational unavailability goal of 0.01 during all plant conditions above cold shutdown. Operational unavailability is defined as DOWN TIME divided by OPERATING TIME. E

13.3.3.1.9 Records Availability

The TSC includes provisions for a complete and up-to-date repository of plant records and procedures at the disposal of TSC personnel to aid in their technical analysis and evaluation of emergency conditions.

13.3.3.2 Emergency Operations Facility

The Emergency Operations Facility (EOF) is an out of scope item which shall be provided by the license applicant and is site specific. The following sections contain a description of a typical EOF and interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive. 13-4 J

13.3.3.2.1 Summary Description

The Emergency Operations Facility (EOF) is a nearsite support facility for the management of overall licensee emergency response (including coordination with Federal, State, and local officials), coordination of radiological and environmental assessments, and determination of recommended public protective actions. The EOF has appropriate technical data displays and plant records as discussed in the site-specific SAR. E

State and local agencies are responsible for implementing emergency response actions involving the general public. The State and local agencies may operate from the EOF or from their own control centers at other locations, dependent upon the site-specific provisions of the emergency plan at each plant. E

J

13.3.3.2.3 Staffing and Training E

The licensee shall address all staffing and training issues. 13K J

13.3.3.2.4 Size E

The EOF building or building complex shall be large enough to provide the following: J

A. Working space for the personnel assigned to the EOF as specified in the licensee's emergency plan, including State and local agency personnel, at the maximum level of occupancy without crowding (minimum size of working space provided is approximately 75 sq ft/person).

   The EOF working space is sized for at least 35 persons, including 25 persons designated by the licensee, 9 persons from NRC, and 1 person from FEMA. This minimum size is increased if the maximum staffing levels specified in the licensee's emergency plan, including representatives from State and local agencies, exceed 25 persons.

B. Space for EOF data system equipment needed to transmit data to other locations. E

C. Sufficient space to perform repair, maintenance, and service of equipment, displays, and instrumentation.

D. Space for ready access to communications equipment by all EOF personnel who need communications capabilities to perform their functions.

E. Space for ready access to functional displays of EOF data.

F. Space for storage of plant records and historical data or space for means to readily acquire and display those records.

G. Separate office space to accommodate at least five NRC personnel during periods that the EOF is activated for emergencies.

13.3.3.2.5 Radiological Monitoring

To ensure adequate radiological protection of EOF personnel, radiation monitoring shall be provided in the EOF. These systems shall continuously indicate radiation dose rates and airborne radioactivity concentrations inside the EOF while it is in use during an emergency. These monitoring systems shall include local alarms with trip levels set to provide early warning to EOF personnel of adverse conditions that may affect the habitability of the EOF. Detectors to distinguish the presence or absence of radioiodines at concentrations as low as 10^{-7} microcuries/cc shall be provided.

13.3.3.2.6 Communications

The EOF shall have reliable voice communications facilities to the TSC, the control room, NRC, and State and local emergency operations centers. The normal communication path between the EOF and the control room shall be through the TSC. The primary functions of the EOF voice communications facilities are:

A. EOF management communications with the designated senior licensee manager in charge of the TSC.

B. Communications to manage licensee emergency response resources.

C. Communications to coordinate radiological monitoring.

D. Communications to coordinate offsite emergency response activities.

E. Communications to disseminate information and recommended protective actions to responsible government agencies.

The EOF voice communications facilities shall include reliable primary and backup means of communication. Voice communications shall include private telephones, commercial telephones, radio networks, and intercommunications systems as appropriate to accomplish the EOF functions during emergency conditions. The licensee shall provide a means for EOF telephone access to commercial telephone common-carrier services that bypasses any local telephone switching facilities that may be susceptible to loss of power during emergencies. The licensee shall ensure that spare commercial telephone lines to the plant are available for use by the EOF during emergencies.

The EOF voice communications equipment shall include:

13.3.3.4 Laboratory Facilities

13.3.3.4.1 Summary Description

The Laboratory Facilities are out of scope items which shall be provided by the license applicant. Consistent with the requirements stated in NUREG-0654, II.H.9 and NUREG-0737, II.B.3, the System 80+ Standard Plant design makes provisions for inclusion of both hot and conventional Laboratory Facilities. Hot facilities are currently located in the Nuclear Annex; additional hot facilities should be located in a Radwaste Building. Space for a large conventional laboratory should be provided in the Station Services Building. Locations for other, smaller lab facilities are allocated at various places throughout the plant. The facilities themselves shall be designed according to particular owner preference, but they shall support efforts to monitor plant systems and environmental samples for compliance with technical specifications. Complete descriptions of the facilities shall be provided by the licensee. 13-4

The following sections contain interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive.

13.3.3.4.2 Function

J

The laboratory facilities shall provide for the following primary functions:

A. to provide plant support services for routine analyses required for personnel protection, surveys, and related health physics functions.

B. to provide normal and post-accident cold chemical analyses on required plant chemistry samples.

C. to provide routine and post-accident counting on all plant radioactivity samples.

D. to provide grab sample analyses used as a check on the accuracy of the continuous on-line process monitoring instrumentation.

E. to provide a facility to store and secure radioactive calibration and check sources and instruments undergoing calibration, maintenance, or repair.

13.3.3.6 Onsite Decontamination Facilities

13.3.3.6.1 Summary Description

The Onsite Decontamination Facilities (ODF), located in the Nuclear Annex (el. 91+9) and in the Radwaste Facility, are out of scope items which shall be provided by the license applicant. These facilities shall be provided to remove or reduce radioactive contaminants from plant equipment, protective clothing, and personnel. These facilities shall be designed according to particular owner preference, but shall be supplied by the major decontamination equipment, including various spray nozzle assemblies, chemical and/or abrasive supply systems, collection and storage tanks, high pressure pumps, filters, demineralizers and piping connections to waste processors. Complete descriptions of the facilities shall be provided by the licensee. 134

The following sections contain a description of a typical ODF and interface requirements which must be met to ensure adequacy with the System 80+™ Standard Design. The word "shall" is used to distinguish interface requirements that are mandatory from text that is purely descriptive.

The ODF shall include the hot laundry facilities, hose washdown stations, personnel decontamination fixtures, hot shower, radiation detection equipment and personnel decontamination supplies. Also equipment necessary to decontaminate small tools and instruments as well as larger tools and pieces of equipment shall be provided. J

These facilities shall be designed to meet the requirements as stated in 10 CFR 50 Appendix E, IV.E.3; and 10 CFR 50.47 (b) (8). The role(s) of the Onsite Decontamination Facilities in the event of a plant emergency shall be described in the emergency planning documents provided by the licensee.

13.3.3.6.2 Function

The Onsite Decontamination Facilities shall provide for the following functions:

A. To facilitate equipment disposal by reducing contamination and radiation levels to releasable limits.

B. To facilitate equipment repair by reducing contamination and radiation levels consistent with ALARA guidelines.

13.3.3.6.5 Decontamination Methods and Procedures

Selection of decontamination methods to be employed in the Onsite Decontamination Facilities at a specific generating plant is the responsibility of the individual licensee. Some of the decontamination requirements may be met by using portable or otherwise transportable facilities at the discretion of the individual licensee. Description of those methods and rationale for their selection shall be provided by the licensee. 13-4

Decontamination and radwaste control procedures are considered to be a fundamental part of the plant operations documentation. The licensee plant operations documents shall contain these detailed procedures. J

All decontamination methods and procedures should be consistent with accepted industry practice, and shall meet the intent of the referenced section of the Code of Federal Regulations.

13.4 REVIEW AND AUDIT

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

13-5

13.5 PLANT PROCEDURES

Information concerning the site operator's plant procedures is within the site operator's scope and shall be provided in the site-specific SAR. 13-6

13.5.1 PLANT OPERATING PROCEDURES DEVELOPMENT PLAN

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

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

C. The scope of the plan shall include the applicable operating procedures in Subsection 13.5.1.1

D. The Plan shall ensure that POPs follow standard formats implemented through Writer's Guides (e.g., per References 1 and 8).

E. The Plan shall specify that the POPs' technical bases are documented to ensure that their content is consistent with plant design basis material including applicable procedure guidelines, task analyses, and PRA, (all provided via OSIP), and applicable plant-specific aspects, per Reference 1.

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

G. The plan shall specify the POP validation activities that demonstrate the acceptability of the completed procedures for the scope specified in Item C above.

H. The plan shall specify that the POPs comply with the applicable requirements of References 1 through 7.

13.5.1.1 Procedures Included in Scope of Plan

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

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

   a. Reactor Coolant System
   b. Control Rod Drive System (including part-length rods)
   c. Shutdown Cooling System
   d. Emergency Core Cooling System

1.2.12 RADIOACTIVE WASTE MANAGEMENT SYSTEMS

Radioactive sources and waste management systems are described in Chapter 11. Design considerations to minimize exposure to radioactivity are summarized in Chapter 12.

A description of the Radwaste Building which houses the Solid and Liquid Waste Management Systems is provided in Section 1.2.16.4.

1.2.13 PHYSICAL PLANT SECURITY AND PROTECTION FROM SABOTAGE

The System 80+ Standard Design features which protect against sabotage are listed in Appendix A to Chapter 13. The owner-specific plan will provide details on implementation of certain sabotage protection requirements. 13-7

1.2.14 COOLING WATER SYSTEMS

1.2.14.1 Condenser Circulating Water System

The Condenser Circulating Water System provides cooling water for the turbine condensers and rejects heat to the normal heat sink.

See Section 10.4.5 for a description of this system.

1.2.14.2 Station Service Water System

The Station Service Water System (SSWS) is an open system that takes suction from the Ultimate Heat Sink (UHS) and provides cooling water to remove heat released from plant systems, structures and components. The SSWS returns the heated water to the UHS. The SSWS cools the Component Cooling Water System (CCWS) which in turn cools essential and non-essential reactor auxiliary loads.

A description of the Station Service Water System is presented in Section 9.2.1.

1.2.14.3 Component Cooling Water System

The Component Cooling Water System is a closed loop cooling water system that, in conjunction with the SSWS and the UHS, removes heat generated from the plant's essential and non-essential components connected to the CCWS. Heat transferred by these components to the CCWS is rejected to the SSWS via the component cooling water heat exchangers.

A description of the Component Cooling Water Heat Exchanger Structure is provided in Section 1.2.16.8.

A description of the Component Cooling Water System is provided in Section 9.2.2.

13.5.2 ADMINISTRATIVE CONTROL PROCEDURES

13-9

Such procedures will be a COL action item including "Review and Modify Procedures for Removing Safety-Related Systems from Service" and "Guidelines for Upgrading Other Procedures." 13-9

To avoid excessive fouling and plugging of the screens near the IRWST suction inlets during an accident (see Section 6.8 and Appendix 19.8A, Subsection 2.9), the containment must be cleaned of sand, maintenance debris, and other particulate materials prior to startup from a refueling outage. There are no specific requirements for determining acceptable cleanliness, but maintenance practices should be consistent with generally accepted practices for nuclear power plant containment interiors. This is a DRAP item; see Section 17.3.

The COL applicant/holder shall consider the guidance of NUMARC-8700, "Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors," (11/20/87) in developing plant procedures for severe weather conditions such as hurricanes and tornadoes.

13.6 INDUSTRIAL SECURITY

Information concerning the site operator's industrial security is within the COL applicant's scope and will be presented by the COL applicant in a separate document. 13-7

13.6.1 INTERFACE REQUIREMENTS

Site security is an out of scope item which shall be provided by the COL applicant. The COL applicant shall verify that the following interface requirements are met to ensure adequacy with the System and Standard Design:

A. The design of the physical security system shall be in conformance with 10 CFR Part 73, 73.55 including:

1. 10 CFR Part 73, 73.55 in its entirety and Part 73 Appendices B and C
2. 10 CFR Part 25 and 10 CFR Part 95
3. Regulatory Guide 5.44
4. NUREG-0674
5. 10 CFR 73.56
6. 10 CFR Part 50, 50.70 (b) (3)
7. Regulatory Guide 5.12
8. Regulatory Guide 5.20
9. Regulatory Guide 5.65
10. Regulatory Guide 5.66

B. A comprehensive listing and evaluation of all vital equipment, vital piping, vital power sources, vital water storage facilities, etc., shall be developed (A standard listing of vital equipment within the standard Design scope is given in Appendix 13B). This Listing and evaluation should include all support functions vital to equipment operation (e.g. diesel generator cooling water, D/G fuel, HVAC considerations for vital electrical equipment, cooling water for component cooling, etc). This listing and evaluation shall be controlled in accordance with current security safeguards information (SGI) procedures and guidelines.

C. The design of the security system shall include an evaluation of its impact on plant operation, testing, and maintenance. This evaluation shall assure that the security restrictions for access to equipment and plant regions are compatible with required operator actions during all operating and emergency modes of operation (i.e., loss of off-site power, access for fire protection, health physics, maintenance, testing and local operator), and shall include an evaluation of access control system failures.

14.2 SPECIFIC INFORMATION TO BE INCLUDED IN FSAR

14.2.1 SUMMARY OF TEST PROGRAM AND OBJECTIVES

14.2.1.1 Summary of the Startup Test Program

The Startup Test Program includes testing activities commencing with the completion of construction and installation and ending with the completion of the power ascension testing. This test program demonstrates that components and systems operate in acccrdance with design requirements and meet the requirements of 10 CFR 50, Appendix B, Criterion XI. The Startup Test Program results confirm that performance levels meet the operational safety requirements and verify the adequacy of component and system design and system operability over their operating ranges. It also aids in the establishment of baseline performance data and serves to verify that normal operating and emergency procedures accomplish their intended purposes. The Startup Test Program consists of Prerequisite Testing plus the following four phases:

A. Phase I: Preoperational Testing

B. Phase II: Fuel Loading and Post Core Hot Functional Testing

C. Phase III: Initial Criticality and Low Power Physics Testing

D. Phase IV: Power Ascension Testing

Specific Administrative Controls established for use during the Startup Program are addressed in the site-specific SAR. 14.2

14.2.1.1.1 Prerequisite Testing

Prerequisite Testing consists of tests and inspections required to assure construction is complete and that systems are ready for Phase I Testing.

Prerequisite testing verifies that construction activities associated with structures, components, and systems have been satisfactorily completed. Prerequisite testing consists of preliminary tests and inspections which include, but are not limited to, initial instrument calibration, flushing, cleaning, circuit integrity and separation checks, hydrostatic pressure tests, and functional tests of components. Delineation of specific prerequisite test requirements will be established in accordance with the site-specific administrative procedures.

Responsibilities associated with startup test programs include the preparation of test procedures, performance of applicable initial tests, and the preparation of appropriate test related documentation. Test procedures are prepared by the cognizant Startup or Operations Departments (as applicable) with assistance from ABB C-E, the architect engineer, and other vendors, as required. These procedures are subject to review and comment by the appropriate project organizations.

The organizations assigned responsibility for conducting the tests are responsible for establishing specific requirements for scheduling and accomplishing testing, as well as for providing the necessary direction and coordination of groups having responsibility for specific activities in the startup test program.

The site operator is responsible for specifying a startup organization for conducting the four phased test programs for the plant and for the technical and functional aspects of the Startup program including the conduct of the Prerequisite and Phases I through IV programs. These include the following responsibilities:

A. Approval of Startup Administrative Control Procedures.

B. Review and recommend approval of requests for modifications or changes required during the test program.

C. Approval of prerequisite and Phases I through IV test procedures.

D. Maintain liaison with the project vendors through onsite representatives keeping them informed of status, problems, and support requirements.

The COL Applicant is responsible for developing the specific organization and staffing level appropriate for its facility. 14-1

The site operator's startup organization consists of System Engineers who have assigned responsibility for specific systems and Startup Engineers who have responsibility for testing evolutions and/or specific tests.

14.2.2.2 Systems Engineer

A. Assigned responsibility for a specific system or subsystem.

B. Provide technical guidance and assistance in the preparation of test procedures.

C. Determine the testing requirements, sequence, and test method on assigned systems. Recommend plant scheduling changes as necessary to support the testing effort.

D. Coordinating resolution of problem areas by providing technical support and liaison with the Startup Organization and the A/E construction and design groups.

E. Providing startup assistance as requested.

14.2.2.11 Qualifications

The recommendations of Regulatory Guide 1.58 will be followed to insure that the qualification requirements, indoctrination, and training of personnel who perform inspections, examinations, and testing are accomplished and maintained.

14.2.2.12 Utilization of the Plant Staff

The plant operating, maintenance, and engineering personnel are utilized to the extent practicable during the Startup Test Program. The plant staff operates permanently installed and powered equipment for Phases I through IV and subsequent system tests. Service personnel such as instrument, chemistry, computer, radiation protection, and maintenance personnel are used extensively to perform tests and inspections applicable to their field of specialization.

14.2.3 TEST PROCEDURES

The site operator has the responsibility for assuring the preparation and designating the approval process for prerequisite and Phases I through IV test procedures. Detailed procedure guidelines and procedures provided by the appropriate design organization are utilized to develop various system test procedures. Thus, test procedures are based on requirements of system designers and applicable Regulatory Guides.

The COL Applicant is responsible for preparing the site-specific test procedures and/or guidelines that will be used for the conduct of the plant startup program. Submittal of these procedures and/or guidelines to the NRC Staff for review shall be conducted as described in Section 14.2.11. The COL Applicant will prepare a startup administrative manual. The COL Applicant will also provide preoperational and startup test summaries which contain testing objectives and acceptance criteria applicable for its scope of the plant design. The COL Applicant will develop a startup administrative manual and supporting documents that delineate plant operational conditions at which tests are to be conducted, testing methodologies to be utilized, specific data to be collected, and data reduction techniques. The startup administrative manual and supporting documents will be available for review during the COL application process. Testing performed at other than design operating conditions for systems will be reconciled either through the test acceptance criteria or post-test data analysis. The COL Applicant will provide this information in conjunction with the development of the startup manual. 14-2

E. System Initial Conditions

F. Environmental Conditions

G. Special Precautions

H. Detailed Procedure (Including Data Collection)

I. Restoration

J. Documentation of Test Results

Test procedures are reviewed as specified by the site-specific administrative control procedures. At the completion of these reviews, any required changes are incorporated into each test procedure by the originating organization.

14.2.3.3 Special Test Procedures

Special test procedures may become necessary during the Phases I through IV test program for investigative purposes. The preparation, review, and approval of these special procedures are governed by site-specific administrative control procedures. Special test procedures that deal with nuclear safety are processed under the same controls as normal startup test procedures.

14.2.4 CONDUCT OF TEST PROGRAM (PHASES I THROUGH IV)

The COL Applicant is responsible for planning and, subsequently, executing the plant startup program approved for the site-specific facility. 14-2

When a Phases I through IV system test procedure has been released for performance, a Startup Engineer will be assigned responsibility for:

A. Ensuring that prerequisites are satisfactorily met or allowable exceptions are noted in accordance with administrative procedures.

B. Verifying that the testing is performed as required by the procedure.

The test is then performed by operating personnel or others in accordance with the approved test procedure.

The Operations Shift Supervisor is responsible for the safe operation of the plant during testing and may stop any system test in progress and place the plant in a safe condition.

Required data resulting from the test is compiled within the test procedure in specified data blanks, on specially prepared data sheets, or as otherwise specified by administrative control

The startup testing phases (Phases II, III, and IV) of the test program are subdivided into the following categories:

A. Initial fuel load

B. Post-core hot functional testing

C. Initial criticality

D. Low power physics testing

E. Power ascension testing. It ends with the completion of testing at 100% power.

Each subdivision is a prerequisite which must be completed, reviewed, and approved before tests in the next category are started. Power ascension tests will be scheduled and conducted at pre-determined power levels.

The plateaus for the power ascension testing are indicated in Table 14.2-5. Results from each test conducted at a given plateau will be evaluated prior to proceeding to the next level. For those tests which result in a plant transient for which a realistic plant transient performance analysis has been performed, the test results will be compared to the results of the realistic transient analysis rather than the results of the transient analysis based on accident analysis assumptions.

Following completion of testing at 100% of rated power, final test results will be reviewed, evaluated, and approved.

14.2.6 TEST RECORDS

A single copy of each test procedure is designated as the official copy to be used for testing. The official copy and information specifically called for in the test procedure, such as completed data sheets, instrumentation calibration data and chart recordings, are retained for the life of the plant by the COL Applicant in accordance with Regulatory Guides for record retention. 14-3

14.2.7 CONFORMANCE OF TEST PROGRAMS WITH REGULATORY GUIDES

The Startup Test Program is consistent with the recommendations of the following Regulatory Guides associated with startup (with exceptions as noted and revisions as specified in Section 1.8):

Regulatory Guides: 1.9, 1.18, 1.20, 1.30, 1.37, 1.41, 1.52, 1.68, 1.68.2, 1.68.3, 1.79, 1.95, 1.108, 1.116, 1.118, 1.139 and 1.140.

14.2.7.1 Regulatory Guide 1.68, Initial Test Programs for Water-Cooled Reactor Power Plants

The following exceptions and/or clarifications address only significant differences between the proposed test program and the applicable regulatory position. Minor terminology differences, testing not applicable to the plant design, and testing that is part of required surveillance tests will not be addressed. Reference is made to the applicable portion of Regulatory Guide 1.68.

14.2.7.1.1 Reference Appendix A, Section 1.h.(5)

Cold Water Interlocks are not applicable to the System 80+ design. This testing will not be performed as it is not applicable.

14.2.7.1.2 Reference Appendix A, Section 1.i.(21)

A containment penetration cooling system is not a design requirement for the System 80+. This testing will not be performed as it is not applicable.

14.2.7.1.3 Reference Appendix A, Section 1.k.(2)

Personnel monitors and radiation survey instruments are site-specific items to be addressed by the site operator. The site operator will define the appropriate testing to demonstrate proper operation of personnel monitors and radiation survey instruments. 14-5

14.2.7.1.4 Reference Appendix A, Section 1.n.(15)

A shield cooling system is not a design requirement for the System 80+. This testing will not be performed as it is not applicable.

14.2.7.1.5 Reference Appendix A, Section 2.b

This section suggests that rod drop times be measured for all control element assemblies (CEAs) at hot and cold full-flow and no-flow conditions.

The CEA drop-time testing is consistent with the recommendations of the regulatory guide; however, tests which do not provide meaningful data will be deleted. As outlined in Test Summary (Section 14.2.12.2.4), the CEA drop-time testing will consist of:

A. One drop of each CEA at hot, full-flow conditions.

14.2.7.3 Regulatory Guide 1.68.3, Preoperational Testings of Instrument and Control Air Systems

Position C.9 requires that testing demonstrate that the plant equipment designated by design to be supplied by the Instrument Air System is not degraded when supplied by the Station Air System which may have less restrictive air quality requirements. The SYSTEM 80+ Instrument Air System has no interconnection to any other compressed Air System, and, therefore, ingress of less quality air is not possible. Consequently, Position C.9 does not apply.

14.2.7.4 Regulatory Guide 1.79, Preoperational Testing of Emergency Core Cooling Systems for Pressurized Water Reactors

The intent of Section C.1.c(2), Isolation Valve Test, is satisfied by opening the valves under maximum differential pressure (RCS at ambient pressure) using normal electrical power only. Conditions at the valve motor are independent of the power source for this test. The breaker response and the response of the valves to the "confirmatory open" signal is verified during the Integrated Safety Injection Actuation System Test.

14.2.7.5 Security System Test

The COL Applicant will develop the detailed description of test and acceptance criteria for the Security System. 14-6

14.2.8 UTILIZATION OF REACTOR OPERATING AND TESTING EXPERIENCE IN DEVELOPMENT OF INITIAL TEST PROGRAM

ABB C-E maintains an ongoing effort which continually provides feedback to its startup organization during the development of, and throughout, the Initial Test Program. This information reflects both ABB C-E operating and test experience and industry wide experience concerning Pressurized Water Reactors.

Unit Operations reviews reactor operating and testing experiences at other facilities similar in design and capacity to the unit starting up.

This review is accomplished by circulating Licensee Event Reports (LERs) or summaries of LERs and NRC I&E Bulletins, circulars, and Information Notices to Startup and Operation personnel so that pertinent information can be utilized in the startup program.

14.2.9 TRIAL USE OF PLANT OPERATING AND EMERGENCY PROCEDURES 14-4

The COL Applicant developed schedule for the development of the plant operating and emergency procedures should allow sufficient time for trial use of these procedures during the Initial Test Program. 14-4

14.2.10 INITIAL FUEL LOADING AND INITIAL CRITICALITY

14.2.10.1 Initial Fuel Loading

Overall direction, coordination, and control of the initial fuel loading evolution is the responsibility of the site operator. ABB C-E will provide technical assistance during the initial fuel loading evolution. 14-2

The fuel loading evolution will be controlled by use of approved plant procedures which will be used to establish plant

14.2.10.2.1 Safe Criticality Criteria

Criteria for ensuring a safe and controlled approach to criticality require:

A. That high flux trip setpoints be reduced to a value consistent with the Technical Specification limits.

B. That a sustained startup rate of one decade per minute not be exceeded.

C. That CEA withdrawal or boron dilution be suspended if unexplainable changes in neutron count rates are observed.

D. That CEA withdrawal or boron dilution be suspended if the extrapolated inverse count rate ratio predicts criticality outside the tolerance specified in the procedure.

E. That the Technical Specifications are met.

F. That criticality be anticipated at any time positive reactivity is added by CEA withdrawal or boron dilution.

G. That a minimum of one decade of overlap be observed between the startup and log safety channels of the ex-core nuclear instruments.

14.2.11 TEST PROGRAM SCHEDULE

The schedule for plant startup is developed by the COL Applicant to allow sufficient time to systematically perform the required testing in each phase. No specific time periods for each phase are required. 14-2

The scheduling of individual tests or test sequences is made to ensure that systems and components that are required to prevent or mitigate the consequences of postulated accidents are tested prior to fuel loading. Tests that require a substantial core power level for proper performance are performed at the lowest power level commensurate with obtaining acceptable test data.

Phase I test procedures are scheduled to be approved and available for review by the NRC inspectors at least 60 days prior to their scheduled performance date. Phases II through Phase IV Startup Test Program administrative control procedures, the majority of the individual test procedures, and the following milestone controlling procedures: Fuel Loading, Post-core HFT, Initial Criticality, Low Power Physics Test and Power Ascension, are scheduled to be approved and available for review at least 60 days prior to fuel load. The remaining individual test

procedures will be scheduled for approval and available for review by the NRC inspectors at least 60 days prior to their intended performance date.

14.2.11.1 Testing Sequence

The site operator shall specify the testing sequence to ensure that the plant's safety is not compromised during the test program. The test sequence should ensure that the conduct of a specific test does not place the plant in a condition for which untested systems would be relied on for safety. 14-2

15.7.3.4 Conclusions

This analysis assumes a catastrophic failure of the BAST. Although the BAST is a Seismic Category I ASME III Class 3 tank equipped with an overflow line, this analysis is considered to envelope any potential failure of a radioactive liquid containing tank located outdoors.

The results of this analysis should be used to establish site acceptance criteria for the minimum dilution flow required to limit the concentration at the nearest potable water source to less than 10 CFR Part 20, Appendix B of Sections 20.1001 - 20.2402, Table 2, Column 2 limits. This analysis is based on the once through purification of the letdown flow and liquid from the Equipment Drain Tank and Reactor Drain Tank. Also, average values for the concentration of the distillate and concentrate are assumed to determine the concentration factor in the Boric Acid Concentrator (BAC). The concentration of the influent stream to the BAC must be sampled to verify the concentration factor used is valid.

15-1

17.0 QUALITY ASSURANCE PROGRAM

17.1 QUALITY ASSURANCE DURING THE DESIGN PHASE

The ABB-CE Quality Assurance Program is described in the topical report CENPD-210-A, "Quality Assurance Program." The list of specific equipment covered by this program is contained in Table 3.2-1 of CESSAR-DC. In regard to Three Mile Island (TMI)-2 Item I.F.2, one part of subpart 3, (inclusion of QA personnel in design activities) is covered by the quality assurance program for the System 80+ design, described in CENP-210-A.

The COL Applicant will develop and implement a construction QA program [COL Item 17-1]. This will include the site-specific information to address the issues in TMI Action Plan Item II.J.3.1.

NC 17-1

17.1.1 VERIFICATION PROCESS FOR DESIGN BASIS EVENTS

The goal of the Design Certification Program is certification of the System 80+ Standard Plant design by the Nuclear Regulatory Commission under Part of the Code of Federal Regulations.

The starting point for the System 80+ Design Certification program was the System 80 design as represented by CESSAR-F (which holds a Final Design Approval from the NRC in conformance with existing regulations) and the Duke Power Company's Cherokee and Perkins (P-81) balance-of-plant (BOP) design. A full complement of final design detail is available for the System 80 Nuclear Steam Supply System (NSSS) and for CESSAR-F. The P-81 BOP design progressed to the PSAR stage and was awarded a Construction Permit by the NRC before the project was canceled.

Certain analyses of design bases events included in CESSAR-DC are not intended to be repeated by the COL applicant. Accordingly, such non-repetitive safety analyses have been subjected to design verification prior to an award of a contract. The traditional design verification process for a nuclear power plant, consistent with the requirements of NQA-1, is finished after the detailed design. However, in the design certification process, since a portion of the detailed design is yet to be completed, the design verification process cannot follow this sequence. In order to address the design verification needs for a Certified Design, the scope of the ABB-CE design verification process used for the System 80+ Standard Plant covers all the non-repetitive safety analyses. Specifically, these non-repetitive safety analyses include all the design basis event analyses presented in Chapters 5, 6, and 15; analyses that set safety-related design parameters, including those described in the Certified Design Material (CDM); and an Appendix 6B analysis performed to verify the System 80+ capability to safely handle a hypothetical small break LOCA-boron dilution event. In addition, the work performed outside the traditional NSSS design has been verified.

17.2 QUALITY ASSURANCE DURING THE OPERATIONS PHASE

The COL Applicant will develop and implement an operation QA program [COL Item 17-1]. This will include the site-specific information to address the issues in TMI Action Plan Items I.F.2 and II.J.3.1.

NC. 17-1

17.3 RELIABILITY ASSURANCE PROGRAM DURING THE DESIGN PHASE

This section presents the System 80+ Design Reliability Assurance Program (D-RAP).

17.3.1 INTRODUCTION

The System 80+ Design Reliability Assurance Program (D-RAP) is a program that will be performed by the designers during detailed design and specific equipment specification phases to assure that the important System 80+ reliability assumptions of the Probabilistic Risk Assessment (PRA) will be identified and considered throughout the plant life. The PRA evaluates the plant response to initiating events to assure that plant damage has a very low probability and risk to the public is very low. The PRA also evaluates improvements in overall plant safety relative to previous designs, and identifies the relative risk significance of the plant's structures, systems and components (SSCs). Input to the PRA includes details of the plant design and assumptions about the reliability of the plant risk-significant SSCs. The plant owner/operator will complete the site specific D-RAP and will have an operations reliability assurance process. The COL applicant/holder should incorporate the operational reliability assurance process objectives into existing programs (e.g., quality assurance or maintenance) that will monitor equipment performance to provide reasonable assurance that the plant is operated and maintained with an acceptably low risk commensurate with PRA assumptions. [COL Item 17-3].

17-2 17-3

The D-RAP will include the design evaluation of the System 80+. It will identify relevant aspects of plant operation, maintenance, and performance monitoring of important plant SSCs for owner/operator consideration in assuring safety of the equipment, maintenance of critical functions, and limited risk to the public. The policy and implementation procedures will be specified by the owner/operator (See Section 17.3.13).

Also included in this explanation of the D-RAP is a descriptive example of how the D-RAP will apply to one potentially important plant system, the Component Cooling Water System (CCWS). The CCWS example shows how the principles of D-RAP will be applied to other systems identified by the PRA as being significant with respect to risk.

17.3.2 SCOPE

The System 80+ D-RAP will include the design evaluation of the System 80+, and it will identify relevant aspects of plant operation, maintenance and performance monitoring of plant risk-significant SSCs. The PRA for the System 80+ and other industry sources will be used to identify and prioritize those SSCs that are important to prevent or mitigate plant transients or other events that could present a risk to the public.

The Project Director is responsible for the programmatic aspects of the plant design as well as the overall direction of the project, certification and licensing issues. The NSSS Design Manager is responsible for the design of the nuclear steam supply system. The Regulatory Conformance Manager has the responsibility of addressing any regulatory concerns and bringing these concerns to the attention of the Project Integration Manager and PRA and D-RAP Program Manager.

The Nuclear Steam Supply System (NSSS) Design Engineering organization is the core of the RAP and it is responsible for the design of the System 80+ NSSS. It is in this group where the NSSS design and drawings are developed with inputs from the mechanical, Instrument and Controls, Reactor, and Fluid Systems subgroups. It is also in this organization where the PRA models are developed as well as the Technical Specifications and plant procedures.

The PRA and D-RAP Program Manager is responsible for managing and integrating the D-RAP Program and has direct access to the System 80+ Project Integration Manager and is responsible for keeping him abreast of D-RAP critical items, program needs and status. The PRA and D-RAP Program Manager or his designee will attend all of the design review and progress meetings. He has organizational freedom to:

A. Identify D-RAP problems;

B. Initiate, recommend or provide solutions to problems through designated organizations;

C. Verify implementation of solutions; and

D. Function as an integral part of the design team and final design process.

The PRA and D-RAP Program Manager is in the Reliability Analysis Services Department which performs reliability analyses, risk assessments and PRAs. This group is part of ABB-CE Nuclear Services and reports to the NSSS Design Manager, through the PRA and D-RAP Program Manager (Figure 17.3-1). The PRA input to the D-RAP and any of the System 80+ reliability analyses will be performed in this organization and will be integrated into the System 80+ design.

The Quality Assurance organization provides quality control by performing regular audits and participating in the scheduled meetings to discuss System 80+ issues.

The COL applicant completing detailed design and equipment selection during the design phase, should submit its specific D-RAP organization for the NRC to review (See Section 17.3.13) [COL Item 17-2].

For those risk-significant SSCs, as indicated by the PRA or other sources, component redesign (including selection of a different component) will be considered as a way to reduce the Core Damage Frequency (CDF) contribution. (If the system unavailability or the CDF is acceptably low, less effort will be expended toward redesign). If there are practical ways to redesign a risk-significant SSC, it will be redesigned and the change in system fault tree results will be calculated. Following any redesign, dominant SSC failure modes will be identified so that protection against such failure modes can be accomplished by appropriate activities during plant life. The design considerations that will go into determining an acceptable, reliable design and the SSCs that should be considered for the operations reliability assurance process are illustrated in Figure 17.3-2.

Using the PRA or other design documents, the designer will identify to the COL applicant/holder the risk-significant SSCs, their associated failure modes and consequence, and reliability and availability assumptions, including any pertinent bases and uncertainties considered in the PRA. The designer will also provide this information for the COL applicant/holder to consider in developing an operations reliability assurance process to help assure that the PRA results will be achieved over the life of the plant. This information can be used by the COL applicant/holder for establishing appropriate reliability and availability targets and the associated maintenance practices for achieving them.

17-3

The COL applicant/holder shall develop, as part of the D-RAP and operations reliability asurance process, a life-cycle management plan to aid in the design and operation activities intended to achieve the design life objectives. The life-cycle management plan shall be initiated early enough ~~in~~ the design completion process to; 1) aid in the application, selection, and procurement of components with optimum design life characteristics, and 2) develop an aging management plan capable of assuring the plant's original design basis throughout its life.

The aging management plan shall cover (but not necessarily be limited to) containment structures, liner plates, embedded or buried structural components, piping, and other components. The plan shall consider the potential causes of corrosion which ultimately may be present at the site, including the potential corrosion from copper ground mats. The plan should be initiated early in the design process so that adequate provisions for mitigation measures can be made.

In developing the life-cycle management plan, the COL applicant/holder shall consider the design life requirements prescribed in Section 11.3 ["Design Life"] of the EPRI Utility Requirements Document (URD) and the insights gained from the Nuclear Plant Aging Research Program (e.g., NUREG/CR-4731 and NUREG/CR-5314).

operation. Maintenance that will be performed more frequently than refueling outages must be planned so as to not disrupt operation or be likely to cause reactor scram, engineered safety feature (ESF) actuation, or abnormal transients. Maintenance, planned for performance during refueling outages, must be conducted in such a way that it will have little or no impact on plant safety, on outage length, or on other maintenance work.

As plant experience data accumulates, the failure rates and human error rates in the operations reliability assurance process should be updated. These failure rates were used by the designer in the PRA.

The COL applicant should provide a complete operations reliability assurance process description to be reviewed by the NRC (see Section 17.3.13) [COL Item 17-3]. 17-3

17.3.10 OPERATIONS RELIABILITY ASSURANCE PROCESS

The operations reliability assurance process that is expected to be prepared and implemented by the COL applicant [COL Item 17-3], should make use of the information provided by the designer. This information will help the owner/operator determine activities that should be included in the operations reliability assurance process. Examples of elements that might be included are as follows: 17-3

this whole Section is bracketed

Reliability Performance Monitoring -- Measurement of the performance of equipment to determine that it is accomplishing its goals and/or that it will continue to operate with low probability of failure and high availability. Monitoring should preferably be predictive in nature to prevent loss of critical functions.

Reliability Methodology -- Methods by which the plant/operator can compare plant data to the SSC data in the PRA.

Problem Prioritization -- Identification, for each of the risk- significant SSCs, of the importance of that item as a contributor to its system unavailability and assignment of priorities to problems that are detected with such equipment.

Root Cause Analysis -- Determination, for problems that occur regarding reliability of risk-significant SSCs, of the root causes, those causes which, after correction, will not recur to again degrade the reliability of equipment.

Corrective Action Determination -- Identification of corrective actions needed to restore equipment to its required functional capability and reliability, based on the results of problem identification and root cause analysis.

Corrective Action Implementation -- Carrying out identified corrective action on risk-significant equipment to restore equipment to its intended function in such a way that plant safety is not compromised during work.

Corrective Action Verification -- Post-corrective action tasks to be followed after maintenance on risk-significant equipment to assure that such equipment will perform its intended functions.

Plant Aging -- Some of the risk-significant equipment is expected to undergo age related degradation that will require equipment replacement or refurbishment.

Feedback to Designer -- The plant owner/operator should periodically compare performance of risk-significant equipment to that specified in the PRA and D-RAP, and, at its discretion, may send SSC performance data to plant or equipment designers in those cases that consistently show performance below that specified. The plant owner/operator should consider participation in the CEOG.

Programmatic Interfaces -- Reliability assurance interfaces related to the work of the several organizations and personnel groups working on risk-significant SSCs.

Maintenance Rule Integration -- The plant owner/operator should consider the integration or interface of operations reliability assurance process and the requirements of 10 CFR 50.65 which require the operator to develop a maintenance program for risk significant SSCs or SSCs that could produce trips or transients.

17-3

The plant owner's operations reliability assurance process should address the interfaces with construction, startup testing, operations, maintenance, engineering, safety, licensing, quality assurance and procurement of replacement equipment.

17.3.11 D-RAP IMPLEMENTATION

An example of implementation of the D-RAP is given for the Component Cooling Water System (CCWS). This system was selected as an example because it was a support system and was found in the earlier System 80 PRA to contain risk-significant components. Because of this finding, and through the D-RAP organization described in Section 17.3.5, the design was changed. The design and analytical results, as presented in this chapter, is presented only as a D-RAP example and does not necessarily correspond to the current System 80+ design.

17.3.11.1 CCWS Function

The Component Cooling Water System (CCWS) is a closed loop system that provides cooling water flow to remove heat released from plant systems, structures, and components. The CCWS functions to cool the safety-related and non-safety-related reactor auxiliary loads.

Heat transferred by these components to the CCWS is rejected by the Station Service Water System (SSWS) via the CCWS heat exchangers.

17.3.13 COL INFORMATION

A. Policy and Implementation Procedures for D-RAP

[The COL applicant will specify the policy and implementation procedures for using D-RAP information. (See Subsection 17.3.1) [COL Item 17-2]] 17-2

B. D-RAP Organization

[The COL applicant completing its detailed design and equipment selection during the design phase, must submit its specific D-RAP organization for NRC review. (See Subsection 17.3.5) [COL Item 17-2]] 17-2

C. Provision for Operations Reliability Assurance Process

[The COL applicant will implement an operations reliability assurance process, to be reviewed by the NRC in the plant's maintenance program, QA program, or other existing programs. (See Subsection 17.3.9)[COL Item 17-3]] 17-3

Corrective Action Verification -- Post-corrective action tasks to be followed after maintenance on risk-significant equipment to assure that such equipment will perform its intended functions.

Plant Aging -- Some of the risk-significant equipment is expected to undergo age related degradation that will require equipment replacement or refurbishment.

Feedback to Designer -- The plant owner/operator should periodically compare performance of risk-significant equipment to that specified in the PRA and D-RAP, and, at its discretion, may send SSC performance data to plant or equipment designers in those cases that consistently show performance below that specified. The plant owner/operator should consider participation in the CEOG.

Programmatic Interfaces -- Reliability assurance interfaces related to the work of the several organizations and personnel groups working on risk-significant SSCs.

Maintenance Rule Integration -- The plant owner/operator should consider the integration or interface of operations reliability assurance process and the requirements of 10 CFR 50.65 which require the operator to develop a maintenance program for risk significant SSCs or SSCs that could produce trips or transients.

17-3

The plant owner's operations reliability assurance process should address the interfaces with construction, startup testing, operations, maintenance, engineering, safety, licensing, quality assurance and procurement of replacement equipment.

17.3.11 D-RAP IMPLEMENTATION

An example of implementation of the D-RAP is given for the Component Cooling Water System (CCWS). This system was selected as an example because it was a support system and was found in the earlier System 80 PRA to contain risk-significant components. Because of this finding, and through the D-RAP organization described in Section 17.3.5, the design was changed. The design and analytical results, as presented in this chapter, is presented only as a D-RAP example and does not necessarily correspond to the current System 80+ design.

17.3.11.1 CCWS Function

The Component Cooling Water System (CCWS) is a closed loop system that provides cooling water flow to remove heat released from plant systems, structures, and components. The CCWS functions to cool the safety-related and non-safety-related reactor auxiliary loads.

Heat transferred by these components to the CCWS is rejected by the Station Service Water System (SSWS) via the CCWS heat exchangers.

17.3.13 COL INFORMATION

A. Policy and Implementation Procedures for D-RAP

[The COL applicant will specify the policy and implementation procedures for using D-RAP information. (See Subsection 17.3.1) [COL Item 17-2]] 17-2

B. D-RAP Organization

[The COL applicant completing its detailed design and equipment selection during the design phase, must submit its specific D-RAP organization for NRC review. (See Subsection 17.3.5) [COL Item 17-2]] 17-2

C. Provision for Operations Reliability Assurance Process

[The COL applicant will implement an operations reliability assurance process, to be reviewed by the NRC in the plant's maintenance program, QA program, or other existing programs. (See Subsection 17.3.9)[COL Item 17-3]] 17-3

18.9.3 VALIDATION

18.9.3.1 Design Validation

The purpose of design validation is to ensure that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EPG provides a usable HSI ensemble that supports the successful accomplishment of the operator's required tasks. Design validation will be conducted using a facility that physically represents the MCR configuration and dynamically represents the operating characteristics and responses of the System 80+ design. Design validation includes operator interaction with the ensemble and EPG or operating sequences to meet the following objectives:

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

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

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

D. Validate the allocation of functions and support for operating crew situational awareness;

E. Validate operator communication and team interaction;

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

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

Each of the plant accident, abnormal, normal, and HSI and I&C equipment failure operating sequences will be performed on a facility that physically represents the MCR configuration and dynamically represents the operating characteristics and responses of the System 80+ design.

The design validation team will be debriefed after each scenario to identify and define discrepancies. These discrepancies will be documented. The design validation activities will be conducted until the completed control complex is validated.

18.9.3.2 Operating Ensemble Validation Plan

Information concerning the site operator's operating ensemble validation is within the site operator's scope and shall be provided in the site-specific SAR. 18-1

on the ratio of the DB to RLE and the criteria outlined in EPRI NP-6041-SL[176], the HCLPF was determined. Generic Equipment Ruggedness Spectra (GERS) were used where applicable.

Solid state switching devices and electromechanical relays will be used in the NUPLEX 80+ protection and control systems. Solid state switching devices are inherently immune to mechanical switching discontinuities such as contact chatter. Robust electromechanical relays are selected for NUPLEX 80+ applications such that inherent mechanical contact chatter is within the requisite system performance criteria. Therefore, contact chatter has no effect on system operation and was, therefore, not included in the seismic analysis. [The COL must confirm the use of seismically robust electromechanical relays in the engineered safety features actuation and control systems.] [COL Item 19-10]

19-10

Similarly, for equipment qualified by analysis, the design basis parameters, including damping and anchorage safety factors as well as response spectra, were assessed to determine seismic margins. For example, a seismic margin exists for an equipment item that is seismically qualified using 3% damping, if a higher 5% damping is permitted in the CDFM approach. Margins for each of the significant parameters were determined, and considered with inelastic energy absorption capability for ductile failure modes, to calculate HCLPFs. Seismic fragilities for equipment items that are inherently rugged were based on available industry data.

The NSSS components that were reviewed include:

A. Reactor Vessel
B. Steam Generators
C. Reactor Coolant Pumps
D. Reactor Internals
E. Pressurizer
F. NSSS Piping

These NSSS components were assessed by reviewing the various design basis parameters to identify seismic margins. The stress margins were determined by comparing the loads from the System 80+ RCS analysis and those in existing stress reports. Load combinations in accordance with Section 6 of EPRI NP-6041-SL[176] were evaluated. The HCLPF values were calculated using the CDFM approach and the equations discussed above.

Table 19.7.5.1-1 lists all components that are in the seismic models and presents either the failure rates for independent failures or the component or structure HCLPF value for seismic failures. Table 19.7.5.1-2 lists the structural fragilities calculated for the System 80+ structures and the NSSS component fragilities. All HCLPF values are presented in terms of peak ground acceleration.

capability sequence. The results of these sensitivity analyses are summarized in Table 19.7.5.3-2. This table defines the component or component group for which the HCLPF is being changed, presents the base component HCLPF and the changed component HCLPF, and presents the new "Min Sequence" HCLPF and the new plant HCLPF. These sensitivity analyses basically confirmed the intuitive importance of the component HCLPFs. That is, if the HCLPF for a component that appears as a dominant contributor to a sequence HCLPF is decreased below the plant or "Min Sequence" HCLPF values, the plant and/or "Min Sequence" HCLPF value will decrease to the lower value. On the other hand, if the HCLPF for that component or group of components is increased, the plant and "Min Sequence" HCLPF values do not change.

None of the seismic core damage sequences had a HCLPF less than two times the design basis earthquake. In addition, the dominant sequence is a seismically induced failure of the containment vessel which leads to core damage and containment failure. Therefore, no additional containment isolation failure analyses were performed.

The COL applicant will be required to verify that key assumptions for structures, systems and components considered in the SMA are valid for the as-built plant conditions [COL Item 19-4]. This will include evaluation of HCLPF values for structures which house non-safety related equipment relied upon in the SMA evaluations such as the combustion gas turbine. The verification process will include a seismic walkdown, including development of detailed procedures, [COL Item 19-4] to ensure that as-built conditions conform to the assumptions used in the SMA and to assure that proper anchorage for equipment has been provided and that the potential for seismic spatial system interaction does not exist. Deviations from assumptions will be evaluated to determine if vulnerabilities have been introduced. Also, if equipment is qualified for site-specific requirements (Appendix 3.9A, Section 1.4.3.2.1.2, Option 4), the impact on the SMA HCLPF will be evaluated.

The details for verifying that key assumptions for structures, systems, and components considered in the SMA are valid for as-built plant conditions should be modeled after approved NRC SMA procedures and should incorporate insights from SMAs conducted at operating plants. The verification process is expected to consist of the following steps:

1. Preparation for Plant Walkdown

2. Plant Seismic Logic Model Walkdown

3. Assessment of As-Built SMA HCLPF Values

4. Seismic Plant Walkdown

5. Validation of Plant Level HCLPF Calculations

These steps will ensure that as-built plant design characteristics are evaluated; critical component, structural, and sequence HCLPF values are reviewed; and deviations from design assumptions and vulnerabilities which could reduce the plant level HCLPF value below 0.5g are exposed.

19-4

In Section 19.1.2.2.3 (page 19-149) of the Draft Safety Evaluation Report for CESSAR-DC, it stated:

> "As the seismic analysis is being redone, there is a need to augment the internal events model to the extent possible, by explicit inclusion of structural and other passive failures that were excluded from the internal events model."

19-2

This is COL action Item 19-2. As part of the model development for the Seismic Margins Analysis, the internal events model was updated to include structural and passive failures. This completes COL action item 19-2.

The Draft Safety Analysis Report for CESSAR-DC contained an additional COL Item, 19.1.2.2.6-1, (Item 19-6 in Table 1.10-1) which stated that the COL Applicant should factor site-specific spectra into the analysis and verify the layout and anchorage of critical components. This COL Item is covered by the SMA and the seismic walkdown to be performed by the COL applicant as discussed above.

A-46

D. The concept of defense in depth applies to shutdown modes as well as Mode 1. The more ways that the operator can maintain coolant inventory and remove decay heat, the lower the risk. The presence of SIS capability in shutdown is an example of added defense in depth.

E. The ability of the operator to be able to align the SCS train for makeup of inventory or to use for a feed and bleed operation is important for defense in depth.

F. There are two trains of SCS and it is important that the COL applicant maintain a configuration management system for maintenance activities on the SCS and its support systems. Configuration control is important because all plant risks, all accidents and incidents, and all accident precursors arise because of critical configurations which have occurred. If configurations were managed so that critical, high-risk configurations did not occur, then the risks would be small and accidents or incidents would occur rarely. Table 19.8.1-4 (developed from the more extended dependency Table 19.6.1-1) is an example of the systems that support each SCS train. The COL applicant should identify the systems, structures and components (SSCs) that support DHR (as well as other safety functions). The COL applicant should consider the overall effect of removing SSCs identified above from service on the DHR safety function. The COL applicant should limit normal maintenance on combinations of equipment so that an additional single or common cause failure would not cause total loss of DHR. A configuration management system should help to insure the availability of the standby SCS.

19-9

G. If one train is lost because of fire, flood, or random component failure, it is important that the other train have the highest possible availability. The COL applicant should develop procedures and a configuration management strategy to handle the period of time when one of the two DHR paths is unavailable. In this case (a technical specification violation) the operator should suspend the maintenance and testing activities on equipment that support the operating SCS train. Given failure of one train, the operator should restore any systems that support the other train and are out for maintenance.

H. During plant shutdown, risk can be minimized by appropriate outage management, administrative controls, procedures and operator knowledge of plant configuration. The COL applicant should develop the appropriate administrative controls, procedures and operator training for shutdown operations. (See also insights F, ~~and~~ G ~~above~~ and I.) [COL Item 19-9]

I. During plant shutdown operation, the integrity of fire and flood barriers between areas in the same division, such as quadrants, where systems comprising the alternate shutdown are located should be maintained. The COL applicant should incorporate in its configuration control program a requirement that, during Modes 4, 5, and 6, the water tight flood doors and fire doors will be maintained closed on at least one quadrant within the subsphere (containing either an SCS or CSS pump) to help prevent common-mode failures from internal floods or fires. The SCS or CSS pump in this quadrant shall be operable. If the flood or fire doors to this quadrant must be opened for reasons other than to permit normal access, a fire watch will be established for the affected door. [COL Item 19-9]

NC
A-9

Loss of DHR Insights

A. Reduced inventory is the most critical operation. The operator should be aware of this and plant activities should be scheduled accordingly. Use of nozzle dams is encouraged as a method of limiting the time spent in this mode.

I. During plant shutdown operation, the integrity of fire and flood barriers between areas in the same division, such as quadrants, where systems comprising the alternate shutdown are located should be maintained. [The COL applicant should incorporate in its configuration control program a requirement that, during Modes 4, 5, and 6, the water tight flood doors and fire doors will be maintained closed on at least one quadrant within the subsphere (containing either an SCS or CSS pump) to help prevent common-mode failures from internal floods or fires. The SCS or CSS pump in this quadrant shall be operable. If the flood or fire doors to this quadrant must be opened for reasons other than to permit normal access, a fire watch will be established for the affected door. [COL Item 19-9]]

NC 19-9

Loss of DHR Insights

A. Reduced inventory is the most critical operation. The operator should be aware of this and plant activities should be scheduled accordingly. Use of nozzle dams is encouraged as a method of limiting the time spent in this mode.

2.1 PROCEDURES

2.1.1 ISSUE

The operational guidance provided by the plant designer to the owner/operator might not be sufficient to ensure that procedures to avoid, detect, mitigate, and/or recover from abnormal events initiated from shutdown operations can be developed by the plant owner/operator.

2.1.2 ACCEPTANCE CRITERIA

The operational guidance provided by the plant designer to the owner/operator shall be sufficient to properly utilize design features that are available to detect, mitigate and assist recovery from abnormal events initiated during shutdown operations.

2.1.3 DISCUSSION

The System 80+ design incorporates advanced features which promote safer and simpler plant operation. The features include redundancy and diversity of components and systems, dedicated and/or permanently aligned systems, and an advanced information system which better informs the operations staff of plant status, potential adverse system interactions, and available recovery paths if an abnormal event occurs. These features also contribute to improved operability and maintainability that should significantly reduce the initiating situations that have contributed to increased shutdown risk.

19-9

The plant owner/operator is responsible for preparing detailed procedures for normal, abnormal, and emergency operations using guidance developed by the plant designer and plant site specific information. The plant designer's guidance generally is in the form of suggested operational sequences that preserve the safety bases of the design. Since shutdown operations must be intimately connected to an outage strategy, specific procedures cannot be imposed by the plant designer to cover the array of possible shutdown events. However, the plant designer can provide guides which instruct the plant owner/operator in the use of design features which can detect, mitigate, and assist recovery from abnormal events that can occur during shutdown operations.

The operational guidance contained in this appendix will be provided to the plant owner/operator through the plant designer's Operational Support Information (OSI) program. The intent of the OSI program is to insure that features of the System 80+ design are effectively utilized in the operation of the plant as specified in the plant owner/operator's operations program. The OSI program also provides a formal means to transfer design related bases for operations, regulatory operational commitments and related information that is typically provided to and required by a plant license applicant. The OSI program is staged to develop more detailed information as the plant design matures and is expected to be completed during the

Section 19.15.1. Insights about the System 80+ design gained from the internal events risk profile and the external events risk profile are summarized in Sections 19.15.2 and 19.15.3, respectively. Shutdown and low-power operation are included as part of the System 80+ PRA, and the insights gained from the risk associated with these modes of operation are summarized in Section 19.15.4. The use of PRA in the design process is summarized in Section 19.15.5. The use of PRA results and insights to support certification and followup activities is summarized in Section 19.15.7. Significant PRA-based safety insights for the System 80+ design are provided in Table 19.15-1.

During the detailed design phase for System 80+, site specific information and system design details will become available. The COL applicant should update the PRA using the final design information and site specific information. As deemed necessary, the update should include the shutdown risk evaluation and the internal fire and flood evaluation. Based on site specific information, the COL applicant should also re-evaluate the qualitative screening of external events. If any site specific vulnerabilities are found, the applicable external event(s) should be included in the updated PRA. [COL Item 19-6]

In updating the internal fire evaluation, the COL applicant should verify the details and layout of critical components and the fire suppression systems. [COL Item 19-3] The applicant should also evaluate the potential effect of the fire suppression systems on the behavior of other systems. [COL Item 19-3]

In updating the internal flood evaluation, the COL should evaluate the interaction of the potential internal flood sources and the details of the layout of the critical components. [COL Item 19-3]

TABLE 19.15-1

(Sheet 1 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
1. The COL applicant should perform a seismic walkdown to ensure that the as-built plant conforms to the assumptions in the System 80 + PRA -based seismic margins analysis and to assure that seismic spatial systems interactions do not exist. Details of the seismic walkdown will be developed by the COL applicant.	COL Item 19-4 Section 19.7.5.3
2. ABB-CE will maintain a list of the SSC HCLPF values used in the System 80+ Seismic Margins Assessment in the D-RAP. The COL Applicant should compare the as-built SSC HCLPFs to those assumed in the System 80+ seismic margins analysis (SMA). Deviations from the HCLPF values or assumptions in the SMA should be evaluated by the COL Applicant to determine if any vulnerabilities have been introduced.	COL Item 19-4 Section 19.7.5.3
3. ABB-CE will maintain a list of risk significant SSCs in the D-RAP	D-RAP
4. The COL will maintain an O-RAP based on the system reliability information derived from the PRA and other sources. The COL Applicant should incorporate the list of risk important systems, structures and components (SSCs) as presented in Table 19.15.6-1 in its D-RAP and O-RAP.	COL Item 17-3 Section 17.3.1 COL Item 19-7 Section 19.15.6
5. Integrity of divisional separation between redundant safety-related equipment is a key assumption in the System 80+ fire and flood risk analyses. This divisional separation, which is extended also in the service water and component cooling water structures, prevents fires and floods from propagating from one division to the other. There are no doors or passageways connecting the divisions of safety-related equipment up to elevation 70+0.	Addressed in all safety-related structures and systems. Certified Design Material
6. The control room has its own dedicated ventilation system. This eliminates the possibility of smoke, hot gases, and fire suppressants, originated in areas outside the main control room, to migrate via the ventilation system to the control room.	Certified Design Material

1. COL information item;
See DCD introduction 1.5 2.

TABLE 19.15-1

(Sheet 3 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
12. [[During plant shutdown operation, the integrity of fire and flood barriers between areas in same division, such as quadrants, where systems comprising the alternate shutdown success paths are located, should be maintained. This will require configuration control of fire/flood barriers for shutdown operation by the COL applicant.]] [[The COL applicant should incorporate in its configuration control program a requirement that, during modes 4, 5, and 6, the water tight flood doors and fire doors will be maintained closed on at least one quadrant within the subsphere (containing either an SCS or CSS pump) to help prevent common-mode failures from internal floods or fires. The SCS or CSS pump in this quadrant shall be operable. If the flood or fire doors in this quadrant must be opened for reasons other than to permit normal access, a fire watch will be established for the affected door.]]	[[COL Item 19-9 Section 19.8.1.2]][1] [[COL Item 19-9 Section 19.8.1.2]][1]
13. The grid system for System 80+ will include at least two preferred power circuits, each having sufficient capacity. They will be continuously energized and available to provide power to safety related loads. The two designated offsite power transmission lines shall be designed and routed to minimize, to the extent practicable, the likelihood of their simultaneous failure. These circuits shall be routed to ensure no single event, such as a tower falling or a line breaking can simultaneously affect both circuits in a way such that neither can be returned to service. The two offsite power circuits shall terminate at two switchyards that are physically separate and electrically independent to the extent practicable.	Certified Design Material
14. [[During plant shutdown, risk can be minimized by appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration. This will be an important COL applicant activity.]]	[[COL Item 19-9 Section 19.8.1.2]][1]
15. Divisional separation exists also between redundant charging pumps and their power supplies and redundant trains of instrument air.	Figure 1.2-4 Sections 8.3.1.1.2.1 & 9.3.1.2.1

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 4 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
16. [The COL applicant will develop procedures for manually aligning the alternate AC power supply (combustion turbine) when one of the two diesel generators is unavailable during a loss of offsite power event].	[COL Item 19-8][1].
Breakers between the Permanent Non-Safety (PNS) and the class 1E buses will be interlocked so that a PNS bus cannot be aligned to a class 1E bus that is being powered by an EDG.	Certified Design Material
17. To provide sufficient diversity and defense in depth to mitigate all postulated accidents, even assuming a common cause failure within the Plant Protection System, the System 80+ Instrumentation and Control Systems provides the Manual Hardwired ESFAS Actuation System for the controls, and for display there are Hardwired Key Indications of Critical Function Status for post accident monitoring.	Certified Design Material

during

For display

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 13 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
29. A control room fire will not impact the instrumentation and controls located at the Remote Shutdown Panel, or the equipment which is required to place the plant in cold shutdown, due to the following features of the System 80+ design:	
The main control room and the remote shutdown room are located at different elevations and in different fire areas.	Certified Design Material
The main control room ventilation system is different from the ventilation system for the remote shutdown room.	Certified Design Material
The stairwells connecting the main control room and the remote shutdown room are pressurized, thus not allowing smoke, hot gases and fire suppressants to migrate from one room to the other.	Section 9.4, Figures 1.2-5A through 1.2-9
The main control room is continuously pressurized to prevent the entry of smoke, hot gases, dirt and fire suppressants from other areas.	Certified Design Material
30. All fire barriers which provide separation between the two divisions are rated for at least 3 hours.	Certified Design Material
It was assumed that all fire doors and penetrations within the fire barriers are maintained with high reliability during power operation to prevent the propagation of fire from one area to the next.	D-RAP
31. The possible sources of internal flooding within the Nuclear Annex and Reactor Building are located below elevation 70+0.	Certified Design Material
32. [[Solid state switching devices and electro-mechanical relays resistant to relay chatter will be used in the Nuplex 80+ protection and control systems.]] Use of these devices and relays either eliminates or minimizes the mechanical discontinuities associates with similar devices at operating reactors.	Sections 7.1.1.7, 7.2.1.1 & 7.3.1.1 [[COL Item 19-10 (Relay Chatter Resistance)]].
33. The Startup Feedwater System (SFWS), a non-safety related system, can be used to deliver feedwater to the SGs following a reactor trip. The SFWS pump is powered from the Permanent Non-Safety (PNS) bus and can be powered by the AAC. The SFWS pump can be aligned to the CST or the deaerator storage tank. With alignment to either storage facility, the NPSH for the pump is adequate to prevent pump cavitation and failure.	Sections 10.4.7.2.3 & 10.4.7.2.4 Figure 8.3.1-1

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 14 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
34. There will be a diverse RCP seal injection capability using a positive displacement pump that is diverse from the CVCS and can be powered from either the EDG or the AAC. The alternative positive displacement seal injection pump is located in such a manner as to minimize its vulnerability to internal floods and fires that could also affect the primary means of providing RCP seal cooling or RCP seal injection.	Certified Design Material Figure 1.2-5A
35. An emergency containment spray backup function provides a means of supplying water to the containment spray header from a station AC independent external source. The final design of the ECSBS is not completed. The design of the ECSBS is envisioned to include the following design features: (1) an 8-inch diameter "tee" connection to the containment spray recirculation line, (2) an extension of 8-inch diameter Class 2 piping from the "tee" connection from the containment spray recirculation line to the exterior of the Nuclear Annex, (3) external connections for temporary hookup of an external source of water that are located at or near grade, (4) a portable pumping source (e.g., fire truck) that is independent of site AC power buses. This pumping device will be capable of supplying sufficient flow to the containment spray header at 24 hours after a severe accident to provide sufficient heat removal capability via the spray droplets to prevent the containment pressure from exceeding the service level C pressure. Preliminary calculations indicate a flow rate of 750 gpm would be sufficient, and (5) all necessary hoses, fittings and spool pieces would be stored with the pumping device or at or near the "tee" connections.	Certified Design Material Sections 6.5.5 and 19.11.3.8
[[The detailed system design and location of all associated valves and connections should take into account expected radiation levels and shielding requirements for any required local operator actions]]'	[[COL Item 19-5 Sections 19.11.3.8 and 6.5.5]].'
[[The specific flow rate for the pumping device will be determined as part of the detailed design]].'	[[COL Item 19-5 Section 19.11.3.8 and 6.5.5]].'
[[Detailed procedures for use of the system will be developed by the COL applicant]]'	[[COL Item 19-8 Section 19.15.6]].'

1. COL information item; see DCD information section 1.5.2.

TABLE 19.15-1

(Sheet 15 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
36. There is a Hydrogen Mitigation System (HMS) utilizing ignitors to control hydrogen during a severe accident.	Certified Design Material
[[The accident management procedures will address use of the HMS.]][1]	[[COL Item 19-8 Section 19.15.6]]
37. The Hydrogen purge Vent to the annulus is not credited in the PRA. However, the use of this vent could decrease the late containment failure probability.	EOGs
38. Each half of the subsphere is compartmentalized to separate redundant safe shutdown components, to the extent practicable while maintaining accessibility requirements. The subsphere, which houses the front line safety systems is compartmentalized into quadrants, with two quadrants on either side of the divisional structural wall. Flood barriers provide separation between quadrants, while maintaining equipment removal capability. Emergency feedwater pumps are located in separate compartments within the quadrants with each compartment protected by flood barriers. Flood barriers also provide separation between electrical equipment and fluid mechanical systems at the lowest elevation within the Nuclear Annex.	Certified Design Material
Elevated equipment pads prevent equipment from being inundated in the event of flooding.	Section 3.4.4.1
There are three-hour fire barriers as well as flood barriers between quadrants in the subsphere.	Certified Design Material
Within each division, there are two Class 1E 4160 KV (4.16 KV) switchgears. These are separated by three-hour fire barriers and are arranged to be associated with one of the subsphere quadrants. Power cables from the diesel generator room in a given division to their associated switchgear are fully separated, and the cables from the switchgear to their associated pumps are fully separated.	Section 9.5.1.14

1. COL information item; see DCD introduction Section 1.5.2.

TABLE 19.15-1

(Sheet 16 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
39. Flood protection is integrated into the floor drainage systems. The floor drainage systems are separated by division and Safety Class 3, Seismic Category 1 valves which prevent backflow of water to areas containing safety related equipment. Each subsphere quadrant contains its own separate sump equipped with redundant Safety Class 3, Seismic Category 1 sump pumps and associated instrumentation. These pumps are also powered from the diesel generators in the event of loss of offsite power. The Nuclear Annex also has its own divisionally separated floor drainage system, having no common drain lines between divisions. Floors are gently sloped to allow good drainage to the divisional sumps. Floor drains are routed to the lowest elevation to prevent flooding of the upper elevations. The lowest elevation in each division has adequate volume to collect water from a break in any system without flooding the other division. In addition, potential discharge of fixed fire suppression systems and fire hoses is considered in the sizing of floor drains to preclude flooding of areas should the fire protection systems be initiated.	Certified Design Material Section 9.3.3
40 [[The COL should maintain a well trained and prepared fire brigade]]. 1	Section 19.15.3.2
41. The System 80+ low pressure systems which interface with the RCS are protected against ISLOCA by a combination of increases in the piping pressure limits and autoisolation capability based on pressure sensors.	Certified Design Material
42 [[The COL applicant should consider the information on risk important operator actions from the PRA as presented in Table 19.15.6-2 in developing and implementing procedures, training and other human reliability related programs]]. 1	[[COL Item 19-8 Section 19.15.6]]. 1
43 [[During detailed design phase, the COL applicant should update the PRA using the final design information and site specific information. As deemed necessary, the COL applicant should update the PRA, including the shutdown risk evaluation, and the internal fire and flood evaluation. Based on site specific information, the COL applicant should also re-evaluate the qualitative screening of external events. If any site specific susceptibilities are found, the applicable external event should be included in the updated PRA]]. 1	[[COL Item 19-6 Section 19.15]]. 1

1. COL information item;
See DCD Introduction Section 1.5.2.

TABLE 19.15-1

(Sheet 17 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
44. The structure that houses the combustion gas turbine must have a HCLPF of at least that of the gas turbine itself, or must be designed in such a manner so that failure of this structure following a seismic event up to HCLPF of the gas turbine will not affect the operability of the gas turbine.	Section 19.7.5.3
45. During the HFE V&V, the risk significance of tasks impacted by findings will be considered in the finding resolution process. The resolution process will qualitatively confirm that the findings, as dispositioned, will not lead to a risk-significant increase in error potential from that represented in the HRA, or additional risk-significant errors not modeled in the HRA. ("Human Factors Engineering Verification and Validation Plan for NUPLEX 80+", NPX80-IC-VP790-03, Section 8.1)	Supports Certified Design Material
46. No water lines are routed above or through the control room and the computer room. HVAC water lines contained in rooms around the control room are located in rooms with raised curbs to prevent leakage from entering the control room.	Section 3.4
47. A reactor cavity flood system is provided to enhance the coolability of ex-vessel core debris. [[Procedures for use of the cavity flood system during a severe accident will be developed by the COL applicant as part of their plant-specific severe accident management procedures. The reliability of the cavity flood system and associated valves is important. The COL applicant will ensure the reliability of the cavity flood system.]][1]	Certified Design Material [[COL Item 19-8, Section 19.15.6]]. D-RAP, Table 19.15.6-1

1. COL information item; see DCD introduction section 1.5.2.

19.15.3 EXTERNAL EVENTS RISK PROFILE INSIGHTS

The external events analyses for the System 80+ design included both qualitative and quantitative analyses. Bounding site characteristics were used for the quantitative analyses to minimize potential future restrictions on plant siting. The qualitative external events evaluation involved the following: (1) identification of the external events to be considered, (2) grouping of events with similar plant effects and consequences, (3) establishment of screening criteria to eliminate events that are insignificant contributors to risk, and (4) identification of events that require further quantitative evaluation. Based on the qualitative evaluation, most of the external events were eliminated from further quantitative evaluation. Four external events (tornado, fire, flood, and seismic) were identified as having the potential to induce system failures and therefore required further quantitative evaluation.

The major findings and insights obtained for tornados, fires, floods, and seismic events are provided in Sections 19.15.3.1, 19.15.3.2, 19.15.3.3, and 19.15.3.4, respectively.

19.15.3.1 Insights from the Tornado Strike Analysis

The core damage frequency due to tornado strike events is calculated to be 2.5E-07 per year. The dominant contributors to the core damage frequency of tornado strike events are provided in Table 19.15.3-1. For the System 80+ PRA, the following assumptions were made for the tornado strike accident sequences.

A. It was assumed that offsite power will be lost for more than 24 hours and the plant will rely on the emergency diesel generators during this period.

B. The turbine/generator will be unable to run back and pickup hotel loads following a tornado strike.

C. The alternate AC power source was conservatively assumed to be unavailable following a tornado strike.

D. The Station Service Water System (SSWS) intake structure was assumed to be vulnerable to accumulation of debris due a tornado strike event and was included in the models. The protection of the SSWS intake structure against the accumulation of debris due to a tornado strike could prevent or minimize the loss of suction to the SSWS pumps. The COL applicant should re-evaluate the vulnerability of the SSWP intake to tornado-generated debris. [COL Item 19-1]

NC 19-1

E. Safety related structures outside the nuclear island will not be destroyed by a tornado strike.

19.15.6 RISK SIGNIFICANT SSCs FOR CONSIDERATION IN THE RAP AND OTHER ACTIVITIES

Table 19.15.6-1 presents a list of risk significant Systems Structures and Components (SSCs) that should be included in the D-RAP as described in Section 17.3. The COL applicant should consider inclusion of these SSCs in their D-RAP and operations reliability assurance process [COL Item 19-7]. These SSCs were selected based on their risk importance as determined in the Level 1 analyses, the Level 2 analyses, the Level 3 analyses, the shutdown risk evaluation, the internal fire and flood evaluation, and the seismic margins evaluation. For the Level 1 analyses and the shutdown risk analyses, systems and components were included as risk significant if their Risk Achievement Worth (RAW) was greater than or equal to 5.0 or their Risk Reduction Worth (RRW) was 1.10 or greater. SSCs with a RAW between 2.0 and 5.0 were selected if their RRW was greater than 1.05. For the Seismic Margins Assessment, a SSC was included if it was a dominant contributor to the Plant HCLPF. For the Level 2, Level 3, and internal fire and flood analyses, items were included based on engineering judgement. SSCs were also included in the list if specific engineering commitments were made by the system designers. Table 19.15.6-1 contains three columns. The first column identifies the system, structure or component. The second column presents the rationale (basis) for including the SSC in the D-RAP (i.e., RAW > 5.0, Level 2 considerations, engineering judgement, engineering commitment, etc.). The third column briefly describes the item and any associated insights. The third column also identifies any test interval or maintenance assumptions that were used in the PRA. This table does not include any failure rate or unavailability information. All component failure rates are documented in Section 19.5 and its associated appendices. The random failure rates for the individual components for the specific failure modes of concern are summarized in Table 19.5-2. The common cause failure rates are summarized in Table 19.5-3. The maintenance unavailabilities are summarized in Table 19.5-4. The component and structure HCLPF values are summarized in Tables 19.7.5.1-1 and 19.7.5.1-2. Table 3.9-15 summarizes the In-Service Testing program for all safety related pumps and valves and presents the applicable test intervals.

NC 19-7

Table 19.15.6-2 presents a list of Important Operator Actions selected from the PRA. These operator actions were selected based on their risk importance as determined in the Level 1 analyses, the Level 2 analyses, the Level 3 analyses, the shutdown risk evaluation, the internal fire and flood evaluation, and the seismic margins evaluation. For the Level 1 analyses and the shutdown risk analyses, operator actions were included as important if their Risk Achievement Worth (RAW) was greater than or equal to 5.0 or their Risk Reduction Worth (RRW) was 1.10 or greater. Operator actions with a RAW between 2.0 and 5.0 were selected if their RRW was greater than 1.05. For the Seismic Margins Assessment, an operator action was included if failure to

perform that action could result in a lower overall plant HCLPF value. For Level 2, Level 3, and internal fire and flood analyses, items were included based on engineering judgement.

The COL applicant is responsible for developing all plant procedures. These procedures include, but are not limited to, the normal operating procedures, system operating procedures, maintenance procedures, emergency operating procedures and severe accident procedures. The Emergency Operating Guidelines (EOGs) provide guidance to the COL applicant for developing the detailed Emergency Operating Procedures. Appendices to the EOGs provide guidance on severe accident procedures and emergency operating considerations during shutdown operations. In developing and implementing procedures, training and other human reliability related programs, the COL applicant should consider the information on risk important operator actions presented in Table 19.15.6-2. [COL Item 19-8]

In the severe accident management procedures, the COL applicant should include procedures for the use of the Cavity Flood System, the Hydrogen Mitigation System, and the Emergency Containment Spray Backup function of the CSS. [COL Item 19-8]

The COL should develop procedures for manually aligning the Alternate AC power supply when one of the two emergency diesel generators is unavailable during a loss of offsite power. [COL Item 19-8]

In particular, the determination of core damage frequency attributable to internal events (e.g., LOCAs and Loss Of Offsite Power) used the standard small-event-tree/large-fault-tree methodology, with full fault tree linking used for the solution of core damage event sequences. External events such as tornadoes and earthquakes are also addressed in the PRA. The evaluation of the containment performance employed methodologies consistent with NUREG-1150 (Reference 1). The determination of public risk was based on a calculation of the radiological dose at one-half mile from the plant using bounding site characteristics supplied by EPRI. The methodology employed was consistent with the methodology described in NUREG-2300 (Reference 2). The results of this PRA show that the System 80+ Standard Design plant meets the industry goal of a mean severe core damage frequency of less than $1x10^{-5}$ per reactor year and a mean frequency for occurrence of doses greater than 25 REM beyond one-half mile radius from the reactor of less than $1x10^{-6}$ events per reactor year.

A Design Reliability Assurance Program ensures that PRA assumptions and basic results are provided as input to the owner's operations reliability assurance process (see Section 17.3).

In summary, a PRA has been performed for the System 80+ Standard Design and meets the requirements of the Standardization Rule, (10 CFR 52). Requiring the owner-operator to implement an operability assurance program is intended to ensure that the PRA remains valid during plant operation. Therefore, this issue is resolved for the System 80+ Standard Design.

REFERENCES

1. NUREG-1150, "Reactor Risk Reference Document", U.S. Nuclear Regulatory Commission, January 1987.

2. NUREG-2300, "PRA Procedures Guide", U.S. Nuclear Regulatory Commission, January 1983.

20.2.106 PERFORMANCE TESTING OF PWR SAFETY AND RELIEF VALVES

ISSUE

Generic Safety Issue II.D.1 addresses the guidance identified in NUREG-0737 (Reference 1) for qualification testing to be performed on the block, relief, and safety valves of the Reactor Coolant System (RCS).

After the TMI accident, the NRC determined that there was a need for performance testing of the RCS block, relief, and safety valves. This determination was made because the TMI accident demonstrated that these RCS valves may not operate as expected. The NRC established new guidance in NUREG-0737 which addresses the qualification testing of these valves. Qualification testing of these valves includes testing based upon both normal and accident conditions.

ATTACHMENT 3

Table 1-2: Index of ADM Items Requiring NRC Approval for Change

Item	Reference
ASME Boiler & Pressure Vessel Code, Section III	Table 1-3
AISC-N690 and ACI-349 Industrial Codes	Tables 1-4, 1-5
Design, Qualification and Preoperational Testing for Motor-Operated Valves	Table 1-6
Equipment Seismic Qualification Methods	Table 1-7
Piping Design Acceptance Criteria	Table 1-8
First Cycle Fuel and Control Rod Design	Table 1-9
Instrumentation & Controls Setpoint Methodology	Table 1-10
Instrumentation & Controls Hardware and Software Changes	Table 1-11
Instrumentation & Controls Environmental Qualification	Table 1-12
Control Room Human Factors Engineering	Table 1-13

Note: The applicable portion of the designated Tier 2 reference material specified in Tables 1-3 through 1-13 is shown italicized within the identified Approved Design Material [ADM] text or table.

Table 1-3: ASME Boiler & Pressure Vessel Code, Section III

Commitment	ADM Reference
ASME Boiler and Pressure Vessel Code, Section III, Rules for Construction of Nuclear Power Plant Components, Divison I, Division II	Table 1.8-6
ASME Boiler and Pressure Vessel Code, Section III, Division 1, Subsection NE, "Class MC Components"	3.8.2.2

Table 1-4: AISC-N690 Industrial Code

Commitment	ADM Reference
AISC-N690, Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities	Table 1.8-6
Analysis and Design of Seismic Category I Steel Structures	3.8.4.5.2

Table 1-5: ACI-349 Industrial Code

Commitment	ADM Reference
ACI-349, Code Requirements for Nuclear Safety-Related Concrete Structures	Table 1.8-6
Analysis and design of Seismic Category I Concrete Structures	3.8.4.5.1

Table 1-6: Design, Qualification and Preoperational Testing for Motor-Operated Valves

Commitment	ADM Reference
Design and qualification requirements for motor-operated valves	3.9.6.2.1.1
Pre-operational testing of safety-related motor operated valves	3.9.6.2.1.2

Table 1-7: Equipment Seismic Qualification Methods

Commitment	ADM Reference
Sesimic qualification requirements for mechanical and electrical equipment	3.10.1.1
Selection of qualification method	3.10.1.2
Methods and procedures for qualifying Seismic Category I electrical equipment and instrumentation	3.10.2.1
Methods and procedures for qualifying Seismic Category I mechanical equipment including motors	3.10.3.1

Table 1-8: Piping Design Acceptance Criteria

Commitment	ADM Reference
ASME Code and code cases for System 80+ piping and pipe support design	1.8; App 3.9A [1.1]
Analysis methods; experimental stress analysis, independent support motion, inelasic analysis, small-bore piping, non-seismic/seismic interaction, buried piping	3.7.3.9; 3.7.3.8; 3.7.3.12; 3.7.3.13; 3.9.1.3; App 3.9A [1.1]
Piping modeling; piping benchmark program, decoupling criteria	3.9.1.2.1; App 3.9A [1.5.2.2]
Pipe stress analysis criteria; loading and load combinations, damping values, combination of modal responses, high frequency modes, thermal oscillations in piping connected to the reactor coolant system, thermal stratification, safety-related valve design, installation and testing, functional capability, combination of inertial and seismic motion effects, welded attachments, modal damping for composite structures, minimum temperature for thermal analyses.	3.7.2.15; 3.9.3.1; 3.9.3.3; 3.9.3.1.4.3; App 3.9A [1.4.3.2.1.3, 1.4.3.2.1.4, 1.4.3.2.1.5, 1.4.3.2.1.6, 1.4.2, 1.4.7, 1.5.2.2, 1.6.5]; Tbl 3.7-1
Pipe support criteria; applicable codes, jurisdictional boundaries, pipe support baseplate and anchor bolt design, use of energy absorbers and limit stops, pipe support stiffness, seismic self-weight excitation, design of supplementary steel, consideration of friction forces, pipe support gaps and clearances, instrumentation line support criteria	3.9.3.4; App 3.9A [1.10.1, 1.10.2, 1.7.2.3, 1.7.2.8, 1.7.2.9, 1.7.2.10, 1.7.4, 1.7.5]

Table 1-9: First Cycle Fuel and Control Rod Design

Commitment	ADM Reference
Fuel and initial core design description and permissible changes	4.1.1
Design features and acceptance criteria for fuel and intital core design	Tables 4.1-1, 4.1-2

Table 1-10: Instrumentation & Controls Setpoint Methodology

Commitment	ADM Reference
Generation of safety system setpoints	7.1.2.27

Table 1-11: Instrumentation & Controls Hardware and Software Changes

Commitment	ADM Reference
Design, verification, implementation and validation of computer systems software changes in safety-related systems	7.1.2.32

Table 1-12: Instrumentation & Controls Environmental Qualification

Commitment	ADM Reference
Environmental qualification of electrical equipment	3.11.1

Table 1-13: Control Room Human Factors Engineering

Commitment	ADM Reference
Human factors program plan	18.4.2
HFE verification and validation plan	18.4.9
Functional task analysis, workload & environmental assumptions and bases	18.5.1.1
Task decomposition and data framework	18.5.1.3; 18.5.1.3.2; 18.5.1.3.3
Workload loading criteria	18.5.1.4
Nuplex 80+ control room functional task analysis, scope, PRA and critical tasks, information and control requirements, time profile/workload evaluation, identification of overload situations	18.5.1.5.1; 18.5.1.5.2; 18.5.1.5.3;18.5.1.5.4; 18.5.1.5.6
Main control room annunciator, display and control inventory	18.5.4
Control room staffing assumptions	18.6.2.2
Control room console panel profiles	18.6.5.7
Nuplex 80+ information presentation	18.7.1
Nuplex 80+ safety-related information	18.7.1.8.1
Remote shutdown panel safety-grade instrumentation and controls	18.8.1.1

TABLE 1.8-6

(Sheet 1 of 2)

SYSTEM 80+ INDUSTRIAL CODES AND STANDARDS

Code	Edition	Title
ANSI/American Concrete Institute [ACI]		
318	1989	Building Code Requirements for Reinforced Concrete, 1991 Printing
349	1985	Code Requirements for Nuclear Safety-Related Concrete Structures
ANSI/American Institute of Steel Construction [AISC]		
N690	1984	Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities
	1989	Manual of Steel Construction, Allowable Stress Design, Ninth Edition
ANSI/American Nuclear Society [ANS]		
2.8	1992	Determining Design Basis Flooding of Power Reactor Sites
13.1	1993	Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities
51.1	1983	Nuclear Safety Criteria for the Design of Stationary PWR Plants
55.4	1993	Gaseous Radioactive Waste Processing Systems for Light Water Reactor Plants
56.2	1989	Containment Isolation Provisions for Fluid Systems after a LOCA
57.2	1976	Design Objectives for LWR Spent Fuel Storage Facilities at Nuclear Power Stations
58.1	1982	Plant Design Against Missiles
58.2	1988	Design Basis for Protection of LWRs against Effects of Pipe Rupture
58.8	1984	Time Response Design Criteria for Safety-Related Operator Action
58.9	1987	Single Failure Criteria for LWR Safety Related Fluid Systems
ANSI/American Petroleum Institute [API]		
650	1988	Welded Steel Tanks for Oil Storage
ANSI/American Society of Civil Engineers		
7	1990	Minimum Design Loads for Building and Other Structures [ANSI A58.1]
ANSI/American Society of Mechanical Engineers [ASME]		
BPVC	1989	Section II; Materials Specifications
BPVC	1989	Section III; Rules for Construction of Nuclear Power Plant Components; Division I, Division II
BPVC	1989	Section V, Non-Destructive Examination
BPVC	1989	Section VIII; Rules for Construction of Pressure Vessels
BPVC	1989	Section IX; Qualification Standard for Welding and Brazing
BPVC	1989	Section XI; Rules for Inservice Inspection of Nuclear Power Plant Components; Editions and Addenda As Applicable
AG-1	1991	Code on Nuclear Air and Gas Treatment
B31.1	1992	Power Piping
OM-S/G	1990	Standards and Guides for Operation and Maintenance of Nuclear Power Plants; through 1992 Addenda.

The process line and penetration flued head making up the pressure boundary are consistent with the system piping materials; fabrication, inspection, and analysis requirements are as required by the ASME Code, Section III, Subsection NC. All welds on the process pipe are accessible for inspection in accordance with the ASME Code, Section XI.

High energy lines and selected engineered safety system and auxiliary lines require the typical "Hot Penetration" assembly shown on Figure 3.8-2 which features an exterior guard pipe for protection of other penetrations in the building annular space. Other lines use the typical "Cold Penetration" assembly also shown in Figure 3.8-2 since a leak into the annular space would not cause a personnel hazard or damage other penetrations in the immediate area. Mechanical bellows are provided where necessary to minimize reactions on the steel containment vessel. The bellows are designed to maintain containment integrity under all load conditions.

Mechanical penetrations are leak tested in accordance with 10CFR50 Appendix J.

3.8.2.1.3.5 Containment Electrical Penetration Assemblies

Medium voltage containment electrical penetration assemblies for reactor coolant pump power (shown in Figure 3.8-2) use sealed bushings for conductor seals. The assemblies incorporate dual seals along the axis of each conductor. Low voltage power, control, and instrumentation cables enter the containment vessel through containment electrical penetration assemblies which are designed to provide two leak-tight barriers in series with each conductor.

All containment electrical penetration assemblies, including seals, are designed to maintain containment integrity for Design Basis Accident conditions, including pressure, temperature, and radiation. Double barriers permit testing of each assembly in accordance with 10CFR50 Appendix J to verify that containment integrity is maintained.

The containment electrical penetration assemblies are designed, fabricated and tested in accordance with IEEE-317. The pressure boundary portion of the assembly is designed, fabricated and tested in accordance with Section III, Subsection NE of the ASME Code.

3.8.2.2 Applicable Codes, Standards, and Specifications

The design, materials, fabrication, erection, inspection, testing, and inservice surveillance of the steel containment and penetrations is covered by the following codes, standards, specifications, and regulations:

* 1-3 ASME

For Tier 2*, the wording in the FSER is appropriate, i.e. design and construction

(1)

Codes	Title
ASME	Boiler and Pressure Vessel Code, Section II, "Material Specifications"
ASME	Boiler and Pressure Vessel Code, Section III, Division 1, Subsection NE, "Class MC Components"
ASME	Boiler and Pressure Vessel Code, Section V, "Nondestructive Examination"
ASME	Boiler and Pressure Vessel Code, Section IX, "Welding and Brazing Qualifications"
ASME	Boiler and Pressure Vessel Code, Section XI, Rules for Inservice Inspection of Nuclear Power Plant Components, Subsection IWE "Requirements for Class MC and Metallic Liners of Class CC Components of Light-Water Cooled Power Plants"

Regulatory Guides	Title
1.11	Instrument Lines Penetrating Primary Reactor Containment (Safety Guide 11)
1.50	Control of Preheat Temperature for Welding of Low-Alloy Steel
1.54	Quality Assurance Requirements for Protective Coatings Applied to Water Cooled Nuclear Power Plants
1.57	Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components
1.63	Electric Penetration Assemblies in Containment Structures for Nuclear Power Plants
1.84	Design and Fabrication Code Case Acceptability - ASME Section III, Division 1

possible events are determined for comparison with the allowable safety factors listed in Section 5.0 of Appendix 3.8A.

All Seismic Category I removable walls and hatch plugs are positively anchored to withstand the design pressures and inertia loads.

Design and analysis results for selected areas of the Nuclear Annex are presented in Appendix 3.8B.

3.8.4.5 Structural Acceptance Criteria

Code Edition provided in Table 1.8-6

3.8.4.5.1 Concrete Structures

Analysis and design of Seismic Category I concrete structures use the ultimate strength design method in accordance with ACI 349 when supplemented by the following provisions:

1. Special consideration is given to anchorage pull-out capacity (i.e. - reduced concrete failure cone) especially when;

   a) the anchor is near the free edge of the concrete, and/or,
   b) the anchors are closely spaced, and/or
   c) the anchor(s) are placed in the tension zone of the slab

2. Baseplate flexibility is accounted for when calculating anchor bolt loads.

3. The failure cone angle used is consistent with recent test data for the specific application.

4. The embedment length of ductile anchors is chosen such that the ratio of the anchor pull-out capacity (concrete) to the anchor minimum tensile capacity (steel) is greater than or equal to 1.50.

5. Expansion anchor bolts are designed to have the following minimum factor of safety between the bolt design load and the bolt ultimate capacity determined from static tests.

   a) Four (4.0) for wedge and sleeve anchor bolts.

   b) Three (3.0) for undercut anchors.

   The ultimate capacity of the anchor bolt accounts for shear-tension interaction, minimum edge distance, and proper bolt spacing.

6. The energy absorption capability (deformation capability after yield) is considered for the anchor material.

7. The effects of cyclic loading are considered in the anchor bolt design.

ACI 349 is used to determine the required quantity of shear, tension, and compression reinforcing in Seismic Category I structures. In addition ACI 318, Chapter 21 is used to determine the required anchorage and splicing of reinforcing to assure ductility at the structural connections. ACI 318, Chapter 21 is also used to determine the configuration of reinforcing in the structural joints, and regions where reinforcing is spliced, and required placement of stirrups and hoop steel. Typical connection details are provided in Appendix 3.8B, Section 6.0.

Masonry block walls are not used in ~~Seismic Category I or II~~ structures.

Code Edition Provided in Table 1.8-6

3.8.4.5.2 Steel Structures

Seismic Category I structural steel analysis and design are in accordance with ANSI/AISC N690 when supplemented by the following provisions:

1-4

1. In Section Q1.0.2, the definition of secondary stress applies to stresses developed by temperature loading only.

2. The following notes are added to Section Q1.3:

   "When any load reduces the effects of other loads, the corresponding coefficient for that load shall be taken as 0.9, if it can be demonstrated that the load is always present or occurs simultaneously with other loads. Otherwise, the coefficient for that load shall be taken as zero."

   "Where the structural effects of differential settlement are present, they should be included with the dead load 'D'."

   "For structures or structural components subjected to hydrodynamic loads resulting from LOCA and/or SRV actuation, the consideration of such loads should be as indicated in the Appendix to the SRP Section 3.8.1. Any fluid-structure interaction associated with those hydrodynamic loads and those from postulated earthquake(s) should be taken into account."

3. The stress limit coefficients (SLC) for compression in Table Q1.5.7.1 are as follows:

   1.3 instead of 1.5 [stated in footnote (c)] in load combinations 2, 5, and 6.

   1.4 instead of 1.6 in load combinations 7, 8, and 9.

   1.6 instead of 1.7 in load combination 11.

4. The following note is added to Section Q1.5.8:

   "For constrained (rotation and/or displacement) members supporting safety related structures, systems, or components, the stresses under load combinations 9, 10, and 11 should be limited to those allowed in Table Q1.5.7.1 as modified by provision 3 above. Ductility factors of Table Q1.5.8.1 (or provision 5 below) should not be used in these cases."

5. For ductility factors 'μ' in Sections Q1.5.7.2 and Q1.5.8, are substituted provisions of Appendix A, II.2 of SRP Section 3.5.3 in lieu of Table Q1.5.8.1.

6. In load combination 9 of Section Q2.1, the load factor applied to load P is 1.5/1.1 = 1.37, instead of 1.25.

7. Sections Q1.24 and Q1.25.10 is supplemented with the following requirements regarding painting of structural steel:

   a) Shop painting shall be in accordance with Section M3 of Reference 17.

   b) All exposed areas after installation shall be field painted (or coated) in accordance with the applicable portion of Section M3 of Reference 17.

   c) The quality assurance requirements for painting (or coating) of structural steel shall be in accordance with Reference 18 as endorsed by Regulatory Guide 1.54, "Quality Assurance Requirements for Protective Coatings Applied to Water Cooled Nuclear Power Plants".

Welding activities associated with Seismic Category I structural steel components and their connections shall be accomplished in accordance with written procedures and shall meet the requirements of AWS D1.1 (Reference 25). The visual acceptance criteria shall be as defined in NCIG-01 (Reference 24).

3.8.4.5.3 Concrete and Steel Structures

In addition to satisfying the load combinations for structural adequacy against the design loadings, the load combinations to ensure safety factors against overturning, sliding, and flotation are checked to ensure overall stability of Seismic Category I structures. The following events are checked as a minimum:

A. The overturning about the toe of the foundation supported on soil.

conditions, pump curve testing will be used to assess pump degradation. The following provisions shall be complied with in the use of pump curve testing for the CCW/SSW pumps:

A. Pump curves are developed, or manufacturer's pump curves are validated, when the pumps are known to be operating acceptably.

B. The reference points used to develop or validate the curve are measured using instruments at least as accurate as required by the Code.

C. Pump curves are based on an adequate number of points, with a minimum of five.

D. Points are beyond the "flat" portion (low flow rates) of the curves in a range which includes or is as close as practicable to design basis flow rates.

E. Acceptance criteria based on the curves does not conflict with Technical Specifications or CESSAR-DC design bases.

F. If vibration levels vary significantly over the range of pump conditions, a method for assigning appropriate vibration acceptance criteria should be developed for regions of the pumps curve.

G. When the reference pump curve may have been affected by repair, replacement, or routine service, a new reference curve shall be determined or the previous curve revalidated by an inservice test.

3.9.6.2 Testing of Safety-Related Valves

3.9.6.2.1 Motor-Operated Valves

For each motor-operated valve assembly (MOV) with an active safety-related function, the design basis and required operating conditions (including testing) under which the MOV will be required to perform are established for the development and implementation of the design, qualification, and preoperational testing.

3.9.6.2.1.1 Design and Qualification Requirements for Motor-Operated Valves

Plant-specific information will include the following design and qualification requirements and acceptance criteria for these requirements. By testing each size, type, and model the torque and thrust (as applicable to the type of MOV) requirements to operate the MOV will be determined to ensure the adequacy of the torque and thrust that the motor-operator can deliver under design (design basis and required operating) conditions. Each size, type, and model will be tested under a range of differential pressure and flow conditions up to the design

1-6

conditions. These design conditions include fluid flow, differential pressure (including pipe break), system pressure, fluid temperature, ambient temperature, minimum voltage, and minimum and maximum stroke time requirements. This testing of each size, type and model shall include test data from the manufacturer, field test data for plant-specific dedication, empirical data supported by test, or test (such as a prototype) of similar valves which support qualification of the required valve where similarity must be justified by technical data. This preoperational testing will demonstrate that the results of the testing under in-situ or installed conditions can be used to ensure the capability of the MOV to operate under design conditions. Test data will be used to ensure that the structural capability limits of the individual parts of the MOV will not be exceeded under design conditions. Additional guidelines to justify prototype qualification testing are contained in Generic Letter 89-10, Supplement 1, Questions 22, 24, 25, 26, 27, and 28. Test data will be used to ensure that the valve specified for each application is not susceptible to pressure locking and thermal binding. 1-6

The concerns and issues identified in Generic Letter 89-10 and its supplements for MOVs will be addressed prior to plant startup and ~~The following~~ testing requirements and acceptance criteria are applicable to each motor-operated valve assembly (MOV with an active safety-related function).

3.9.6.2.1.2 Pre-Operational Testing of Safety-Related Motor-Operated Valves

Each MOV will be tested in the open and closed directions under static and maximum achievable preoperational conditions using diagnostic equipment which measures torque and thrust (as applicable to the type of MOV), and motor parameters. The MOV will be tested under various differential pressure and flow conditions up to maximum achievable conditions and perform a sufficient number of tests to determine the torque and thrust requirements at design conditions. The torque and thrust requirements to close the valve to the position at which there is diagnostic indication of hard seat contact will be determined. 1-6

The determination of design torque and thrust requirements will be made for such parameters as differential pressure, fluid flow, undervoltage, temperature and seismic dynamic effects for MOVs which must operate during these transients. The design torque and thrust requirements will be adjusted for diagrostic equipment inaccuracies. For the point of control switch trip, any loss in torque produced by the actuator and thrust delivered to the stem for increasing differential pressure and flow conditions (referred to as load sensitive behavior) will be determined. The design torque and thrust requirements will be compared to the control switch trip torque and thrust by subtracting margin for load sensitive behavior, control switch repeatability, and

degradation. The total thrust and torque delivered by the MOV under static and dynamic conditions (including diagnostic equipment inaccuracies and control switch repeatability) will be measured and compared to the allowable structural capability limits for the individual parts of the MOV. Tests will be conducted for proper control room position indication of the MOV. 1-6

The parameters and acceptance criteria for demonstrating that the above functional performance requirements have been fulfilled are as follows:

A. As required by the safety function, the valve must fully open, or the valve must fully close with diagnostic indication of hard seat contact.

B. The control switch settings must provide adequate margin to achieve design requirements including consideration of diagnostic equipment inaccuracies, control switch repeatability, load sensitive behavior, and margin for degradation.

C. The motor output capability at degraded voltage must equal or exceed the control switch setting including consideration of diagnostic equipment inaccuracies, control switch repeatability, load sensitive behavior and margin for degradation.

D. The maximum torque and thrust (as applicable for the type of MOV) achieved by the MOV including diagnostic equipment inaccuracies and control switch repeatability must not exceed the allowable structural capability limits for the individual parts of the MOV.

E. The remote position indication testing must verify that proper disk position is indicated in the control room.

F. Stroke time measurements taken during valve opening and closing must meet minimum and maximum stroke time requirements.

3.9.6.2.1.3 Inservice Testing of Safety-Related Motor-Operated Valves

The inservice testing of MOVs will rely on diagnostic techniques which are consistent with the state of the art and which will permit an assessment of the performance of the valve under actual loading. Periodic testing per Generic Letter 89-10 Paragraphs D and J will be conducted under adequate differential pressure and flow conditions which allow a justifiable demonstration of continuing MOV capability for design basis conditions. The detailed IST program will include the optimal frequency of this periodic verification. The frequency and test conditions will be sufficient to demonstrate continuing design basis and required

VIRGIL SEP 2 0 '94

3.10 SEISMIC AND DYNAMIC QUALIFICATION OF MECHANICAL AND ELECTRICAL EQUIPMENT

This section describes the tests, analyses, procedures, and acceptance criteria applied to two categories of mechanical and electrical equipment to assure operability and structural integrity under the full range of normal, transient, seismic and accident loadings.

The two categories are safety related (Seismic Category I) equipment and non-safety related equipment whose failure can prevent the satisfactory accomplishment of safety functions (Seismic Category II). The safety related equipment are those necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures in excess of 10 CFR 100 guidelines. Non-safety related equipment whose failure could reduce the performance of safety related equipment is designated as Seismic Category II.

Examples of mechanical and electrical equipment included in these two categories are pumps, valves, fans, valve operators, valve operator motors, solenoid valves, pump and fan motors, compressors, chillers, air handlers, blowers, fuel rod assemblies, control rod drive mechanisms, battery and instrument racks, control consoles, cabinets, panels, pressure switches, level transmitters, and electrical penetrations.

The licensee at the time of COL will make the specific details of the plant-specific seismic and dynamic qualification program available for NRC evaluation. This includes a description of administrative control procedures; equipment qualification reports and records; results of in-plant tests; and, if used, documentation on qualification by experience.

3.10.1 SEISMIC QUALIFICATION CRITERIA

3.10.1.1 Requirements

The seismic and dynamic qualification program ensures that equipment classified as Seismic Category I can meet functional performance requirements, as defined in the equipment's design specification, during and after the dynamic loadings due to normal operating, transient, seismic and accident conditions. For Seismic Category II equipment it is demonstrated that structural integrity is maintained under normal operating, transient, seismic and accident loads and therefore this equipment will not be a missile hazard or in some other manner damage nearby safety-related equipment.

The seismic and dynamic qualification program conforms to the requirements of Regulatory Guide 1.100, Rev. 2 and IEEE Std. 344-1987. The seismic and dynamic testing portion of the qualification program is performed in a sequence consistent with the requirements of Section 6 of IEEE Standard 323-1974. I-7

3.10.1.2 Selection of Qualification Method

Seismic and dynamic qualification of mechanical and electrical equipment is accomplished by test, analysis, a combination of test and analysis, or experience.

In general, Seismic Category I equipment, for which functional operability must be demonstrated, is qualified by tests.

Under certain conditions functional operability may be qualified by analysis or a combination of analysis and test. Analysis alone, without testing, may be used for qualification only if the necessary functional operability of the equipment is assured by structural integrity alone. An example of this type of equipment is the reactor internals core support structures. For equipment whose functional operability cannot be demonstrated by structural integrity alone and because of its size, complexity, or limitations of test facilities cannot be fully tested, a combination of test and analysis may be used. An example of this would be the qualification of a main control panel by analysis with local modal surveys to verify the analysis. The equipment in the main control panel would be tested.

An example of mechanical equipment qualified by a combination of test and analysis is the control element drive mechanisms. The pressure boundary is qualified by design analysis, while operability is demonstrated by tests.

Seismic Category II equipment, for which only structural integrity must be demonstrated, is generally qualified by analysis.

Qualification of equipment by experience shall be used only on a case-by-case basis. If used, site-specific documentation will be submitted describing the class of equipment and the methodology to be used to qualify the equipment. I-7

3.10.1.3 Input Motion

The input motions for the seismic qualification of equipment and supports are generated from the building dynamic analysis, as described in Section 3.7. The buildings dynamic analyses envelope all sites forming the design basis for the standard design. The buildings dynamic analyses provide response spectra or time histories for elevations in each building. Envelopes of these seismic input motions are used directly for qualification or to perform dynamic analyses to generate input motions at other equipment mounting locations. The equipment input motion due to normal, transient and accident loads are considered in addition to the seismic input motion.

3.10.2 SEISMIC AND DYNAMIC QUALIFICATION OF ELECTRICAL EQUIPMENT

Instrumentation and electrical equipment used for post-accident monitoring, the Reactor Protective System (RPS), the Engineered Safety Features Actuation System (ESFAS), the actuation devices for ESF system actuated components, and the emergency power system are designed to Seismic Category I requirements to assure the ability to initiate required protective actions during, and following, a Safe Shutdown Earthquake (SSE) and for all static and dynamic loads from normal, transient and accident conditions; and, to supply power, following an SSE and for all static and dynamic loads from normal, transient and accident conditions, to components required to mitigate the consequences of events which require safety system operation.

Instrumentation and electrical equipment designated Seismic Category II are shown to maintain their structural integrity and not adversely impact safety related equipment during an SSE and for all static and dynamic loads from normal, transient and accident conditions.

Methods and procedures for qualifying electrical equipment and instrumentation are described below, and meet the requirements of Regulatory Guide 1.100, Revision 2, and IEEE Standard 344-1987.

3.10.2.1 Methods and Procedures for Qualifying Seismic Category I Electrical Equipment and Instrumentation

Seismic Category I instrumentation and electrical equipment required to perform a safety action during a seismic event and for all static and dynamic loads from normal, transient and accident conditions; after a seismic event and for all static and dynamic loads from normal, transient and accident conditions; or both are qualified with appropriate documentation in accordance with the requirements of the equipment specifications. These requirements are consistent with those of IEEE Standard 344-1987, "Seismic Qualification of Class 1 Electrical Equipment for Nuclear Power Generating Stations", and Regulatory Guide 1.100, Rev. 2. The methods and procedures used for qualifying Seismic Category I electrical equipment and instrumentation include the following:

* A. Testing and analyses are used to confirm the operability of the instrumentation and electrical equipment during and after an SSE and for all static and dynamic loads from normal, transient, and accident conditions. Prior to SSE qualification, it is demonstrated that the equipment can withstand the application of five (5) cycles of 1/2 SSE excitations without loss of structural integrity. Analyses alone, without testing, is used as a basis for qualification only if the necessary functional operability of the

1-7

equipment is assured by its structural integrity alone. If complete testing is impractical, a combination of test and analysis is utilized.

When equipment that has been previously qualified by means of tests and analysis equivalent to those described here is utilized, documentation of such tests and analyses is provided.

B. Equipment is tested in the operational condition. Operability is verified during and after testing. Loadings simulating those of plant normal operation, if any, are concurrently superimposed upon the seismic and other pertinent dynamic loading.

C. The seismic and dynamic excitation for which the equipment must qualify is determined based on location in the plant. I-7

D. The characteristics of the required seismic and dynamic input motion is specified by one of the following:

1. response spectrum

2. power spectral density function

3. time history

These characteristics, derived from the structures or systems seismic and dynamic analyses, are representative of the input motions at the equipment mounting locations.

E. The actual input motion is characterized in the same manner as the required input motion. Conservatism in amplitude and multi-frequency energy content is demonstrated. That is, the test response spectrum (TRS) is demonstrated to envelope the required response spectrum (RRS) over the entire frequency range.

F. Multifrequency input motion is used whenever possible. However, single frequency input, such as sine beats, are utilized provided one of the following conditions is met:

1. The characteristics of the required input motion indicate that the motion is dominated by one frequency (i.e., by structural filtering effects).

2. The anticipated response of the equipment is adequately represented by one mode.

3. The input has sufficient intensity and duration to excite all modes to the required magnitude, such that the testing response spectra envelope the corresponding response spectra of the individual modes.

G. The input motion is applied to one vertical and one principal (or two orthogonal) horizontal axes simultaneously except where it is demonstrated that the equipment response along the vertical direction is not sensitive to the vibratory motion along the horizontal direction, and vice versa. The time phasing of the inputs in the vertical and horizontal directions is such that a purely rectilinear resultant input is avoided. The acceptable alternative is to have vertical and horizontal inputs in-phase, and then repeated with inputs 180 degrees out-of-phase. In addition, the test is repeated with the equipment rotated 90 degrees horizontally. Biaxial and triaxial input motion is utilized where practical.

H. Dynamic coupling between the equipment and related systems, if any, such as other mechanical components, is considered.

I. The fixture is designed to meet the following requirements:

1. Simulate the actual service mounting.

2. Cause no extraneous dynamic coupling to the test item.

I-7

J. The in-situ application of vibratory devices to simulate the seismic vibratory loadings on the complex active device for operability testing is acceptable when application is justifiable and meets the requirements of IEEE Std. 344-1987.

K. The test program may be based upon selectively testing a representative number of electrical components according to type, load, level, size or other appropriate classification on a prototype basis.

L. Selection of damping values for equipment to be qualified is made in accordance with Regulatory Guide 1.61 and IEEE Std. 344-1987. Higher damping values are used only if justified by documented test data with proper identification of the source and mechanism.

3.10.2.2 **Methods and Procedures of Analysis or Testing of Supports of Electrical Equipment and Instrumentation**

Analyses or tests are performed for all supports of electrical equipment to assure their structural capability.

The analytical results include the required input motions to the mounted equipment as obtained and characterized in the manner stated in Section 3.10.2.1.D above.

3.10.3 SEISMIC AND DYNAMIC QUALIFICATION OF MECHANICAL EQUIPMENT INCLUDING MOTORS

3.10.3.1 Methods and Procedures for Qualifying Seismic Category I Mechanical Equipment Including Motors

Dynamic loads of mechanical equipment are combined as specified in Table 3.9-2. Qualification of mechanical equipment and their supports meet the requirements of Regulatory Guide 1.100 Rev. 2 and IEEE Std. 344-1987. Methods and procedures of testing and analysis for confirming the operability of equipment for the defined loads are presented in the following paragraphs.

A. Tests and analyses are performed to confirm the operability of the mechanical equipment during and after an earthquake of magnitude up to and including the SSE, and for all static and dynamic loads from normal, transient and accident conditions. Prior to SSE qualification, it is demonstrated that the equipment can withstand the application of five (5) cycles of 1/2 SSE excitations without loss of structural integrity. Analyses alone, without testing, is used as a basis for qualification only if the necessary functional operability of the equipment is assured by its structural integrity alone. If complete testing is impractical, a combination of test and analysis is utilized.

When equipment that has been previously qualified by means of tests and analyses equivalent to those described here is utilized, documentation of such tests and analyses is provided.

B. Equipment is tested in the operational condition. Operability is verified during and/or after the testing, as applicable to the equipment being tested. Loadings simulating those of plant normal operation, such as thermal and flow-induced loading, if any, are concurrently superimposed upon the seismic and other pertinent dynamic loading to the extent practicable. Particular attention is paid, in operability qualification of mechanical equipment subjected to flow-induced loading, to incorporate degraded flow conditions such as those that might be encountered by the presence of debris, impurities, and contaminants in the fluid system.

C. The characteristics of the required seismic and dynamic input motions are specified by response spectra, time histories, or power spectral density functions. These characteristics, derived from the structures or systems seismic and dynamic analyses, are representative of the input motions at the equipment mounting locations.

D. For seismic and dynamic loads, the actual test input motion are characterized in the same manner as the required input

motion, and conservatism in amplitude and frequency content is demonstrated.

E. Since seismic and the dynamic load excitation generally have a broad frequency content, multi-frequency vibration input motion is used. However, single frequency input motion, such as sine beats, is utilized if the motion is dominated by one frequency (e.g., by structural filtering effects), or the anticipated response of the equipment is adequately represented by one mode, or in the case of structural integrity assurance, the input has sufficient intensity and duration to produce sufficiently high levels of stress for such assurance. Components that have been previously tested to IEEE Std. 344-1971 are reevaluated to justify the appropriateness of the input motion used, and requalified if necessary.

F. For the seismic and dynamic portion of the loads the test input motion is applied to one vertical axis and one principal horizontal axis (or two orthogonal horizontal axes) simultaneously unless it is demonstrated that the equipment response in the vertical direction is not sensitive to the vibratory motion in the horizontal direction, and vice versa. The time phasing of the inputs in the vertical and horizontal directions is such that a purely rectilinear resultant input is avoided. The alternative is to test with vertical and horizontal inputs in-phase, and then repeat the test with inputs 180 degrees out-of-phase. In addition, the test is repeated with the equipment rotated 90 degrees horizontally.

Components that have been previously tested using a single axis test input motion are requalified using biaxial test input motions or a justification for using a single axis test input motion is provided.

G. Dynamic coupling between the equipment and related systems, if any, such as connected piping and other mechanical components, is considered.

H. The fixture is designed to simulate the actual service mounting and will not cause any significant dynamic coupling to the test item.

I. For pumps and valves, the loads imposed by the attached piping along with the sustained dynamic and seismic loads are taken into account. In order to assure operability under combined loadings, the stresses resulting from the applied test loads envelope the specified service stress limit for which the component's operability is intended. Refer to Section 3.9.3.2 for further discussion of pump and valve operability assurance.

J. If the dynamic testing of a pump or valve assembly is impracticable, static testing of the assembly is performed with end loadings conservatively applied and equal to or greater than postulated event loads. All dynamic amplification effects are accounted for, the component is in the operating mode during and after the application of loads, and an adequate analysis is made to demonstrate the validity of the static application of loads.

K. The in situ application of vibratory devices to simulate the seismic and dynamic vibratory motions on a complex active device may be utilized to confirm the operability of the device after it is shown that a meaningful test can be made in this way.

* L. The test program is based upon selectively testing a representative number of components according to type, load level, size, etc., on a prototype basis.

1-7

M. Selection of damping values for equipment to be qualified is made in accordance with Regulatory Guide 1.61 and IEEE Std. 344-1987. Higher damping values are used if justified by documented test data with identification of the source and mechanism.

N. When complete testing is not practicable, the features listed below are incorporated into a test and analysis operability assurance program for pumps and valves. Similar programs are developed for other types of equipment.

1. Simple and passive elements, such as valve and pump bodies and their related piping and supports are analyzed to confirm structural integrity under postulated event loadings. However, where practical, complex active devices such as pump motors, valve operator and gate or disk assemblies, and other electrical, mechanical, pneumatic, or hydraulic appurtenances which are vital to the pump or valve operation are tested for operability.

2. The following are typical analyses which are used for qualification.

   a. An analysis to determine the vibratory input to the valve or pump.

   b. An analysis to determine the system natural frequencies and the movement of the pump or valve during the dynamic events.

   c. An analysis to determine the pressure differential and the impact energy on a valve disc during a

1.8 REGULATORY COMPLIANCE, INDUSTRY CODES AND STANDARDS

System 80+ compliance with U.S. NRC Regulatory Guides, Generic Letters, Bulletins, and elements of the Standard Review Plan is documented in this section. Regulatory Guides, the guide date or revision, and System 80+ compliance with applicable Guides are summarized in Table 1.8-1.

Operational experience information highlighted in Regulatory Bulletins and Letters has been incorporated into the System 80+ design. Generic Letters and NRC Bulletins from 1980 through December, 1993 are identified in Tables 1.8-2 and 1.8-3. The applicability of each Generic Letter or Bulletin to System 80+ is assessed, with additional information for applicable issues provided in the referenced sections of this report.

System 80+ deviations from the U.S. NRC Standard Review Plan, NUREG-0800 [LWR Edition, June 1987], are listed in Table 1.8-4. Specific sections are also identified where further details relevant to each SRP deviation are discussed. Site-specific compliance with individual Standard Review Plan sections is provided in Table 1.8-5.

Table 1.8-6 identifies the industrial Codes and Standards, and code editions, invoked for certification of the System 80+ Standard Design. Where a particular structure, system, or component requires a code edition different from that listed in Table 1.8-6, an explanation of such difference is provided in the appropriate text. Other Codes and Standards that are utilized but not invoked as essential for design certification are incorporated into the individual chapters of this Safety Analysis Report. Revisions to accepted industry codes applied to System 80+ will be evaluated on a case-by-case basis. The applicability of code editions will be confirmed by the Combined Operating License applicant in the site-specific Safety Analysis Report.

ASME Section III, Division 1 Code Cases applicable to System 80+ are identified in Table 1.8-7. Except for N-122-1, these Code Cases are consistent with those identified in Regulatory Guide 1.84, Revision 29, for design and fabrication, or Regulatory Guide 1.85, Revision 29, for materials and testing, that were in effect on July 31, 1993.

Cross-references to subsections of this report discussing Unresolved and Generic Safety Issues, the Three Mile Island Rule [10 CFR 50.34 (f)], and new NRC policy issues (SECY-93-087) are provided in Tables 1.8-8, 1.8-9, and 1.8-10.

[Later code cases that may be used for System 80+ piping and pipe support design will be provided with plant-specific information.]*

details of inelastic piping analysis methods, if used; details of independent support motion response spectrum analysis methods, if used;

3.7 SEISMIC DESIGN

The COL applicant referencing the System 80+ Standard Design will provide site and plant-specific seismic design information which will include evaluation of interactions between Seismic Category I and non-Seismic Category I structures, systems, and components; procedures for pre-earthquake planning and post-earthquake actions; and site-specific confirmatory analyses, as required.

3.7.1 SEISMIC INPUT

This section discusses the seismic design parameters and methodologies being used for the design of those systems and subsystems important to safety and classified as Seismic Category I in Section 3.2.

3.7.1.1 Design Response Spectra

The System 80+ Standard Design as defined by CESSAR-DC is not based on a specific site. The design response spectra which define the free field design ground motion or control motion specified either at the site soil surface or on a hypothetical rock outcrop are shown in Figure 2.5-5. Generic site conditions were selected to cover a range of possible conditions for the System 80+ sites. For the Nuclear Island, sets of representative cases from each of four generic site categories were evaluated. Ground surface and foundation level spectra which correspond to the design response spectra of control motions CMS1, CMS2 and CMS3 for rock and soil cases are shown in Section 2.5. Out of 12 soil cases analyzed in Section 2.5.2, ten are used in the soil structure interaction (SSI) analyses. The two cases eliminated in the SSI analysis (B3 and D1) were non-governing cases whose soil response levels were enveloped by other cases. See Section 2.5.2 for details of this analysis phase. Two rock cases were analyzed, one with no backfill (fixed base at bottom of basemat) and one with concrete backfill (fixed base at all subsurface elevations). The ten soil cases and the two rock cases were analyzed for all three control motions (CMS1, CMS2, and CMS3).

A sensitivity study was performed to demonstrate that the selected motions and the soil profiles provide a conservative design envelope for the System 80+ structures. In this study, a simplified analytical model of the 3D NI structure was developed and analyzed with five soil profiles and the CMS2 control motion. Three of the soil profiles were part of the 12 profiles selected for the System 80+ 3D SSI analyses (B-1, B-1.5, B-2). The remaining two soil profiles were developed to serve as "test" profiles. The two new profiles were chosen such that they have low strain soil properties that are in-between the soil properties of cases B-1, B-1.5 and B-2. Hence, they were named B-1.25 and B-1.75. Response parameters such as maximum in-structure acceleration, maximum base shear and maximum base

overturning moment were used as the key parameters that determine the adequacy of the soil profile selection. The sensitivity analyses showed that structural response corresponding to the "test" soil cases B-1.25 and B-1.75 was under the envelope of structural response from the three generic cases B-1, B-1.5 and B-2. Therefore, it is concluded that the 12 generic soil profiles provide a conservative envelope of structural response and they cover a broad range of sites.

The effect of differential seismic displacement on the equipment and supports is included in the analysis as described in Section 3.7.3.1.

3.7.1.2 Design Time History

Since the System 80+ Standard Design is designed for generic site conditions, for the time history method of analysis, the generic free-field ground surface time histories are used as control motions in the analyses. In the soil-structure interaction analyses, for each generic site, the corresponding two horizontal and one vertical time histories at the free-field ground surface are used with the SSI model of that site. For the fixed-base analyses, the rock outcrop time histories are directly used as the control time histories.

The response spectra at 2, 5 and 7% damping of control motion CMS1, and 1, 2, 5 and 7% damping of control motions CMS2 and CMS3 and the corresponding spectral ordinates of the matching time histories are shown in Figures 3.7-1 to 3.7-12. The Power Spectral Densities of all time histories are included in Section 2.5.

Each time history that is used in the SSI and rock analyses contains 20.48 seconds. For the SSI analyses, a time step of 0.005 sec is used. For the Nuclear Island rock analyses, a time step of 0.0025 sec is used.

For Category I structures not on the Nuclear Island a time step of 0.005 sec. is used for both SSI and rock analyses.

3.7.1.3 Critical Damping Values

Damping values used for various nuclear safety-related structures systems and components are based upon Regulatory Guide 1.61 or ASME Code Case N-411-1 (See Figure 3.7-32). These values are expressed in percent of critical damping and are given in Table 3.7-1. When the response spectra method of analysis is used for piping, damping values are based on Code Case N-411-1.

β_j = composite modal damping for mode j,

β_i = critical modal damping associated with component i,

ϕ_j = mode shape vector,

$\{M_i\}$ = subregion of mass matrix associated with component i, and

[M] = the mass matrix of the system.

For direct integration method, viscous damping proportional to the mass and stiffness matrix is used; thus

Sect. 3.7.2.15

$$\{C\} = \alpha[K] + \beta[M]$$

where [C] is the damping matrix, [K] is the stiffness matrix and [M] is the mass matrix. The values of α and β are selected such that the damping in the range of frequency of interest is approximately equal to the damping of the structure.

Where composite modal damping is used for piping, the input damping for piping elements is in accordance with Table 3.7-1. That is, for the Safe Shutdown Earthquake, the damping is 2.0 percent of critical damping for piping of diameter ≤ 12 inches and is 3.0 percent of critical damping for piping of diameter > 12 inches.]*

3.7.3 SEISMIC SUBSYSTEM ANALYSIS

3.7.3.1 Seismic Analysis Methods

The seismic analysis of the Seismic Category I structures, subsystems, and components other than piping is performed by either the response spectrum or time history method as described in Section 3.7.2.1.1 or an equivalent static method described in Section 3.7.3.5.

When analyzed using the response spectrum method, four options are available for the choice of response spectra. These are described in Appendix 3.9A, Section 1.4.3.2.1.2. Appendix 3.7D shows sample spectra for use in the three options not related to plant specific analysis.

For Seismic Category I piping, each piping system is idealized as a mathematical model consisting of lumped masses connected by elastic members. The stiffness matrix for the piping subsystem is determined using the elastic properties of the pipe. This includes the effects of torsional, bending, shear, and axial deformations as well as changes in stiffness due to curved members. Generally, a response spectrum analysis is performed using the envelope of all applicable spectra to account for inertia effects. The effects of rocking and torsion are implicitly included because the spectra at the support points

include motions due to rocking and torsion. The total seismic response of the piping is then calculated by absolute summing the results of the response spectrum analysis and a static analysis which accounts for the relative displacement effects between support locations. Since the displacement effects are self-limiting, it is justified to place them in the secondary stress category.

As an alternative to the modal response method, a time history method of analysis may be used. This method is also used for other types of dynamic analyses such as LOCA and hydraulic transients. Either a direct integration method or a modal superposition method is used to solve the equations of motion.

3.7.3.2 Determination of Number of Earthquake Cycles

The procedure used to account for the fatigue effect of cyclic motion associated with seismic excitation recognizes that the actual motion experienced during a seismic event consists of a single maximum or peak motion, and some number of cycles of lesser magnitude. The total or cumulative usage factor can also be specified in terms of a finite number of cycles of the maximum or peak motion. Based on this consideration, Seismic Category I subsystems, components, and equipment are designed for a total of two SSE events with 10 maximum stress cycles per event (20 full cycles of the maximum SSE stress range). Alternatively, an equivalent number of fractional vibratory cycles to that of 20 full SSE vibratory cycles may be used (but with an amplitude not less than one-third (1/3) of the maximum SSE amplitude) when derived in accordance with Appendix D of IEEE Standard 344-1987.

3.7.3.3 Procedure Used for Modeling

The modeling techniques incorporate either a single or multidegree of freedom subsystem consisting of discrete masses connected by spring elements. The associated damping coefficients are consistent with Table 3.7-1. The degree of complexity of each model is sufficient to accurately evaluate the dynamic behavior of the component. For additional details on pipe modeling, see the section below.

Valves (i.e., with natural frequencies greater than the frequency corresponding to the zero period acceleration (ZPA)) are included in the piping system model as lumped masses on rigid extended structures. If it is shown by test or analysis that a valve has a frequency less than a frequency corresponding to the ZPA, then a multimass, dynamic model of the valve, including the appropriate stiffnesses, is developed for use in the piping system model.

3.7.3.6 Three Components of Earthquake Motion

Seismic responses resulting from analysis of subsystems due to three components of earthquake motions are combined in the same manner as the seismic response resulting from the analysis of building structures (Section 3.7.2.6).

The following description is applicable to safety-related components and systems:

The system and equipment response is determined using three earthquake components, two horizontal and one vertical. Floor response spectra are generated for two perpendicular horizontal directions, (i.e., N-S, E-W) and the vertical direction. Piping and equipment analysis is performed with these response spectra components applied in the N-S, E-W, and vertical directions.

The damping values used in the analysis of equipment are those given in Table 3.7-1.

3.7.3.7 Combination of Modal Responses

When a response spectrum method of analysis is used to analyze a subsystem, the maximum response (accelerations, shears, and moments) in each mode is calculated independent of time. If the frequencies of the modes are well separated, the SRSS method of mode combination gives acceptable results; however, where the structural periods are not well separated, the modes are combined in accordance with Regulatory Guide 1.92. This is automatically performed by the piping analysis computer program SUPERPIPE.

The effects of seismic response of supports and equipment are not directly included in the seismic analysis of piping initially as equipment and supports are normally designed and analyzed subsequent to the piping analysis.

3.7.3.8 Analytical Procedures for Piping

All Seismic Category I piping is analyzed for seismic effects as described in Section 3.7.3.1.

3.7.3.8.1 Dynamic Analysis

Each piping system is idealized as a mathematical model consisting of lumped masses connected by elastic massless members. Appendages having significant dynamic effects on the piping system, such as motors attached to motor-operated valves, are included in the model. Using the elastic properties of the

9T [If inelastic methods are used in any System 80+ piping analysis, the details of the inelastic method and its acceptance criteria, as well as the scope and extent of its application will be provided with site-specific information.]*

The continuous piping system is modeled as an assemblage of beams. The mass of each beam is lumped equally at its associated end nodes, which are connected by massless elastic members, representing the physical properties of each segment. The pipe lengths between these mass points shall not be greater than the length that would produce a natural frequency equal to the cutoff frequency (ZPA) when calculated based on a simply supported beam. All concentrated weights on the piping system such as main valves, relief valves, pumps, and motors are modeled as lumped masses. The torsional effects of the valve operators and other equipment with offset center of gravity with respect to centerline of the pipe are included in the analytical model.

3.7.3.4 Basis for Selection of Frequencies

The basis for acceptability of the seismic design of equipment and subsystems is that the stresses and deformations produced by vibratory motion of the postulated seismic events, in combination with other coincident loadings, be within the established limits.

The seismic design is accomplished in a manner to account for the seismic response of structures, subsystems and components in their design as well as to maintain the resonant frequencies outside the range that is significantly excited by the forcing frequencies. The stiffness of the restraint and supports system is designed to maintain the fundamental frequencies of equipment and subsystems sufficiently removed from the resonant range and, thereby, maintain the seismic response within the established limits. If the natural frequencies of the equipment and supporting structures are in the same range where resonance can occur, the resonance is accounted for in the analysis.

3.7.3.5 Use of Equivalent Static Load Method of Analysis

The equivalent static load method involves the multiplication of the total weight of the equipment or component member by the specific seismic acceleration coefficient. The magnitude of the seismic acceleration coefficient is established on the basis of the expected dynamic response characteristics of the component. Components that can be adequately characterized as a single degree of freedom system are considered to have a modal participation factor of one. Seismic acceleration coefficients for multi-degree of freedom systems which may be in the resonance region of the amplified response spectra curves are increased by 50% to account conservatively for the increased modal participation. If the equipment natural frequency is above the frequency corresponding to the zero period acceleration (ZPA), the seismic acceleration coefficient is equal to 1.0 times the ZPA.

pipe, the stiffness matrix for the piping system is determined. This includes the effects of torsional, bending, shear, and axial deformations, as well as the local flexibilities of piping curved members. Next, the frequencies and mode shapes for all the significant modes of vibrations are calculated. After the frequency is determined for each mode, the corresponding horizontal and vertical spectral accelerations with appropriate damping are read from the appropriate response spectrum curves. For each mode, the inertia response forces, moments, displacements and accelerations are determined due to excitation in the three directions simultaneously (two horizontal and one vertical). Finally, the stresses are determined by taking the SRSS of the individual components. The relative displacement effects between piping supports are discussed in Section 3.7.3.1.

3.7.3.8.2 Allowable Stresses

Allowable stresses in the piping caused by an earthquake are in accordance with Section III of the ASME Code. Allowable stresses in the earthquake restraint components, such as snubbers, are in accordance with any additional stress limits that may have been established by ASME Code, Section III at the time the restraint components were purchased.

3.7.3.9 Multiple Supported Equipment Components with Distinct Inputs

When the equipment or component is supported at points with different elevations, either the envelope of these elevation response spectra or multiple support excitation is used for the seismic qualification of the equipment. For multiple support excitation, time history analysis methods are used.

3.7.3.10 Use of Constant Vertical Load Factors

In general, Seismic Category I subsystems are analyzed in the vertical direction using the methods specified in Section 3.7.3.1. No vertical static factors are used for subsystems.

3.7.3.11 Torsional Effects of Eccentric Masses

Piping systems are modeled to include projecting masses such as valve motor operators. The actual stiffness of the connecting member is not expected to influence the system appreciably. However, an approximation is made by assuming a member stiffness equal to that of the piping in which the valve is installed.

¶ [If independent support motion (ISM) response spectrum analysis methods are used in any System 80+ piping design, a detailed description of the methodology including a sample analysis and a description of the computer code and its verification will be provided with site-specific information.]*

Torsional effects of eccentric masses are also considered in the analysis of Seismic Category I subsystems other than piping.

3.7.3.12 Piping Outside Containment Structure

3.7.3.12.1 Buried Piping

Class 2 and 3 buried piping systems are designed according to the seismic analysis acceptance criteria for Seismic Category I buried piping systems. These criteria accept either dynamic analyses or equivalent static load methods with the consideration of seismic effects which are induced primarily by seismic wave passage and by differential movements between building attachment points and the ground surrounding the buried pipe.

Seismic effects in buried piping are self-limiting (displacement-induced strains and associated stresses) rather than being in equilibrium with an external load. In accordance with the ASME B&PV Code stress classification rules, the elastically calculated seismic stresses in buried piping, which are the products of strains and Young's moduli of the piping materials, are secondary stresses rather than primary stresses in nature. The design and stress acceptance criteria as provided below have been modified from the Code Subarticles NC/ND-3600. Nomenclatural symbols are defined in the Code unless noted otherwise.

3.7.3.12.1.1 General Requirements

General design requirements for ABB-CE System 80+ buried piping systems are as follows:

A. Areas of direct fault displacement and unstable soil conditions, such as liquefaction, are avoided for buried pipe installation.

B. Conformance to allowable structural and piping stresses after the line penetrates the Nuclear Annex is assured by the use of either expansion joints or flexible seals.

C. Minimum pipe wall thickness is per Code, Equation 3 of NC/ND-3641.1 as follows:

$$t_m = \frac{PD_o}{2(S + Py)} + A$$

D. Allowable external pressure is per NB-3133 as follows:

$$P_a = \frac{4B}{3(D_o/T)}$$

E. Since the failure of long and flexible buried piping in most cases is induced by excessive deflection rather than by high stress level, the total radial deformation of buried piping is limited to within 2% of pipe radius as follows:

$$\delta_r \leq 0.02 \frac{D_o}{2}$$

where, δ_r is the radial displacement of the pipe wall. 7

3.7.3.12.1.2 Weight Effects (Sustained Loads)

Evaluation of weight effects is performed with consideration of the following loads:

A. Dead loads, such as the self weight of pipe and the soil overburden pressure.

B. Live loads, such as weight of water content, highway/railroad loading, and construction equipment loading.

The effects of pressure, weight, and other sustained mechanical loads must meet the requirements of Code Equation 8 of NC/ND-3652 as follows:

$$S_{SL} = B_1 \frac{PD_o}{2t_n} + B_2 \frac{M_A}{Z} \leq 1.5\ S_h$$

3.7.3.12.1.3 Seismic Effects

Buried piping is seismically designed to sustain soil movements during earthquake ground motions. The structural integrity of the piping is evaluated by accounting for two primary effects of earthquake ground motions:

A. Strains and associated stresses induced in a long buried pipe by the free-field vibration resulting from motions of the surrounding soil mass (seismic wave passage). The maximum strains associated with the free-field vibration and the soil are computed based on the guidelines of References 10 and 11. Friction between the pipe and the surrounding soil may be considered using conservative estimates of the associated frictional forces.

B. Seismically induced differential movements of structures which the pipe enters or connects. Equivalent static

analysis is performed using the principles of beams on elastic foundations. The differential movements at the entry points are conservatively assumed as out-of-phase.

Buried piping experiences both axial and bending strains and associated stresses due to seismic wave effects, seismic differential movements, as well as thermal expansion/contraction. These high axial strains and associated stresses, normally insignificant in the aboveground piping systems, are caused mostly by seismic waves in conjunction with the soil friction. Therefore in addition to bending stresses, axial stresses are included in the Code stress check.

Seismic loads on buried piping are considered secondary loads, since they are generated by soil strains transmitted to the pipe and are therefore considered to be self-limiting. The effects of seismic loading, for which Level D (faulted with SSE loading) service limits are designed, must meet the requirements of the following equations in lieu of Code Equation 9 of NC/ND-3655:

Level D (faulted)

$$S_{OL} = \frac{iM_{SSE}}{Z} + \frac{iM_C}{Z} + \frac{F_{a(SSE)}}{A_p} + \frac{F_{at}}{A_p} \leq 3S_H$$

where, M_{SSE} is the range of resultant moments on cross section of pipe due to earthquake loading, including the effects of anchor displacements due to earthquake. The M/Z term can be replaced by the product of strain and Young's modulus of the piping material.

M_c is the range of resultant moments on cross section of pipe due to thermal expansion.

$F_{a(SSE)}$ is the range of axial forces on straight runs of buried pipe due to earthquake loading, including the effects of anchor displacements due to earthquake. The F_a/A_p term can be replaced by the product of strain and Young's modulus of the piping material. Axial stresses due to seismic soil movements are considered significant and are therefore included for the buried pipe stress check.

F_{at} is the range of axial forces on straight runs of pipe due to thermal expansion and contraction frictional forces.

A_p is the cross sectional metal area of the pipe.

D. Allowable external pressure is per NB-3133 as follows:

$$P_a = \frac{4B}{3(D_o/T)}$$

E. Since the failure of long and flexible buried piping in most cases is induced by excessive deflection rather than by high stress level, the total radial deformation of buried piping is limited to within 2% of pipe radius as follows:

$$\delta_r \leq 0.02 \frac{D_o}{2}$$

where, δ_r is the radial displacement of the pipe wall.

3.7.3.12.1.2 Weight Effects (Sustained Loads)

Evaluation of weight effects is performed with consideration of the following loads:

A. Dead loads, such as the self weight of pipe and the soil overburden pressure.

B. Live loads, such as weight of water content, highway/railroad loading, and construction equipment loading.

The effects of pressure, weight, and other sustained mechanical loads must meet the requirements of Code Equation 8 of NC/ND-3652 as follows:

$$S_{SL} = B_1 \frac{PD_o}{2t_n} + B_2 \frac{M_A}{Z} \leq 1.5\ S_h$$

3.7.3.12.1.3 Seismic Effects

Buried piping is seismically designed to sustain soil movements during earthquake ground motions. The structural integrity of the piping is evaluated by accounting for two primary effects of earthquake ground motions:

A. Strains and associated stresses induced in a long buried pipe by the free-field vibration resulting from motions of the surrounding soil mass (seismic wave passage). The maximum strains associated with the free-field vibration and the soil are computed based on the guidelines of References 10 and 11. Friction between the pipe and the surrounding soil may be considered using conservative estimates of the associated frictional forces.

B. Seismically induced differential movements of structures which the pipe enters or connects. Equivalent static

3.7.3.12.1.4 Thermal Expansion and Contraction Effects

The effects of thermal expansion/contraction must meet the requirements of modified Code Equation 10 of NC/ND-3653.2(a) or modified Code Equation 11 of NC/ND-3653.2(c).* Modified Code Equation 11 considers the combined effects of pressure, weight, other sustained mechanical loads, and thermal expansion/contraction. Both Equations 10 and 11 are modified to include axial stresses due to thermal expansion/contraction frictional forces, which are considered to be significant for buried pipes.

THIS PAGE INTENTIONALLY BLANK

Modified Code Equation 10

$$S_E = \frac{iM_C}{Z} + \frac{F_{at}}{A_p} \leq S_A$$

Modified Code Equation 11

$$S_{TE} = \frac{PD_o}{4t_n} + 0.75i\left(\frac{M_A}{Z}\right) + i\left(\frac{M_C}{Z}\right) + \frac{F_{at}}{A_p} \leq (S_h + S_A)$$

where, F_{at} is the range of axial forces on straight runs of buried pipe caused by the frictional forces between the soil and the pipe during thermal expansion and contraction.

3.7.3.12.1.5 Non-Repeating Differential Settlement Effects

The effects of existing permanent, unidirectional and non-repeating differential settlement, including building settlement and the effects due to loss of support, must meet the requirements of Code Equation 10a of NC/ND-3653.2(b):

$$\frac{iM_D}{Z} \leq 3S_C$$

3.7.3.12.2 Above Ground Piping

Seismic design criteria and methods of accounting for the effects of differential movement of buildings on piping and penetrations are described in Sections 3.7.2.1.2 and 3.7.2.7.

3.7.3.13 Interaction of Other Piping with Category I Piping

The protection of Category I piping from possible adverse effects of other piping during an earthquake is accomplished by several methods. Specifically, these methods are:

A. Non-Category I piping systems are designed to be isolated from any Category I piping system by either a constraint or barrier, or are remotely located with regard to the seismic Category I piping system. If it is not feasible or practical to isolate the Category I piping system, adjacent non-Category I piping is analyzed according to the same seismic criteria as applicable to the Category I piping system. For Non-Category I piping systems attached to Category I piping systems, the dynamic effects of the Non-Category I piping is simulated in the modeling of the Category I piping. The attached Non-Category I piping, up

to the first anchor beyond the interface, is also designed in such a manner that during an earthquake of SSE intensity it will not cause a failure of the Category I piping. 7*

B. [All Category I boundary valves are designed to meet seismic criteria.7* A valve always serves as a pressure boundary and constitutes the seismic to non-seismic boundary. If failure in the non-seismic portion of the system could cause loss of function of the safety system, then an appropriate automatic or remote manual operator would be used if the valve is open during normal reactor operation.

C. {The pressure boundary valve is protected by restraining or anchoring the non-seismic portion of the system7* as discussed in Section 3.7.3.13.A.

3.7.3.14 Seismic Analysis of Reactor Internals, Core and CEDMs

3.7.3.14.1 Reactor Internals and Core

The seismic analyses of the reactor internals and core consist of separate analyses performed in the horizontal and vertical directions.

In the horizontal direction, because the relative displacements between the core and core shroud and between the core support barrel and pressure vessel snubbers are sufficiently large to close the gaps that exist between these components, a nonlinear horizontal time history analysis is performed. The horizontal nonlinear analysis is divided into two parts. In the first part, the internals and core are analyzed to obtain the internals' response and the proper dynamic input for the reactor core model. In the second part, the core plate motion from the first part is applied to a more detailed nonlinear model of the reactor core. The input excitation to the internals model is the response time-history of the reactor vessel at the internals support determined from the RCS analysis. Coupling effects between the internals and reactor vessel are accounted for by including a simplified representation of the internals with the RCS model. This is discussed in Section 3.7.2.

In the vertical direction, both linear response spectrum modal analysis and non-linear time history analysis methods are used. For linear analysis cases where the response of the core is sufficiently large to cause it to lift off the core plate, non-linear methods are used. The response accelerations of the reactor vessel flange provide the input for both the linear and non-linear internals vertical analyses.

to the first anchor beyond the interface, is also designed in such a manner that during an earthquake of SSE intensity it will not cause a failure of the Category I piping.]"

B. [All Category I boundary valves are designed to meet seismic criteria.]" A valve always serves as a pressure boundary and constitutes the seismic to non-seismic boundary. If failure in the non-seismic portion of the system could cause loss of function of the safety system, then an appropriate automatic or remote manual operator would be used if the valve is open during normal reactor operation.

C. {The pressure boundary valve is protected by restraining or anchoring the non-seismic portion of the system}" as discussed in Section 3.7.3.13.A.

3.7.3.14 Seismic Analysis of Reactor Internals, Core and CEDMs

3.7.3.14.1 Reactor Internals and Core

The seismic analyses of the reactor internals and core consist of separate analyses performed in the horizontal and vertical directions.

In the horizontal direction, because the relative displacements between the core and core shroud and between the core support barrel and pressure vessel snubbers are sufficiently large to close the gaps that exist between these components, a nonlinear horizontal time history analysis is performed. The horizontal nonlinear analysis is divided into two parts. In the first part, the internals and core are analyzed to obtain the internals' response and the proper dynamic input for the reactor core model. In the second part, the core plate motion from the first part is applied to a more detailed nonlinear model of the reactor core. The input excitation to the internals model is the response time-history of the reactor vessel at the internals support determined from the RCS analysis. Coupling effects between the internals and reactor vessel are accounted for by including a simplified representation of the internals with the RCS model. This is discussed in Section 3.7.2.

In the vertical direction, both linear response spectrum modal analysis and non-linear time history analysis methods are used. For linear analysis cases where the response of the core is sufficiently large to cause it to lift off the core plate, non-linear methods are used. The response accelerations of the reactor vessel flange provide the input for both the linear and non-linear internals vertical analyses.

TABLE 3.7-1

DAMPING VALUES**

Structure	Safe Shutdown Earthquake (Percent of Critical)
Welded steel structures	4.0
Bolted steel structures	7.0
Prestressed concrete structures	5.0
Reinforced concrete structures	7.0
Equipment (steel assembly)	3.0
[Piping* (diameter ≤12 inches)	2.0
Piping* (diameter >12 inches)	3.0]*

* [When response spectra method of analysis is used, damping values may be based on Code Case N-411-1 as limited by Regulatory Guide 1.84.]*

** Soil material dampings are provided in Section 2.5.2.

RCS. For the number of cycles pertaining to fatigue effects of cyclic motion associated with the SSE, refer to Section 3.7.3.2. Design load combinations for ASME Class 1, 2 and 3 components are given in Section 3.9.3.

3.9.1.2 Computer Programs Used in Stress Analyses

3.9.1.2.1 Code Class Systems, Components, and Supports

The following paragraphs provide a summary of the applicable computer programs used in the stress and structural analyses for ASME Code Class systems, components, and supports in the CESSAR-DC scope. The summaries include individual descriptions and applicability data. The computer codes employed in these analyses have been verified in conformance with design control methods, consistent with the quality assurance program described in Chapter 17.

If computer codes that are not listed below are used, they will be compared to NRC-benchmarked or approved codes. Computer codes used for piping dynamic analysis will be benchmarked in accordance with NUREG/CR-6128. See also Section 3.9.

3.9.1.2.1.1 MDC STRUDL

The MDC STRUDL computer program provides the ability to specify characteristics of framed structure and three-dimensional solid structure problems, perform static and dynamic analyses, and reduce and combine results.

Analytic procedures in the pertinent portions of MDC STRUDL apply to framed structures. Framed structures are two- or three-dimensional structures composed of slender, linear members that can be represented by properties along a centroidal axis. Such a structure is modeled with joints, including support joints, and members connecting the joints. A variety of force conditions on members or joints can be specified. The member stiffness matrix is computed from beam theory. The total stiffness matrix of the modeled structures is obtained by appropriately combining the individual member stiffness.

The stiffness analysis method of solution treats the joint displacements as unknowns. The solution procedure provides results for joints and members. Joint results include displacements and reactions and joint loads as calculated from member end forces. Member results are member end forces and distortions. The assumptions governing the beam element representation of the structure are as follows: linear, elastic, homogeneous, and isotopic behavior, small deformation, plane sections remain plane, and no coupling of axial, torque, and bending.

The program is used to define the dynamic characteristics of the structural models used in the dynamic seismic analyses of the reactor coolant system components. The natural frequencies and mode shapes of the structural models and the influence coefficients which relate member end forces and moments and support reactions to unit displacements are calculated. The

Class CS components are shown in Table 3.9-1. The System 80+ design basis events are nearly identical to System 80. The format has been revised to detail the individual transients considered in the design basis. A small number of events (e.g., frequency control) have been added in response to the EPRI Utilities Requirement Document (URD). The 60-year frequency of occurrence for all events was re-computed based on the latest industry databases (References 48 and 49). Particular emphasis was placed on severe transients (i.e., feeding cold feedwater to a hot steam generator) and/or transients with a high design frequency of occurrence (i.e., frequency control). Where appropriate, excessive conservatism has been removed from the System 80 values. The resulting System 80+ events and frequencies conservatively represent the 60-year design basis.

The design basis events are classified as normal, upset, emergency, faulted and test. The normal and test events are planned operations that will occur during the life of the plant. Upset events are occurrences that may occur during the life of the plant (i.e., anticipated operational occurrences). Emergency and faulted events are not expected to occur (i.e., accidents) but are included in the design basis for additional design margin. The normal and test events are selected by reviewing the expected plant operations. The upset, emergency and faulted events are determined by reviewing industry databases (References 48 and 49) for events that have occurred, or that may be postulated to occur, based on observed plant behavior.

Normal and test event frequencies are determined by summing the number of expected plant operations over the 60-year design life. The frequencies for upset, emergency and faulted events are determined on a probabilistic basis utilizing industry databases (see References 48 and 49). The stated 60-year design frequency of occurrence (see Table 3.9-1) is always greater than the expected frequency of occurrence.

Conservative mathematical models and methodology are used to determine the thermal-hydraulic consequences of the design basis events on individual plant components. The design margin is further enhanced by enveloping similar events and using the most conservative thermal-hydraulic consequences to represent a composite group. The group frequency is then determined by algebraically summing the individual design frequencies.

Pressure and thermal stress variations associated with the design transients are considered in the design of supports, valves, and piping within the reactor coolant pressure boundary (RCPB).

In addition to the design transients listed above and included in the fatigue analysis, the loadings produced by the SSE are also applied in the design of components and support structures of the

3.9.1.2.2.9 COSMOS

COSMOS is a general purpose program, commercially available, which can be used to perform finite element, dynamic, eigenvalue, response spectra, random vibration, and other structural evaluations. The program has advanced features which include complex geometry mesh generation, color graphics and postprocessing. COSMOS can solve problems using models with up to 5000 nodes and 8000 degrees of freedom. It has a library of 60 element types which can be represented with linear, isotropic, orthotropic, non-linear and composite material.

Some of the non-linear capabilities include non-linear buckling, large strains, stress stiffening, kinematic hardening, gaps and friction.

Some of the postprocessing features include node and element plots, color stress contour plots, various view capabilities, zoom features, shade and animation.

The COSMOS program can also communicate with ANSYS (Section 3.9.1.2.2.2).

3.9.1.3 Experimental Stress Analyses

[When experimental stress analysis is used, it is performed in accordance with Appendix II of ASME Boiler and Pressure Vessel Code, Section III, Division I.]*

3.9.1.4 Considerations for the Evaluation of the Faulted Condition

3.9.1.4.1 Seismic Category I RCS Items

The major components of the reactor coolant system (RCS) are designed to withstand the forces associated with the design basis pipe breaks discussed in Section 3.6, in combination with the forces associated with the Safe Shutdown Earthquake and normal operating conditions. For structural evaluation, the design basis pipe breaks are those breaks for which leak-before-break cannot be demonstrated. Since the dynamic effects of breaks in piping systems listed in Section 3.6.2.2.1 are eliminated by leak-before-break, the pipe break loads analysis procedure considers only those branch line pipe breaks not eliminated by leak-before-break.

See Section 3.9.3 for discussion of loading combinations.

Analyses are performed to generate component loads and motions due to the forces associated with branch line pipe breaks. The analyses account for the reactor vessel and supports, major

SAPIV has been applied to the eigenvalue and response spectra analyses of spent fuel storage racks and lifting rig structures.

The SAPIV code is used in the computation of dynamic response of control element drive mechanisms under mechanical and seismic loads. Both modal analysis and response spectrum capabilities of the code are used to find the natural frequencies and mode shapes and the dynamic loads in CEDM components. ANSYS (3.9.1.2.2.2) is also used as an alternative to SAPIV.

SAPIV is commercially available software and has had sufficient use to justify its applicability and validity. Extensive verification of the C-E version has been performed to supplement the public documentation.

3.9.1.2.2.7 CEFLASH-4B

The CEFLASH-4B computer code (Reference 14) predicts the reactor pressure vessel pressure and flow distribution during the subcooled and saturated portion of the blowdown period of a Loss-of-Coolant-Accident (LOCA). The equations for conservation of mass, energy and momentum along with a representation of the equation of state are solved simultaneously in a node and flow path network representation of the primary reactor coolant system.

CEFLASH-4B provides transient pressures, flow rates and densities throughout the primary system following a postulated pipe break in the reactor coolant system.

The CEFLASH-4B computer code is a modified version of the CEFLASH-4A code (References 15 through 17). The CEFLASH-4A computer code has been approved by the NRC (References 18 and 19). The capability of CEFLASH-4B to predict experimental blowdown data is presented in Reference 14.

3.9.1.2.2.8 LOAD

LOAD calculates the applied forces of the axial internals model which is contained within water control volumes using results from the CEFLASH-4B blowdown loads analysis as input. The fluid momentum equation is applied to each volume and a resultant force is calculated. Each force is then apportioned to the various structural nodes contained within the volume. Use of the fluid momentum equation takes into account pressure forces, fluid friction, water weight, and momentum changes within each volume. The resultant forces are combined with the reactor vessel motions obtained from the reactor coolant system analysis before the structural responses are determined. The LOAD code has been verified by demonstrating that its solutions are substantially identical to those obtained from hand calculations.

Reactor coolant loop piping and associated components and component supports are designed and analyzed by Combustion Engineering. Loading conditions, stress limits, design transients, and methods of analysis for ASME Code Class 1 reactor coolant loop piping and associated components and component supports are discussed in Section 3.9.3.1.

The site-specific SAR will provide information on the specific edition of the ASME Code used in the site-specific design. See also Section 1.8.

3.9.3.1 Loading Combinations, Design Transients and Stress Limits

The loading combinations specified for the design ASME B&PV Section III Code Class 1 components, supports, and piping are categorized as normal, upset, emergency and faulted. The following specific loading combinations are specified for design:

A. The concurrent loadings associated with the Level-A (normal) plant conditions of dead weight, pressure and the thermal and expansion effects during startup, hot standby, power operation and normal shutdown to cold shutdown conditions.

B. The concurrent loadings associated with either the normal plant condition or the Level-B (upset) plant condition. The vibratory motion of the Safe Shutdown Earthquake (SSE) is included in the fatigue evaluation in accordance with Section 3.7.3.2.

C. The concurrent loadings associated with the Level-C (emergency) condition.

D. The concurrent loadings associated with the Level-A (normal) plant condition, the vibratory motion of the SSE, and the dynamic system loadings associated with the Level-D (faulted) system condition (postulated pipe rupture for branch line breaks not eliminated by leak before break analysis). [The SSE and pipe rupture loadings are combined by the SRSS method in accordance with the guidelines of NUREG-0484, Rev. 1, 1980 or by a more conservative method.]*

The specific design transients specified for design are discussed in Section 3.9.1.1. The loading combinations of the section and the stress limits associated with them, as defined in the Code, also apply to the internals parts which are essential to the component in performing its safety function.

ASME B&PV Code Class 1, 2 and 3 piping and components of fluid systems are designed and constructed in accordance with Section III of the ASME Boiler and Pressure Vessel Code. Hydrostatic testing is performed per Section III.

Design pressure, temperature, and other loading conditions that provide the bases for design of fluid systems are presented in the sections which describe the systems.

Stress analysis is performed to determine structural adequacy of pressure components under the operating conditions of normal, upset, emergency or faulted, as applicable.

Significant structural discontinuities such as nozzles and flanges are considered. In addition to the design calculation required by Section III of the ASME B&PV Code, stress analysis is also performed by methods outlined in the Code appendices or by other methods by reference to analogous codes or other published literature.

3.9.3.1.1 ASME Code Class 1 Components and Supports

Design transients for core support structures and ASME Code Class 1 components, supports and piping are discussed in Section 3.9.1.1. Loading combinations for ASME Code Class 1 components are described in Table 3.9-2. Stress limits for ASME Code Class 1 components, supports and piping are described in Table 3.9-3. The operating pressures of Code Class 1 active valves are limited to the pressures taken from the applicable primary pressure class pressure-temperature rating of the ASME Code, Section III, for the maximum temperature for the applicable condition.

3.9.3.1.2 Core Support Structures (Class CS) and Internal Structures (Class IS)

Design transients for core support structures and reactor internals structures are discussed in Section 3.9.1.1. Loading combinations and stress limits are presented in Section 3.9.5.

3.9.3.1.4.3 [Functional Capability, ASME Code Class 1, 2 and 3

To satisfy functional capability requirements, the piping is designed to meet a D/t ratio of <50 in accordance with NUREG-1367 and the allowable stress from the ASME Code of $3.0S_m$ (Class 1) or $3.0S_h$ (Class 2 and 3), but not greater than $2.0S_y$.]*

3.9.3.1.5 Preparation of Design Specifications

Design specifications for ASME Section III components and supports are prepared using guidelines given in Reference 42.

3.9.3.2 Pump and Valve Operability Assurance

3.9.3.2.1 Active ASME Code Class 2 and 3 Pumps and Class 1, 2 and 3 Valves Furnished with the NSSS

3.9.3.2.1.1 Operability Assurance Program

Active pumps and valves are defined as pumps and valves and those components that must perform a mechanical motion in order to shut down the plant, maintain the plant in a safe shutdown condition, or mitigate the consequences of a postulated event. The operability (i.e., performance of this mechanical motion) of active components during and after exposure to design bases events is confirmed by:

A. Designing each component to be capable of performing all safety functions during and following design bases events. The design specification includes applicable loading combinations, and conservative design limits for active components. The specification requires that the manufacturer demonstrate operability by analysis, by test, or by a combination of analysis and test. The results are independently reviewed by the NSSS Supplier considering the effects of postulated failure modes on operability. Internals parts which are essential to the component in performing its safety function are analyzed and/or tested as an assembled component to validate operability.

B. Analysis and/or test demonstrating the operability of each design under the most severe postulated loadings. Methods/results of operability demonstration programs are detailed in Sections 3.9.3.2.1.2 and 3.9.3.2.1.3.

C. Inspection of each component to assure compliance of critical parameters with specifications and drawings. This inspection confirms that specified materials and processes were used, that wall thicknesses met code requirements, and that fits and finishes met the manufacturer's requirements based on design clearance requirements.

D. Shop testing of each component to verify "as-built" conditions, as defined in Sections 3.9.3.2.1.2 and 3.9.3.2.1.3.

E. Startup and periodic in-service testing in accordance with ASME Boiler and Pressure Vessel Code, Section XI to demonstrate that the active pumps and valves are in operating condition throughout the life of the plant.

NSSS active pumps are listed below with a brief description of active safety function of each. NSSS active valves are listed in Table 3.9-4.

Active Components	Active Safety Function
Safety injection pumps	Operate at flow rates to runout
Shutdown cooling pumps	Operate at design flow
Containment spray pumps	Operate at design flow

3.9.3.2.1.2 Operability Assurance Program Results for Active Pumps

Operability of the Safety Injection, Shutdown Cooling and Containment Spray pumps under required conditions demonstrated by analyses of the assemblies and by analyses and tests of the motors.

For the safety injection, shutdown cooling and containment spray pumps, allowable stresses are not exceeded, clearances are acceptable and shaft and pedestal bolt deflections do not cause stresses to exceed the normal values.

Where necessary, lumped mass models are used with the computer programs to determine the natural frequencies and displacements. The models are conservative (i.e., simplifications tend to make them more flexible).

To verify "as-built" conditions the pumps are hydrostatically tested in accordance with the ASME B&PV Code, Section III to confirm acceptability of structural integrity of pressure retaining parts, tested for seal leakage, and tested for performance and NPSH characteristics in accordance with the Hydraulic Institute Standard to verify operation within specified parameters. The motors are Class IE and are tested in accordance with IEEE Standard 112A-1978 to verify operation within specified parameters. Additionally, IEEE Standard 323-1974, as endorsed by Regulatory Guide 1.89, and IEEE Standard 344-1987 as endorsed by Regulatory Guide 1.100 Rev. 2 dated June 1988, are applicable for motors to assure operability during and following design basis events.

Due to the simple characteristics of check valves and other compact valves, they are qualified by the following tests and analysis:

A. Stress analysis of the attached piping for SSE loads.

B. In-shop hydrostatic test.

C. In-shop seat leakage test.

D. Periodic valve exercise and inspection to assure the functional ability of the valve.

Using the methods described, safety-related active valves in the system are qualified for operability during a seismic event.

3.9.3.3 Design and Installation Details for Mounting of Pressure Relief Devices

Safety valves and relief valves are analyzed in accordance with the ASME Section III Code.

[The method of analysis for safety valves and relief valves suitably accounts for the time-history of loads acting immediately following a valve opening (i.e., first few milliseconds). The fluid-induced forcing functions are calculated for each safety valve and relief valve using one-dimensional equations for the conservation of mass, momentum, and energy. The calculated forcing functions are applied at locations along the associated piping where a change in fluid flow direction occurs. Application of these forcing functions to the associated piping model constitutes the dynamic time-history analysis.]* The dynamic response of the piping system is determined from the input forcing functions. Therefore, a dynamic amplification factor is inherently accounted for in the analysis. [Alternately, an equivalent static analysis may be used following the criteria of Appendix O of the ASME Code Section III as supplemented by the additional criteria of SRP3.9.3, Section II.2.]*

Snubbers or strut-type restraints are used as required. The stresses resulting from the loads produced by the sudden opening of a relief or safety valve are combined with stresses due to other pertinent loads and are shown to be within allowable limits of the ASME Section III Code. Also, the analyses show that the loads applied to the nozzles of the safety and relief valves do not exceed the maximum loads specified by the manufacturer. Jurisdictional boundaries between ASME Section III Class 1, 2 and 3 component supports and the building structure are established in accordance with ASME Section III, Subsection NF.

3.9.3.4 Component Supports

Jurisdictional boundaries between ASME Section III Class 1, 2 and 3 component supports and the building structure are established in accordance with ASME Section III, Subsection NF.

ASME B&PV Code Section III Class 1, 2 and 3 component supports are designed and constructed in accordance with Section III of the ASME B&PV Code and Code Case(s).

Seismic Category I component supports are designed to meet the requirements of Subsection NF, Section III of the ASME Code. Welding fabrication and installation, nondestructive examination (NDE) and acceptance standards shall be in accordance with Subsection NF, Section III of the ASME Code. In addition, visual weld acceptance criteria shall be per the Nuclear Construction Issue Group (NCIG) standard NCIG-01 (Reference 51).

Radiographic examinations will be accepted by a nondestructive examination (NDE) Level III examiner prior to final acceptance. See also Section 3.9.

Confirmation that facility welding activities are in compliance with the certified design commitments shall include verifications of the following by individuals other than those who performed the activity:

1. Facility welding specifications and procedures meet the applicable ASME Code requirements.

2. Facility welding activities are performed in accordance with the applicable ASME Code requirements.

3. Welding activities related records are prepared, evaluated and maintained in accordance with the ASME requirements.

4. Welding processes used to weld dissimilar base metal and welding filler metal combinations are compatible for the intended applications.

5. The facility has established procedures for qualifications of welders and welding operators in accordance with the applicable ASME Code requirements.

6. Approved procedures are available and are used for pre-heating and post-heating of welds, and those procedures meet the applicable requirements of the ASME Code.

7. Completed welds are examined in accordance with the applicable examination method required by the ASME Code.

D. For engineered, large bore snubbers, issuance of a design specification to the snubber supplier, describing the required structural and mechanical performance of the snubber; verification that the specified design and fabrication requirements are met.

E. Verification that snubbers are properly installed and operable prior to plant operation, through visual inspection and through measurement of thermal movements of snubber-supported systems during start-up tests.

F. A snubber in-service inspection and testing program, which includes periodic maintenance and visual inspection, inspection following a faulted event, a functional testing program, and repair or replacement of snubbers failing inspection or test acceptance criteria.

Sect. 3.9.3.4

Site-specific information will include a listing of all safety-related components which utilize snubbers, in accordance with SRP 3.9.3.

Energy absorbing and/or non-linear piping restraints may be used on System 80+. If used, a description of the methodology used to analyze and design the piping systems incorporating these elements will be provided with site-specific information. TAG

3.9.4 CONTROL ELEMENT DRIVE MECHANISMS

3.9.4.1 Descriptive Information of CEDM

The control element drive mechanism (CEDMs) are magnetic jack type drives used to vertically position and indicate the position of the control element assemblies (CEAs). Each CEDM is capable of withdrawing, inserting, holding, or tripping the CEA from any point within its 153-inch stroke in response to operation signals.

The CEDM is designed to function during and after all normal plant transients. The CEA drop time for 90% insertion is 4.0 seconds maximum. The drop time is defined as the interval between the time power is removed from the CEDM coils to the time the CEA has reached 90% of its fully inserted position. The CEDM pressure boundary components have a design life of 60 years. The CEDM is designed to operate without maintenance for a minimum of 1-1/2 years and without replacing components for a minimum of 3 years. The CEDM is designed to function normally during and after being subjected to seismic loads. The vibratory motion of the Safe Shutdown Earthquake is included in the fatigue evaluation in accordance with Section 3.7.3.2. The CEDM will allow for tripping of the CEA during and after a Safe Shutdown Earthquake.

The design and construction of the CEDM pressure housing fulfill the requirements of the ASME boiler and Pressure Vessel Code, Section III, for Class 1 vessels. The CEDM pressure housings are part of the reactor coolant pressure boundary, and they are designed to meet stress requirements consistent with those of the vessel. The pressure housings are capable of withstanding, throughout the design life, all normal operating loads, which include the steady-state and transient operating conditions specified for the vessel. Mechanical excitations are also defined and included as a normal operating load. The CEDM pressure housings are service rated at 2500 psi at 650°F. The loading combinations and stress limit categories are presented in Table 3.9-14 and are consistent with those defined in the ASME code.

The design duty requirements for the CEDM is a total cumulative CEA travel of 100,000 feet operation without loss of function.

The test programs performed in support of the CEDM design are described in Section 3.9.4.4.

3.9.4.1.1 Control Element Drive Mechanism Design Description

The CEDMs are mounted on nozzles on top of the reactor vessel closure head. The CEDMs consist of the upper and lower CEDM pressure housings, motor assembly, coil stack assembly, reed switch assemblies, and extension shaft assembly. The CEDM is shown in Figure 3.9-8. The drive power is supplied by the coil stack assembly, which is positioned around the CEDM housing. Two position indicating reed switch assemblies are supported by the upper pressure housing shroud, which encloses the upper pressure housing assembly.

The lifting operation consists of a series of magnetically operated step movements. Two sets of mechanical latches are utilized engaging a notched extension shaft. To prevent excessive latch wear, a means has been provided to unload the latches during the engaging operations. The magnetic force is obtained from large dc magnet coils mounted on the outside of the lower pressure housing.

Power for the electromagnets is obtained from two separate supplies. A control programmer actuates the stepping cycle and moves the CEA by a forward or reverse stepping sequence. Control element drive mechanism hold is obtained by energizing one coil at a reduced current, while all other coils are deenergized. The CEAs are tripped upon interruption of electrical power to all coils. Each CEDM is connected to the CEAs by an extension shaft.

1.0 PIPING DESIGN

1.1 GENERAL

[Seismic Category I small and large bore piping]* as defined in Section 3.2.1, [is designed to meet the analysis requirements of the ASME Boiler and Pressure Vessel (B&PV) Code, Section III, Subarticles NB-3650, NC-3650, or ND-3650.]*

Seismic Category II small and large bore piping, as defined in Section 3.2.1, is analyzed to ensure that the SSE does not adversely impact safety-related equipment or components. Category II requirements are normally satisfied by analyzing the piping to the same criteria as Seismic Category I, or ASME B 31.1.

The analysis requirements described in this appendix apply only to Seismic Category I and II large and small bore piping.

1.2 DESIGN CONSIDERATIONS

1.2.1 PRESSURE

The pipe wall thickness is sized to accommodate the specified internal pressures and meet the requirements of the ASME B&PV Code, Section III, Subarticles NB-3640, NC-3640 or ND-3640. Stresses due to the system design pressures and maximum peak pressures are included in the acceptance criteria (see Section 1.6 of this appendix).

1.2.1.1 Intersystem LOCA

Low-pressure piping systems that interface with the reactor coolant pressure boundary (RCPB) are sized for Intersystem LOCA criteria, as discussed in Section 3.3 of Appendix 5E.

1.2.2 GRAVITY

The weight of the pipe, in-line components, contents of the pipe and insulation are included. The weight of water during hydrostatic testing is considered for steam or air-filled lines.

1.2.3 THERMAL

The effect of thermal expansion of the system due to the design temperature is included. Possible operating modes of the system that result in more severe thermal expansion stresses than the entire system at design temperature are considered.

The effects of anchor movement due to thermal expansion of equipment or other piping are considered.

1.2.4 SEISMIC

The effects of earthquake loading are considered. The inertia loads and movements, including earthquake anchor movements, and the effects of fatigue are included in the analysis.

1.2.4.1 Seismic Anchor Movements

Seismic anchor motion is included for piping supported by more than one structure by applying; 1) the building seismic movements, and/or 2) equipment seismic movements, as support movements on the pipe.

The support movements are included in the most conservative combination for adjacent structures to give the maximum stress in the pipe, unless the relative time phasing of the motions of the supporting structures or equipment is determined by simultaneous time history analyses. The effects of seismic anchor motion on the piping are included for the safe shutdown earthquake (SSE).

Seismic anchor movements of headers are also considered in the analysis of decoupled branch lines.

1.2.5 WIND/TORNADO

Exposed piping is designed to withstand wind and tornado loads. Simultaneous wind and tornado loads are not considered.

1.2.6 FLUID TRANSIENT LOADINGS

1.2.6.1 Relief/Safety Valve Thrust

Relief valve thrust loads are considered for both open and closed valve discharge cases. The relief valve thrust load is a function of the valve opening time, flow rate, fluid properties, and flow area. Loads are input as static loads in the piping analysis with appropriate dynamic load factors applied. Alternatively, a dynamic analysis is performed where the static analysis results in an overly conservative design. The analysis methods are discussed in Section 1.4.5 of this appendix. Where conditions exist which result in water or steam hammer effects, they are evaluated and identified for inclusion in the piping analysis.

1.2.6.2 Water and Steam Hammer

Water and steam hammer are dynamic loadings on piping that are caused by a sudden change in momentum of the flow medium due to a rapid system transient and are considered in the analysis. Typically, transients are caused by pump start or pump trip, filling a voided line, check valve actuation, relief valve operation, steam turbine trip, and rapid control valve operation.

1.2.6.3 Other Loadings

Other fluid transient loadings such as pump start, check valve slam, pressure forces on unbalanced expansion joints, and filling empty lines are considered.

value of Young's modulus at temperature, E_{hot}. The ASME Code requires that stresses be based on E_{cold}. This is accomplished by multiplying the analysis results by E_{cold}/E_{hot}.

All possible operating modes are evaluated to determine the highest range of thermal expansion stress. The effects of anchor movement due to thermal expansion of equipment or other piping are also considered.

[Lines with maximum temperatures less than 150°F which connect to equipment with thermal movements < 1/16 inch are not analyzed for thermal expansion.]*

1.4.3 SEISMIC ANALYSIS

Seismic analysis of a piping system generally are performed using both dynamic and static techniques. A dynamic analysis is performed to evaluate the inertia loads developed as the mass of the piping is accelerated due to seismic motion. The static analysis is performed to determine loading resulting from differential seismic movements of structures or large lines to which piping is attached.

1.4.3.1 Static Analysis

The equivalent static load method involves the multiplication of the total weight of the equipment or component member by the specific seismic acceleration value. The magnitude of the seismic acceleration coefficient is established on the basis of the expected dynamic response characteristics of the component. Components that can be adequately characterized as a single degree of freedom system are considered to have a modal participation factor of one. Therefore, the acceleration value from the spectrum which corresponds to the single degree of freedom frequency is used. Seismic acceleration values for multi-degree of freedom systems are determined by increasing the peak acceleration from the applicable amplified response spectra curves by a factor of 1.5 to account conservatively for the increased modal participation. If the equipment natural frequency is above the frequency corresponding to the zero period acceleration (ZPA), the seismic acceleration value is equal to 1.0 times the ZPA. The ZPA is the response spectrum acceleration in the rigid range of the spectrum. It corresponds to the peak acceleration of the input on which the response spectrum is based. The ZPA frequency is the lowest frequency at which the response returns to approximately the zero-period acceleration.

The following points are considered in performing the analysis:

A. Inertia loads are applied separately in the x, y, and z directions, and the results of the 3 separate analyses are combined by SRSS.

1.2.7 PIPE BREAK LOADS

Pipe break loadings consist of pipe whip, jet impingement, differential pressure, support movements, or temperature increases resulting from the rupture of nearby pipes other than the line under consideration. Pipe break loads are considered.

1.2.8 THERMAL STRATIFICATION

Piping subjected to stratified flow conditions are evaluated for the effects of thermal stratification.

1.2.9 MISSILE LOADS

Piping subjected to the loads described in Section 3.5.1 are evaluated for the effects of missiles.

1.2.10 THERMAL TRANSIENTS

Thermal transient loadings are considered in the analysis of ASME Class 1 lines.

1.3 DESIGN LOAD COMBINATIONS

Loading combinations, in accordance with Section 3.9.3.1, applicable to ASME Class 1 piping, are detailed in Table 3.9-10.

Load combinations applicable to ASME Class 2 and 3 piping, are detailed in Table 3.9-11.

1.4 ANALYSIS

Static and dynamic analyses, as defined in this section, are based on linear elastic analysis methods.

1.4.1 GRAVITY ANALYSIS

The gravity analysis includes the weight of the pipe or piping component, the weight of the enclosed fluid, the weight of all other sustained mechanical loads, and the weight of any attached insulation. Also, if the system contents vary during operation, the analysis considers all modes of operation. Weight due to attached support/restraints is considered (see Section 1.7.2.12 of this appendix).

1.4.2 THERMAL ANALYSIS

A thermal analysis of piping systems takes into account forces and moments resulting from expansion and contraction. For all analyses, the ambient temperature is 70°F. Flexibility analyses are based on the material property values at the temperature under consideration. Therefore, the analyses are based on the

envelops the site requirements and is appropriate for the site conditions.

Peak broadening or peak shifting methods are used. The method for peak shifting is detailed in ASME Code, Section III, Division I, Appendix N, Section N-1226.3. When this method is used, the entire peak shifting process is performed independently for each of the three directions of excitation.

1.4.3.2.1.3 Damping

[Damping values are provided in]* Section 3.7.1.3 and [Table 3.7-1.]* As an alternative to Table 3.7-1 damping values, variable damping values in accordance with the requirements and limitations of the ASME Code Case N-411-1 are used in piping analysis. No combination of the two damping criteria is used. The variable damping curve is provided in Figure 3.7-41. Composite modal damping is used in the analysis in accordance with the procedure described in Section 3.7.2.15.

1.4.3.2.1.4 Modal Cutoff and Rigid Range Acceleration Effects

The number of modes included in the analysis is chosen to correspond with the range of seismic excitation frequencies up to the frequency corresponding to the ZPA. At modal frequencies above the frequency corresponding to the ZPA, pipe members are considered rigid. The acceleration associated with these rigid modes is usually small. In certain situations [the response of high frequency modes can significantly affect support loads, particularly axial restraints on long runs. To account for these effects, a missing mass correction is applied.]*

One method used to calculate the missing mass correction is as follows:

For each degree of freedom in the direction of excitation, and for a steady-state 1-g acceleration,

(1) determine the inertial force for each mode used in the analysis,

(2) sum the inertial forces in (1) over all modes used,

(3) determine the total inertial force based on the total mass at the d.o.f.,

(4) calculate the "missing" inertial force, (3)-(2).

Apply the resulting force system, multiplied by the ZPA, in a static analysis. Add the results of that analysis to the modal results using a method at least as conservative as SRSS.

Repeat the above procedure for the other two excitation directions.

Although this method uses a different computational procedure from NUREG-0800, Section 3.7.2, Appendix A, the two methods produce the same result. NUREG-0800 requires the correction to be made only when the missing mass at one or more d.o.f.'s exceeds 10% of its total, but it is always conservative to do so.

An alternate method of calculating the missing mass is as follows:

Modal responses are computed for enough modes to ensure that the inclusion of additional modes does not increase the total response by more than ten percent. Modes that have natural frequencies less than that at which the spectral acceleration approximately returns to the ZPA are combined in accordance with Regulatory Guide 1.92, "Combining Modal Responses and Special Components in Seismic Response Analysis." Higher-mode responses are combined algebraically (i.e., retain sign) with each other. The absolute value of the combined higher modes is then added directly to the total response from the combined lower modes.

1.4.3.2.1.5 Modal and Direction Result Combination

As stated in Section 3.7.3.7, [the seismic response of each mode is calculated and combined with the other modal responses using the methods described in Regulatory Guide 1.92,]* "Combining Modal Responses and Spatial Components in Seismic Response Analysis".

If the modes are not closely spaced (two consecutive modes are defined as closely spaced if their frequencies differ from each other by 10 percent or less of the lower frequency), the results are combined by the square root of the sum of the squares (SRSS). Closely spaced modes are combined by one of the following methods: (1) Grouping Method, (2) Ten Percent Method, or, (3) Double Sum Method.

The responses due to each of the three separate directions of seismic excitation are combined by SRSS.

1.4.3.2.1.6 Seismic Anchor Movements

[The effects of seismic anchor motion are considered in the seismic analysis by combining with SSE inertia by absolute summation (ASUM). For models with piping in more than one building, it is assumed that the buildings move 180° out of phase.]* Movements within all buildings except the Reactor Building are assumed to be in phase. [Within the Reactor Building there are differential movements between the Reactor Building, the Containment Vessel, Reactor Interior Structures, and the NSSS. These movements are assumed to act 180° out of phase. The resulting relative movement is applied as static support

envelops the site requirements and is appropriate for the site conditions.

Peak broadening or peak shifting methods are used. The method for peak shifting is detailed in ASME Code, Section III, Division I, Appendix N, Section N-1226.3. When this method is used, the entire peak shifting process is performed independently for each of the three directions of excitation.

1.4.3.2.1.3 Damping

[Damping values are provided in] Section 3.7.1.3 and [Table 3.7-1.] As an alternative to Table 3.7-1 damping values, variable damping values in accordance with the requirements and limitations of the ASME Code Case N-411-1 are used in piping analysis. No combination of the two damping criteria is used. The variable damping curve is provided in Figure 3.7-41. Composite modal damping is used in the analysis in accordance with the procedure described in Section 3.7.2.15.

1.4.3.2.1.4 Modal Cutoff and Rigid Range Acceleration Effects

The number of modes included in the analysis is chosen to correspond with the range of seismic excitation frequencies up to the frequency corresponding to the ZPA. At modal frequencies above the frequency corresponding to the ZPA, pipe members are considered rigid. The acceleration associated with these rigid modes is usually small. In certain situations [the response of high frequency modes can significantly affect support loads, particularly axial restraints or long runs. To account for these effects, a missing mass correction is applied.]

One method used to calculate the missing mass correction is as follows:

For each degree of freedom in the direction of excitation, and for a steady-state 1-g acceleration,

(1) determine the inertial force for each mode used in the analysis,

(2) sum the inertial forces in (1) over all modes used,

(3) determine the total inertial force based on the total mass at the d.o.f.,

(4) calculate the "missing" inertial force, (3)-(2).

Apply the resulting force system, multiplied by the ZPA, in a static analysis. Add the results of that analysis to the modal results using a method at least as conservative as SRSS.

displacements with all dynamic supports active. J*

For branch line models at decoupled header locations, the header seismic anchor movements are run as separate load cases and the results are combined using the SRSS method.

1.4.3.2.1.7 Fatigue

The cyclic load basis for fatigue analysis of the safe shutdown earthquake (SSE) for Class 1 piping systems is given in Section 3.7.3.2.

1.4.3.2.2 Time History Analysis

1.4.3.2.2.1 General

Time history analysis is used as an alternative method to response spectrum analysis for any piping system.

For those piping systems analyzed by time history methods, development of mathematical models, which define flexibility and mass, and calculation of natural frequencies and mode shapes, as described in Section 1.4.3.2.1.1 of this appendix, is first performed.

1.4.3.2.2.2 Piping Dynamically Decoupled from the NSSS

Most piping systems are dynamically decoupled from the nuclear steam supply system (NSSS), following the guidelines of Section 1.5.2.1 of this appendix.

The solution of the differential equations of motion, which describe the dynamic response of a system to a seismic excitation, is obtained by the method of modal superposition or by the method of direct integrations, using time history analysis. These methods are described in Section 3.7.2.1.1.2.

When modal superposition is used, the number of modes analyzed is selected to account for the principal vibration modes of the system based upon mass and stiffness properties, modal participation factors and closeness to amplified region of the response spectrum of the input time history. As required on a case by case basis, the analysis is repeated with more modes in order to verify the chosen number of modes.

For time history analysis by direct integration, the integration time step is chosen to be a maximum of 1/10 of the period of the highest frequency of the system. As required on a case by case basis, the time step is reduced and the analysis repeated in order to verify the choice of time step. When time history analyses are performed for subsystems by direct integration, the time step is shifted up to ±15% to account for uncertainties.

The mathematical model is subjected to seismic excitations at the anchor points (terminal ends) and at building supports. For statistically independent earthquake motions, input excitations in all three translation directions and, as applicable, in all three rotational directions are applied simultaneously to the anchor points and building supports.

Input of multiple time history excitations, which allow calculation of the effects of both differential motion and inertia, are used in a multi-supported system such as a piping system. An alternate time history method used, as described in ASME Code, Section III, Division I, Appendix N, Section N-1228.4, is to input an "envelope" time history excitation to calculate the inertia response, and separately to determine the effects of differential support motion using a static analysis. The ASME B&PV Code defines the envelope excitation as a time history whose response spectrum envelopes the response spectra for the individual support motions.

1.4.3.2.2.3 Piping Dynamically Coupled to the NSSS

The only piping system that is dynamically coupled to the NSSS for the purpose of structural analysis is the main coolant loop piping. The main coolant loop piping is seismically analyzed as an integral part of the reactor coolant system structure, using methods described in Sections 3.7.2.1.2 and 3.7.2.6.2.

1.4.4 WIND/TORNADO ANALYSIS

Exposed piping is designed to withstand forces generated by wind and tornados. Maximum wind speeds are given in Section 3.3. Tornado loads are based upon the NRC Staff interim position based on NRC Regulatory Guide 1.76, "Design Basis Tornado for Nuclear Power Plants".

1.4.5 FLUID TRANSIENT ANALYSIS

Transient fluid dynamic loadings on piping are evaluated and the resulting loads included in the piping analysis. The loads considered are those significant loads due to transients caused by pump start or pump trip, filling a voided line, check valve actuation, relief valve operation, steam turbine trip, and rapid control valve operation. Potential loadings are evaluated and defined for each problem on a case-by-case basis. Multiple safety valve discharges are analyzed so as to maximize piping stresses and support/restraint design loads except where another discharge sequence is justified.

1.4.5.1 Safety/Relief Valve Thrust

Safety/relief valves produce transient and steady-state loads on the valve inlet piping and discharge piping (if used). The thrust load, F, is a function of fluid type (water or steam), operating pressure, and valve throat area.

differences in the surge line walls due to thermal stratification were related to the mode of plant operation. These data confirmed that the maximum temperature differences in the surge line were bounded by the difference in temperature between the pressurizer and the hot leg. The System 80+ surge line is designed for the maximum temperature difference that will be experienced between the pressurizer and the hot leg.

In summary, System 80+ conforms to NRC Bulletins 88-08 and 88-11 for all piping connected to the Reactor Coolant System. Available data from operating reactors has been evaluated and incorporated into the design of System 80+. The design will continue to be assessed as new data becomes available and will be evaluated as to its applicability to System 80+.

S.1.4.7

[Piping systems subjected to stratified flow are evaluated for additional thermal stresses due to thermal stratification.]* Stratified flow exists when a hotter fluid flows over a colder region of fluid. This condition induces a vertical thermal gradient, resulting in increased overall bending stresses and localized thermal gradient stresses. Stratified flow effects consist of (1) local stresses due to temperature gradients in the pipe wall and (2) additional thermal pipe bending moments generated by the restraining effect of supports on the stratified-flow-induced curvature of the piping. The extent of stratification is reduced by sloping generally horizontal pipe runs and is mitigated by carefully selecting designs and operating procedures.

Structural evaluations are performed using elastic and/or simplified elastic-plastic analyses in accordance with the ASME Code considering the applicable loadings of Section 1.3 of this appendix in addition to the stratified flow loadings.

1.4.7.1 Piping Analysis

The stratified-flow-induced curvature of the piping and local stresses due to a temperature gradient are obtained in two-dimensional finite element analyses. These analyses provide the local effects and pipe rotations for an unsupported pipe segment. A stratified flow thermal hydraulic model with the top half of the fluid at the hot temperature and the lower half of the fluid at the colder temperature is employed to determine the pipe wall temperature, based on the thermal hydraulic conditions. Two-dimensional heat transfer and structural thermal stress analyses are performed in order to determine the rotations and local stresses. Rotations are considered to act over all horizontal portions of the pipe. The resulting bending stresses are calculated in the piping analysis by allowing the pipe to thermally expand unconstrained and by then applying a set of equal and opposite displacements at the rigid support points. Local stress effects due to top-to-bottom thermal gradients are

NRC Bulletin 88-08

Following the issuance of Bulletin 88-08, the owners and operators of ABB-CE plants established a program to respond to the NRC. The objectives of this program included:

1. identification of unisolable piping that could be subjected to stratification;

2. inplant inspections to confirm the integrity of the identified lines;

3. obtaining plant data on pipe wall temperatures to confirm if stratification does exist in these lines; and

4. performing analyses to evaluate stress levels and fatigue usage factors for lines subjected to thermal stratification loads.

Results obtained from this program are used to evaluate the presence of stratified flow and the influence on thermal stresses in these lines for System 80+.

The results of this program indicate that thermal stratification can exist in the isolable portions of the safety injection lines of certain operating plants. The System 80+ counterpart to the safety injection line is the direct vessel injection (DVI) line. Available data is used to evaluate the thermal stresses in the DVI lines due to thermal stratification.

Certain plants indicated stratification in the lines between the power operated relief valves and the pressurizer nozzles. The power operated relief valves in System 80+ are represented by the Safety Depressurization System (SDS). The location and orientation of the SDS will minimize the presence of condensed steam in these lines, which is believed to be the cause of thermal stratification in these lines. Thus, thermal stratification should not occur in these lines.

The System 80+ shutdown cooling lines are similar to the arrangements in CE operating plants; a long section of horizontal line connected through a vertical run of pipe to a nozzle on the bottom of the hot leg. Measurements obtained to date are inconclusive. However, program conclusions will be incorporated in the design of the System 80+ shutdown cooling lines.

NRC Bulletin 88-11

In response to Bulletin 88-11, the owner and operators of ABB-CE plants sponsored a program to obtain operating plant data which was needed to characterize thermal stratification in surge line. Data obtained at four operating plants showed that temperature

1.4.12 EXPANSION JOINTS

Expansion joints allow limited relative lateral and axial displacements and bending rotations between the ends of the joint, depending on the type of joint in use. Expansion joints are considered in the analysis.

1.5 ANALYSIS TECHNIQUES

1.5.1 MODEL BOUNDARIES

Piping models ideally run from anchor to anchor (equipment nozzle, or penetration). Where this is not feasible, the piping is separated by decoupling, overlapping, isolation, or in-line anchors as described in the following subsections to form more manageable models for analysis. Where the piping cannot be separated to form smaller analysis models by these methods, the use of an intermediate anchor is considered in order to separate models, subject to the considerations of Section 1.5.5 of this appendix.

1.5.2 DECOUPLING

1.5.2.1 General

Small branch lines are allowed to be decoupled from larger run piping regardless of seismic classification. In some instances, decoupling is also applied for in-line pipe size changes (such as at a reducer or reducing insert). In the description in Section 1.5.2.2, the smaller line is defined as the "branch" and the larger line is defined as the "run". To meet decoupling criteria, piping meets the size or moment of inertia ratios as detailed in the following paragraphs. For decoupling criteria to be meaningful, the branch line must be designed flexible enough to absorb the anchor motions of the run pipe. Therefore, the branch line flexibility is maintained by avoiding placement of branch line supports close to the run pipe.

1.5.2.2 Branch Decoupling Criteria

[Branch lines meeting the following criteria may be decoupled from the main run:

(a) $D_b/D_r \leq 0.33$, or

(b) $I_b/I_r \leq 0.04$,] where

D_b = Branch nominal pipe size

D_r = Run nominal pipe size

I_b = Branch moment of inertia

I_r = Run moment of inertia

An appropriate stress intensity factor (SIF) is included on the branch and main run lines at the point where the piping is decoupled. Mass effects of the branch line are considered in the analysis of the run line. The branch point is considered as an anchor in the analysis of the branch pipe. Thermal and seismic anchor movement analyses of the decoupled branch lines are performed with the thermal, seismic inertial, seismic anchor movement (SAM), or pipe break movements of the larger pipe header applied as anchor displacements and/or rotations to the smaller branch line wherever these movements are significant. The inertia effects of the run pipe on branch pipe are considered, where significant.

Piping is also decoupled at flexible hose wherever each interfacing analysis considers the flexible hose weight and significant stiffness, and wherever the flexible hose qualifies for the net end displacements of the interfacing analysis problems. Analysis results of the interfacing problems are not combined. The flexible hose is not allowed to experience loads beyond those recommended by the manufacturer.

Also refer to Section 3.7.2.3.3 for general decoupling criteria.

1.5.2.3 **Seismic to Non-seismic Decoupling Criteria**

Two methods for designing the region of a seismic/non-seismic piping interface are as follows:

A. Use of structural anchors for isolation

Structural isolation anchors provide an effective means of protecting seismic piping from the seismic response of non-seismically designed piping. Anchors are designed assuming that a plastic hinge forms at the interface with non-seismic piping.

B. Use of isolation restraints

Piping restraints are utilized to isolate the seismic response of non-seismically designed piping from seismically designed piping. Isolation restraints are designed as follows:

- Two restraints located in each of the three orthogonal directions are used to isolate the seismically caused pipe moments, and forces from the non-seismic piping to the seismic piping.

An appropriate stress intensity factor (SIF) is included on the branch and main run lines at the point where the piping is decoupled. Mass effects of the branch line are considered in the analysis of the run line. The branch point is considered as an anchor in the analysis of the branch pipe. Thermal and seismic anchor movement analyses of the decoupled branch lines are performed with the thermal, seismic inertial, seismic anchor movement (SAM), or pipe break movements of the larger pipe header applied as anchor displacements and/or rotations to the smaller branch line wherever these movements are significant. The inertia effects of the run pipe on branch pipe are considered, where significant.

Piping is also decoupled at flexible hose wherever each interfacing analysis considers the flexible hose weight and significant stiffness, and wherever the flexible hose qualifies for the net end displacements of the interfacing analysis problems. Analysis results of the interfacing problems are not combined. The flexible hose is not allowed to experience loads beyond those recommended by the manufacturer.

Also refer to Section 3.7.2.3.3 for general decoupling criteria.

1.5.2.3 **Seismic to Non-seismic Decoupling Criteria**

Two methods for designing the region of a seismic/non-seismic piping interface are as follows:

A. Use of structural anchors for isolation

Structural isolation anchors provide an effective means of protecting seismic piping from the seismic response of non-seismically designed piping. Anchors are designed assuming that a plastic hinge forms at the interface with non-seismic piping.

B. Use of isolation restraints

Piping restraints are utilized to isolate the seismic response of non-seismically designed piping from seismically designed piping. Isolation restraints are designed as follows:

- Two restraints located in each of the three orthogonal directions are used to isolate the seismically caused pipe moments, and forces from the non-seismic piping to the seismic piping.

1.6.2 ASME CLASS 2 AND 3 PIPING

The allowable stress limits for the specified loading combinations for ASME Class 2 and 3 piping are shown in Table 3.9-11 and Reference 4.12.

1.6.3 ALLOWABLE NOZZLE LOADS

Equipment nozzle loads are minimized to be within equipment vendor specifications. The design nozzle load values are provided to equipment vendors as part of the procurement specification.

1.6.4 ALLOWABLE PENETRATION LOADS

Piping systems are designed such that loads and displacements on containment penetration assemblies, as shown in Figure 3.8-2, meet manufacturer's allowables.

1.6.5 WELDED ATTACHMENTS

Per ASME Section III, Subarticle NC/ND 3645, external and internal attachments to piping are designed so as not to cause flattening of the pipe, excessive localized bending stresses, or harmful thermal gradients in the pipe wall. Such attachments are designed to minimize stress concentrations in applications where the number of stress cycles, due either to pressure or thermal effects, are relatively large for the expected life of the equipment.

Local stresses due to all support loads acting on a welded attachment are evaluated and added directly to the nominal pipe stresses at the point of the attachment. The sum of the stresses are compared against the allowable stresses given in Tables 3.9-10 and 3.9-11. Methods for evaluating local stresses due to welded attachments are provided in ASME Code Cases N-318 and N-392. Methods and criteria are supplemented by NRC-approved PVRC and EPRI testing and research.

1.6.6 FUNCTIONAL CAPABILITY REQUIREMENTS

See Section 3.9.3.1.4.3.

1.6.7 VALVE REQUIREMENTS

Piping systems are designed such that valve accelerations meet the allowable manufacturer's requirements for seismic acceleration. In lieu of specific values, reasonable generic seismic valve acceleration limits for SSE conditions and water hammer type loads are established. The design values are included in the procurement specification. The loads on supports

attached to valve operators are also evaluated. The valve operator support does not support the pipe.

1.6.8 EXPANSION JOINT REQUIREMENTS

Expansion joints are evaluated to ensure compliance with vendor allowables based on the stress report provided by the vendor.

1.6.9 WELDING AND WELD ACCEPTANCE CRITERIA

Welding fabrication and installation, nondestructive examination (NDE) and acceptance standards for ASME Code Class 1, 2, and 3 piping shall be in accordance with Articles 4000 and 5000 of Subsections NB, NC, and ND in Section III of the ASME Code.

Radiographic examinations will be accepted by a nondestructive examination (NDE) Level III examiner prior to final acceptance. See also Sections 3.9 and 3.9.3.4.

Confirmation that facility welding activities are in compliance with the certified design commitments shall include verifications of the following by individuals other than those who performed the activity:

1. Facility welding specifications and procedures meet the applicable ASME Code requirements.

2. Facility welding activities are performed in accordance with the applicable ASME Code requirements.

3. Welding activities related records are prepared, evaluated and maintained in accordance with the ASME requirements.

4. Welding processes used to weld dissimilar base metal and welding filler metal combinations are compatible for the intended applications.

5. The facility has established procedures for qualifications of welders and welding operators in accordance with the applicable ASME Code requirements.

6. Approved procedures are available and are used for pre-heating and post-heating of welds, and those procedures meet the applicable requirements of the ASME Code.

7. Completed welds are examined in accordance with the applicable examination method required by the ASME Code.

Welding activities involving non-ASME pressure retaining piping shall be accomplished in accordance with written procedures and shall meet the requirements of the ANSI B31.1 Code. The weld acceptance criteria shall be as defined for the applicable nondestructive examination method described in ANSI B31.1.

(TAM). All possible thermal conditions, including ambient thermal, are be evaluated when combining thermal loads with other load cases to obtain the worst loading on the supports. The pipe also experiences radial expansion due to temperature increases. To minimize local stresses within the pipe, supports are designed to allow for this expansion. See Section 1.7.2.10 of this appendix concerning support gaps.

Pipe supports are also evaluated for environmental thermal conditions. Temperature increases in the area around the support cause the support itself to tend to thermally expand. In addition, local high temperatures can exist close to the pipe wall. Support elements which are subjected to these elevated temperatures are evaluated for thermal effects. Material property values consistent with the associated temperature are used.

Thermal expansion of the pipe support and/or the building structure from which the support is attached is evaluated for its effects on the piping analysis.

1.7.2.3 Seismic Loads

The building response to earthquake motion causes seismic acceleration of the piping system. [Earthquake inertia forces are applied to supports that restrain the seismic movement of the piping system.]* Additional seismic movements can be caused by seismic acceleration of terminal end points of the piping system such as branch lines and vessels. These forces are referred to as seismic anchor movements (SAM).

[The response of the support itself due to seismic acceleration is also evaluated.]* Typically, the inertia response of the support mass is evaluated using a response spectrum analysis similar to the piping analysis as described in Section 1.4.3.2.1 of this appendix. Damping values for welded and bolted structures are provided in Table 3.7-1.

1.7.2.4 Dynamic Fluid Loads

Dynamic fluid loads are a result of fluid transients due to safety/ relief valve thrust, water hammer, and steam hammer. These events are evaluated in the piping analysis. Supports are designed to meet the requirements of the piping analysis.

1.7.2.5 Wind/Tornado Loads

Exposed piping and support structures are designed to withstand forces generated by wind and tornados. Wind and tornado loading on the piping are evaluated in the piping analysis. The effects

1.7 PIPE SUPPORT DESIGN REQUIREMENTS

1.7.1 GENERAL

Pipe supports are designed to meet the intended functional requirements of the stress analysis as well as the specified stress limits for the support components. Support components include typical structural steel members as well as manufactured catalog items for typical support components.

Component support building structures are designed to meet the criteria in Section 3.8.4.

Supports are idealized in the piping analysis as providing restraint in the analyzed direction while providing unrestricted movement in the unrestrained direction. Since the design of supports cannot completely duplicate the idealized condition, supports are designed to minimize their effects on the piping analysis. Additionally, it is confirmed that the support design does not invalidate any assumptions used in the analysis of the piping system.

In addition to loads defined by the stress analysis, any additional forces the support are subjected to are considered in the support qualification.

1.7.2 DESIGN CONSIDERATIONS

1.7.2.1 Deadweight Loads

Gravity loads of the pipe are typically restrained by two types of supports. The piping analysis defines whether the support is designed as a rigid or flexible support. Flexible supports are specified when the pipe must be restrained for its gravity weight, however must remain free to move during thermal expansion. Vendor supplied spring components with specified spring constants are typically provided in this application.

In addition to gravity loads from the piping analysis, the deadweight of the support itself is considered in the support design.

1.7.2.2 Thermal Loads

Temperature changes within the piping system, including thermal stratification, cause the pipe to thermally expand. Thermal loads are induced into supports which restrain the piping system from being able to freely expand. Additional thermal loads could be a result of "anchor" displacements. Movements at the terminal end points of the piping system, such as branch lines and vessels, induce loads into supports which resist these movements. These forces are usually referred to as thermal anchor movements

of wind and tornado on the support structure are also considered in the support qualification. Design wind speeds are provided in Section 3.3.

1.7.2.6 Missile Loads

Supports subjected to loads described in Section 3.5.1 are evaluated for the effects of missiles.

1.7.2.7 Pipe Break Loads

The dynamic effects of pipe breaks on the piping system are considered in the piping analysis unless eliminated by leak-before-break (LBB) methodology (see Section 1.9 of this appendix). The effects of pipe whip, jet impingement, and temperature increases on the support structure are considered in the support qualification.

1.7.2.8 Support Stiffness

Supports are modeled in the piping analysis by using the actual support stiffness values or by using rigid stiffness values. When the actual support stiffnesses are used, the flexibility of all support components as well as the effects of the building structure are included in the total stiffness value.

Rigid stiffness values are typically used; however, actual stiffness values for flexible supports (e.g., spring cans) are included in the piping analysis. When rigid stiffnesses are used, all supports in a given piping analysis are typically designed with a reasonably equal stiffness. This reduces the effects of load redistribution to stiffer supports due to the deflection of the more flexible supports. Deflections of rigid support are limited to 1/16 inch in the restrained direction based on the greater of SSE loadings or the maximum design loads of Section 1.7.2.13 of this appendix. In addition, the maximum deflection is limited to 1/8 inch based on the maximum load combinations.

Since supports are usually modeled with one stiffness value for both directions of a support axis, supports are designed to have similar stiffnesses in both directions.

Rigid supports are designed to ensure that the stiffness of the supports do not affect the pipe frequency.

1.7.2.9 Friction

Temperature changes in the piping system causes movement in the unrestrained direction of the pipe. If the pipe is free to slide across a support, frictional forces are developed between the support surface and the pipe. The amount of frictional force

developed is a function of the coefficient of friction of the sliding surfaces and the support stiffness in the direction of movement. Since friction is due to gradual movement of the pipe, such as thermal expansion, frictional forces are considered in the support design under combined deadweight and thermal loading only. Friction forces are applied in both directions of thermal expansion.

To account for these forces, the friction force is calculated by using the smaller of CN or KX, where C is the coefficient of friction and N is the component of force normal to the movement and K is the stiffness of the support in the direction of X.

Typical coefficients of friction are:

0.3 for steel to steel
0.1 for low friction slide/bearing plates

Typically, frictional forces are neglected in the analysis of the piping system because supports are designed to minimize the effects of friction on the piping analysis.

1.7.2.10 Support Gaps

Small gaps are provided for frame type supports built around the pipe. These gaps allow for radial thermal expansion of the pipe as well as allowing for pipe rotation. Total gaps of 1/8 inch or less in the restrained direction are negligible and are considered to be zero in the piping analysis.

1.7.2.11 Support Mass

Typically, the mass of the support is not included in the piping analysis. Therefore, the weight of components supported by the pipe is limited to the extent possible. For example, spring supports include the weight of the components below the spring in the spring load setting, thus negating that part of the spring support weight that is supported by the pipe. However, due to the seismic response of the attached mass, supports which add substantial mass to the pipe are evaluated for the effects on the piping analysis.

1.7.2.12 Welded Pipe Attachments

Welded attachments to the pipe wall are avoided where possible. However, certain design requirements such as anchors or axial restraints require the use of welded lugs or trunnions. All welded attachments require the evaluation of the local stresses induced into the pipe. Materials used as welded attachments are compatible with the piping material.

developed is a function of the coefficient of friction of the sliding surfaces and the support stiffness in the direction of movement. Since friction is due to gradual movement of the pipe, such as thermal expansion, frictional forces are considered in the support design under combined deadweight and thermal loading only. Friction forces are applied in both directions of thermal expansion.

To account for these forces, the friction force is calculated by using the smaller of CN or KX, where C is the coefficient of friction and N is the component of force normal to the movement and K is the stiffness of the support in the direction of X.

Typical coefficients of friction are:

0.3 for steel to steel
0.1 for low friction slide/bearing plates

Typically, frictional forces are neglected in the analysis of the piping system because supports are designed to minimize the effects of friction on the piping analysis.

1.7.2.10 Support Gaps

Small gaps are provided for frame type supports built around the pipe. These gaps allow for radial thermal expansion of the pipe as well as allowing for pipe rotation. Total gaps of 1/8 inch or less in the restrained direction are negligible and are considered to be zero in the piping analysis.

1.7.2.11 Support Mass

Typically, the mass of the support is not included in the piping analysis. Therefore, the weight of components supported by the pipe is limited to the extent possible. For example, spring supports include the weight of the components below the spring in the spring load setting, thus negating that part of the spring support weight that is supported by the pipe. However, due to the seismic response of the attached mass, supports which add substantial mass to the pipe are evaluated for the effects on the piping analysis.

1.7.2.12 Welded Pipe Attachments

Welded attachments to the pipe wall are avoided where possible. However, certain design requirements such as anchors or axial restraints require the use of welded lugs or trunnions. All welded attachments require the evaluation of the local stresses induced into the pipe. Materials used as welded attachments are compatible with the piping material.

1.7.2.13 Minimum Design Loads

In order to provide some uniformity in load carrying ability, all supports are designed to minimum loads.

All supports are designed for the largest of the following three loads:

- 100% of the Level A condition load from the piping stress analysis
- The weight of a standard ANSI B31.1 span of water filled, schedule 80 pipe
- Minimum value of 150 pounds

1.7.3 LOAD COMBINATIONS

Load combinations are in accordance with Section 3.9.3.1 and are detailed in Table 3.9-12. For common supports, the SRSS method for combination of dynamic loads is used.

1.7.4 ACCEPTANCE CRITERIA

Pipe supports are either linear or plate and shell type devices. A linear type component support is defined as acting under essentially a single component of direct stress. Such devices may also be subjected to shear stresses. Plate and shell type of supports are fabricated from plate and shell elements and are normally subjected to a biaxial stress.

Seismic Category I pipe support members are designed to meet the requirements defined in ASME Code, Section III, Subsection NF. For A500 Grade B tube steel, NF requirements are supplemented by the weld requirements of AWS D1.1, "Structural Welding Code" (Reference 4.26). Welding activities of Seismic Category I pipe supports shall be as defined in Section 3.9.3.4.

Category II pipe support members are designed to meet the requirements of ANSI/AISC N690 - "Nuclear Facilities - Steel Safety-Related Structures for Design Fabrication and Execution," as amended by Section 3.8.4.5.

Standard support manufactured catalog items are designed to meet the requirements of MSS-SP-58, "Pipe Hangers and Supports-Materials, Design and Manufacture." The application of catalog components is consistent with the manufacturer's requirements and are designed to meet the manufacturer's load rated capacities for the items. The piping design is consistent with the manufacturers' requirements for pipe deflection limits at pipe supports, such as requirements for travel in snubbers and hangers, or with industry practice, such as requirements for the sway angle in rod or strut supports. These deflection limits are considered at the stage in the piping design at which the piping supports are spotted, oriented and specified.

THIS PAGE INTENTIONALLY BLANK

Materials used for support devices are structural elements or standard components. Standard components include:

- snubbers, mechanical or hydraulic;
- constant or variable spring support hangers;
- rigid supports consisting of anchors, guides, restraints, rolling or sliding supports, and rod type hangers;
- sway braces and vibration dampeners;
- structural attachments such as ears, shoes, lugs, rings, clamps slings, straps and clevises;
- any other NRC approved devices.

{ Concrete expansion anchors are designed to meet the requirements of ACI-349, "Code Requirements for Nuclear Safety Related Concrete Structures," as amended by Section 3.8.4.5.1. }

This assures that the design strength of concrete for a given expansion anchor or group of anchors is greater than the strength of the anchor steel, accounts for the effect of shear-tension interaction, and considers minimum edge distance and bolt spacing on expansion anchor capacity. { Base plate flexibility is accounted for in the calculation of expansion anchor bolt loads. }

Stress limits for steel structural members of pipe supports shall meet the requirements defined in ANSI/AISC N690, as amended by Section 3.8.4.5.

1.7.5 JURISDICTIONAL BOUNDARIES

{ The jurisdictional boundaries are defined in ASME Section III, Subsection NF. }

1.8 POSTULATED PIPE BREAKS

1.8.1 CLASSIFICATION

1.8.1.1 High Energy

High energy piping systems are those systems or portions of systems that are maintained pressurized at either temperatures in

excess of 200°F or at pressures exceeding 275 psig during any of the following normal plant operating modes. For systems containing process fluids other than water, the atmospheric boiling temperature is applied in place of the 200°F criterion.

- Reactor Startup
- Hot Standby
- Operation at any Power Level
- Reactor Cooldown to Cold Shutdown

Exceptions:

A. Non-liquid piping systems (air, gas, steam) with a maximum pressure less than or equal to 275 psig are not considered high energy regardless of the temperature.

B. Piping which operates at pressures and/or temperatures meeting high energy requirements is not considered high energy if the total time spent in operation at high energy conditions is less than two percent of the time period required to accomplish its system design function.

C. Piping of one-inch nominal pipe size and less is not considered "high energy."

1.8.1.2 Moderate Energy

Moderate energy piping systems are those systems or portions of systems, that during any of the normal plant operating modes are maintained pressurized at a maximum temperature of 200°F or less and a maximum pressure of 275 psig or less including all piping excluded from high energy.

Exceptions:

A. Open-ended vents and drains are not considered moderate energy.

B. Piping of one-inch nominal pipe size and less is not considered moderate energy.

1.8.2 POSTULATED RUPTURE LOCATIONS

1.8.2.1 Break Locations in ASME Class 1 Piping Runs

See Section 3.6.2.1.4.1.A.

Reconciliation of the as-built piping systems with the final design will be documented in a LBB Evaluation Report. The LBB Evaluation Report shall contain results of the LBB evaluations for as-built piping. The LBB evaluations shall employ methods described in Section 1.9 of this appendix. Reconciliation of each as-built piping system qualified for LBB will be made by demonstrating that:

1 the as-built piping system meets the screening criteria of Section 3.6.3,

2 the dimensional and material properties of the as-built piping system are consistent with the parameters used in the development of the final LBB PED(s) for that piping system,

3 the as-built piping responses meet the ASME Code allowables and the final LBB PED criteria.

See also Sections 3.6 and 3.6.3.8.

1.10 TUBING

1.10.1 GENERAL

{ Design, analysis and loading considerations that are used for piping and supports are used for tubing.] Due to the amount of tubing, bounding analyses are performed. This analysis method is also used for small-bore piping. These criteria apply to safety-related tubing.

Non-safety related manifold valves, solenoid valves, and instruments located over or near safety-related equipment or components are supported using the same criteria, except where justified by analysis. This prevents damage, degradation, or interference with the performance of equipment required for safety functions.

1.10.2 SUPPORT AND MOUNTING REQUIREMENTS

Two support mechanisms are used, free tube spans and tube track supports. Criteria for each tube support mechanism are determined as described above. The following are additional support and mounting considerations:

A. [Tubing that is routed in two or more Seismic Category I structures] (i.e., Reactor Building, Containment, Main Steam Valve House, Nuclear Annex, Diesel Generator Building) [are verified to have sufficient flexibility to allow for differential building displacements.]*

B. [Span lengths are chosen and supports and tube details are designed to accommodate heat tracing and/or insulation requirements.

C. All reservoirs, valves, and other in-line components are independently supported.

D. Movements of the root valve (SAM and TAM) between the pipe and the tubing are considered.]*

2.0 HVAC DUCTWORK AND SUPPORT/RESTRAINTS

2.1 GENERAL

HVAC ductwork is designed and supported to withstand the loading combinations presented in this section, as applicable. The design and analysis guidelines herein apply to Seismic Category I and II HVAC ductwork and HVAC ductwork supports/restraints (S/Rs) to maintain ductwork stresses within allowables, to limit ductwork displacements to maximum deflection (Δ_{max}) criteria, and to maintain S/R stresses within allowables.

Seismic Category II HVAC ductwork and HVAC ductwork S/R systems, as defined in Section 3.2.1, are analyzed to ensure that their failure does not adversely impact safety-related equipment or components. Seismic Category II requirements are conservatively satisfied by analyzing the HVAC ductwork and HVAC ductwork S/R systems to the same criteria as Seismic Category I.

Non-seismic HVAC ductwork and non-seismic HVAC ductwork S/R systems are designed to meet Sheet Metal and Air Conditioning Contractors' National Association (SMACNA) standards.

Ductwork constructed of piping is designed to meet the analysis requirements of Section 1.0 of this appendix, as applicable.

2.2 DESIGN CONSIDERATIONS

2.2.1 PRESSURE

Internal pressure loads (P) are considered in the design of ductwork. The duct skin thickness and stiffener requirements are based on the design pressure. SMACNA guidelines (References 22 and 23) are used in the determination of skin thickness and stiffener requirements.

Internal pressures generally have no impact on HVAC ductwork S/R design, but supports adjacent to flexible expansion joints are evaluated for associated pressure thrusts.

2.2.2 GRAVITY

Dead weight (DW) loads include the weight of the ductwork itself, in-line components (e.g., dampers), externally mounted components and insulation. Dead weight loads are typically increased by 10% for design to account for the weight of bolts, conduit, fireproofing, etc.

In addition to the dead weight loads from the HVAC ductwork analysis, the dead weight of the S/R itself is considered in the S/R qualification.

LIST OF FIGURES (Cont'd)

CHAPTER 4

Figure	Subject
4.3-25	Second Cycle Assembly Fuel Loadings, Water Hole and Burnable Absorber Rod Placement
4.3-26	Assembly Average Burnup Distribution at Beginning of Second Cycle
4.3-27	Planar Average Power Distribution at Beginning of Second Cycle, Unrodded
4.3-28	Planar Average Power Distribution at Middle of Second Cycle, Unrodded
4.3-29	Planar Average Power Distribution at End of Second Cycle, Unrodded
4.3-30	Third Cycle Fuel Loading Pattern
4.3-31	Third Cycle Assembly Fuel Loadings, Water Hole and Burnable Absorber Rod Placement
4.3-32	Assembly Average Burnup Distribution at the Beginning of the Third Cycle
4.3-33	Planar Average Power Distribution at the Beginning of the Third Cycle, Unrodded
4.3-34	Planar Average Power Distribution at the Middle of the Third Cycle, Unrodded
4.3-35	Planar Average Power Distribution at the End of the Third Cycle, Unrodded
4.3-36	Daily Reactor Power Maneuvering, ASI and Reactivity Control by (P)CEA Only, No Boron, 100-50-100 Near Beginning of Cycle (0-8 hrs)
4.3-36a	Daily Reactor Power Maneuvering, ASI and Reactivity Control by (P)CEA Only, No Boron, 100-50-100 Near Beginning of Cycle (8-24 hrs)

LIST OF FIGURES (Cont'd)

CHAPTER 4

Figure	Subject
4.3-37	Daily Reactor Power Maneuvering, ASI and Reactivity Control by PSCEA Only, No Boron, 100-50-100 at 90% of Cycle (0-8 hrs)
4.3-37a	Daily Reactor Power Maneuvering, ASI and Reactivity Control by PSCEA Only, No Boron, 100-50-100 at 90% of Cycle (8-24 hrs)
4.3-38	F^N_Q vs Time for a 100%-50%-100% Load Following Transient
4.3-39	F^N_Q vs Time for a 100%-50%-100% Load Following Transient
4.3-40	Normalized Power Distribution of Unshimmed Assembly Used in Sample DNB Analysis in Section 4.4.2.2
4.3-41	Fuel Temperature Coefficient vs Effective Fuel Temperature
4.3-42	Moderator Temperature Coefficient vs Moderator Temperature at BOC 1
4.3-43	Moderator Temperature Coefficient vs Moderator Temperature at EOC 1
4.3-44	Moderator Density Coefficient vs Moderator Density
4.3-45	Fuel Temperature Contribution to Power Coefficient at EOC
4.3-46	Control Element Assembly Locations
4.3-47	CEA Group Identification
4.3-48	Typical Power Dependent CEA Insertion Limit (PDIL)
4.3-49	Typical Integral Worth vs Withdrawal at Zero Power, EOC 1 Conditions
4.3-50	Typical Integral Worth vs Withdrawal at Hot Full Power, EOC 1 Equilibrium Xenon Conditions

by function. The stress values of all structural members under normal operating and expected transient conditions are not greater than those established by Section III of the ASME Code. The effect of neutron irradiation on the materials concerned is included in the design evaluation. The effect of accident loadings on the internals is included in the design analysis.

During normal operation, reactivity control is provided by two independent systems: the Control Element Drive System and the Chemical and Volume Control System. The Control Element Drive System controls short term reactivity changes and is used for rapid shutdown. The Chemical and Volume Control System is used to compensate for long-term reactivity changes and can make the reactor subcritical without the benefit of the Control Element Drive System. The design of the core and the Reactor Protective System prevents fuel damage limits from being exceeded for any single malfunction in either of the reactivity control systems. During accidents, the Safety Injection System also provides a safety-grade method of boron injection.

4.1.1 FUEL AND INITIAL CORE DESIGN DESCRIPTION AND PERMISSIBLE CHANGES

The fuel system design, nuclear design, and thermal and hydraulic design are described in Sections 4.2, 4.3 and 4.4, respectively. Changes to certain features and evaluated parameters for these designs may be made by the COL applicant/licensee for the initial core without prior NRC review and approval provided those changes are within certain acceptance criteria. [The design features and evaluated design parameters that may change and the associated acceptance criteria are given in Tables 4.1-1 and 4.1-2, respectively.] In addition, the arrangement of the different fuel assembly batches within the core may be varied from that shown in Section 4.3 as long as the acceptance criteria for the evaluated design parameters are met.

T2* 1-9

TABLE 4.1-1

[[DESIGN FEATURES AND ACCEPTANCE CRITERIA FOR FUEL AND INITIAL CORE DESIGN

Design Feature	Acceptance Criteria*
Fuel Design	
Maximum Fuel Rod Burnup	≤60,000 MWd/MTU
Fuel Rod U-235 Enrichment	≤3.7 wt%
Integral ~~Er_2O_3~~ Burnable Absorber Concentration	≤2.0 wt% Er_2O_3 OR ≤7.0 wt% Gd_2O_3
Number of ~~Integral Er_2O_3~~ Burnable Absorber ~~Pins~~ Rods Per Fuel Assembly	≤124 Er_2O_3 OR ≤ 16 Gd_2O_3 OR ≤ 16 Al_2O_3-B_4C
Natural or Low Enrichment Uranium Axial Blanket Length (Top and Bottom of Fuel and ~~Er_2O_3~~ Burnable Absorber Rods)	≤7.5 inches
~~Er_2O_3~~ Burnable Absorber Rod Cutback Length (Top and Bottom)	≤15.0 inches
Initial Core Design	
Core Power Level	≤3914 MWt
Cycle Length	≤16,000 MWd/MTU]]

* Acceptance Criteria are nominal values.

TABLE 4.1-2

EVALUATED DESIGN PARAMETERS AND ACCEPTANCE CRITERIA FOR FUEL AND INITIAL CORE DESIGN

Evaluated Design Parameter	Acceptance Criteria*
Core Average U-235 Enrichment	≤2.6 wt%
Maximum Unrodded 3-Dimensional Peaking Factor (F_Q)	≤2.28
Maximum Unrodded Integrated Radial Peaking Factor (F_R)	≤1.55
Minimum DNBR	≥1.24
Net CEA Shutdown Worth (HFP)	≥8.86%$\Delta\rho$
Moderator Temperature Coefficient (HFP, ARO)	≤-0.1×10^{-4} $\Delta\rho$/°F, ≥-3.5×10^{-4} $\Delta\rho$/°F
Power Coefficient	<0.0 $\Delta\rho$/(kW/ft)
Critical Boron Concentration (HFP, BOC, ARO, Equilibrium Xenon)	≤1056 ppm

* Acceptance Criteria are nominal values.

The allowble length of the top and bottom burnable absorber cutback region is given in Table 4.1 -1.

the pellet column, provides space for axial thermal differential expansion of the fuel column and accommodates the initial helium loading and evolved fission gases. (See Sections 4.2.1.2.5.1 and 4.2.1.2.5.2.) The specific manner in which these factors are taken into account, including the calculation of temperatures for the gas contained within the various types of rod internal void volume, is discussed in References 15-17.

4.2.2.3 Burnable Absorber Rod

Fixed burnable neutron absorber rods are included in selected fuel assemblies to reduce the beginning-of-life moderator coefficient. They replace fuel rods at selected locations. The three alternative burnable absorber rod designs are described below.

A. Al_2O_3 - B_4C Burnable Absorber Rod

The burnable absorber rods shown in Figure 4.2-9 are mechanically similar to fuel rods, but contain a column of burnable absorber pellets instead of fuel pellets. The burnable absorber material is alumina with uniformly-dispersed boron carbide particles. The balance of the column consists of Zircaloy-4 spacers, with the total column length the same as the column length in fuel rods. The burnable absorber rod plenum spring is designed to produce a smaller preload on the pellet column than that in a fuel rod because of the lighter material in the burnable absorber pellets.

B. Gd_2O_3 - UO_2 Burnable Absorber Rod

The burnable absorber rods shown in Figure 4.2-10 are mechanically similar to fuel rods, but consist of Gd_2O_3 admixed in natural UO_2 in the central rod portion (axially) and natural UO_2 at the top and bottom. The total column length is the same as the column length in fuel rods.

C. Er_2O_3-UO_2 Burnable Absorber Rod

The burnable absorber rods shown in Figure 4.2-12 are mechanically similar to fuel rods, but consist of Er_2O_3 admixed in enriched UO_2 in the central rod portion (axially) and natural UO_2 at the top and bottom. The total column length is the same as the column length in fuel rods.

Each burnable absorber rod assembly includes a serial number and visual identification mark. The serial number is used to record fabrication information for each component in the rod assembly. The identification mark is unique to burnable absorber rods and provides a visual check on the pellet burnable absorber content during fuel bundle fabrication.

C. Irradiation Stability of Absorber Materials

Irradiated properties of the absorber materials are discussed in Section 4.2.1.4. Irradiation-induced chemical transmutations are produced in both the B_4C and the Ag-In-Cd. Neutron bombardment of B-10 atoms results in the production of lithium and helium. The percent of helium released is given by the expression in Section 4.2.1.4.

Ag-In-Cd alloy, which has an initial chemical composition of 79 wt% minimum Ag, 15 ± 0.35 wt% In, 5 ± wt% Cd and 0.2 wt% maximum impurities, is expected to undergo small changes in composition. Formation of 3 wt% tin due to the transmutation of indium and an increase in cadmium content to about 10 wt% due to the transmutation of silver is expected. These affect the thermal conductivity and linear expansion characteristics of the alloy and are accounted for in the design of the control elements.

Irradiation-enhanced swelling characteristics of the absorber materials are given in Section 4.2.1.4. Accommodations for swelling of the absorbers have been incorporated in the design of the control elements and include the following measures:

1. All B_4C pellets have rounded edges to promote sliding of the pellets in the cladding due to differential thermal expansion and irradiation enhanced swelling.

2. Dimensionally stable Type 304 stainless steel spacers are located at the bottom of all absorber stacks adjacent to the nose cap to minimize strain at the weld joint. full-strength, twelve-element CEAs.

3. A felt metal sleeve containing reduced diameter B_4C pellets is located in the bottom length of the absorber stacks in ~~full-length control elements.~~ The felt metal sleeve laterally positions the reduced diameter B_4C pellets uniformly with respect to the clad and absorbs the differential thermal expansion and irradiation induced swelling of the B_4C pellets, thereby limiting the amount of induced strain the clad.

4. A hole is provided in the center of the Ag-In-Cd cylinder to accommodate swelling in excess of the amount expected over the life of the control element.

TABLE 4.2-1

(Sheet 6 of 7)

MECHANICAL DESIGN PARAMETERS

Burnable Absorber Rod (Cont'd)

Gadolinia - Urania Burnable Absorber Rod Design

Absorber material	UO_2-Gd_2O_3
Pellet diameter, inches	0.3255
Pellet length, inches, min	0.390
Pellet density (% theoretical), min	94.5
Theoretical density, UO_2, g/cm^3	10.96
Theoretical density, Gd_2O_3, g/cm^3	7.41
Clad material	Zircaloy-4
Clad ID, inches	0.332
Clad OD, inches	0.382
Clad thickness, (nominal), inches	0.025
Diametral gap, (cold, nominal), inches	0.0065
Active length, inches	~~136~~ 150*
Plenum length, inches	7.938

* Includes top and bottom cutback regions

TABLE 4.2-1

(Sheet 7 of 7)

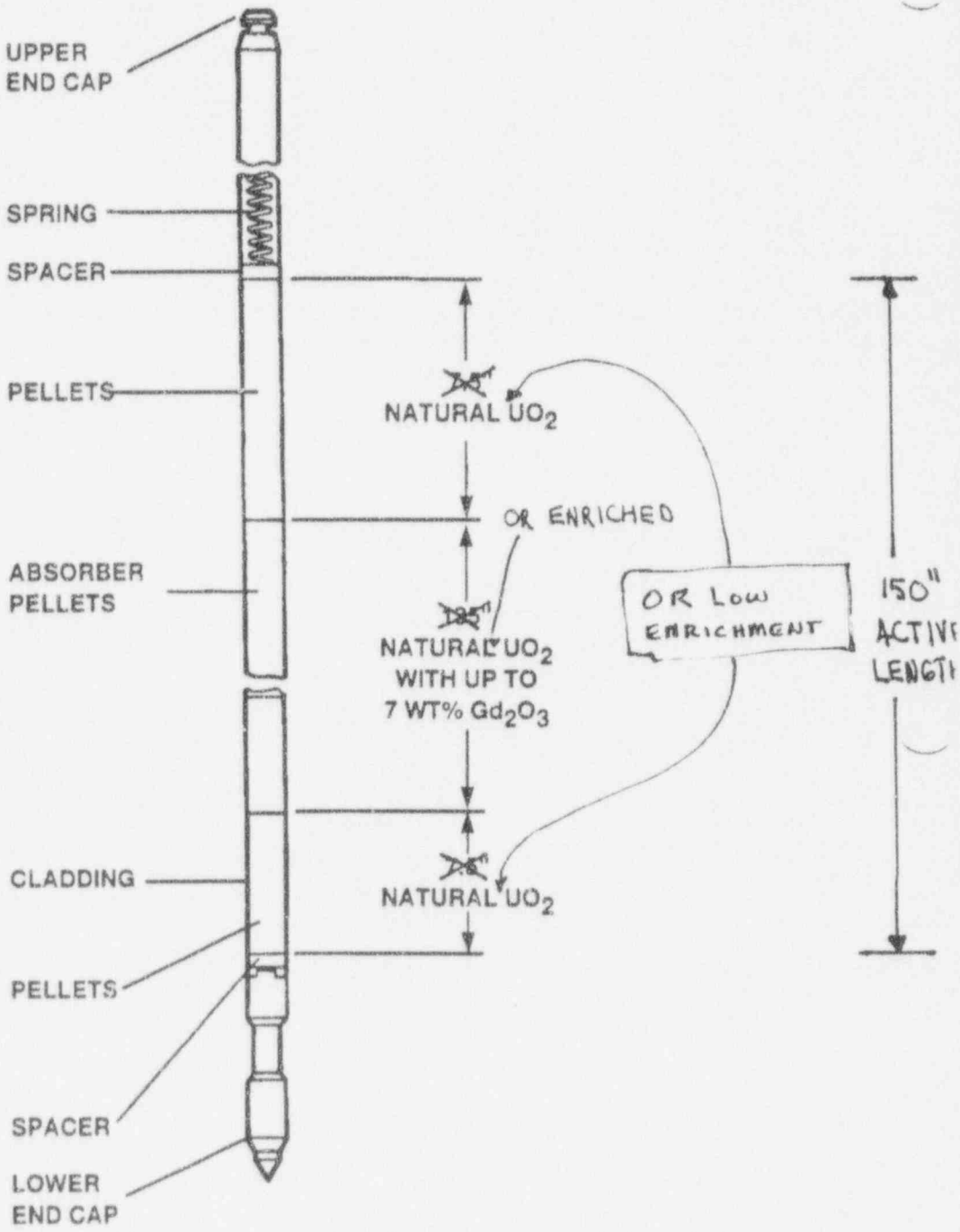
MECHANICAL DESIGN PARAMETERS

Burnable Absorber Rod (Cont'd)

Erbia - Urania Burnable Absorber Rod Design

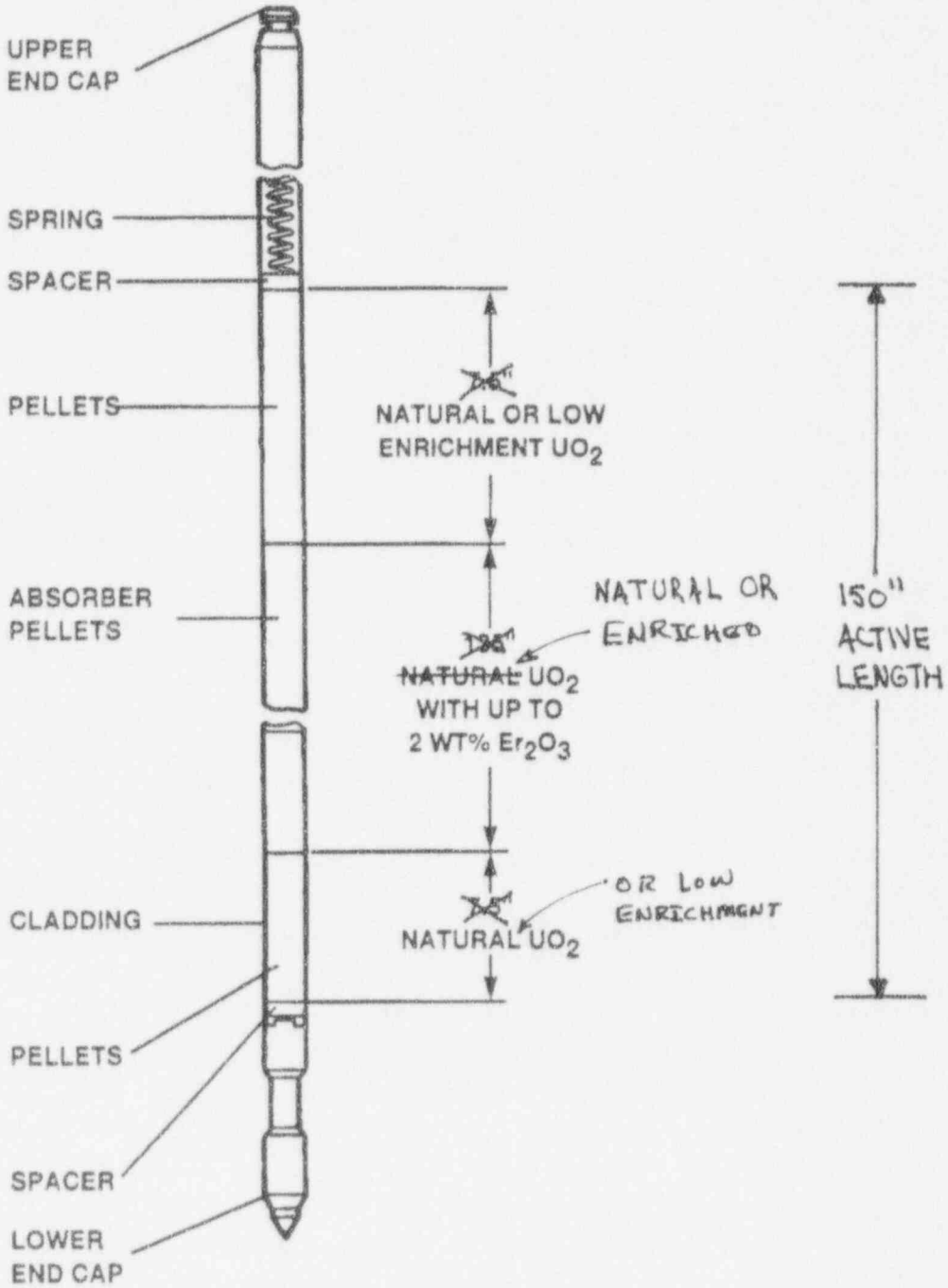
Absorber material	UO_2-Er_2O_3
Pellet diameter, inches	0.3255
Pellet length, inches, min	0.390
Pellet density (% theoretical), min	94.5
Theoretical density, UO_2, g/cm^3	10.96
Theoretical density, Er_2O_3, g/cm^3	8.64
Clad material	Zircaloy-4
Clad ID, inches	0.332
Clad OD, inches	0.382
Clad thickness, (nominal), inches	0.025
Diametral gap, (cold, nominal), inches	0.0065
Active length, inches	~~136~~ 150*
Plenum length, inches	7.938

*Includes top and bottom cutback regions



Amendment 4/5 6/28/94

SYSTEM 80+™	UO_2-Gd_2O_3 BURNABLE ABSORBER ROD	Figure 4.2 - 10



Amendment

SYSTEM 80+™	UO_2-Er_2O_3 BURNABLE ABSORBER ROD	Figure 4.2 - 12

Amendment E

December 30,

SYSTEM 80+	DAILY REACTOR POWER MANEUVERING, ASI AND REACTIVITY CONTROL BY PSCEA ONLY, NO BORON 100-50-100 NEAR BEGINNING OF CYCLE (0-8 HRS)	Figure 4.3-36

Amendment E

December 30, 1988

SYSTEM 80+	DAILY REACTOR POWER MANEUVERING, ASI AND REACTIVITY CONTROL BY PSCEA ONLY, NO BORON 100-50-100 NEAR BEGINNING OF CYCLE (8-24 HRS)	Figure 4.3-36a

Amendment F

December 30, 1

SYSTEM 80+	DAILY REACTOR POWER MANEUVERING, ASI AND REACTIVITY CONTROL BY PSCEA ONLY, NO BORON 100-50-100 AT 90% OF CYCLE (0-8 HRS)	Figure 4.3-37

Amendment E

December 30, 1988

SYSTEM 80+	DAILY REACTOR POWER MANEUVERING, ASI AND REACTIVITY CONTROL BY PSCEA ONLY, NO BORON 100-50-100 AT 90% OF CYCLE (8-24 HRS)	Figure 4.3-37a

required to be functional. If more than one type of radiation is significant, each type may be considered separately.

The COL applicant will make the specific details of the plant specific environment qualification program available for NRC evaluation. This includes a detailed maintenance/surveillance program and documentation of test reports and analyses.

3.11.1 EQUIPMENT IDENTIFICATION AND ENVIRONMENTAL CONDITIONS

Appendix 3.11B lists the equipment required to [illegible]

[[NRC staff approval is required prior to implementing a change in certain sections of these guidelines. The affected sections are identified in Section 9 of Reference 2. See DCD Introduction Section 3.2.]]

[illegible] has been reviewed and [illegible] as an acceptable methodology for environmental qualification of nuclear steam supply system safety-related electrical equipment. The NRC's approval of Reference 1 includes references to Amendment 9 of CESSAR-F. The development of CESSAR-DC necessitated a review of Reference 1 which resulted in a review of Section 3.11 of CESSAR-F, Section 3.11 and appendix J of supplement No. 3 to NUREG-0852 (Safety Evaluation Report for CESSAR System 80), and the NRC's approval letter (the NRC approval letter is included as an integral part of Reference 1). As a result of these reviews, ABB-CE has determined that there is no basis for including references to Amendment 9 of CESSAR-F in the review of CESSAR-DC. Therefore, the intent of CESSAR-DC is to utilize CENPD-255-A, Rev. 3, independent of reference to Amendment 9 of CESSAR-F. In instances where CESSAR-DC and CENPD-255-A, Rev. 3 differ, CESSAR-DC takes precedence.

B. Environmental qualification of electrical equipment located in mild environments within Combustion Engineering's scope of supply will be in accordance with the methodologies outlined in NPX80-IC-QG790-00, Qualification Guidelines for Instrumentation and Controls Equipment for Nuplex 80+ (Reference 2).

LIST OF FIGURES

CHAPTER 7

Figure	Subject
7.2-1	PPS Basic Block Diagram
7.2-2	PPS Functional Interface and Testing Diagram
7.2-3	Typical PPS Low Reactor Coolant Flow Trip Setpoint Operation
7.2-4	Typical PPS Measurement Channel Functional Diagram (Pressurizer Pressure Wide Range)
7.2-5	Reed Switch Position Transmitter Assembly Schematic
7.2-6	Reed Switch Position Transmitter Cable Assemblies
7.2-7	Core Protection Calculator
7.2-8	Ex-Core Neutron Flux Monitoring System
7.2-9	Reactor Coolant Pump Speed Sensors Typical for Each Reactor Coolant Pump
7.2-10	Trip Logic Calculator Functional Block Diagram
7.2-11	PPS Bistable Trip Logic Functional Block Diagram
7.2-12	PPS Reactor Trip System Simplified Functional Logic Diagram
7.2-13	Typical PPS Channel Functional Bistable Trip Channel Bypass
7.2-14	Typical PPS Channel Functional RPS Initiation Logic
7.2-15	Typical PPS Variable Setpoint Operation (Manual Reset)
7.2-16	PPS Testing Overlap
7.2-17	Interface and Test Processor Block Diagram

[VDU changes]

LIST OF ABBREVIATIONS

CHAPTER 7

ACC	-	Advanced Control Complex
ADS	-	Atmospheric Dump System
AFAS	-	Alternate Feedwater Actuation Signal
ALMS	-	Acoustic Leak Monitoring System
AMSAC	-	ATWS Mitigating Systems Actuation Circuitry
AOO	-	Anticipated Operational Occurrence
APS	-	Alternate Protection System
ARTS	-	Alternate Reactor Trip System
ATWS	-	Anticipated Transient Without Scram
BCS	-	Boron Control System
BDAL	-	Boron Dilution Alarm Logic
CCL	-	Component Control Logic
CCWS	-	Component Cooling Water System
CCS	-	Component Control System
CEA	-	Control Element Assembly
CEAC	-	CEA Calculator
CEDM	-	Control Element Drive Mechanism
CEDMCS	-	Control Element Drive Mechanism Control System
CET	-	Core Exit Thermocouple
CFS	-	Cavity Flood System
CHRS	-	Containment Hydrogen Recombiner System
CIAS	-	Containment Isolation Actuation Signal
CIS	-	Containment Isolation System
CMI	-	CEA Motion Inhibit
COLSS	-	Core Operating Limit Supervisory System
COMAT	-	Computer Aided Test
CPC	-	Core Protection Calculator
CRT	-	Cathode Ray Tube
CSAS	-	Containment Spray Actuation Signal
CSS	-	Containment Spray System
CWP	-	CEA Withdrawal Prohibit
DBA	-	Design Basis Accident
DBE	-	Design Basis Event
DIAS	-	Discrete Indication and Alarm System
DGS	-	Diesel Generator System
DLS	-	Diesel Load Sequencer
DNBR	-	Departure from Nucleate Boiling Ratio
DPS	-	Data Processing System
DRC	-	Dropped Rod Contact
EFAS	-	Emergency Feedwater Actuation Signal
EFWS	-	Emergency Feedwater System
E/H	-	Electro-hydraulic
EMI	-	Electromagnetic Interference
EOF	-	Emergency Operations Facility
E/P	-	Electro-pneumatic
ESF	-	Engineered Safety Feature

(The term CRT encompasses other display technologies which have similar graphic capabilities)

LIST OF ABBREVIATIONS (Cont'd)

CHAPTER 7

RPCS	-	Reactor Power Cutback System
RPS	-	Reactor Protective System
RPV	-	Reactor Pressure Vessel
RRS	-	Reactor Regulating System
RTS	-	Reactor Trip System
RTSS	-	Reactor Trip Switchgear System
RSCR	-	Remote Shutdown Control Room
RSP	-	Remote Shutdown Panel
RTSG	-	Reactor Trip Switchgear
SBCS	-	Steam Bypass Control System
SCL	-	Subgroup Control Logic
SCS	-	Shutdown Cooling System
SDS	-	Safety Depressurization System
SGT	-	Selective Group Test Logic
SIAS	-	Safety Injection Actuation Signal
SIS	-	Safety Injection System
SIT	-	Safety Injection Tank
SMM	-	Saturation Margin Monitoring
SPDS	-	Safety Parameter Display System
SPS	-	Supplementary Protection System
SSWS	-	Station Service Water System
TCS	-	Turbine Control System
TD	-	Time Delay
TSC	-	Technical Support Center
UEL	-	Upper Electrical Limit
VDU	-	Video Display Unit

7.1.1.9 System Diversity

The design of Nuplex 80+ systems maintains diversity in key areas to provide a defense-in-depth approach against the effects of common mode failures.

Nuplex 80+ employs diversity in the system designs as follows:

Function	System Design Type 1	System Design Type 2
Reactor Trip	Plant Protection System	Alternate Reactor Trip Within Process-CCS
Fluid System Controls	Emergency Success Paths (e.g. Emergency Feed-water) via ESF-CCS	Normal Success Paths (e.g., Main Feedwater) via Process-CCS
Reactivity Controls	Emergency Boration via ESF-CCS	Normal CEA Control - via Power Control System
Alarm and Indication	Alarm Tiles and Discrete Indicators - via DIAS	VDU(1) Displays - via DPS

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Comparison of the design with applicable Regulatory Guide recommendations and the degree of compliance with the appropriate design bases, General Design Criteria, standards, and other documents used in the design of the systems listed in Section 7.1.1 is described in Sections 7.1.2.2 through 7.1.2.34, and in each of the sections describing the system. (Refer to Sections 7.2 through 7.6.)

7.1.2.1 Design Bases

The design bases for the safety-related instrumentation and control of each safety-related system are presented in the section of this chapter that discusses the system to which the information applies.

Consideration has been given to instrument error in the selection of all safety system setpoints (Refer to Section 7.1.2.27). Where setpoints are listed in Chapter 7, it is understood that these are nominal values. The actual setpoint may vary within

(1) The term "VDU" is an initialism for Video Display Unit and encompasses Cathode Ray Tube (CRT) technology. Some material may continue to use the term "CRT", where this is the case, the terms "CRT" and "VDU" should be considered interchangeable unless otherwise clarified.

remote operator's modules located in the control room. In addition, the status of each bypass is provided to the plant Data Processing System.

7.1.2.21.3 ESF Components Inoperable

The bypassed and/or inoperable condition of ESF components is monitored by the ESF-CCS, as described in Section 7.3. ESF-CCS status outputs are provided to the Data Processing System (DPS) which processes logic to indicate at the system level, the bypassing, inoperability or deliberate inducing of inoperability of an ESF system. The DPS also provides status information at the component level. The operator has the ability to activate each ESF system level bypass indicator manually in the control room. Inoperable indication is shown on the DPS ~~CRTs, Integrated~~ VDU's Process Status Overview (IPSO) panel and Discrete Indication and Alarm System (DIAS) alarm tiles as further described in Sections 7.7.1.4 and 7.7.1.5.

7.1.2.22 Conformance to Regulatory Guide 1.62

Manual initiation of the RPS is described in Sections 7.2.1.1.1.11 and 7.2.2.3.2. Manual initiation of the ESFAS is described in Section 7.3.2.3.2. Conformance to Regulatory Guide 1.62, "Manual Initiation of Protective Actions," is as follows:

A. Each of the above systems can be manually actuated.

B. Manual initiation of a protective action is provided at the system level and causes the same actions to be performed by the protection system as would be performed if the protection system had been initiated by automatic action.

C. Manual switches are located in the control room, ESF-CCS and at the RTSS for use by the operators. Some ESF functions also have manual actuation at the Remote Shutdown Panel.

D. The amount of equipment common to the manual and automatic initiation paths is kept to a minimum, usually just the actuation devices. No single credible failure in the manual, automatic, or common portions of the protective system will prevent initiation of a protective action by manual or automatic means.

E. Manual initiation requires a minimum of equipment consistent with the needs of A, B, C, and D above.

F. Once initiated, manual protective action will go to completion.

7.1.2.26 Conformance to Regulatory Guide 1.97

The design of the post-accident monitoring instrumentation and information display via the DPS and DIAS is described in Sections 3.1 and 7.5. The design conforms to Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident."

7.1.2.27 Conformance to Regulatory Guide 1.105

[[The generation of safety system setpoints conforms to ISA-S67.04-1987, "Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants."]] Tier 2*

The setpoint methodology is similar to that explained in CEN-278(V), "Selection of Trip Setpoint Values for the Plant Protection System," submitted on the Palo Verde Nuclear Generating Station Unit 1 Docket, STN-50-528, and approved by the USNRC. The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst case time of the required Reactor Trip or Engineered Safety Feature Actuation. This environment may be different for different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

The reference leg heating component uncertainties for steam generator level also take into account pressure and temperature variation within the steam generator.

For all temperature and pressure setpoints, the trip will be initiated at a point that is not at saturation for the equipment. For level setpoints, no analysis setpoint is within 5% of the ends of the level span.

7.1.2.28 Conformance to Regulatory Guide 1.106

Conformance to Regulatory Guide 1.106, "Thermal Overload Protection for Electric Motors on Motor-Operated Valves," is accomplished as follows. Thermal overload protection devices are not used in safety-related motor-operated valve control circuits. Thermal overload signals are used only for status annunciation.

The ESF-CCS, as described in Section 7.3, has the design capability to provide MOV thermal overload status which is available via the DIAS and DPS described in Section 7.7.1.4 and 7.7.1.7.

* NRC staff approval is required prior to implementing a change in this information. See DCD Introduction Section 3.2

are located in a protected environment, such that they will not be subject to adverse environmental conditions. Implementation of an In-containment Refueling Water Storage Tank, for example, eliminates the concern of measuring this safety related tank level out of doors.

7.1.2.32 Conformance to Regulatory Guide 1.152

Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," states that the requirements set forth in ANSI/IEEE-ANS-7-4.3.2-1982 provide a method acceptable to the NRC staff for designing software, verifying software, implementing software, and validating computer systems in safety-related systems of nuclear power plants. The software development program used for Nuplex 80+ is described in "Nuplex 80+ Software Program Manual" (Reference 3) and the Nuplex 80+ Software Safety Plan Description (Reference 5). INSERT C

A. The Core Protection Calculator (CPC) described in Section 7.2.1.1.2.5 is a digital computer system that generates reactor trip signals for low DNBR and high Local Power Density. The CPC software is developed and tested in accordance with Regulatory Guide 1.152.

B. The Plant Protection System (PPS) described in Section 7.2 is a multiple microprocessor based system that generates RPS and ESF initiation signals. The PPS software is developed and tested in accordance with Regulatory Guide 1.152.

C. The ESF Component Control System (CCS) described in Section 7.3 is a multiple microprocessor based system that controls and actuates ESF fluid system components. The ESF-CCS software is developed and tested in accordance with Regulatory Guide 1.152.

D. The Discrete Indication and Alarm System (DIAS) described in Section 7.7.1.4 is a microprocessor based system that includes PAMI. The DIAS software is developed and tested in accordance with Regulatory Guide 1.152.

7.1.2.33 Conformance to Regulatory Guide 1.156

Conformance to Regulatory Guide 1.156, "Environmental Qualification of Connection Assemblies for Nuclear Power Plants", is as described in Sections 7.1.2.5, 7.1.2.8 and 7.1.2.18.

INSERT 7.1.2.32

[[The program for utilization of commercial grade hardware and software is described in "Requirements for the Supply of Commercial Digital Computer Hardware and Software Components to be used in Reactor Protection Safety System" (Reference 6).

NRC approval is required prior to implementing a change in certain sections of these guidelines. The affected sections are identified in Section 7 of Reference 3, and Section 7 of Reference 6.
See DCD Introduction Section 3.2.]]

REFERENCES FOR SECTION 7.1

1. "Qualification of Combustion Engineering Class 1E Instrumentation," Combustion Engineering, Inc., CENPD-255-A-1983, Revision 03, October 1985.

2. "Seismic Qualification of Instrumentation Equipment," Combustion Engineering, Inc., CENPD-182, May 1977.

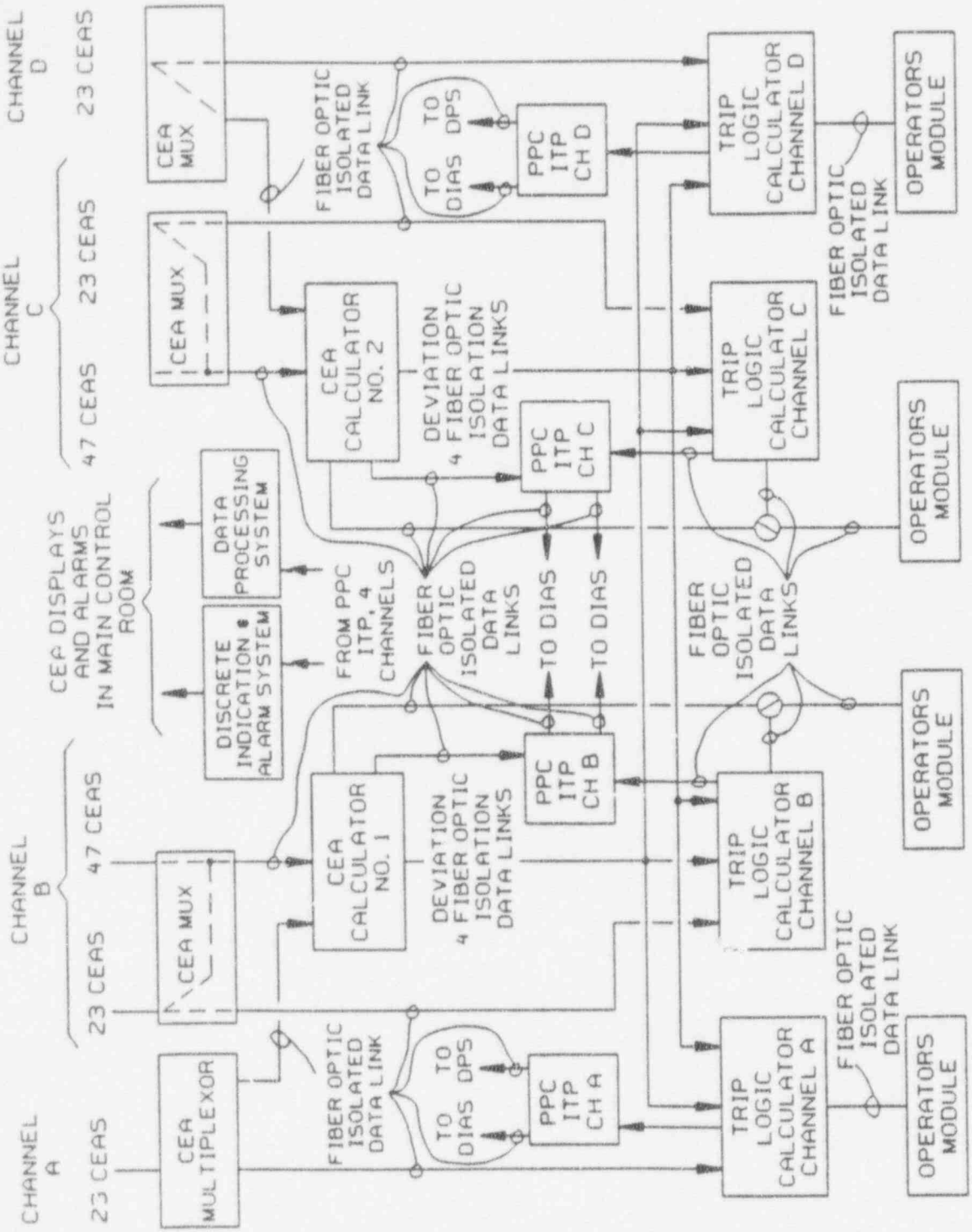
3. "Nuplex 80+ Software Program Manual," ABB-CE Inc., NPX80-SQP 0101.0.

4. "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans", U.S. Nuclear Regulatory Commission Report, NUREG-0908, August 1982.

5. "Nuplex 80+ Software Safety Plan Description," ABB-CE Inc., NPX80-IC-QP790-02.

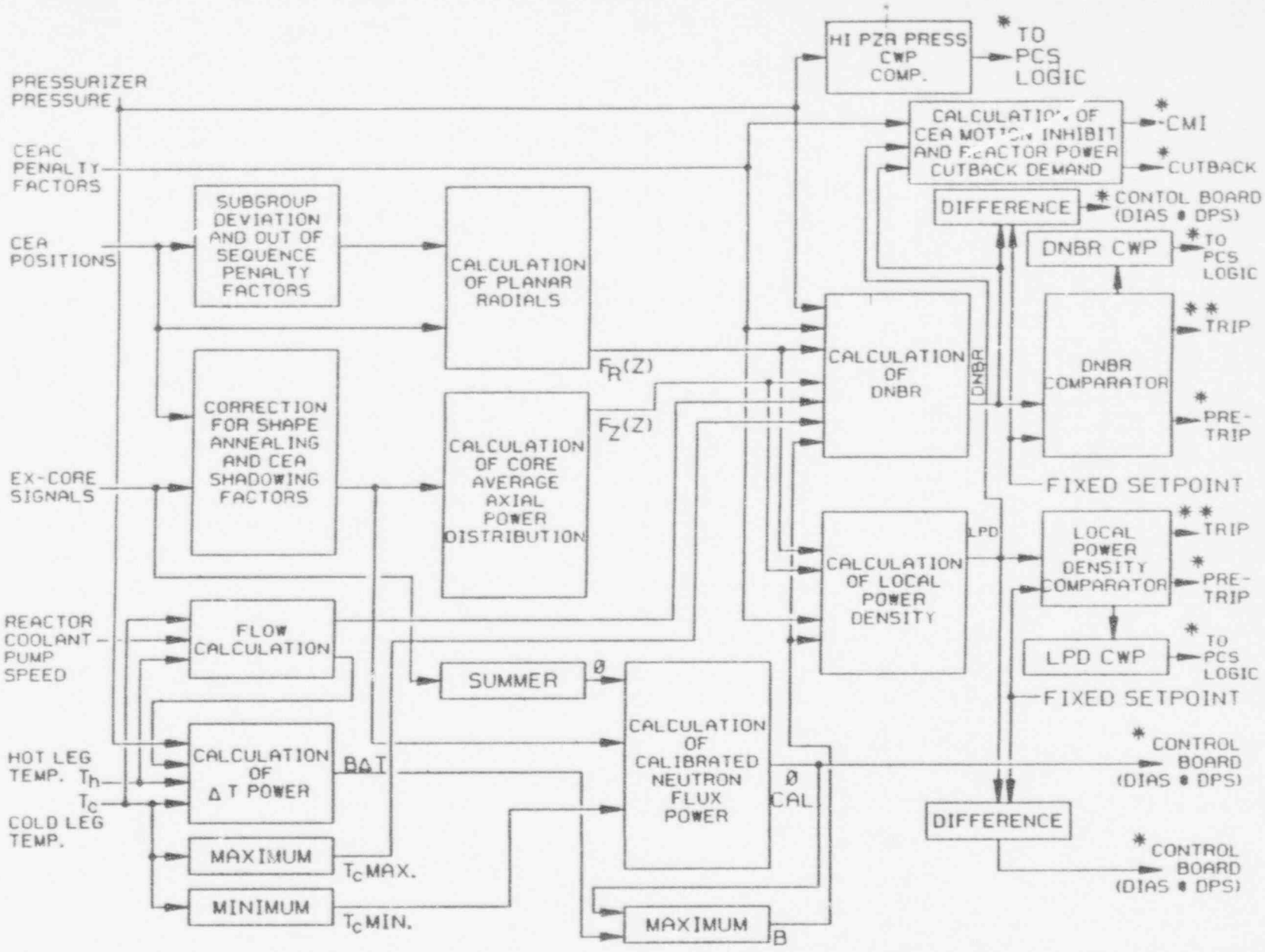
6. "Requirements for the Supply of Commercial Digital Computer Components Hardware and Software to be Used in Nuplex 80+ Safety Systems", ABB-CE Inc., NPX80-QPS-0101.1.

CLAMA FILE:
I.SYS80ISYS80FIG724



Amendment N
April 1, 1993

SYSTEM 80+	TRIP LOGIC ~~CORE PROTECTION~~ CALCULATOR FUNCTIONAL BLOCK DIAGRAM	Figure 7.2-7



CALMA FILE: I.SYSBOISYSBOFIG714

SYSTEM 80+™

CORE PROTECTION ~~TRIP LOGIC~~ CALCULATOR FUNCTIONAL ~~BLOCK~~ DIAGRAM

Figure 7.2 - 10

Amendment V - 4/29/94

component control switches, respectively. These ESF-CCS multiplexers are independent to the extent that credible single failures will impact one multiplexer only.

7.3.1.1.1 ESFAS Measurement Channels

Process measurement channels, similar to those described in Section 7.2.1.1.2.1 are utilized to perform continuous monitoring of each selected generating station variable, provide indication of operational availability of each sensor to the operator, and transmit analog signals to bistables within the ESFAS initiating logic. All protective parameters are measured with four independent process instrument channels.

A typical measurement channel is shown in Figure 7.2-4. It consists of a sensor/transmitter, current loop resistors, loop/power supply, fiber-optic isolated outputs for the process control systems, DPS and DIAS. The DPS and DIAS receive digitized information over data links which are not part of the process measurement loop.

Each measurement channel is separated from other like measurement channels to provide physical and electrical separation of the signals to the ESFAS coincidence logic. Cabling is separated within the cabinets and signals to non-1E systems are isolated. Each channel is supplied from a separate 120 volt vital AC distribution bus.

7.3.1.1.2 Logic

7.3.1.1.2.1 ESFAS Bistable and Coincidence Logic

The ESFAS Bistable Logic compares the analog signal from the sensors with predetermined fixed or variable setpoints (see Figure 7.2-12). If the input signal exceeds the setpoint the bistable produces trip signals which are transmitted to the Local Coincidence Logics (LCLs).

The setpoint values are controlled administratively and automatically monitored continuously. The fixed setpoints are adjusted at the PPS cabinet. Access for setpoint adjustment is limited by keylock with access annunciated by DIAS. The bistable setpoints are capable of being displayed at the PPS cabinet and DPS CRT displays in the main control room. Some setpoints are externally variable to avoid inadvertent initiation during normal operations such as startup, shutdown, cooldown, and evolutions such as low power testing. The steam generator and pressurizer pressure setpoints can be manually decreased by the operator and will automatically increase as pressure increases.

of the ESFAS through to the actuation of the components. The components for each ESFAS are grouped. Testing is conducted one group at a time, thus preventing the complete undesired actuation of an ESF system during testing. Since this testing causes components to actuate, an ESFAS signal from the PPS will not be impeded and the ESF system will proceed to full actuation.

The operator, using a written procedure, performs the following actions when making a selective group test.

A. Determines if the group test can be performed based on the plant conditions and lineup.

B. Selects the component group to be tested.

C. Depresses a test pushbutton, latching the test group selection and initiating a "Stop-and-Think" time delay.

D. Places the test group components and other related components in a test lineup (via component control switches).

E. A "Test Enabled" light will illuminate after the "Stop-and-Think" time delay. The operator then initiates the actuation of the group components to their ESFAS required state.

F. Confirms that the group components have actuated to the ESFAS required state for the group being tested (via component control switch indicators).

G. Places components back to their initial lineup via component control switches).

The Stop-and-Think interlock is provided in the ESF-CCS. This feature enables the test actuation logic (Step E above) for a fixed period after the group to be tested is latched (Step C above). Each time a new group is selected the time delay is reset preventing further testing. The operator must re-initiate the delay for subsequent testing.

The DPS CRT Displays can be used as an operational aid during the Selective Group Testing described above.

The operator may use the DPS to:

A. Store the initial state (position) of each component in the test group prior to placing the components in a test lineup.

OK JKM

and Success Path Monitoring displays to permit verification of proper valve alignments during post-accident conditions (refer to Section 7.7 and Chapter 18).

C. All manual valves that are not required to operate on initiation of safety injection, in the injection flow path, are locked in the post accident position. Administrative controls ensure that the valves are locked in the correct position.

D. Periodic pump and valve group tests and inspections are performed, as defined in Section 7.3.1.1.8, to verify proper operation of each active component of the safety injection system.

7.3.2.7 Containment Hydrogen Recombiner System (CHRS)

The Containment Hydrogen Recombiner System (CHRS) prevents the concentration of hydrogen in containment from reaching flammability limits following a design basis loss-of-coolant accident (LOCA). The CHRS is an Engineered Safety Features (ESF) System designed to be manually initiated. Emergency ~~Procedures~~ Operations Guidelines require hooking up and turning on the hydrogen recombiners within 84 hours following a LOCA. The hydrogen recombiners then operate continuously, i.e., they are left on rather than cycled on and off. CHRS controls and instrumentation are discussed in Section 6.2.5.

7.3.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INTERFACE REQUIREMENTS

Refer to Section 7.1.3 for system interfaces.

7.5 SAFETY RELATED DISPLAY INSTRUMENTATION

7.5.1 DESCRIPTION

This section includes a description of that safety-related display instrumentation which is available to the operator to allow him to monitor conditions in the reactor, the Reactor Coolant System, containment, and safety-related process systems, for all operating conditions of the plant so that he may perform manual actions important to plant safety.

The Nuplex 80+ Control Room uses an integrated information display hierarchy to present both safety-related and non-safety-related plant data for monitoring and control by the operator. All information is integrated (in accordance with Regulatory Guide 1.97) such that the same instrumentation used for accident monitoring is also used for normal plant operation. If an accident scenario develops, this integration allows the operators to diagnose and monitor the event using instruments with which they are most familiar. The Nuplex 80+ information systems also include automatic signal validation, through cross channel data comparison, prior to data presentation or alarm generation. This ensures that the process information displayed to the operator is correct. Multiple diverse systems are utilized to process and display the data to ensure that information processing errors are detected and alarmed. This integrated information display hierarchy is composed of the following major elements:

A. Integrated Process Status Overview (IPSO) Panel

A simplified large panel mimic is provided to allow a quick assessment of the status of the plant power production process and safety functions.

B. Discrete Indication and Alarm System (DIAS)

Discrete indicators are used to display validated safety and non-safety plant process parameters. Alarms are generated, processed and presented in an integrated manner through the use of alarm indications, message displays and the DPS ~~CRT display~~ VDU pages.

C. Data Processing System (DPS)

The DPS acquires plant data, validates it, and executes monitoring and performance calculations for presentation of information through a hierarchical set of ~~CRT displays~~ VDU pages.

for each CEA. The RSPT provides an analog position indication signal and three physically separate discrete reed switch position signals. The analog position indication system utilizes a series of magnetically actuated reed switches spaced at 1.5-inch intervals along the RSPT assembly and arranged with precision resistors in a voltage divider network. The RSPT is affixed adjacent to the CEDM pressure housing, which contains the CEA extension shaft and actuating magnet. The analog output signal is proportional to the CEA position within the reactor core. The three discrete reed switch position signals are contact closure signals from three separately located reed switches. These signals are an Upper Electrical Limit (UEL), a Lower Electrical Limit (LEL) and a Dropped Rod Contact (DRC).

The analog reed switch CEA position signals are input to the Core Protector Calculator system (see Section 7.2). CEA position information is provided to the Trip Logic Calculators (TLC's) and also to the CEA Calculators. The CEA Calculators display the position of each regulating, shutdown, and part-strength rod on demand by the operator in a bar chart format on channels B and C CPC operator modules at the main control board. The operator can address any analog position signal for display on the CPC operator's module. In addition to the displays, CEA deviation information is provided by the CEA Calculators to the CPCs and a CEA deviation alarm. A CEA deviation alarm is provided in the event a CEA Calculator indicates that the difference between the highest and lowest CEA positions in a subgroup exceeds a predetermined allowable deviation. The CEA deviation information is used in the TLC determination of power distribution. The power distribution is then factored into the low DNBR and high local power density trip function. Pre-trip alarms are initiated if the DNBR or LPD trip limits are approached. A pre-trip alarm indication is provided on the PPS operator's control panel (both local and remote). Also, a pre-trip alarm is provided to the plant annunciator system (DIAS).

The three discrete CEA position reed switches (UEL, LEL, DRC) provide contact closure signals to the Control Element Drive Mechanism Control System (CEDMCS). These signals and the CEA positions based on CEDMCS pulse counting are utilized for CEDMCS CEA control and position indication on the main control panel.

The DPS provides a validated CEA position VDU display based on the RSPT and CEDMCS pulse counting CEA position information. The validation logic identifies and alarms discrepancies between them.

7.5.1.1.5 Post-Accident Monitoring

The Post-Accident Monitoring Instrumentation (PAMI) listed in Table 7.5-3 is provided to allow the operator to assess the state of the plant following Design Basis Events. Most of these indications monitor instruments, equipment, or systems that provide automatic action for the Design Basis Event.

The Main Control Room (MCR) design utilizes the following three methods to integrate SPDS and PAMI. The design is in accordance with the intent of Regulatory Guide 1.97 as depicted in Figure 7.5-1.

A. Seismically qualified DIAS channel P processors and displays dedicated to continuously monitor and display Regulatory Guide 1.97 Category 1 individual parameters. These displays are located on the MCR Safety Monitoring Panel.

B. Seismically qualified DIAS channel N displays are integrated into the MCR panels for normal operations as well as for providing Regulatory Guide 1.97 Categories 1, 2, and 3 parameters. These displays provide the ability to select various PAMI channels and are isolated from the DIAS channel P displays.

C. The DPS provides VDU displays for all Regulatory Guide 1.97 variables in a manner that is isolated from DIAS channels P and N. The system provides integrated displays, in accordance with Chapter 18 HFE design requirements, for Critical Safety Functions, Inadequate Core Cooling Monitoring and other safety related plant parameters. The DPS also includes historical data storage, retrieval and trending. The DPS design includes data links to the On-Site Technical Support Center and Emergency Operations Facility to provide the capability for monitoring plant conditions.

7.5.1.1.6 Automatic Bypass Indication on a System Level

Automatic bypass indication on a system level as defined in Regulatory Guide 1.47 is described in Section 7.1.2.21.

7.5.1.1.7 Inadequate Core Cooling Monitoring Instrumentation

This section provides a description of the generic Nuplex 80+ approach to NUREG-0737, Section II.F.2, Inadequate Core Cooling (ICC) requirements.

The instrument sensor package selected to monitor the ICC event progression consists of:

A. Resistance Temperature Detectors (RTDs)

B. Pressurizer Pressure Sensors

C. Reactor Vessel Level Monitors employing the Heated Junction Thermocouples (HJTC) design concept

D. Core Exit Thermocouples

The signals from the RTDs, unheated thermocouples in the HJTC system, and pressure sensors can be combined to indicate the loss of subcooling, occurrence of saturation and achievement of a subcooled condition following core recovery. The reactor vessel level monitors provide information to the operator on the decreasing liquid inventory in the reactor pressure vessel (RPV) regions above the fuel alignment plate (FAP), as well as the increasing RPV liquid inventory above the FAP following core recovery. The core exit thermocouples (CETs) monitor the increasing steam temperatures associated with ICC and the decreasing steam temperatures associated with recovery from ICC.

As shown in Figure 7.5-1, these sensors are inputs to:

A. DIAS channel P processing equipment for continuous display along with other Regulatory Guide 1.97 Category 1 variables located on the Safety Monitoring Panel in the Main Control Room.

B. DIAS channel N processing equipment for display along with other plant parameters used by the operator for normal monitoring as well as post-accident monitoring.

C. Data Processing System for integration into the VDU plant process display pages. The DPS also processes saturation margin, reactor vessel level and ICC algorithms for critical safety functions for display and alarming.

All of the above display methods provide validated information to the operator as further described in Sections 7.7.1.4, 7.7.1.7 and Chapter 18.

7.5.1.1.7.1 Sensor Design

Detailed information on the associated ICC sensors is presented in the following sections.

channels to assure operational availability of these channels as discussed in Sections 7.2.1.1.9 and 7.3.1.1.8. The following design criteria were used in the selection of plant instrumentation:

A. Provide continuous monitoring of validated process parameters required by the operator.

B. Provide a permanent record via the DPS of those parameters for which trend information is useful from a safety standpoint.

C. Provide display information to the operator that is reliable, comprehensible, and timely.

D. Provide multiple channels of indication for the RPS and ESFAS process parameters to allow cross-checking of channels.

E. Provide instrumentation display that adequately monitors the parameters over the ranges required for various conditions.

The information provided is sufficient to allow the operator to accurately assess the conditions within the reactor systems, and perform those appropriate actions in a timely manner to maintain the reactor systems within the conditions assumed by the safety analysis in Chapter 15 and the Human Factors Engineering Task Analyses described in Chapter 18. In addition, the information allows the operator to perform the cross-checking of measurement channels to assure operational availability of these channels as discussed in Sections 7.2.1.1.9 and 7.3.1.1.8.

7.5.2.2 Analysis of Reactor Trip System Monitoring

Sufficient information is provided to the operator to allow confirmation that a trip has occurred and to determine the process parameter that has provided a trip input.

CEA insertion information can be determined by the operator after a trip by ~~CRT~~ VDU bar chart information and CEA limit indication (refer to Section 7.5.1.1.4).

Indication of neutron flux levels in the reactor core, as well as other reactor and Reactor Coolant System information, is provided for the operator.

The following design criteria were used in the selection of information that is provided to the operator:

C. The DPS monitors the same measurement channels and processes the data for display in the same manner as DIAS channel N. Both systems conduct the validation sequence described in B above. However, the systems employ diverse hardware and software to enhance the reliability of the overall Nuplex 80+ information display system. The DPS continuously compares its validation results to that of DIAS channel N and DIAS channel P and alarms unacceptable deviations. The DPS displays normal and accident monitoring information in the context of color graphic plant mimics and function achievement displays selectable at any VDU in the Nuplex 80+ ACC. As with DIAS channel N, the signal validation and cross system comparison technique provides the most accurate unambiguous displays to operating and technical support personnel allowing the same display media to be used for normal and accident monitoring.

7.5.2.5.3 Power Source

The PAMI displays are capable of operating independent of offsite power as follows:

Category 1: Independent Class 1E power busses are provided for each redundant sensor instrument channel up to and including the channel isolation devices. The DIAS channel P processing units and displays are powered from isolated Class 1E power busses. The DIAS channel N processors and displays are powered from isolated Class 1E, battery backed, A and B instrument busses. The DPS is powered from non-safety, battery backed computer busses.

Category 2: These variables are displayed on DIAS channel N and DPS with power supplies from the non-safety instrument busses and computer bus, respectively. Both are battery backed. Instrument channels are powered from the X or Y instrumentation bus.

Category 3: Although no specific provisions are recommended by Regulatory Guide 1.97, these variables may be displayed on DIAS channel N and/or DPS with power supplies from the non-safety instrument busses and computer bus, respectively. Instrument channels are powered from X or Y instrumentation busses.

7.5.2.5.4 Channel Availability

The system is designed to permit any one channel or method of display to be maintained when required during normal power operation. During such operations the active parts of the system

system. The transmission of signals for other non-safety related use from safety-related PAMI channels is also provided through isolation devices.

Category 3: No specific provisions are required. Therefore, these parameters are interfaced without isolation devices.

7.5.2.5.10 Servicing, Testing and Calibration

Categories 1, 2, and 3: The design permits the administrative control of access to all sensor adjustments, module calibration adjustments, and test points. Periodic checking, testing, calibration, and verification will be done in accordance with intent of Regulatory Guide 1.118 pertaining to testing of sensor channels.

Means are provided for removing DIAS processing units and displays from service. Administrative control of these actions will be developed by the site operator. Changes to constants, alarm setpoints and calibration must be made off-line and will be similarly controlled. Redundant processing units will assure continuous display or availability of Regulatory Guide 1.97 variables during adjustments. Administrative controls will also be required for the DPS. The display systems are designed to allow control of access to constants, alarm setpoints, calibration and test points. The DPS continuously checks the validated DIAS data against its own and alarms any deviations. Isolation devices are located outside containment so that they may be accessed by personnel for maintenance during accident conditions.

7.5.2.5.11 Human Factors

Categories 1, 2 and 3: The DIAS allows repair, adjustment or replacement of the display and processing system. The DPS is also designed to facilitate repair, replacement and adjustment of processing modules and ~~CRTs~~ VDUs.

Functional task analysis is used to determine the type and location of all displays in the Nuplex 80+ control room, including the Regulatory Guide

for a discussion of the Chemical and Volume Control System (CVCS). To allow the operator to maintain the required boron concentration in the reactor coolant, the Volume Control Tank contents may be maintained at a prescribed boron concentration either manually or automatically. To assist the operator in maintaining the proper boric acid concentration in the RCS, indications of boron concentration, in parts per million (ppm), are available on a DIAS discrete indicator, the DPS ~~CRTs~~ VDUs and trends described in Sections 7.7.1.4, 7.7.1.7 and Chapter 18. These signals are supplied by the Boronometer. Additional discrete indicators and ~~CRT displays~~ VDUs indicate reactor makeup water flow and boric acid makeup flow which can be used to determine whether boron addition or dilution is occurring.

The Boronometer detects the boron concentration by passing reactor coolant around a neutron source. Refer to Figure 7.7-10 for the Boronometer block diagram. Around the source are BF_3 neutron detectors. As the boron concentration decreases the neutron flux detected will increase. The circuitry converts this flux signal, corrected for sample temperature, to a ppm boron signal in the signal processing drawer. These processed signals are sent to the DPS and Discrete Indication and Alarm System (DIAS) for display in the control room.

The information supplied by the Boronometer system is used in addition to regular sampling of the reactor coolant to determine boron concentration.

At power, the boron concentration and the CEA position determine reactor coolant temperature. Because of the long time required to change the boron concentration, the boron is used for long term effects such as fuel burnup and fission product build up. Boron concentration control can also be used for load following. By adjusting the boron concentration, the CEAs can be withdrawn to provide an adequate shutdown margin. Boron control is provided via the Process-CCS.

7.7.1.1.8 In-Core Instrumentation System

The in-core neutron flux instrumentation is used to monitor the core power distribution and are fixed in place at all times during operation.

There are 61 fixed in-core monitoring assemblies with five self-powered Rhodium detectors in each location. The 61 assemblies are strategically distributed about the reactor core and the five detectors are axially distributed along the length of the core at 10, 30, 50, 70 and 90% of core height. This permits representative three dimensional flux mapping of the

Ex-core detector channels also provide neutron flux information, in the power operating range of 1% to 125%, to the Reactor Regulating System for use during automatic turbine load-following operation (see Section 7.7.1.1.1). Each channel consists of detectors and signal conditioning equipment including power supplies, a linear amplifier, and test circuitry.

7.7.1.1.10 Boron Dilution Alarm System

Reactivity control in the reactor core is affected, in part, by soluble boron in the RCS. The Boron Dilution Alarm Logic (BDAL) (see Figure 7.7-11) utilizes the ex-core detector instrumentation signals to detect a possible inadvertent boron dilution event while in Modes 3-6. The BDAL is implemented separately in the DIAS and DPS to ensure detection and alarming of the event.

The BDAL detects a possible inadvertent boron dilution event by monitoring the neutron flux indications. When these neutron flux signals increase (during shutdown) to equal or greater than the calculated alarm setpoint, alarm signals are generated by the DIAS and DPS. The alarm setpoint is periodically, automatically lowered to be a fixed amount above the current neutron flux signal. The alarm setpoint will only follow decreasing or steady flux levels, not an increasing signal. The current neutron flux indication and alarm setpoint are available via the DIAS flat panel and DPS CRT displays. There is also a reset capability to allow the operator to acknowledge the alarm and reinitialize the system.

7.7.1.1.11 Alternate Protection System

The Alternate Protection System (APS) augments the Reactor Protective System to address 10 CFR 50.62 requirements for the reduction in risk of Anticipated Transients Without Scram (ATWS) and the use of ATWS Mitigating Systems Actuation Circuitry (AMSAC).

The APS design includes an Alternate Reactor Trip Signal (ARTS) and Alternate Feedwater Actuation Signal (AFAS) that are separate and diverse from the Plant Protection System (PPS). The ARTS equipment provides a simple, yet diverse mechanism to significantly decrease the possibility of an ATWS and the AFAS provides added assurance that an ATWS event could be mitigated if it were to occur. The measurement channels for this system are shown on Figures 7.7-24, 25a, 25b.

The ARTS will initiate a reactor trip when pressurizer pressure exceeds a predetermined value (see Table 7.7-1). Turbine tripped signals can also initiate ARTS if the Reactor Power Cutback System is out of service. The ARTS turbine trip input is

Refer to Section 3.11 for the definition of environmental design requirements (temperature, humidity, radiation, pressure) relevant to the ACC equipment. Monitoring of the environmental space where the equipment cabinets are located is provided by the Heating, Ventilation, Air Conditioning (HVAC) system which is discussed in detail in Section 9.4, and by the Fire Protection system which is discussed in Section 9.5.

The main control and remote shutdown panel arrangements, layouts, information displays and controls on these panels are designed, verified and validated in accordance with the human factors design criteria and analyses provided in Chapter 18. Refer to that chapter for panel layouts and information displays utilized.

7.7.1.3.1 Main Control Room and Panels

Conformance to the GDC 19, "Control Room," is achieved by the implementation of the Nuplex 80+ Advanced Control Complex. The controlling workspace of the main control room is designed to continuously accommodate the normal operating crew and accommodate the shift crew defined in Section 18.3.2 during emergencies. The main control room, which includes offices adjacent to the controlling workspace, can accommodate the operating staff as defined in Section 18.3.2.

The main control panels are designed as compact workstations segmented as shown on Figure 7.7-14. Each workstation integrates in a human engineered fashion miniaturized back lighted component control switches, process controllers, discrete indicators, alarm tiles, message windows and video display units (CRTs, plasma and electro-luminescent displays) such that both safety and non-safety display devices are routinely used by the operator. Descriptions of the DIAS, IPSO and DPS which drive these information display devices are contained in Sections 7.7.1.4, 7.7.1.5, 7.7.1.7 and Chapter 18.

The main control panels are designed to maintain structural integrity, such that no control room missile hazards result as a consequence of a seismic event. Any safety-related Class 1E components mounted in the panels are seismically qualified to perform their safety functions. Modular equipment is used and the panels are designed for rear access to accommodate most routine maintenance activities.

All NSSS and BOP instrumentation, controls and alarms interface with the DIAS, DPS or CCS for routing to the control panels; except for operator's modules dedicated to specific plant components (e.g., Plant Protection System, Turbine Control System, CEDMCS).

The ACC Data Processing System provides the necessary interfaces with the TSC, EOF and NDL to make the same information that is available to the operating staff available to other interested personnel. The DPS equipment includes [redacted] work stations and line printers installed as shown on Figure 7.7-15 and described further in Section 7.7.1.7. See Chapter 13 for a description of the TSC and EOF.

7.7.1.4 Discrete Indication and Alarm System (DIAS)

The DIAS is designed to provide displays and alarms that utilize signal validation, automatic ranging, alarm filtering, alarm prioritization, pattern recognition and other features designed to improve the man-machine interface in accordance with the Nuplex 80+ Human Factors Engineering criteria established in Chapter 18. Refer to that chapter for the definition of the display and alarm format conventions that ensure consistency and compatibility with the DPS displays.

The DIAS receives analog and digital signals from both safety and non-safety systems, analyzes the data and presents the information to the operator via discrete indicators, alarm tiles and message windows located on the main control panels. The system interfaces with the DPS to integrate alarm and process status information into its displays. DIAS is designed to support continuous plant operation should the DPS be unavailable.

7.7.1.4.1 DIAS System Architecture

The DIAS is a segmented, distributed architecture. The system consists of a DIAS channel P segment for display of post-accident monitoring Regulatory Guide 1.97 Category-1 variables and DIAS channels N1 through N7 for the remaining segments as listed in Table 7.7-2. Each segment is configured to consist of:

A. Input/Output (I/O) data links and multiplexors

B. Central Processing Units (CPUs)

C. Display and alarm devices

The DIAS uses a segmented design to provide a degree of hardware independence and fault resistance between the various segments. The DIAS channel P segment is designed to be physically and electrically independent from the remaining DIAS channel N segments and the DPS such that a single failure will not cause a loss of more than one of the three display methods (DIAS-P or DIAS-N or DPS).

7.7.1.4.2 Discrete Indicators

The DIAS processors for each segment drive discrete indicators located on the main and remote shutdown control panels. They provide continuous display of all frequently monitored plant information. Data reduction and increased accuracy of this information are provided by validation algorithms and automatic scaling of displays. Both these techniques reduce the amount of information processing required of the operator by using the DIAS processor to perform these functions. The discrete indicator is a flat panel display device with touch screen controls. A typical discrete indicator display is shown on Figure 7.7-18. Discrete indicators also provide the operator touch screen access to a variety of parameters related to a given system or component. The most important parameter is displayed normally with menu access to other parameters or channels.

The discrete indicators are driven by the DIAS processors for a given segment. Input signals are received from safety and non-safety instrumentation channels and a validation and range selection process is performed by the DIAS processor. Comparison to the post-accident monitoring channel(s) is also performed as part of the validation. Output is then provided to the appropriate discrete indicator display device. Selected parameters are displayed continuously with alternate parameters available for display if selected at the discrete indicator.

The DIAS-DPS network interface provides all validated parameter values from DIAS to the DPS for display [redacted]. The DPS independently performs the validation algorithm and periodically checks its results against the DIAS results. If a discrepancy in the validated parameter exists, a discrepancy alarm is actuated.

The failure of an individual discrete indicator has no adverse impact on the DIAS CPU. Validation continues and validated data are still sent to the DPS and IPSO for display.

Each digital display provides a means to determine when a failure has occurred in the DIAS. A rotating running indicator is used for an immediate check of system availability. A discrete display page or alarm is used to access more detailed diagnostic information.

If the DIAS logic cannot validate a parameter, it is identified to the operator via the discrete indicator so that the parameter of choice can be selected and displayed.

The DIAS-P indicators will continuously display alphanumeric values for all Regulatory Guide 1.97 Category-1 parameters.

Alarms are categorized into 3 priorities (Priority 1, Priority 2, and Priority 3) to help establish a hierarchy for responding to abnormal conditions. All Priority 1 and Priority 2 alarms and Priority 3 alarms which degrade to Priority 2 and 1 conditions are processed by DIAS.

Refer to Chapter 18 for more information regarding the alarm logic algorithms, prioritization, mode dependencies, first out alarms, other dynamic features and HFE design aspects.

Individual DIAS segments are designed such that a failure of one segment's processor or a communications link will not affect any segment's alarms. Additional failures may result in the degradation of one (or more) segment's displays. If this occurs, alarms and alarm discrepancies are still provided independently by the DPS [redacted] displays and printer logs.

Since message displays are driven by the DIAS segments as previously described, their failure modes are the same as described above for the alarms. If they should fail, descriptive alarm information will be available independently via the DPS [redacted] displays and printer logs.

The failure of an individual alarm indication and message display has no adverse impact on that segment's CPU. The CPU still functions to generate alarms that are transmitted to the DPS for display and acknowledgement.

7.7.1.4.4 DIAS Environmental Qualification

Class 1E instrument channels are seismically and environmentally qualified up to and including the channel isolation device (fiber optic modems) such that the instrument channel is not degraded.

The DIAS displays and central processing units are non-Class 1E designed to meet control room and electronic equipment room ambient temperature, pressure and humidity requirements. Each cabinet containing DIAS computer equipment is provided with a temperature switch and associated alarm in the main control room, to alert the operator if the temperature within the cabinet reaches the upper limit specified for the environment in that location.

All DIAS displays and CPUs are seismically qualified for physical and functional integrity to enhance control room information availability.

DIAS equipment is qualified according to an established plan for electromagnetic compatibility (EMC) that requires the equipment to function properly when subjected to electrical surges, electromagnetic interference (EMI), electrostatic discharge (ESD) and radio frequency interference (RFI). Qualification is applied for equipment based on operating environment and/or inherent design characteristics.

7.7.1.4.5 DIAS Quality Classification

The DIAS performs no direct plant safety function since it strictly monitors and displays data. However, due to its importance, DIAS is designed in accordance with a quality program to assure product quality commensurate with the intended use of the equipment.

Although the DIAS is a non-safety system, it receives both Class 1E and non-Class 1E input signals. All DIAS input/output equipment is qualified to not generate faults that would degrade the channel A, B, C and D Class 1E inputs. As shown in Figures 7.5-1 and 7.7-17, the Class 1E signal interface equipment uses qualified fiber-optic network interfaces to maintain isolation.

7.7.1.4.6 DIAS Verification and Validation Requirements

The DIAS is subject to a thorough and systematic verification and validation program to assure that the system is correctly implemented and satisfies all its functional requirements. The program is implemented in accordance with Reference 3.

7.7.1.5 Integrated Process Status Overview (IPSO)

The IPSO provides a single location to allow quick assessment of key information indicative of critical plant power production and safety functions. The IPSO displays information that both the operators and supervisory personnel require for quickly assessing overall plant status. It indicates existence of Priority 1 alarms, deviations from control setpoints, key parameter values, and system operational status and non-operational availability in a schematic representation. The IPSO is implemented as a big board mimic display located above the Master Control Console (MCC) in the Nuplex 80+ control room (see Chapter 18) and as a top level DPS display page.

The plant systems represented on the IPSO will be the major heat transport path systems and systems that are required to support the major heat transport process, either power or safety related. These systems include those that require availability monitoring per Regulatory Guide 1.47.

The following systems have dynamic representations on IPSO:

CCW	-	Component Cooling Water
CD	-	Condensate
CI	-	Containment Isolation
CS	-	Containment Spray
CW	-	Circulating Water
EF	-	Emergency Feedwater
FW	-	Feedwater
IA	-	Instrument Air
SDC	-	Shutdown Cooling
RCS	-	Reactor Coolant
SI	-	Safety Injection
SW	-	Service Water
TB	-	Turbine Bypass

The IPSO design basis is to present high level process overview information by which the plant staff can quickly: determine the plant's operating status, identify major operational concern and establish priorities for operator actions. This is accomplished by selecting key plant parameters and data for presentation in accordance with Human Factors Engineering design criteria identified in Chapter 18.

Also refer to Chapter 18 for the bases used to select the parameters and other indications that are used on IPSO.

7.7.1.5.1 IPSO Configuration

The high availability of IPSO data presented to the operator is achieved by using two different display methods and systems (big board and DPS CRTs) as depicted on Figure 7.7-19. The loss of either display system will not significantly reduce the operator's ability to assess the plant's status since the big board is visible throughout the controlling work space and the IPSO page is accessible on all CRTs. In addition, both systems include redundancy and are powered by redundant battery backed non-vital instrument power busses.

7.7.1.5.2 IPSO Big Board Panel

The large panel IPSO display, as described in Chapter 18, is driven by a display processor which receives data from both the DPS and DIAS-N. Data is provided to IPSO independently from the DPS and DIAS as shown on Figure 7.7-19. The total complement of DIAS data is sent from one processor after being collected via a data bus from the others.

Component and system status and availability and deviations from control setpoints are calculated by the DPS and transmitted to the large panel IPSO. Individual validated key parameters, Priority 1 alarm actuations and parameter trends are based on calculations by the appropriate DIAS segments for display on the large panel IPSO. This allows key data to remain on the large panel IPSO with either the loss of DPS or DIAS information.

IPSO normally receives data from the DPS. In the event of failure of the DPS the operator can switch IPSO to DIAS. DIAS provides process instrumentation alarms, digital values and trends. The operator can also monitor existing DIAS displays to assess operational availability and performance of the plant systems.

High reliability of the IPSO data presented is achieved by each system using validated parameter values. In addition, DIAS results are verified independently by the DPS calculations.

The IPSO big board designed to maintain physical integrity during seismic event

7.7.1.5.3 DPS O Display

The IPSO will also the top level display page in the DPS display page hierarchy. This allows access to the IPSO from any control room panel or from remote locations such as the Technical Support Center and Emergency Operations Facility.

7.7.1.6 NSSS Integrity Monitoring System

The NSSS integrity monitoring system detects selected conditions which indicate a deterioration or which could lead to a deterioration of the RCS pressure boundary. The system consists of the following three subsystems:

A. Internals Vibration Monitoring System,

B. Acoustic Leak Monitoring System, and

C. Loose Parts Monitoring System.

7.7.1.6.1 Internals Vibration Monitoring System (IVMS)

Function

The primary function of the Internals Vibration Monitoring System (IVMS) is to provide data from which changes in the motion of the reactor internals can be detected.

The secondary function of the IVMS is to provide data that can be used to diagnose the reason for these changes.

Theory of Operation

Internals vibration monitoring utilizes the linear power detector signals from each of the ex-core channels. The system detects the time variations in the neutron flux produced by changes in the neutron absorption path lengths caused by motion of the reactor internals, specifically the fuel assemblies and the core support barrel.

The change in the motion of these components is generally reflected in a change in either or both the frequency and

depicted in Figure 7.7-20. The information is derived from plant sensors, other I&C systems and self-contained algorithms called application programs. The DPS makes the information available to the plant operations staff both on a real-time and historical basis.

The DPS is designed to enhance overall power plant operation, availability and efficiency. This is accomplished through the use of integrated plant information displays and early warning of conditions that could lead to shutdown. Through analysis of data it assists the plant staff in operating the plant within specified limits while evaluating the performance of the reactor core, primary and secondary plant systems and components.

The DPS performs in a supervisory monitoring capacity for the NSSS and BOP steam and electrical production processes. It allows the plant operations staff to obtain detailed plant data via its man-machine interfaces. These man-machine interface devices are integrated into the ACC main control panels such that they complement the other instrumentation and controls (DIAS, IPSO and CCS) in a manner that meets the Human Factors Engineering design criteria discussed in Chapter 18.

The major functions performed by the DPS include plant wide data acquisition, validation of sensed parameters, the execution of NSSS application programs and BOP performance calculations, the monitoring of plant safety and gereral status, the presentation of status and calculation results for display, the provision of logs, and the determination of alarm conditions. It includes the capability of direct interaction with plant control systems to provide permissive or control inputs to these systems based upon calculational determinations of plant conditions.

7.7.1.7.1 DPS Functions

The DPS performs complex algorithmic processing of input data. Output results from this processing are transmitted externally to other systems, as required, and is made available to the plant operator via workstation VDUs.

The DPS consists of host processors, intelligent display generators, VDUs and other support devices. The host processors perform applications processing of the received data and transmits computed results to the intelligent display system. In turn, the intelligent display system processes these data for output to the VDUs, and also serves as the man-machine interface for operator requests made via the VDU touch screens.

The major functions performed by the DPS include:

A. Acquires plant I/O data from the other plant systems via data networks.

B. Performs applications processing on the acquired data via NSSS, BOP and general plant monitoring program tasks.

C. Provides detailed plant process data to the operating staff via a ~~CRT~~ display system.

D. Provides for data archive and retrieval.

E. Provides safety parameter displays to assist the operations staff during abnormal or accident conditions and provides these data to the control room, technical support center and emergency operations facility.

F. Generates alarm information, including flood and fire door status, and integrates alarm processing with the DIAS system.

G. Generates log reports.

H. Provides the man-machine interface to the DPS.

I. Provides plant status and alarm data to the Integrated Process Status Overview (IPSO) system.

J. Provides on-line diagnostics for continuous self health monitoring.

K. Performs signal validation on input signals such that a single value is determined that best represents a given parameter being sensed by multiple sensors.

L. Performs a cross-check of validated parameters independently calculated by the DIAS and DPS.

M. Accommodates the failure of any single hardware element so that no single failure within the DPS will disable any of the aforementioned functions. Hardware redundancy coupled with continuous on-line diagnostics provides high availability.

The following types of DPS displays are provided at each ~~CRT~~ VDU workstation:

- o Plant system mimics
- o Directories
- o Alpha-numeric text
- o Video trends
- o Bar charts

These displays are accessed via touch screen menu selections from within the display page hierarchy illustrated on Figure 7.7-21 and further described in Chapter 18.

Intelligent alarm processing is built into the DPS so that the total number of alarms presented to the operator is minimized and spurious alarm (nuisance alarm) generation is minimized. Alarm priority categories are established to inform the operator of the relative importance of any alarm.

Behavior attributes such as blink, color change, and inverse video are utilized to convey the appropriate alarm state information to the operating staff.

The DPS alarm system works in conjunction with the DIAS so that alarms acknowledged via DIAS are also automatically acknowledged on the DPS and, similarly, alarms acknowledged on DPS are automatically acknowledged on DIAS. (The DIAS/DPS alarm coordination is further discussed in Chapter 18).

The DPS is designed with sufficient alarm buffer capacity in place so that no alarms are "lost" during high DPS loading conditions and/or during conditions of a high influx of alarms.

7.7.1.7.2 DPS Configuration

Figure 7.7-22 provides a high level overview of the interrelationships between the DPS components. The Data Processing System architecture is based on a distributed fault tolerant design. DPS data networks acquire plant process data from other plant systems and transmit it to the host processors.

The system configuration is based upon high speed distributed host processors and redundant peripherals. The hosts communicate information to and from a number of plant instrumentation and control systems, process the received data, and supply information to the operations staff via ~~CRTs~~ VDUs and line printers. Communications between the hosts and plant instrumentation and control systems are accomplished via fiber-optic data networks to maintain isolation. If a communication error occurs, an appropriate message is generated. Diagnostic tests are then applied to isolate the cause of the communication error.

Host processors independently receive the requisite plant data and information for its applications from the plant systems shown on Figure 7.7-22 and actively processes the received data. Host processors output required data to the plant systems, the ~~CRTs~~ VDUs and the printers. A backup host processor is in a watchdog state and assumes the function of the failed processor only when a failure is detected in the primary processor.

Each processor has one disk assigned to itself which it may read from or write to. The disk is used to boot-up the assigned processor, load the operating system, application programs and data base, store historical data from the assigned processor, store time dependent variable data from the assigned processor, temporarily store data while formatting output logs and store other programs, data and files as required.

Optical disks are used for permanent archive of historic data. In addition, each of the host processors has one assigned tape device, that is used in conjunction with the data collection snapshot function and general software support.

Each host processor is supplied with a 19 inch color monitor which is the primary system communication device for the programmer. The host processor is composed of a high speed RISC based CPU. Variable loading, caused by asynchronous system demands, is handled by the processor schedules such that the periodic application executions are not impacted.

High speed laser printers are provided for the programmer, control room operating staff, Technical Support Center and Emergency Operations Facility.

The DPS control room operator man-machine interface is primarily achieved via touch screen color ~~CRT~~ VDU workstations and other touch panel devices (e.g., DIAS annunciator tiles) as described in Sections 7.7.1.4 and Chapter 18. ~~CRT~~ VDU workstations are also provided for the control room offices, Technical Support Center, Remote Shutdown Panel and Emergency Operations Facility.

Loss of electrical power to a DPS ~~CRT~~ VDU results in a blank screen. Loss of electrical power to a host processor results in activation of the backup host processor. Loss of electrical power to multiple host processors results in a "Bad Data" status symbol on the affected display(s).

All applications are programmed using structured programming rules and techniques. The developed code is commented consistently throughout the source listings.

The software is composed of modular, structured programs. DPS on-line operation minimizes reliance on any electromechanical peripherals. All major applications (as appropriate) are memory resident and are structured to allow continued execution in the event of a disk, printer, or magnetic tape failure.

An application executive program is implemented to control the scheduling of the DPS host programs. The application executive also handles (as appropriate) diagnostic scheduling messages generated on-line by the constituent programs.

One of the following actions is taken for out-of-range sensors:

A. Automatic replacement of the failed sensor by an equivalent sensor (when available).

B. Automatic function termination when adequate process information is not available.

C. Substitution of constants for selected COLSS inputs (performed under administrative control).

If an out-of-range sensor is detected, an alarm is actuated and corrective action is automatically initiated. A more detailed discussion of sensor validity checks is included in CEN-312, "Overview Description of the Core Operating Limit Supervisory System", (Reference 2).

The core power distribution is continually monitored by COLSS, and a core average axial shape index is computed. Operation of the reactor at or below this power operating limit assures that the peak linear heat rate is never more adverse than that postulated in the LOCA analysis.

Core parameters affecting the DNBR margin are continually monitored by COLSS, and a core power operating limit based on DNBR is computed. Operation of the reactor at or below this power operating limit ensures that the most rapid DNBR transient that can result from an AOO does not result in a reduction of DNBR to a value less than the Specified Acceptable Fuel Design Limit (SAFDL).

A core power operating limit based on licensed power level is also monitored by COLSS. Operation of the reactor at or below this operating limit ensures that the total core power is never greater than that assumed as an initial condition in the safety analyses.

The core power and the core power operating limits based on peak linear heat rate, DNBR limits and axial shape index are continually indicated on the control board. The margin between the core power and the nearest core power operating limit is also provided as part of the DPS CRT displays. A DIAS alarm is initiated in the event that the COLSS calculated core power level exceeds a COLSS calculated core power operating limit.

In addition to the above calculations, the azimuthal flux tilt is calculated in COLSS. The azimuthal flux is not directly monitored by the plant protection system; rather, an azimuthal flux tilt allowance, based on the maximum tilt anticipated to

K. Historical Data Storage and Retrieval Program

The Historical Data Storage and Retrieval (HDSR) application program records, stores, recalls, and displays historical information as it is needed by plant personnel. This program provides a means of monitoring events before and after a plant trip. Important pre-selected process parameters may be periodically stored on a dedicated optical disk. Multiple optical disk platters are provided for redundancy.

The HDSR displays data in two forms:

1. A CRT representation made available through CRT trend displays.
2. A CRT listing or hard copy printout of individual data points in a log format.

L. Sequence of Events Program

The sequence-of-events program monitors PPS bistable trip status and other RPS and ESF equipment status. The program records changes (channel trips) with a resolution of several milliseconds to monitor events before and after plant trip.

M. ESF Computer Aided Test Program

The Computer Aided Test (COMAT) program monitors Engineered Safety Feature system pre-test plant line-ups for correct initial conditions, monitors and records test results, and monitors post-test plant line-ups. COMAT, a program in the Data Processing System, receives input from the ESF-CCS operator modules and feedback signals from each ESF actuated component.

N. Reactor Coolant Pressure Boundary (RCPB) Leakage Program

The DPS calculates and records RCPB leakage. Leakage detection systems are described in Section 5.2.5.

Each of the above DPS functions is intended to assist the plant operator in supervision or analysis of plant conditions. None of these functions are required to ensure plant safety or permit plant operation.

7.7.1.8.3 NSSS Interactive Programs

The DPS application programs that provide input to plant control systems are described below:

10. vital auxiliary systems control
11. electric generation control
12. ultimate heat rejection control

B. Success Path Monitoring

The Success Path Monitoring (SPM) program continuously monitors the status and performance of the plant systems and components to determine their ability to satisfy the critical safety functions (items A.1 thru A.8 above).

The SPM program provides the capability to display the success path status for each critical safety function and initiates alarms when they become bypassed or inoperable.

C. CFM Man-Machine Interface

The CFM operator interface consists of DPS human-engineered graphic and alphanumeric displays, alarms, and user input capability as described in Section 7.7.1.7.1.

The CFM provides the user with concise, understandable, integrated information to assist in assessing plant status during all modes of plant operation. The CFM displays meet the human-engineering principles discussed in Chapter 18.

Movement through the display hierarchy is provided by using the DPS touch screen menus.

7.7.2 ANALYSIS

The plant control systems and equipment are designed to provide high reliability during steady state operation and anticipated transient conditions. The RPS analysis of Section 7.2.2 encompasses the failure modes of these control systems and demonstrates that these systems are not required for safety.

The safety analyses of Chapter 15 do not require these systems to remain functional.

The man-machine interface for the control complex are designed in accordance with the Human Factors Engineering criteria described in Chapter 18 which meet applicable TMI Action Plan guidance.

of yr

The DPS provides alarms for conditions associated with reactor trip, pre-trip and ESF actuation which would not be affected by the postulated failure. The IPSO display of critical function status and key plant parameters is supported by the DPS and would not be affected by the postulated failure.

Detection of high radiation levels in the secondary system, such as in the SG blowdown or the condenser, is performed by a radiation monitoring system which is diverse from the protection system and would not be affected by the postulated failure. Monitored information from this system is data linked to both the DPS and the DIAS. Therefore, the DPS displays of high radiation alarms in these areas would remain operable with the postulated failure.

2.3 BASIS FOR OPERATOR RESPONSE TIME ESTIMATES

As discussed in Reference 2, the evaluation of the capability of the System 80+ design to provide adequate protection for a common mode failure of protection system software coincident with a Chapter 15 event initiator credits reasonable operator action.

The operator response times for the manual actuations presented in the following discussion are estimated by reviewing the sequence of steps called for in the Emergency ~~Procedure~~ Operations Guidelines (EPGs). The time required for each step is based on information provided in the draft revision to the ANS/ANSI-58.8 Standard, "Time Response Design Criteria for Safety-Related Operator Actions," and its Appendix (Reference 7) and in the Accident Prevention Group Report, "Application of the EPRI Operator Reliability Experiments Data to Update the ANS-58.8 Standard" (Reference 8).

The ANS-58.8 Standard provides analysts with a methodology to evaluate the acceptability of response time intervals afforded to operators by the plant design. The assessment verifies that the design, including its automatic protective features, will provide operators with a sufficient margin for safety-related manual actions. The applicability of ANS-58.8 extends to Design Basis Events (DBEs) that result in (automatic) reactor trip. For such scenarios, the model and criteria of ANS-58.8 have been empirically tested and shown to produce estimates that bound the actual operator response data with 95% confidence. Thus, ANS-58.8 provides conservative estimates for the operator response times to be credited in a safety analysis. To provide a reasonable estimate of the operator response for the beyond design basis analysis presented here, the ANS-58.8 model is adapted based on information provided in its Appendix and in Reference 8 which discuss the empirical operator response data used to verify the conservatism of the values presented in ANS-58.8. In the general ANS-58.8 model, the earliest time for operator action is preceded by a diagnostic time interval. It

TABLE OF CONTENTS (Cont'd)

CHAPTER 18

Section	Subject	Page No.
18.6.6	CONTROL ROOM ENVIRONMENT AND COMMUNICATION	18.6-17
18.6.6.1	Environmental Design Criteria	18.6-17
18.6.6.2	Communications Design Criteria	18.6-18
18.7	INFORMATION PRESENTATION AND PANEL LAYOUT EVALUATION	18.7-1
18.7.1	NUPLEX 80+ INFORMATION PRESENTATION	18.7-1
18.7.1.1	Information Presentation Conventions	18.7-9
18.7.1.1.1	Representational Features	18.7-9
18.7.1.1.2	Coding Techniques and Display Conventions	18.7-11
18.7.1.1.3	Labeling, Text, and Data	18.7-16
18.7.1.1.4	Alarm Philosophy	18.7-17
18.7.1.1.5	Information Access	18.7-18
18.7.1.1.6	Data Content/Display Density Guidelines	18.7-19
18.7.1.1.7	Size Criteria for Labels and Information	18.7-19
18.7.1.1.8	Information Input	18.7-22
18.7.1.2	Integrated Process Status Overview (IPSO)	18.7-22
18.7.1.2.1	IPSO Representational Characteristics and Features	18.7-23
18.7.1.2.2	Plant Functional Information on IPSO	18.7-24
18.7.1.2.3	Systems Represented on IPSO	18.7-25
18.7.1.2.4	Alarms Presented on IPSO	18.7-26
18.7.1.3	~~CRT~~ DPS Display Pages	18.7-26
18.7.1.3.1	Level 1 Displays	18.7-27
18.7.1.3.2	Level 2 Displays	18.7-27
18.7.1.3.3	Level 3 Displays	18.7-27
18.7.1.3.4	Display Page/Information Access	18.7-28

TABLE OF CONTENTS (Cont'd)

CHAPTER 18

Section	Subject	Page No.
18.7.1.3.5	Historical Data Storage and Retrieval (HDSR)	18.7-29
18.7.1.4	Discrete Indication Displays	18.7-30
18.7.1.5	Alarm Characteristics	18.7-33
18.7.1.5.1	Alarm Status and Representation	18.7-36
18.7.1.5.2	Accessing/Acknowledging Alarm Information Using the Alarm Tiles	18.7-38
18.7.1.5.3	Alarms Presented on ~~CRTs~~ DPS	18.7-39
18.7.1.5.4	Alarm Access via ~~CRT~~ Menu and Directory Pages DPS	18.7-40
18.7.1.5.5	Alarm Acknowledgement	18.7-40
18.7.1.5.6	Special Alarm Features in Nuplex 80+	18.7-42
18.7.1.6	Component Control	18.7-45
18.7.1.6.1	Component Control Man-Machine Interface Features	18.7-45
18.7.1.6.1.1	Switch Types	18.7-45
18.7.1.6.1.2	Valves	18.7-46
18.7.1.6.1.3	Status Controlled Components	18.7-48
18.7.1.6.2	Component Control Strategies	18.7-49
18.7.1.6.2.1	Control Location	18.7-49
18.7.1.6.2.2	ESFAS Control Signals	18.7-49
18.7.1.6.2.3	Bypassed or Inoperable Status Monitoring	18.7-50
18.7.1.6.2.4	ESF Actuation Status Monitoring	18.7-51
18.7.1.6.2.5	Interlocks and Actuation Signals	18.7-52
18.7.1.6.2.6	Operator Selected Automatic Control Signals	18.7-53
18.7.1.6.2.7	Standby Control Functions	18.7-56
18.7.1.6.2.8	Process Signal or Component Selection	18.7-58
18.7.1.6.2.9	Component Discrepancy	18.7-58

TABLE OF CONTENTS (Cont'd)

CHAPTER 18

Section	Subject	Page No.
18.7.2.2.1	Criteria for Determination of Required Devices and Assignment Devices to Functional Groups	18.7-72
18.7.2.2.2	Procedure for Determination of Required Indication and Control Devices and Assignment to Appropriate Functional Groups	18.7-73
18.7.2.3	Part III: Criteria and Procedure for the Detailed Layout of Controls and Indications within Functional Groups	18.7-74
18.7.2.3.1	Detailed Device Layout Criteria	18.7-74
18.7.2.3.2	Criteria for Spacing of Indications and Controls	18.7-76
18.7.2.3.3	Criteria for Device and Functional Group Identification	18.7-76
18.7.2.3.4	Procedure for the Detailed Layout of Controls and Indications within Functional Groups	18.7-77
18.7.2.4	Remote Shutdown Panel Design Criteria	18.7-79
18.7.3	RCS PANEL DESIGN	18.7-81
18.7.3.1	Assignment and Arrangement of Functions on the RCS Panel	18.7-81
18.7.3.2	Determination and Assignment of Required Indication, Alarm and Control Devices for the RCS Panel	18.7-84
18.7.3.2.1	RCS Panel Indication	18.7-86
18.7.3.2.1.1	Discrete Indication	18.7-87
18.7.3.2.1.2	~~CRT~~ Displays	18.7-88
18.7.3.2.1.3	RCS Functional Group Indication	18.7-89
18.7.3.2.1.4	Reactor Coolant Pump (RCP) Functional Group Indication	18.7-96

DPS VDU

TABLE OF CONTENTS (Cont'd)

CHAPTER 18

Section	Subject	Page No.
18.7.3.2.1.5	RCP Seal/Bleed System Functional Group Indication	18.7-99
18.7.3.2.1.6	Sensor Validation	18.7-100
18.7.3.2.2	RCS Panel Controls	18.7-102
18.7.3.2.2.1	RCS Functional Group Controls	18.7-102
18.7.3.2.2.2	RCP Functional Group Controls	18.7-103
18.7.3.2.2.3	RCP Seal/Bleed System Functional Group Controls	18.7-103
18.7.3.2.2.4	~~CRT~~ DPS VDU Controls	18.7-104
18.7.3.2.2.5	Alarm Controls	18.7-104
18.7.3.2.2.6	Lamp Test	18.7-104
18.7.3.2.3	RCS Panel Alarms	18.7-105
18.7.3.2.3.1	RCS Functional Group Alarms	18.7-106
18.7.3.2.3.2	RCP Functional Group Alarms	18.7-108
18.7.3.2.3.3	RCP Seal/Bleed System Functional Group Alarms	18.7-110
18.7.3.2.3.4	Priority 2 Operator Established Alarm	18.7-110
18.7.3.2.3.5	Priority 3 Reactor Coolant System Alarms	18.7-111
18.7.3.2.3.6	Operator Aid Information for the RCP Panel	18.7-112
18.7.3.2.4	Alarms on the ~~CRT~~ DPS VDU	18.7-112
18.7.3.3	Detailed Layout of RCS Panel	18.7-113
18.7.3.3.1	RCS Functional Group Layout	18.7-114
18.7.3.3.2	RCP Functional Group Layout	18.7-116
18.7.3.3.3	RCP Seal/Bleed System Functional Group Layout	18.7-118
18.7.3.4	Alarm Layout	18.7-118
18.7.3.5	~~CRT~~ DPS VDU Layout	18.7-119

Figures	Title
18.6.5-11	Nuplex 80+ MCC Panel Profile For Seated Operation
18.6.5-12	Nuplex 80+ ACSC Panel Profile For Standing Operation
18.7.1-1	Integrated Information Presentation
18.7.1-2	Integrated Process Status Overview (Typical)
18.7.1-3	DPS ~~CRT~~ Display Page Hierarchy
18.7.1-4	Display Page Menu Option Region
18.7.1-5	Primary Display Page Directory
18.7.1-6	Display Page Message for Menu Option Support for Parameter on the Display Page
18.7.1-7	Discrete Indicator with Trend and Menu Formats
18.7.1-8	Description of Nuplex 80+ Alarm Coding Features
18.7.1-9	Alarm Listing
18.7.1-10	Alarm Tile Panel Display Showing Alarm Tiles and Alarm Message
18.7.1-11	Alarm Tile Panel Display Showing Alarm Listing Format
18.7.1-12	Typical ESF Unavailability Monitoring Module
18.7.1-13	Level 1 Critical Function Display Page
18.7.1-14	Level 2 Critical Function Display Page
18.7.1-15	Level 3 Critical Function Display Page
18.7.1-16	Standardized Format for Process Controller Display
18.7.1-17	Process Controller Display Depicting Selection Options Associated with Master Loop Control
18.7.1-18	Process Controller Depicting Subloop Control Setpoint Selection

LIST OF ABBREVIATIONS

CHAPTER 18

AC	-	Auxiliary Console
ACC	-	Advanced Control Complex
ACSC	-	Auxiliary Console and Safety Console
A/E	-	Architect Engineer
ALWR	-	Advanced Light Water Reactor
ANPP	-	Arizona Nuclear Power Plant
APS	-	Alternate Protection System
ARO	-	Assistant Reactor Operator
BOP	-	Balance of Plant
CCS	-	Component Control System
CCWS	-	Component Cooling Water System
CEA	-	Control Element Assembly
CEDMCS	-	Control Element Drive Mechanism Control System
CEDM	-	Control Element Drive Mechanism
CEOG	-	Combustion Engineering Owners Group
CFMS	-	Critical Functions Monitoring System
COL	-	Combined Operating License
COLSS	-	Core Operating Limit Supervisory System
CPC	-	Core Protection Calculator
CRS	-	Control Room Supervisor
CRT	-	Cathode Ray Tube
CVCS	-	Chemical & Volume Control System
DCRDR	-	Detailed Control Room Design Review
DIAS	-	Discrete Indication and Alarm System
DPS	-	Data Processing System
EOF	-	Emergency Operations Facility
EOG ~~EPG~~	-	Emergency ~~Procedure~~ Guidelines
ESF	-	Engineered Safety Features
ESFAS	-	Engineered Safety Features Actuation System
FTA	-	Functional Task Analysis
HF	-	Human Factors
HFE	-	Human Factors Engineering
HFPP	-	Human Factors Program Plan
HFESGB	-	Human Factors Engineering Standards, Guidelines, and Bases for System 80+
HSI	-	Human System Interface
HVAC	-	Heating, Ventilation and Air Conditioning
I&C	-	Instrumentation and Controls
ICR	-	Information and Control Requirements
IPSO	-	Integrated Process Status Overview
LCS	-	Local Control Stations
LOCA	-	Loss of Coolant Accident
MCC	-	Master Control Console
MCR	-	Main Control Room
MDS	-	Megawatt Demand Setter
MOV	-	Motor Operated Valve
NEO	-	Nuclear Equipment Operator
NRC	-	Nuclear Regulatory Commission
NSSS	-	Nuclear Steam Supply System

18.2 DESIGN TEAM ORGANIZATION AND RESPONSIBILITIES

The Nuplex 80+ ACC was designed by a multi-disciplinary team. This design team included human factors specialists, systems engineers, Instrumentation and Controls (I&C) engineers, and senior reactor operators. The design team was responsible for development of standard Nuplex 80+ methodologies and criteria, implementation of those methodologies and criteria in the ACC design, and development of CESSAR-DC documentation. Many members of the man-machine interface design team were also responsible for I&C system designs documented in Chapter 7. This provided close integration of the man-machine interface with the I&C system designs.

A Nuplex 80+ design review team, separate from the design team was formed, comprised of personnel from a variety of organizations and disciplines within C-E. This team included Duke Power Company personnel, to provide nuclear plant construction and operation perspectives. The design review team was responsible for the review of Nuplex 80+ documentation, and participation in design review meetings related to key Nuplex 80+ developments.

18.2.1 NUPLEX 80+ DESIGN TEAM

The Nuplex 80+ design team was comprised of a core of individuals from within the Advanced Instrumentation Design (AID) group of the Instrumentation and Controls Engineering (I&CE) department. Individuals from other organizations, were included in the design group where other areas of expertise were required. Table 18.2-1 identifies the disciplines and number of individuals in each discipline represented on the Nuplex 80+ design team. Note that individuals who worked on the design team essentially full-time are separated from those who have made significant contributions to the Nuplex 80+ design as part-time members of the team. This cross section of disciplines provided a broad technical base from which the various facets of the advanced control room were designed and evaluated.

Table 18.2-2 lists the major activities related to HFE in the Nuplex 80+ design process. The disciplines of the design team member(s) who had primary responsibility for each activity are indicated. In many activities individuals from different disciplines had primary responsibility for different facets of a design activity. For example, three disciplines shared primary responsibility for the RCS panel design and corresponding ~~CRT~~ VDU display development. The senior reactor operator developed the panel layout, related ~~CRT~~ VDU display functional designs and required

processing algorithms. Computer specialists built the ~~CRT~~ VDU displays and programmed the algorithms. An HFE specialist assured that the panel, ~~CRT~~ VDU displays and processing met human factors criteria. In other activities such as the development of the standard HSI methods, multiple individuals in each discipline shared primary responsibility for development of different interface devices. Though responsibility for the design activities was assigned to specific disciplines, all members of the design team were responsible for review and comment on each Nuplex 80+ design activity and its documentation.

Human factors is integrated throughout the production process by all design team members. The HFE Standards, Guidelines, and Bases that are part of the Human Factors Program Plan for System 80+ apply, as appropriate, to all System 80+ system and equipment designs built by ABB Combustion Engineering and its subcontractors.

Job descriptions for the following HSI Design team members are found in (Section 18.4 Reference 9): Manager, Advanced Reactor Instrumentation and Control (I&C); Technical Supervisor, Control Complex Engineering; Consulting Engineer, HFE (I&C Department); Lead Engineer, HFE (Services Department); Senior Engineer, HFE (Services Department); Consulting Engineer, I&C; Lead Engineer, I&C/HF; Lead Engineer, I&C/HF/Operations; Consulting Engineer, I&C/Operations; Technical Supervisor, I&C; Consulting Engineer, I&C; and A/E Liaison and Operations Expert, Duke Engineering and Services.

The HSI design team possesses the following technical expertise: technical project management, nuclear engineering, I&C engineering, HF engineering, nuclear power plant operations, computer systems/software engineering, systems engineering, architectural engineering, nuclear power plant procedures development, personnel training/systems approach to training, systems safety engineering, and Reliability, Availability, Maintainability, and Inspectability engineering.

The Nuplex 80+ design team has evolved from the original design team described here. The Human Factors Program Plan (Section 18.4 Reference 4) describes the design team composition, activities and responsibilities in more detail.

18.2.2 NUPLEX 80+ DESIGN REVIEW TEAM

Early in the design process a Nuplex 80+ design review team was established to review the Nuplex 80+ design developments from a wide variety of engineering perspectives. The disciplines represented on the design review team are listed in Table

TABLE 18.2-2

NUPLEX 80+ DESIGN TEAM RESPONSIBILITIES

Design Process Activities	Primary Responsibilities
Design Process Development	Project Manager Nuclear Systems Engineer
Design Bases	Nuclear Systems Engineer
Functional Task Analysis	HFE Specialist Nuclear Systems Engineer
Control Room Configuration Assessment	Nuclear Systems Engineer Senior Reactor Operator HFE Specialist
Standard Man-Machine Interface Methods	I&C Engineers Computer Specialist HFE Specialist
Panel Design Criteria	HFE Specialist Nuclear Systems Engineer
RCS Panel Design & ~~CRT~~ VDU Displays	Senior Reactor Operator Computer Specialist HFE Specialist
Control Stations Outside the Main Control Room	Nuclear Systems Engineer
Verification & Validation	HFE Specialist Senior Reactor Operator

E. The control room man-machine interface is verified and validated according to accepted HFE principles (e.g., NUREG-0700) in accordance with the HFE Verification and Validation Plan (Section 18.4 Reference 3).

18.3.4 INFORMATION PRESENTATION AND CONTROL DESIGN BASES

The following design bases relate to the Nuplex 80+ information presentation and control methods:

A. The man-machine interface is based on accepted human engineering methods, principles and criteria such as those presented in NUREG-0700. An FTA and a control room validation are included in the human engineering activities.

B. Alarms and displays are presented in a unified information presentation. Redundant and diverse information sources are provided without use of "backup" displays or alarms which are only used during accidents. Information presented through conventional methods and ~~CRTs~~ VDUs is integrated. The information sources used during an accident are the same information sources used normally.

C. The number of physical display devices and the quantity of redundant data presented to the operator are reduced compared to control rooms for current generation plants.

D. Information processing and presentation methods assure acceptable operator information inventory through the use of parameter validation, mode and equipment status dependent logic and setpoints and prioritization of information.

E. The effectiveness of modern man-machine interface devices is demonstrated through the use of prototypes and HFE evaluations.

F. Information is processed and presented via two independent and diverse (yet integrated) display systems. Failure of indications and alarms in either system will not prevent:

1. continued plant operation (for up to 24 hours)
2. achieving cold shutdown
3. accident monitoring

Under degraded conditions operators will continue to have access to all required information. Equipment failures impacting automated data processing and presentation features are accommodated by increased operator surveillance.

The detailed description of the Reactor Coolant System (RCS) panel is submitted to demonstrate the application of the standard methods. Descriptions of the other Main Control Room and Remote Shutdown Room Nuplex 80+ panels are also presented.

The Nuplex 80+ human factors approach described in this chapter allows for certification of the complete System 80+ ACC. The approach provides documentation of all human factors engineering applications in the Nuplex 80+ design process and provides a detailed description of the implementation results. The Nuplex 80+ human factors approach is based on developing standard features for presenting information and providing control in the advanced control room. The standard methods are used for all Nuplex 80+ panels as compared to existing plant designs where individual panels have unique features. All human factors criteria and methods used in the above activities are documented.

Each of the design activities is described in sufficient detail, with supporting documentation where necessary, to allow NRC certification of the Nuplex 80+ design methods and criteria. The detailed submittal of the Nuplex 80+ RCS panel demonstrates the implementation results of the Nuplex 80+ methods and criteria. These provide the NRC with sufficient design results to approve the implementation of the HFE approach criteria and methods and allow certification of the complete System 80+ ACC standard design.

The following sections discuss each of the activities in the Nuplex 80+ design process in more detail.

18.4.2 HUMAN FACTORS PROGRAM PLAN

T2* [The Human Factors Program Plan (HFPP) (Reference 4 of Section 18.4) for System 80+] describes the Human Factors Engineering (HFE) program for the System 80+ Standard Plant design, specifies the elements of the program, and explains how the elements are managed. The document identifies:

1) Human Factors (HF) activities performed for the project to date;

2) HF activities to be performed as part of the ongoing System 80+ Standard Plant design program;

3. Evaluation and Allocation of System Functions
4. Task Analysis
5. Human-System Interface Design
6. Availability Verification
7. Suitability Verification
8. Design Validation

A Tracking-of-Open-Issues function is provided to ensure disposition of HFE issues formally raised during the design, construction, analyses, and evaluations. The Tracking-of-Open-Issues function is part of the performed HFPP. The function is dedicated to tracking human factors issues. It is a long-term, full-scope tracking method. Appendix A of the HFPP provides specific requirements for the Tracking-of-Open-Issues function in Section A.3.1.2.4.

18.4.3 OPERATING EXPERIENCE REVIEW

The purpose of the Operating Experience Review (Reference 1) was to fulfill Element 2, Operating Experience Review of the NRC Program Review Model (Reference 2 of Section 18.4). The Operating Experience Review describes the Operating Experience Review activities performed for Nuplex 80+ in the early phases of this program including: identification of past problems and "lessons learned" for the control room, remote shutdown panel, and local control stations; and the strengths and weaknesses encountered in similar systems of previous designs so that they may be revised or retained as appropriate.

The Operating Experience Review identifies numerous sources of past problems and "lessons learned" and provides Nuplex 80+ design guidance derived wholly or partially from these sources. For each of the issues identified in the design guidance of the report a design resolution is provided. Identified HFE issues that are currently unresolved (i.e., HFE open issues) are entered into the HFE Tracking-of-Open Issues data base.

The guidance and associated Nuplex 80+ design resolutions in the Operating Experience Review apply to the entire Nuplex 80+ design including the Main Control Room (MCR), Remote Shutdown Room (RSR) and those local control stations identified in the Emergency ~~Procedure~~ Operations Guidelines.

Amendment W
~~December 31, 1991~~
6-17-94

The remaining Nuplex 80+ panels are designed using the same methods, criteria, and standard information display, alarm and control techniques. The description of these panels identifies the use of standard indications, alarms and controls on each panel, and details the unique panel features which go beyond standard display and control techniques. These descriptions are provided in Section 18.7.4.

18.4.8 CONTROL AND MONITORING STATIONS OUTSIDE THE MAIN CONTROL ROOM

All System 80+ local control stations are designed in accordance with the criteria in the System 80+ Human Factors Engineering Standards, Guidelines and Bases (Reference 6 of Section 18.4). This assures that accepted HSI design principles are incorporated into local control station design. In addition, local control stations required to perform the System 80+ Emergency Procedure Guidelines (EPG) are designed using task analysis and human factors verification and validation.

The scope of the Nuplex 80+ ACC design includes the Remote Shutdown Panel (RSP). The RSP design bases and information and control requirements were established and a panel design was developed based on accepted HFE criteria.

The Technical Support Center (TSC) and Emergency Operations Facility (EOF) are described in Section 13.3.

18.4.9 VERIFICATION AND VALIDATION

Verification evaluates the design adequacy of the elemental parts of the HSI. Validation evaluates the overall ensemble for collective, dynamic task sufficiency.

T2* [The Human Factors Engineering (HFE) Verification and Validation Plan (Reference 3 of Section 18.4) for Nuplex 80+] describes how the HFE verification and validation is managed, administered, and performed. Additionally, the verification and validation analysis criteria, methodology, required resources (e.g. Emergency Procedure Guidelines, normal and abnormal operating sequences, I&C design requirements, HSI hardware, etc.), schedule for activities, and milestones are provided. Specifically, the HFE Verification and Validation Plan meets the design process requirements and criteria for availability verification, suitability verification, and validation of the ensemble as defined in Sections A-3.6, A-3.7, and A-3.8 of the HFE Program Plan (Reference 4 of Section 18.4).

The remaining Nuplex 80+ panels are designed using the same methods, criteria, and standard information display, alarm and control techniques. The description of these panels identifies the use of standard indications, alarms and controls on each panel, and details the unique panel features which go beyond standard display and control techniques. These descriptions are provided in Section 18.7.4.

18.4.8 CONTROL AND MONITORING STATIONS OUTSIDE THE MAIN CONTROL ROOM

All System 80+ local control stations are designed in accordance with the criteria in the System 80+ Human Factors Engineering Standards, Guidelines and Bases (Reference 6 of Section 18.4). This assures that accepted HSI design principles are incorporated into local control station design. In addition, local control stations required to perform the System 80+ Emergency ~~Procedure~~ Operations Guidelines (~~EPG~~ EOG) are designed using task analysis and human factors verification and validation.

The scope of the Nuplex 80+ ACC design includes the Remote Shutdown Panel (RSP). The RSP design bases and information and control requirements were established and a panel design was developed based on accepted HFE criteria.

The Technical Support Center (TSC) and Emergency Operations Facility (EOF) are described in Section 13.3.

18.4.9 VERIFICATION AND VALIDATION

Verification evaluates the design adequacy of the elemental parts of the HSI. Validation evaluates the overall ensemble for collective, dynamic task sufficiency.

The Human Factors Engineering (HFE) Verification and Validation Plan (Reference 3 of Section 18.4) for Nuplex 80+ describes how the HFE verification and validation is managed, administered, and performed. Additionally, the verification and validation analysis criteria, methodology, required resources (e.g. Emergency ~~Procedure~~ Guidelines, normal and abnormal operating sequences, I&C design requirements, HSI hardware, etc.), schedule for activities, and milestones are provided. Specifically, the HFE Verification and Validation Plan meets the design process requirements and criteria for availability verification, suitability verification, and validation of the ensemble as defined in Sections A-3.6, A-3.7, and A-3.8 of the HFE Program Plan (Reference 4 of Section 18.4).

The HFE V&V Plan applies to all Human System Interface (HSI) and workspace environment in the Main Control Room (MCR), Remote Shutdown Panel (RSP) and those control stations specified in the Emergency ~~Procedure~~ Operations Guidelines (EPG).

There are three distinct types of verification and validation activities, 1) Availability Verification, 2) Suitability Verification, and 3) Validation.

Availability verification takes part in two phases, Phase 1 (availability analysis) and Phase 2 (availability inspection):

The purpose of Phase 1 (Availability Analysis) is to assure the following:

1. System I&C Inventory meets the following requirements:

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

   b. Federally mandated indication and control requirements and,

   c. Fixed position MCR HSI is provided for credited safety function success path tasks identified in the Probabilistic Risk Assessment (PRA) and EPG.

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

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

The purpose of Phase 2 (Availability Inspection) is to compare the as-designed HSI to the availability checklist produced by the Phase 1 analysis, this includes:

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

2. Identifying candidate HSI indications or controls for removal.

Suitability verification addresses the issue of whether the form and arrangement of HSI indications and controls supports operator task accomplishment. It roughly spans the gap between the questions of "is the needed information, and only the needed information, present?" (Availability verification) and "does the

To: Bob Fuld

design, in terms of actual operators, using the full control room, the actual procedures, the real plant dynamics, etc. actually work together as a whole?" (Validation). Suitability therefore overlaps somewhat with both these areas of evaluative and inspection effort.

The purpose of validation is to ensure that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EOC provided usable HSI ensembles that support the successful accomplishment of the operator's required tasks (i.e. validation performance of the integrated Man-Machine system for System 80+). Validation includes operator interaction with the ensemble and EOC. Specifically, validation meets the following objectives:

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

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

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

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

5. Validate operator communication and team interaction;

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

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

Section 18.9 presents a more detailed description of verification and validation.

C. PGICRs

Procedure Guideline-based Information and Control Requirements resulting from the FTA will be afforded by the systems-based instrument and controls inventory and will be verified to be available in the control room, per HFPP requirements.

D. Event Sequences

Event sequences are representative examples of normal, abnormal, and emergency operating scenarios. Event sequences are generic cases based on the combined operator requirements of expected plant responses and proceduralized operating strategies (i.e., excluding complex interactions, error propagation, and sabotage.) The analysis of generic cases provides adequate data for the FTA's evaluation of operator workload and behavioral requirements. Selected event sequences are specified in Section 18.5.1.5.1; these sequences will be incorporated in validation activities per HFPP requirements.

E. Level of Detail

Event sequences are detailed by evaluating the necessary operator tasks per the applicable procedure guidelines (e.g., Reference 5) along a time line. Event sequences identify decision points and basic decisions, but do not pursue variations of these basic decisions into multiple contingencies.

F. Simple Additivity

The FTA will consider task elements to be additive and serially processed, unless otherwise noted. No general consideration is given to complex interactions of steps or personnel in the FTA. Formal evaluation of interactions will occur as part of human factors Validation activities.

G. Physical and Mental Workload

Regarding workload, the main concern in the FTA is with mental tasks in control center activities. [The associated physical tasks are within the capabilities of the 5th percentile female operator.] Exceptions to this assumption, such as might occur for a locally performed task, are documented in the data.

T2-4

H. Workload and Human Error

The FTA evaluates operator workload as a comparison of the time available for a task, and the time required to perform it. Loadings which violate the acceptability criteria (see Section 18.5.1.4) are considered error-likely situations to be documented and resolved.

I. Staffing

The FTA considers staffing to be a form of workload capacity. Consistent with the concern for excessive workload, staffing is conservatively assumed to be at the design basis minimum level specified for each event sequence. However, staffing level will not impact the analysis unless a detailed evaluation (per Criterion B of 18.5.1.4) is made.

J. Environmental Hazards

[The workspace environments in the Main Control Room and/or Remote Shutdown Room remain habitable for all design basis events and scenarios.] However, [local control stations included in the FTA shall be individually evaluated for personnel hazards as part of the evaluation of the specified operating sequences and tasks.] T1*

18.5.1.2 Input and Design Documentation Review

System 80+ includes design enhancements and improvements to address experience gained from earlier plant designs, criteria provided by the Advanced Light Water Reactor (ALWR) Requirement Document, and guidance from the NRC's Severe Accident Policy and Standardization Rule. Documentation for the System 80+ design has been reviewed to identify the plant processes, configurations, and modes of operation.

In particular, CESSAR-DC, supported by system descriptions, technical specifications, and training materials for System 80, provides the baseline for describing the operating role of the revised systems in System 80+ and extrapolating their operations for revised procedure guidelines and the FTA. A list of these basic purposes of the plant systems and configurations is maintained as part of the System 80+ FTA data base.

18.5.1.3 Task Decomposition and Data Framework

[The following hierarchical structure was used as the framework to decompose event sequences into components:

I) Gross functions/subfunction
  A) Task
    1) Element]

T2*

Each of these levels is detailed as follows.

18.5.1.3.1 Gross Function/Subfunction Level

Gross functions are high level statements of the operator's general purpose in performing a related set of tasks. They specify a basic operating goal (e.g., "Maintain RCS Heat Removal") from the operator's perspective. Each gross function (or subfunction) statement represents one or more tasks with a single main purpose, and may be comprised in different situations by different sets of tasks. Functions appear within sequences in a generic order of performance, per vendor operating procedure guidelines. Subfunctions are identified if a gross function has multiple purposes; otherwise, the two levels of description are similar.

18.5.1.3.2 Task Level

This level analyzes operator behaviors in terms of a generic, closed-loop information processing model. It utilizes a simple but comprehensive data framework that can accommodate a large variety of specific tasks. [The model views a task as falling into one of four basic categories:]

A. [Input] (Perception) - Collect or obtain needed information.

B. [Process] (Cognition) - Evaluate, plan, calculate, decide (etc.) on a result or course of action based on collected or otherwise known information.

C. [Output] (Action) - Perform the act or manipulation specified.

D. [Feedback] - Monitor the results of output actions and transmit the results back to the input; this either verifies success or cues further processing and corrective action.

Tasks in a sequence tend to cycle through these categories, although well-designed and skillfully performed tasks do not necessarily show four distinct components. The benefit of this framework is that it directs the analyst's attention to the necessary components of deliberate, rule-based (i.e., procedural) behavior (Reference 6).

A single task is expressed by a task statement. A task statement includes two basic parts, which are 1) a verb from the defined verb taxonomy (listed in the FTA data base), and 2) the object of the verb, (a parameter, component, etc.) For example:

Collect	Pressurizer Pressure
(verb)	(object)

09-26-1994 14:55 P.02

These task statements then serve as the centerpiece around which the remaining task element data are organized and documented.

18.5.1.3.3 Element Level

The element level of this analysis specifies critical details that may be associated with each task statement. These data complete the FTA picture of task behavioral requirements; i.e., of how the task must be performed. The additional data include:

A. Cues - Cues are conditions, prompts, alerts, or similar items directing that the task statement should be executed. (A typical default cue for a task statement is its position within a procedure sequence.)

B. Criteria - criteria are qualitative or quantitative values or limits which are necessary references for correct evaluation or execution of the task statement.

C. Time Allowed - The time allowed is the period of time required, as assumed by the analysis, for the execution of the multiple elements comprising the task statement. The initial screening value of time allowed to perform each task statement is one minute (see Section 18.5.1.4).

D. Location - Location is the place or position at which a given task is expected to be performed. Location data provide a basis to perform link analysis.

E. Remarks - Remarks accommodate extra notations or miscellaneous task requirements from data categories with infrequent significance. In the present task analysis, these issues could include, for example, specific workplace suitability issues, task support requirements, communications requirements, crew interaction, or hazard identification.

Elements are the lowest level of the FTA decomposition. An example of a task element data form is shown in Table 18.5.1-1. Additional analyses of the data performed as part of the FTA (i.e., information and controls requirements, and time profile/workload evaluations) are described in Sections 18.5.1.5.3 and 18.5.1.5.4.

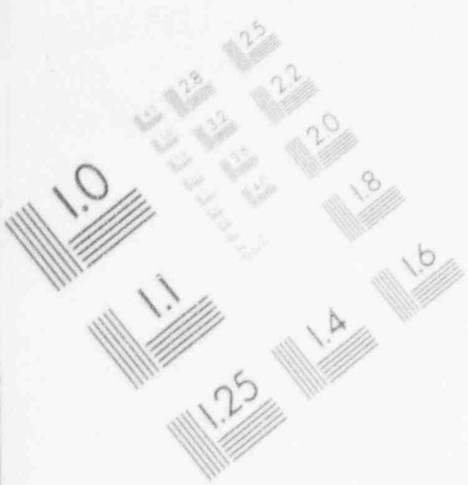
18.5.1.4 Loading Criteria

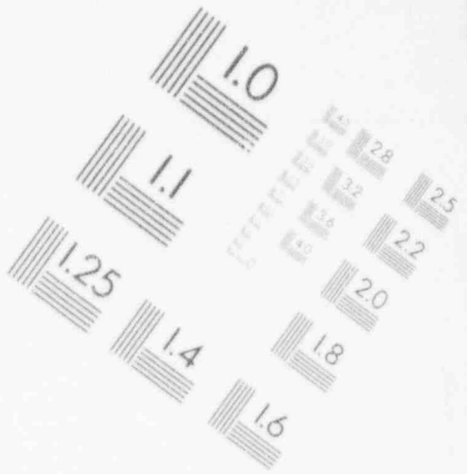
Workload is evaluated on the basis of comparisons between estimates of time available for, and time required by, the elements of a task. Time criteria are as follows:

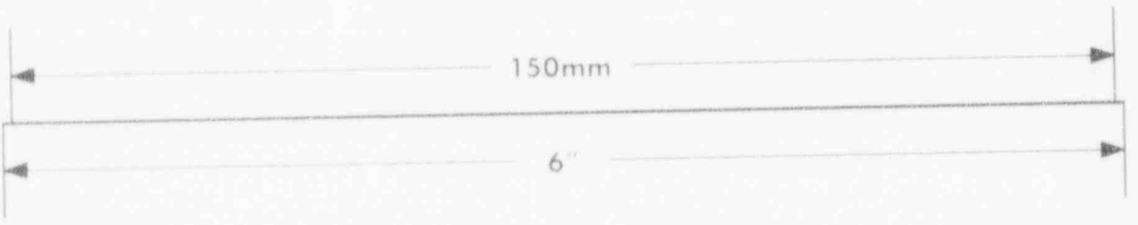
09-26-1994 14:56 P.03

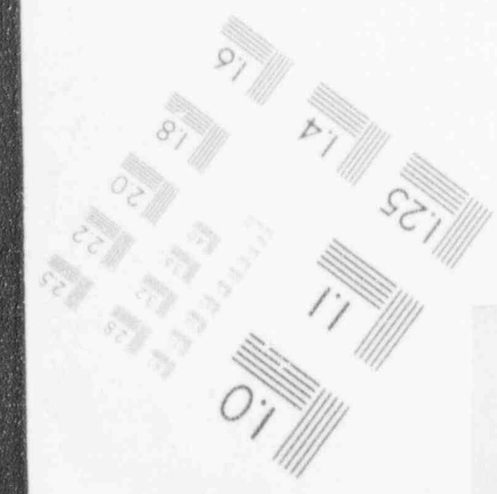
1

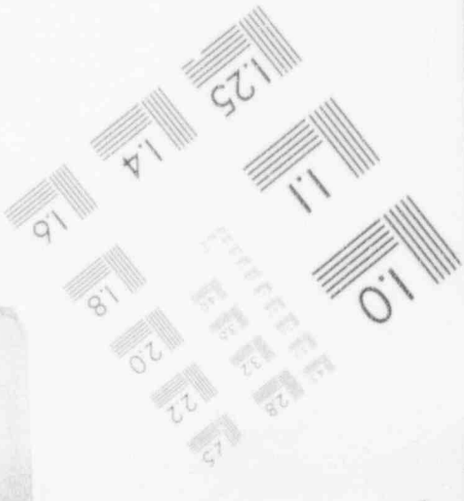
IMAGE EVALUATION
TEST TARGET (MT-3)





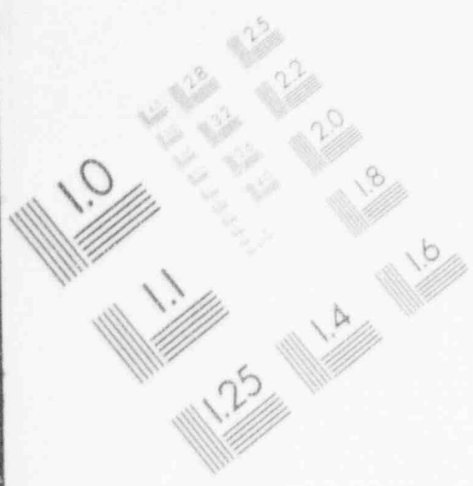


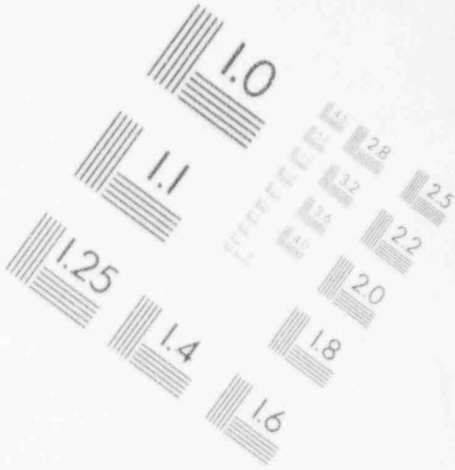


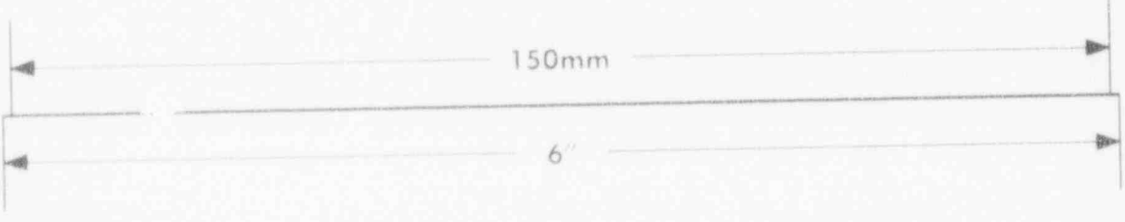


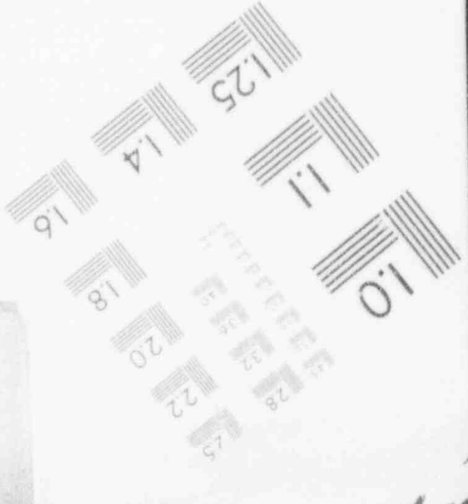
1

IMAGE EVALUATION
TEST TARGET (MT-3)



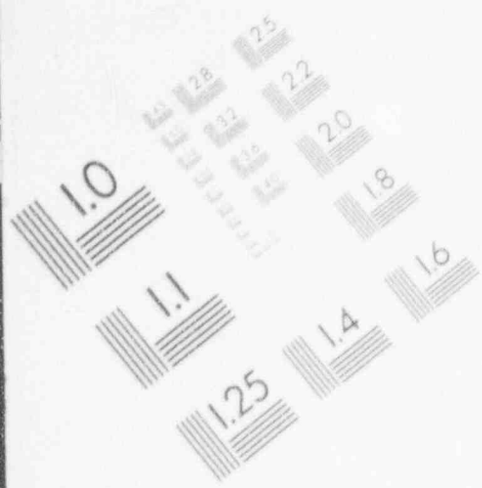


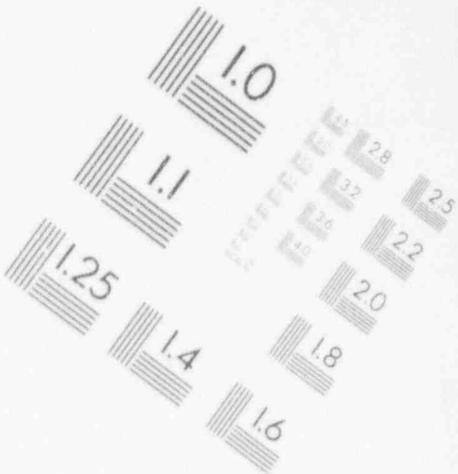


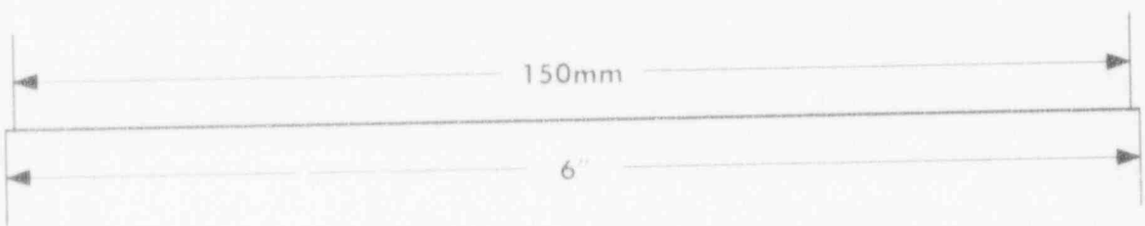


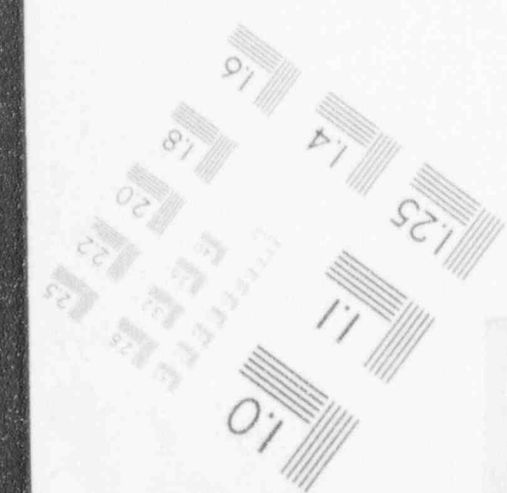
1

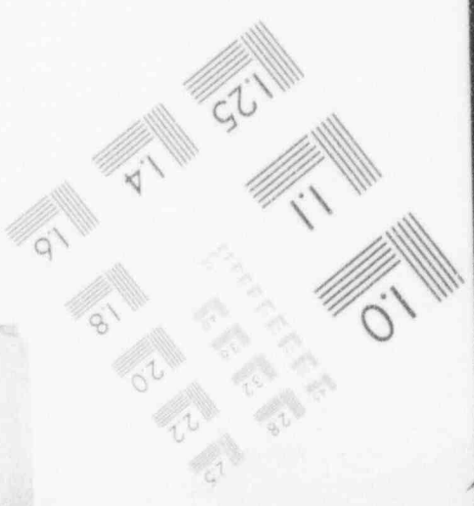
IMAGE EVALUATION TEST TARGET (MT-3)





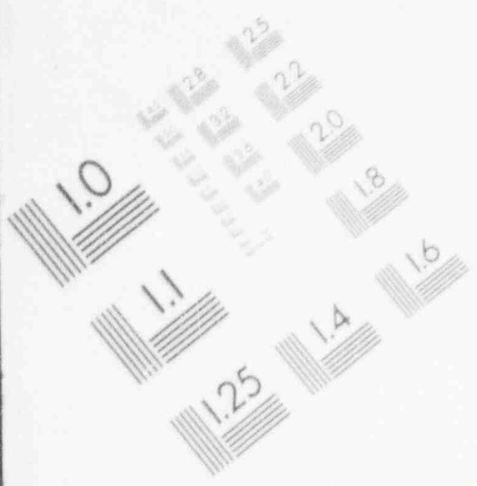


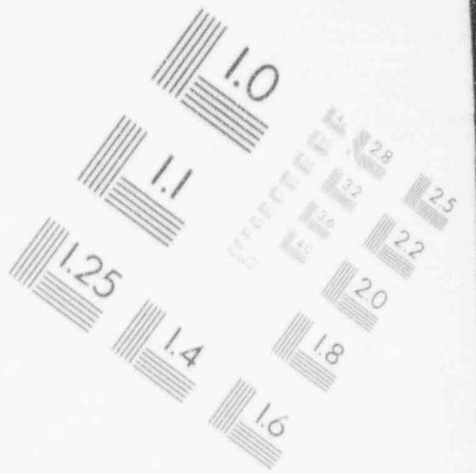


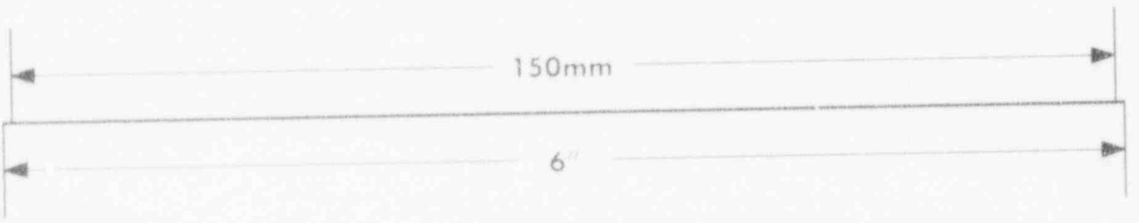


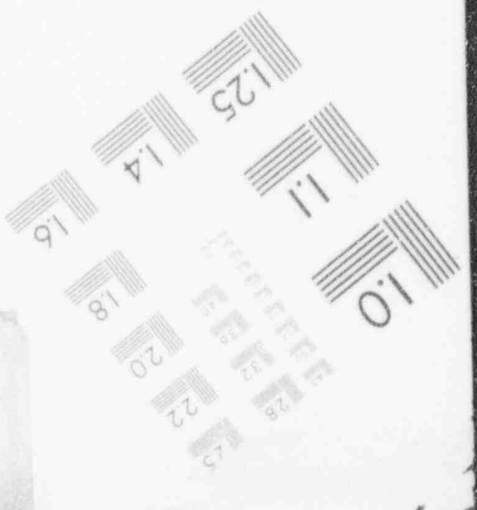
1

IMAGE EVALUATION
TEST TARGET (MT-3)









A. A conservative criterion based on ANSI/ANS 58.8 (Reference 8) provides a minimum of one minute for each required manual manipulation (i.e., task element). This is an initial screening criterion to identify potentially excessive loadings.

B. If task requirements exceed the limits of the screening criterion in 18.5.1.4.A, more detailed evaluation of the human performance requirements is performed, based on a cognitive processing model presented in Reference 7. These evaluations will utilize explicitly stated conservative assumptions, model parameters, and criteria for human and equipment response time performance. Example calculations will be provided.

Failure to meet both criteria A and B above indicates the need for further design assessment and formal resolution. Such findings are entered into the Tracking Open Items (TOI) database, per the requirements of the HFPP.

18.5.1.5 **Analyses**

T2*

18.5.1.5.1 Scope

The following event sequences comprise a representative cross section of operations for the Nuplex 80+ control room FTA, including all Emergency Procedure Guidelines (Reference 5):

A. Startup with Steady State and Transient Power Operations

B. Shutdown with Shutdown Decay Heat Removal

C. Design Basis Shutdown from the Remote Shutdown Area

D. Mid-loop (including Loss of SCS) and Refueling Operations

E. Reactor Trip and Recovery

F. Loss-of-Coolant-Accident

G. Steam Generator Tube Rupture

H. Excess Steam Demand

I. Loss of Feedwater

J. Loss of Offsite Power (LOOP)

K. Station Blackout (LOOP without DGs)

L. Anticipated Transient Without Scram

M. Design Basis Failures of DPS and DIAS

A. A conservative criterion based on ANSI/ANS 58.8 (Reference 8) provides a minimum of one minute for each required manual manipulation (i.e., task element). This is an initial screening criterion to identify potentially excessive loadings.

B. If task requirements exceed the limits of the screening criterion in 18.5.1.4.A, more detailed evaluation of the human performance requirements is performed, based on a cognitive processing model presented in Reference 7. These evaluations will utilize explicitly stated conservative assumptions, model parameters, and criteria for human and equipment response time performance. Example calculations will be provided.

Failure to meet both criteria A and B above indicates the need for further design assessment and formal resolution. Such findings are entered into the Tracking Open Items (TOI) database, per the requirements of the HFPP.

18.5.1.5 Analyses

18.5.1.5.1 Scope

The following event sequences comprise a representative cross section of operations for the Nuplex 80+ control room FTA, including all Emergency ~~Procedure~~ Operations Guidelines (Reference 5):

A. Startup with Steady State and Transient Power Operations

B. Shutdown with Shutdown Decay Heat Removal

C. Design Basis Shutdown from the Remote Shutdown Area

D. Mid-loop (including Loss of SCS) and Refueling Operations

E. Reactor Trip and Recovery

F. Loss-of-Coolant-Accident

G. Steam Generator Tube Rupture

H. Excess Steam Demand

I. Loss of Feedwater

J. Loss of Offsite Power (LOOP)

K. Station Blackout (LOOP without DGs)

L. Anticipated Transient Without Scram

M. Design Basis Failures of DPS and DIAS

N. Selected Abnormal Operating Procedures

O. Selected Tech Spec Surveillances]

18.5.1.5.2 [PRA and Critical Tasks]

In addition to the representative event sequences in Section 18.5.1.5.1, the System 80+ PRA and Associated Human Reliability Analyses (HRA) are used to identify ["Critical Tasks."] These [are operator tasks indicated by PRA to make significant contribution to total plant risk.] The cutoff criterion for Critical Tasks is that they fall within the top 100 events of the Level 1 PRA in order of risk achievement value. This criterion spans almost six orders of magnitude of risk reduction, and divides events analyzed to significantly reduce risk from the residual events (i.e., those with risk achievement approaching an asymptote at 10^0). [Critical Tasks are incorporated as separate event sequences in the Task Analysis database.] Findings from the associated HRA and FTA are dispositioned through the formal documentation and tracking mechanisms of the Human Factors Program Plan (Reference 10).

18.5.1.5.3 [Information and Control Requirements]

T2*

The evaluation of PGICRs summarizes the procedure-based parametric requirements for display and control variables identified by the FTA. Summaries are sorted from the FTA database for each variable. For example, characteristics for 'pressurizer pressure' are summarized for each distinct gross function where pressurizer pressure is utilized. [Characteristics include the following areas:]

A. [Device type]

A recommendation for display/control type for each variable is provided based on the FTA results, operating experience, human performance characteristics, and human factors guidance.

B. [Range]

The required upper and lower value limits for the variable as required for operations is provided based on transient performance figures.

C. [Accuracy]

The instrument accuracy required for each variable is provided based on operations requirements.

D. [Units]

The recommended unit of measure for each variable is provided based on operational experience, industry performance, and engineering judgement.

T2*

E. [Precision]

The display precision of each measured variable is provided based on operator task requirements.

18.5.1.5.1

18.5.1.5.4 [Time Profile/Workload Evaluation

The event sequences identified] in Section 18.5.1.1 [are analyzed and reviewed by experts in plant operations. Event time profiles are then plotted on time lines and sectioned into discrete evaluation intervals (to minimize unnecessary calculation, fewer activities may be summed within longer intervals.) Process time estimates are derived by evaluating data from specific event profiles, based on operator experience and process transient response models. The time profile evaluation considers:

A. The time into the event sequence at which the operator is expected to be cued to perform the tasks in an interval

B. The time available to perform the tasks in the interval (i.e., plant process constraints)

C. The time required to perform the tasks in the interval (i.e., human performance constraints)

D. Whether time required exceeds time available for specified task intervals

Criteria for time required to perform tasks are specified] in Section 18.5.1.4.

18.5.1.5.5 Link Analysis

Link analysis evaluates the distribution and interactions of the operators' panel transitions in a given scenario. [Link analysis is performed for design basis normal operations and plant shutdown during a loss of the DPS.] This is considered to be a limiting case in terms of its impact on the necessary movement of operators within the controlling workspace. Link data shall be precise to the nearest half-panel.

18.5.1.5.6 [Identification of Overload Situations and Recommendations

If time required exceeds time available per Criterion A] of Section 18.5.1.4, [then task loading is a concern. In such cases, the task sequence is reevaluated incorporating more refined timing assumptions per Criterion B. If this detailed evaluation continues to show that more time is required than is available for operator action, the issue is identified in the results, and must receive formal assessment and resolution] per the design process and HFPP.

18.5.1.6 Results Documentation

The FTA data are stored on a personal computer database system to allow manipulation and updating of information. As additions are made to the database, existing portions of the analysis will be updated to reflect any changes to the FTA methodology. This will ensure internal consistency of the final FTA results, and of those results with the System 80+ design.

18.5.1.5.1

18.5.1.5.4 Time Profile/Workload Evaluation

The event sequences identified in Section 18.5.1.1 are analyzed and reviewed by experts in plant operations. Event time profiles are then plotted on time lines and sectioned into discrete evaluation intervals (to minimize unnecessary calculation, fewer activities may be summed within longer intervals.) Process time estimates are derived by evaluating data from specific event profiles, based on operator experience and process transient response models. The time profile evaluation considers:

A. The time into the event sequence at which the operator is expected to be cued to perform the tasks in an interval

B. The time available to perform the tasks in the interval (i.e., plant process constraints)

C. The time required to perform the tasks in the interval (i.e., human performance constraints)

D. Whether time required exceeds time available for specified task intervals

Criteria for time required to perform tasks are specified in Section 18.5.1.4.

18.5.1.5.5 Link Analysis

Link analysis evaluates the distribution and interactions of the operators' panel transitions in a given scenario. Link analysis is performed for design basis normal operations and plant shutdown during a loss of the DPS. This is considered to be a limiting case in terms of its impact on the necessary movement of operators within the controlling workspace. Link data shall be precise to the nearest half-panel.

18.5.1.5.6 Identification of Overload Situations and Recommendations

If time required exceeds time available per Criterion A of Section 18.5.1.4, then task loading is a concern. In such cases, the task sequence is reevaluated incorporating more refined timing assumptions per Criterion B. If this detailed evaluation continues to show that more time is required than is available for operator action, the issue is identified in the results, and must receive formal assessment and resolution per the design process and HFPP.

18.5.1.6 Results Documentation

The FTA data are stored on a personal computer database system to allow manipulation and updating of information. As additions are made to the database, existing portions of the analysis will be updated to reflect any changes to the FTA methodology. This will ensure internal consistency of the final FTA results, and of those results with the System 80+ design.

As with the functional task analysis data, the experience-based control data is modified to accommodate specific System 80+ process and component designs. The generic Nuplex 80+ implementation methods for controls requirements are described in Section 18.7.1. Specific examples pertaining to the RCS are provided in Section 18.7.3 and 18.7.3.2.2, respectively. The functional task analysis allocation evaluation then confirms the acceptability of the Nuplex 80+ design.

18.5.4 [MCR ANNUNCIATOR, DISPLAY, AND CONTROL INVENTORY

Based on the FTA data and results, a subset of the identified annunciators, displays, and controls is specified as the MCR Minimum Inventory required to execute the EPGs and perform the PRA Critical Tasks] (Section 18.5.1.5.2). [Within this scope, the following criteria are used to identify Minimum Inventory entries:

Annunciators and Displays

- Critical Safety Function status indicator
- Preferred/credited Success Path performance indicator
- Indication required to verify Safe Shutdown
- Reg. Guide 1.97 Category 1 variable

Controls

- Preferred/credited Success Path component (i.e., in major flowpath)
- Component required to perform Safe Shutdown

The MCR Minimum Inventory is provided as fixed position HSI per the Certified Design. The term "fixed position" refers to the unique location on IPSO and the MCR panels for annunciators, displays, and controls defined for the parameters in the MCR Minimum Inventory. Standard Features] (Section 18.7.1) [which can be used to provide fixed position annunciator, display, or control functions include DIAS Dedicated Parameter Displays, DIAS Alarm Tile Displays, CCS Switch Configurations, and CCS Process Controller Displays.

The MCR Minimum Inventory (Table 18.5.4-1) is incorporated in the overall Availability verification] (Section 18.9.1) [along with the indication and control requirements from federal regulations, system design specifications, FTA results, and the HFE tracking system. Availability verification assures consistency between these requirements and the completed system I&C inventories, as well as between the system I&C inventories and the as-built HSI.]

As with the functional task analysis data, the experience-based control data is modified to accommodate specific System 80+ process and component designs. The generic Nuplex 80+ implementation methods for controls requirements are described in Section 18.7.1. Specific examples pertaining to the RCS are provided in Section 18.7.3 and 18.7.3.2.2, respectively. The functional task analysis allocation evaluation then confirms the acceptability of the Nuplex 80+ design.

18.5.4 MCR ANNUNCIATOR, DISPLAY, AND CONTROL INVENTORY

Based on the FTA data and results, a subset of the identified annunciators, displays, and controls is specified as the MCR Minimum Inventory required to execute the ~~EPGs~~ EOGs and perform the PRA Critical Tasks (Section 18.5.1.5.2). Within this scope, the following criteria are used to identify Minimum Inventory entries:

Annunciators and Displays

- Critical Safety Function status indicator
- Preferred/credited Success Path performance indicator
- Indication required to verify Safe Shutdown
- Reg. Guide 1.97 Category 1 variable

Controls

- Preferred/credited Success Path component (i.e., in major flowpath)
- Component required to perform Safe Shutdown

The MCR Minimum Inventory is provided as fixed position HSI per the Certified Design. The term "fixed position" refers to the unique location on IPSO and the MCR panels for annunciators, displays, and controls defined for the parameters in the MCR Minimum Inventory. Standard Features (Section 18.7.1) which can be used to provide fixed position annunciator, display, or control functions include DIAS Dedicated Parameter Displays, DIAS Alarm Tile Displays, CCS Switch Configurations, and CCS Process Controller Displays.

The MCR Minimum Inventory (Table 18.5.4-1) is incorporated in the overall Availability verification (Section 18.9.1) along with the indication and control requirements from federal regulations, system design specifications, FTA results, and the HFE tracking system. Availability verification assures consistency between these requirements and the completed system I&C inventories, as well as between the system I&C inventories and the as-built HSI.

REFERENCES FOR SECTION 18.5

1. "Generic Operator Information and Controls Requirements Review Based on Combustion Engineering Emergency Procedure Guidelines," Combustion Engineering, Inc., CE-NPSD-299, July 1985.

2. "C-E Owners Group Generic Information and Control Characteristics Review," Combustion Engineering, Inc., CEN-307, August 1985.

3. "Task Analysis of Nuclear Power Plant Control Room Crews," USNRC, NUREG/CR-3371, 1983.

4. "Human Factors Guide for Nuclear Power Plant Control Room Development," EPRI, NP-3659, August 1984.

5. ~~"Combustion Engineering~~ Revised System 80+ Emergency ~~Procedure~~ Operations Guidelines," ~~Combustion Engineering, Inc., CEN-152, Rev. 3, 1987~~ LD-94-043, June 1994.

6. "Information Processing and Human Interaction," J. Rasmussen, North-Holland: NY 1986.

7. "The Psychology of Human-Computer Interaction," S. Card, T. Moran, A. Newell, Lawrence Erlbaum: NH, 1983.

8. "Time Response Design Criteria for Safety-related Operator Action," American National Standards Institute, ANSI/ANS-58.8.

9. "System 80+ Function & Task Analysis Report," Combustion Engineering, Inc., NPX80-IC-DP790-02.

10. "Human Factors Program Plan for the System 80+ Standard Plant Design," NPX80-IC-DP790-01.

11. "MCR Minimum Inventory of Fixed Position Annunciators, Displays, and Controls," NPX80-IC-RR790-03.

Add Redline

Do not Delete

Start

plant operation. The requirements were generated from a variety of sources. Some were based on industry requirements for future plants (e.g., supporting one person operation between hot standby and full power). Another set of requirements was generated from experience based problems, such as limiting access to the controlling workspace, and overview display visibility. A final set were related to licensing issues. This included the Regulatory Guide 1.97 criterion to integrate displays such that those used during normal operation are also used during accident mitigation. Recent NRC concerns with respect to sabotage are addressed.

These requirements have been incorporated into the Nuplex 80+ design bases and are presented in Section 18.3.2, primarily as the control room staffing and configuration design bases. Some operational requirements affecting the configurations are found in the control panel, and information presentation and control design bases. The operational requirements, along with the human factors criteria presented in the next section, were used as the basis to evaluate each candidate configuration design.

18.6.2.2 [Staffing Assumptions

The Nuplex 80+ control room is designed to provide operational flexibility to accommodate a wide range of control room staffing requirements. A target operating staff was established to allow design and validation of the advanced control complex. The staffing target is indicated below with typical NRC qualifications shown:

Number	Position Title	Qualification
1	Shift Supervisor (SS)	SRO
1	Control Room Supervisor (CRS)	SRO
3	Assistant Reactor Operators (ARO)	RO
1	Shift Technical Advisor (STA)	
2	Nuclear Equipment Operators (NEO)]	

T2+

18.6.3 WORKSPACE AND CONFIGURATION HUMAN ENGINEERING CRITERIA

The development and evaluation of control room configurations also requires a comprehensive set of human engineering criteria related to workspace design.

Workspace and configuration criteria for Nuplex 80+ are based on requirements defined in the Human Factors Engineering Standards Guidelines and Bases (HFESGB) for System 80+ (Section 18.4, Reference 6). Specific configuration criteria utilized for design of the Nuplex 80+ ACC are listed below:

09-26-1994 14:59 P.08

gap between functions and plant systems, the high level ~~CRT~~ display pages, and the critical function monitoring and success path monitoring application programs of the Data Processing System (DPS). Through these programs sufficient critical function information is provided to meet the operator's functional information needs under any plant condition. These programs also satisfy Safety Parameter Display System (SPDS) requirements as an integrated part of the information hierarchy. This is discussed further in Section 18.7.1.

The MCC is divided into two sections relating to NSSS and BOP systems. The functions of each section are assigned to control panels based on the functional task analysis and plant operations experience. Panels and panel sections are arranged at the MCC based on the frequency of their use. Functions performed most frequently are placed toward the center of the console. The MCC design is a five-panel console organized as shown on Figure 18.6.5-2. NSSS panels are provided for functions relating to the RCS (including RCPs), CVCS and plant monitoring and control. BOP panels are provided for feedwater and condensate and the turbine/generator. The panel layouts, including indication and controls for each panel, are provided in Section 18.7. Note that the IPSO display is mounted above and behind the MCC to allow its observation from throughout the controlling workspace and from the control room offices. The IPSO is not attached to nor is it part of the MCC workstation.

As previously identified, the MCC is designed for one person during normal operation. However, it will comfortably accommodate up to one operator per panel section, either during normal operation, emergency operation, or other plant conditions. The MCC is designed for either standing or seated operation. A description of the panel profile is provided in Section 18.6.5.7. A chair with rollers is provided at the MCC to accommodate one person sit-down operation. The geographic location of the MCC panels is similar to that of the Nuplex 80 reference design. This takes advantage of the extensive visibility studies performed during that design process. A reconfigurable MCC mockup was used to determine optimum viewing angles at the MCC panels.

18.6.5.2 Auxiliary Console and Safety Consoles (ACSC)

The Nuplex 80+ ACSC provides indications and controls required for operator functions that are infrequently performed. The Nuplex 80+ ACSC are two distinct functional areas for safety and auxiliary control as shown in Figure 18.6.5-1. The safety console contains controls and indications related primarily to post accident operation of the plant and vital auxiliary systems. The auxiliary console provides indication and

workspace activities and supports verbal communication with operators at the other three Nuplex 80+ consoles. The console location is also designed to limit access to the controlling workspace and provides a location for controlling workspace operations personnel to interface with other plant personnel without requiring entry into the controlling workspace.

The CRS console is designed to accommodate a maximum of two people. This provides a shift supervisor or Shift Technical Advisor (STA) a workstation in the controlling workspace simultaneously with the CRS, if desired. The CRS console meets the CRSs information needs through two DPS ~~CRTs~~ VDUs and visibility of the entire controlling workspace, including IPSO. There are no controls located at the CRS console. Communications located at this console is discussed in Section 18.6.6.

18.6.5.4 Control Room Offices

The Nuplex 80+ control room provides offices for control room personnel when they are not actively participating in operations activities in the controlling workspace. This assures that the design of control room offices is integrated with the overall control room design philosophy. Provisions of the control room offices allow flexibility for utility preferences and accommodates varying plant conditions and staffing requirements. The Nuplex 80+ ACC design features three dedicated offices for the CRS, shift supervisor and a support office that provides workstations for Assistant Reactor Operators (AROs) and Nuclear Equipment Operators (NEOs). These are depicted on Figure 18.6.5-4.

The offices have a set of common characteristics based on the operational requirements of the control room and HFE criteria. These include visibility into the controlling workspace from the SS and CRS offices to allow monitoring of the activities being performed there and to enhance verbal communication with the operating staff. The SS and CRS offices also provide adequate line of sight to the big board IPSO to facilitate maintaining an overview of the plant condition without leaving the office. This provides a fixed constant overview that will direct personnel in the offices to more detailed information on their DPS ~~CRTs~~ VDUs if necessary. The control room offices also provide easy and quick access to the controlling workspace should the operations staff require assistance. In addition to visual communication between the controlling workspace and the control room offices, direct telephone communication is also provided from the MCC and CRS console to each office. To meet information requirements, the

shift supervisor and CRS offices are each equipped with a DPS ~~CRT~~ VDU from which any DPS display page can be accessed including the IPSO. Unique features of each office will be discussed in the following sections. Note that the Technical Support Center (TSC) is shown on Figure 18.6.5-4. This also serves as a control room office during non-emergency situations to allow planning sessions and accommodate visitors without control room interference. The TSC is discussed in Section 13.3.

18.6.5.4.1 Shift Supervisor's Office

The shift supervisor's office is designed to allow him to coordinate activities throughout the plant and perform his normal administrative duties. To facilitate this, communication is provided to local control panels and the controlling workspace (both MCC and CRS console). Communication is also provided to external telephone service for use during emergency conditions. The office location outside the controlling workspace allows him to interface with plant personnel without interfering with operations activities within the controlling workspace. A DPS ~~CRT~~ VDU is available in the shift supervisor's office.

18.6.5.4.2 CRS Office

The CRS office is aligned directly with the center of the controlling workspace to maximize visibility of the controlling workspace and particularly of the MCC. This office is designed to allow the CRS to coordinate control room operations activities including testing and maintenance. Interface with plant personnel can be accomplished at his office without interfering with the controlling workspace activities. Telephone communications are provided similar to that of the shift supervisor office. A DPS ~~CRT~~ VDU is available in the CRS' office.

18.6.5.4.3 ARO/NEO Support Office

The ARO/NEO workstation is located in a control room support office located outside the controlling workspace. It accommodates multiple individuals which include AROs, NEOs and Shift Technical Advisors (STAs). During normal operation, with one man controlling the plant at the MCC, this workspace accommodates the additional operating staff. It supports performance of documentation, surveillance testing, coordination of maintenance activities and other routine tasks. During emergency operation when multiple AROs are in the controlling workspace, the ARO/NEO workstation accommodates the STA and his activities.

The ARO/NEO workstation has two DPS ~~CRTs~~ VDUs to provide plant information to the operating staff or STA. It has adequate desk space for documentation tasks or interface discussions. The ARO/NEO workspace also contains a video hardcopy unit and two printers for support of operation in the controlling workspace. The ARO/NEO support office is shown in Figure 18.6.5-4.

18.6.5.5 Control Room Furnishings

This section describes human factors considerations related to operator furnishings within the control room. The following issues are addressed: desks, chairs, procedure storage and laydown space.

The major control room furnishing features are indicated on Figure 18.6.5-5.

18.6.5.5.1 Furniture

The controlling workspace is provided with sufficient quantities of desks and chairs to support the intended operational staff. Two desks are provided as exemplified on Figure 18.6.5-5. The desks serve as workspace for operators in the controlling workspace but not actively performing monitoring or control actions at the panels. The desks' locations allow a line of sight to the entire controlling workspace. They also allow a seated position for monitoring either the AC or SC. This is particularly useful during long term operations of the ACSC, as would be expected after an accident at the SC and during heatup at the AC. The desks are designed in accordance with desk dimensions required in the HFESGB. The top surface dimensions of each desk are typically 2-1/2 ft by 4 ft. The desk height conforms to HFESGB standards.

Chairs are provided in the controlling workspace at the MCC, desks, and at the CRS console as exemplified on Figure 18.6.5-5. Each chair is designed according to the requirements of HFESGB for seated operator stations. Chairs have adjustable heights and are on wheels to facilitate seated movement, particularly at the MCC.

18.6.5.5.2 Document Lay Down Space

Adequate space for laying down procedures, manuals and other reference materials while they are in use is provided for in the Nuplex 80+ controlling workspace. This is accommodated by rolling bookcases as shown in HFESGB.

18.6.5.6.3 Controlling Workspace Access Evaluation

The Nuplex 80+ control room is designed to accomplish two key controlling workspace access functions. First the Nuplex 80+ configuration permits rapid, direct access to the controlling workspace from any of the control room offices. This is examplified on Figure 18.6.5-4. No hindrances are present to obstruct an operator's access to the controlling workspace. Secondly, the Nuplex 80+ configuration limits the access of plant personnel not directly involved with operation to the controlling workspace. This is facilitated by locations for interface at the CRS console, in the ARO/NEO office and at either the shift supervisors or CRSs office without entering the controlling workspace. The two controlling workspace entry points on either side of the CRS console serve as checkpoints to keep nonessential personnel out of the controlling workspace, particularly during emergency operations. The controlling workspace and control room offices are located within the boundary of a secure area.

18.6.5.7 [Console Profiles]

Two control panel profiles are used in the Nuplex 80+ design. [A panel profile to accommodate both seated and standing operation has been developed for the MCC and RSP. A standing panel profile has been developed for the ACSC. These profiles were based on anthropometric data including the 95th percentile male and the 5th percentile female in the United States.] The anthropometric data for these profiles is based on the Human Factors Engineering Standards, Guidelines and Bases for System 80+ and MIL-STD-1472D (Section 18.6, References 1 and 2). Figures 18.6.5-11 and 18.6.5-12 exemplify the dimensions of the Nuplex 80+ profiles. The relationship of the console profiles to the placement of indications and controls is discussed in Section 18.7.2.

T2*

09-28-1994 14:56 P.09

18.7 INFORMATION PRESENTATION AND PANEL LAYOUT EVALUATION

18.7.1 NUPLEX 80+ INFORMATION PRESENTATION

Safe, reliable and efficient power generation from Nuclear Steam Supply Systems is directly dependent upon rapid and accurate monitoring and control of both thermal and nuclear processes. Information to support operations needs to be readily available and in a format that supports the operator's information requirements.

Nuplex 80+ control room information is available in a number of different formats, which are consistent with particular operator information requirements when performing operational tasks during plant evolutions or responding to unexpected conditions. The operator can obtain plant information from a number of sources in the Nuplex 80+ control room which include:

A. A large plant overview status board known as the Integrated Process Status Overview (IPSO).

B. Alarm tiles and associated alarm message windows.

C. Discrete indicators, which provide critical function and success path performance indicators.

D. ~~CRT~~ DPS display formats containing essentially all power plant information.

E. Component and process control indicators.

The information in the Nuplex 80+ control room is presented in a structured, hierarchical format to:

A. Organize the information in a logical and coherent manner.

B. Provide an arrangement that enhances the operator access of both, overview and more detailed information.

The hierarchy of information is consistently applied throughout the control room to all control panels. This makes the method of obtaining supporting, diagnostic, or overview information consistent and thus reduces the level of effort required and the probability of human error.

At the top of the information hierarchy is the Integrated Process Status Overview (IPSO). The IPSO is a large panel centrally located display format, that presents the highest level operational concerns. The IPSO allows for a quick assessment of overall plant process performance and helps guide the operational staff to more detailed information, see Figure 18.7.1-1. IPSO also helps guide the operator to alarm tiles, discrete indicators associated with particular workstations/control panels, or the

DPS

~~CRT~~ display pages accessible at any panel. The discrete indicators and alarm tiles provide direct guidance (as described in Sections 18.7.1.2.3 and 18.7.1.2.4) to support ~~CRT~~ information and display pages. The entire Nuplex 80+ hierarchy was developed with a consistent set of design conventions which are described in the next subsection. Subsequent sections provide details on the individual hierarchy components.

DPS VDU

Nuplex 80+ discrete indicators and panel alarm tiles are driven by the Discrete Indication and Alarm System (DIAS), whose system architecture is described in Section 7.7.1.4. ~~The CRT~~ displays are driven by the Data Processing System (DPS), as described in Section 7.7.1.7. The IPSO is driven by a display processor which receives data from both, DIAS and the DPS (see Section 7.7.1.5).

The Nuplex 80+ alarms and information displays are designed to provide a reliable, unified yet diverse man-machine interface. High reliability is accomplished through use of redundancy and segmentation within the DIAS and DPS processing and data communications. Diversity allows continued plant operation with a failure in any of the information hierarchy elements. Diversity is accomplished by using both the DPS and DIAS to independently calculate and display the same validated process parameters and alarm conditions. The DPS independently checks the output of DIAS processors and indicates discrepancies. Failure of any display, processing or communication component of either system (including ~~a discrete indicator display or a CRT~~) does not prevent the operator from receiving all required information for plant operation. A suitability analysis established that the information capabilities of the display hierarchy supported actual performance of specific operator tasks, including the adequacy and appropriateness of the organization, content and access methods. The results of the suitability analysis is contained in the Nuplex 80+ Verification Analysis Report (Section 18.7, Reference 3).

ANY INDIVIDUAL VDU

VDUs

Standardized hardware is used to implement the Nuplex 80+ information presentation HSI requirements. This hardware includes switches, ~~CRTs~~, and flat panel hardware that were prototyped and evaluated for suitability. ABB/CENP's response to DSER Open Item 18.8-1 (Section 18.4, Reference 11) discusses how human engineering addresses their selection and/or design.

Nuplex 80+ uses standard HSI monitoring and control design features (i.e., DPS Display Hierarchy, DIAS Alarm Tile Display, DIAS Dedicated Parameter Display, DIAS Multiple Parameter Display, CCS Process Controller Display, and CCS Switch Configuration). These features and their major characteristics are described below.

T2*

A. STANDARD FEATURE: DPS Display Hierarchy

The DPS Display Hierarchy is a standard Human-System Interface (HSI) feature of the Nuplex 80+ Data Processing System (DPS). The major characteristics of the DPS Display Hierarchy are as follows:

1. The DPS Display Hierarchy is an integrated presentation of Nuplex 80+ process information.

2. The DPS Display Hierarchy provides access to displays incorporating system/component status, process parameters and annunciator status/acknowledgement.

3. Touch-screen VDU devices are utilized.

4. On each display page in the DPS Display Hierarchy, a spatially dedicated message area and main menu are provided.

5. The DPS Display Hierarchy permits selectable access to any of its display pages from any DPS terminal.

6. The DPS Display Hierarchy permits acknowledgment of Nuplex 80+ annunciators.

7. The DPS Display Hierarchy automatically provides specific alarm condition messages at the time of alarm acknowledgment.

8. The DPS Display Hierarchy is configured to conform to the System 80+ Human Factors Standards, Guidelines, and Bases.

9. The DPS Display Hierarchy indications are read at the panel.

10. The DPS VDU devices are located on the vertical panel sections.

11. The DPS Display Hierarchy is diverse and independent of the Discrete Indication and Alarm System (DIAS).

B. STANDARD FEATURE: DIAS Alarm Tile Display

The DIAS Alarm Tile Display is a standard Human-System Interface (HSI) feature of the Nuplex 80+ Discrete Indication and Alarm System (DIAS). The major characteristics of the DIAS Alarm Tile Displays are as follows:

1. Software-generated alarm tiles present groups of functionally-related alarm status messages.

2. Touch-screen VDU devices are utilized.

3. On each DIAS Alarm Tile Display device, the status of alarm tiles is presented on a single alarm tile display page; for each tile, an associated alarm list page is available to present the status of the individual alarm conditions.

4. Unacknowledged alarms on a single tile are acknowledged through the display as a group.

5. Alarm condition messages are automatically provided upon alarm tile acknowledgment.

6. Alarm tiles are assigned to control panels by corresponding plant systems.

7. Alarm tile display devices are located on the vertical panel sections.

8. Alarm tiles on the alarm tile display page are spatially dedicated.

9. DIAS Alarm Tile Displays are configured to conform to the System 80+ Human Factors Standards, Guidelines, and Bases.

10. Tile details are read at its panel; tile status is visible across the controlling workspace.

11. Alarm tiles are established for process parameters that provide direct indication of:

    a. Critical Safety Functions
    b. Critical Power Production Functions
    c. Success Path performance
    d. Success Path availability
    e. Damage to major equipment
    f. Personnel hazard.

12. Alarms are presented in one of four states: new, existing, cleared, reset.

13. Alarms are prioritized into three levels: Individual alarm tiles have the capability to indicate either the highest priority of new or cleared alarm (i.e., N1, N2, N3, C1, C2, C3 in that order of priority) while continuing to indicate the highest priority existing alarm.

14. An alarm tile stop flash capability is provided for use during situations of high alarm activity to focus attention on new Priority 1 alarms by temporarily stopping the flashing of all other unacknowledged alarm states.

15. A momentary tone provides an initial audible alert of the transition of one or more alarms to new or cleared states for priority 1 or 2 alarms.

16. A momentary reminder tone provides a recurring audible alert if Priority 1 or 2 alarms remain unacknowledged.

17. Alarm tones emit from the console where the alarming display is located.

C. STANDARD FEATURE: DIAS Dedicated Parameter Display

The DIAS Dedicated Parameter Display is a standard Human-System Interface (HSI) feature of the Nuplex 80+ Discrete Indication and Alarm System (DIAS). The major characteristics of the DIAS Dedicated Parameter Displays are as follows:

1. DIAS Dedicated Parameter Displays are software-generated display representations of process parameters. Each dedicated parameter display presents a single value based on redundant sensor data.

2. DIAS Dedicated Parameter Displays present validated information based on redundant sensor data. Validation failures are indicated on the displays.

3. DIAS Dedicated Parameter Displays present spatially dedicated information.

4. A DIAS Dedicated Parameter Display permits continuous display of the individual data points.

5. DIAS Dedicated Parameter Displays incorporate automatic range change features.

6. Touch-screen VDU devices are utilized.

7. DIAS Dedicated Parameter Displays are assigned to control panels by corresponding plant systems.

8. DIAS Dedicated Parameter Display devices are located on the vertical control panel sections.

9. DIAS Dedicated Parameter Displays are configured to conform to the System 80+ Human Factors Engineering Standards, Guidelines, and Bases.

10. DIAS Dedicated Parameter Display values are read from across the Main Control Console; the Display details are read at the panel.

11. DIAS Dedicated Parameter Displays are provided for the following:

    a. Critical Safety Functions
    b. Success Path performance
    c. PAMI indication
    d. Reg. Guide 1.97.

12. DIAS Dedicated Parameter Displays are diverse and independent of the DPS display system.

D. STANDARD FEATURE: DIAS Multiple Parameter Display

The DIAS Multiple Parameter Display is a standard Human-System Interface (HSI) feature of the Nuplex 80+ Discrete Indication and Alarm System (DIAS). The major characteristics of the DIAS Multiple Parameter Displays are as follows:

1. DIAS Multiple Parameter Displays are software-generated display representations of process parameters.

2. DIAS Multiple Parameter Displays present validated information based on redundant sensor data. Validation failures are indicated on the displays.

3. DIAS Multiple Parameter Displays are digital and analog representations of process parameters.

4. A DIAS Multiple Parameter Display permits selection of its individual data points for continuous display.

5. Touch-screen VDU devices are utilized.

6. Multiple parameters are assigned to control panels and combined into common DIAS Multiple Parameter Display devices based on plant systems relationships.

7. DIAS Multiple Parameter Display devices are located on the vertical control panel sections.

8. DIAS Multiple Parameter Displays are configured to conform to the System 80+ Human Factors Standards, Guidelines, and Bases.

9. DIAS Multiple Parameter Display values are read at the panel.

10. DIAS Multiple Parameter Displays are diverse and independent of the DPS display system.

E. STANDARD FEATURE: CCS Process Controller Display

The CCS Process Controller Display is a standard Human-System Interface (HSI) feature of the Nuplex 80+ Component Control Systems (CCSs). The major characteristics of the CCS Process Controller Displays are as follows:

1. CCS Process Controller Displays are software-generated representations of process control devices and their controlled variables.

2. Touch-screen VDU devices are utilized.

3. CCS Process Controller Display devices are located on the control panel benchboard sections.

4. CCS Process Controller Displays conform to the System 80+ Human Factors Standards, Guidelines, and Bases.

5. CCS Process Controller Displays are read at the panel.

6. Controls are assigned to control panels based on plant systems, and are combined into Process Controller Display devices based on shared functional relationships.

7. The CCS Process Controller display provides capability for monitoring and control of master loop and subloop controls by using static menu regions to select control functions; selected control functions are subsequently manipulated in an adjacent dynamic display region.

8. CCS Process Controller Displays permits selection of operating modes, loop control signal, and loop setpoints.

9. CCS Process Controller is a man-machine interface device only. All control loop electronics are located outside the main control room.

F. STANDARD FEATURE: CCS Switch Configuration

The CCS Switch Configurations are a standard Human-System Interface (HSI) feature of the Nuplex 80+ Component Control Systems (CCSs). The major characteristics of the CCS Switch Configurations are as follows:

1. CCS Switch Configurations utilize physical pushbuttons with backlit legend status indicators.

2. CCS Switch Configurations permit on-line replacement and bumpless transfer.

3. CCS Switch Configurations are assigned to control panels based on plant systems, and combined into multiple component units based on functional relationships.

4. CCS Switch Configuration devices are located on the control panel benchboard sections.

5. CCS Switch Configurations conform to the Human Factors Engineering Standards, Guidelines, & Bases for System 80+.

6. CCS Switch Configuration details are read at the panel.

Sections 18.7.1.1 through 18.7.1.8 provide a more detailed description of these features and their associated characteristics.

18.7.1.1 Information Presentation Conventions

Acceptable information system design utilizes consistent conventions for presenting information on all information presentation features. To accomplish this in Nuplex 80+, conventions for information display and access were developed prior to initiation of design activities. Standardization was applied to conventions, representational features, coding information size and organization, labeling, alarms and information access. These display conventions are discussed in the following subsection. A significant part of the Nuplex 80+ information hierarchy is based on presenting information on ~~CRTs~~ DPS VDU or discrete indicating displays. A comprehensive set of criteria was established to assure consistency during creation of these displays. These criteria are an extension of the overall display conventions and are presented in Section 18.7.1.1.2.

18.7.1.1.1 Representational Features

The following representation features have been established for use in all Nuplex 80+ information presentation techniques.

A. Process Symbols

VDUs

Process symbols help organize information and simplify search tasks. Process symbols are used, when appropriate, on component control switches, IPSO, ~~CRTs~~, process controllers, and control panels. A standard symbol library was developed prior to the design effort for use on all information features. A symbology study was performed using time-response tests to help determine the most appropriate symbols for the library.

B. Process Representations VDUs

Process representations are used, when appropriate on the control panels, IPSO and ~~CRTs~~. Process mimic formats use standard information placement for similar processes, and equipment. Research was performed to develop conventions matching human population stereotypes. For example, fluid system piping representations are standardized top to bottom and left to right. Incoming and outgoing flow path connections are placed at the periphery, and crossovers are prohibited. Related information is grouped by task analysis specifications for comparison, sequence of use, function, and frequency. Process representations/layout are based on the operator's process visualization to maximize the efficiency of his data gathering tasks. In determining an operator's visualization of a system, consideration is given to diagrams used with learning materials and plant design documentation associated with system descriptions, as well as actual physical interpretation.

C. Graphic Layout/Information Coding

Graphic information is presented on display page formats to aid in rapid operator comprehension of processes. Graphic information includes the use of bar graphs, flow charts, trends, and other plots, (e.g., temperature vs. pressure).

1. Bar Graphs

DPS VDUs

Bar Graphs are primarily used to represent flows, pressures and levels. Bar graphs are used on ~~CRTs~~, and discrete indicators for applications such as general monitoring where a specific value is not needed or for convenient data comparison (e.g., two flowrates can be easily compared using two adjacent bar graphs). Bar graphs are also helpful for comparison of numeric quantities.

2. Flowcharts

Flowcharts are used when they aid in the operator's process visualization. Flowcharts may be helpful for understanding control system processes such as the Turbine Control System. Operators learning materials for process control systems are frequently in a flow-chart format, and thus a similar format on a display page will be easy to comprehend.

D. Trends and Graphs

Trends are used on display page formats when functional task analysis indicates that the operator should be informed about parameter changes over time. Additionally, the operator will be able to establish trends of any data base points which reside in the DPS data base.

Scale labels will be divisible by 1, 2, 5, or 10. Tick mark between scale labels are also divisible by 1, 2, 5, or 10. Trended information is typically presented on display pages with a scale of 30 minutes, however the operator shall be able to adjust the scale to suit his needs. Logarithmic axes are established using multiples of 10.

18.7.1.1.2 Coding Techniques and Display Conventions

Color is used to provide clear, salient presentation of important display features. Consistent application of discriminable colors supports visual search, orientation, alerting, and comparison. Color is always applied as a redundant coding technique, to ensure reliable presentation of important information. As appropriate in the context of specific hardware, the color hues below apply to all control panel and instrument features:

A. Red

Component On/Activated, Valves Open.

B. Green

Component Off/Inactive, Valves Closed.

C. Blue

Component Control "select" type control functions, e.g., auto, permissives.

D. Yellow

Alarm Activated Status.

E. Cyan

Label Units and alarm setpoint values for dynamic process parameter on ~~CRTs~~ DPS VDUs.

F. White

Dynamic process parameter values on ~~CRTs~~ VDUs, message area messages, dynamic bar graph and trend information. System's response to operator touch on ~~CRTs~~, e.g., highlighting menu selection until appropriate system response occurs.

G. Orange

An alerting hue for non-ordinary, non-alarm information such as existing operator aids and manual control status. VDUs

H. Purple

Labels for discrete indicators containing Reg. Guide 1.97 Category 1 and 2 and Type A, B, and C parameters on discrete indicators or ~~CRT~~ DPS VDU pages.

Nuplex 80+ Hue Convention Representation Characteristics:

A. Black

Background hue for labels.

B. Grey

Static text, component labels, dividing lines, menu options, piping, inoperable and non-instrumented valves, graph axis and grids, and other applications not covered by other coding conventions.

C. Tan

Control panel surfaces.

D. Light Brown

Control panel demarcations.

The acceptability of the number of hues and intensities used on displays is provided in the following Section 18.4 References (3,6). DPS VDUs

Final validation of the sum of the various HSI features (including the number of hues and different intensities of colors used for ~~CRTs~~) afforded by both the main control room and the remote shutdown area will confirm that the operating ensemble supports the successful accomplishment of the operator's functional role and specific tasks under dynamic, real-time conditions. The criteria to evaluate human performance for the usefulness of the ensemble are provided as part of the HFE V&V plan.

Shape coding/conventions, or attribute coding/conventions, is used in the information system as a primary means to the operator in identifying problems, equipment component status, component type, direction of process data, alarm priorities and operator aids, and target selection items.

D. Minus Symbol - value low "below control band"

E. Dot - value normal

To identify if data is static or dynamic the following color intensity codes are used:

A. Pure white - Dynamic Data

B. Grey - Static Information

Although Nuplex 80+ uses many techniques, the operators can effectively utilize them under conditions in which their unambiguous discrimination is required. The following is a discussion of how operations personnel effectively utilize these codes under various plant conditions.

Alarm and information processing by operators is context dependent. The context specific use (e.g., reading data, processing alarms, determining equipment status, etc.) of the Nuplex 80+ codes reduces the number of codes that require discrimination in a given situation (e.g., normal operation, post trip, etc.) to a manageable set. The Nuplex 80+ alarm and information codes are provided in Table 18.7.1-1 (Nuplex 80+ Coding Matrix). The operator is not required to process the 15 shape, 8 hue, 5 color intensity, 2 flash rate, and 2 switch position codes simultaneously. For example, if an alarm occurs, the Nuplex 80+ information system performs the following: 1) alerts operator by an audible tone, 2) directs his or her search by flashing high intensity yellow tiles on functionally organized alarm tiles or ~~CRT~~ menu selections on ~~CRT~~ pages, 3) directs his or her attention with context specific messages and directory information on the ~~CRT~~, and 4) confirms a cleared alarm by an audible tone and slow flash in low intensity yellow. When in the alarm context, the operator is processing alarm code information, not equipment status, data or other miscellaneous codes. Therefore, only the codes associated with alarms are applicable. Other examples of context dependent use of codes are: 1) the 5 direction shapes are used only to show trend parameter information, the 2 switch position codes are uniquely used to show equipment or position status on only process controllers and switches, and 3) the equipment/component status codes are used only with the equipment/component navigation aids on the ~~CRTs~~ and process controllers.

DPS VDU

DPS VDU

DPS VDUs

Many equipment status, data, and miscellaneous codes are aids to the operator, adding beneficial redundancy to already unambiguous displays rather than adding an additional information processing

burden. In addition, the Emergency ~~Procedure~~ OPERATIONS Guidelines are written to simplify operator actions to tasks that require discrimination of only the most important information (e.g., on/off codes, dynamic data codes) and not require the operator to process alarms, or perform detailed diagnostic activities to which many of the codes are applicable.

HFE has verified the adequacy of the present codes through suitability analysis. Validation of the collective application of the codes will be performed later in the design process to confirm that the operator can acceptably use the coding scheme as part of the HSI. Additional, empirical data showing that operators can effectively utilize the properties and parameters encoded, all colors, and the shape/symbol codes under normal, abnormal, and emergency operations and under all modes of plant operation is not required.

The complete Nuplex 80+ Coding Matrix and notes correlating them to HSI devices is presented in Table 18.7.1-1.

18.7.1.1.3 Labeling, Text, and Data

Labels include panel titles, display page titles, function identifiers, equipment identifiers, process identifiers, and parameter identifiers. The following conventions apply to all labels, text, and data in the Nuplex 80+ design.

A. Label Size

Labeling sizes are standard for similar label types (e.g., Control Panel, Group, Subgroup, ~~CRT~~ VDU page titles, Component Identifiers). Labeling size is based on viewing distances in supporting of information gathering tasks. Labels also help establish a hierarchy for information provided on the control panels and ~~CRT~~ VDU displays. The labeling hierarchy used in the Nuplex 80+ design is specified in Section 18.7.2.3.3.

B. Label Placement

Labels of similar types are placed in consistent locations with respect to panels, demarcations, mimic diagram representations, and component controls.

C. Abbreviations

A standard set of abbreviations has been established for use on all control panel and display pages.

D. Units

A standard set of units has been established for application to all data.

18.7.1.1.4 Alarm Philosophy

Alarm information is integrated into the Nuplex 80+ design. Early in the design process an informal scoping analysis was completed to demonstrate the effectiveness of the alarm methodology in reducing alarms. Final validation of the sum of the various HSI features (including the quantity of alarms and displays) afforded by both the main control room and the remote shutdown area will confirm that the operating ensemble supports the successful accomplishment of the operator's functional role under dynamic, real-time conditions. The criteria to evaluate human performance for the usefulness of the alarms and displays are provided as part of the HFE verification and validation plan. Alarm information is presented on IPSO, ~~CRT's~~ DPS VDUs, and alarm tiles.

Nuplex 80+ alarms warn the control room operator of abnormal conditions that require his or her attention because they require significant operator action to maintain safe and reliable plant operation.

Nuplex 80+ alarms are categorized as follows:

critical safety function violations
critical power production function violations
major damage to equipment
success path availability violations
success path performance violations
personnel hazards.

The categories determine alarm display locations. Nuplex 80+ alarms are assigned priorities based on the number of sequential warnings related to the "Significant Operator Action" condition.

Alarms are prioritized to help operators order their responses to abnormal conditions. The priorities are:

A. Priority 1

The last warning (and, in some cases the only warning) prior to reaching a "Significant Operator Action" condition.

B. Priority 2

Next to last warning prior to reaching a "Significant Operator Action" condition.

C. Priority 3

Any number of warnings prior to the next to last warning before reaching a "Significant Operator Action" condition. In some cases where no significant operator action condition can result, it is the only warning.

In addition to alarms, an information notification category "Operator Aids" has been established for information that may be helpful for operations but is not representative of deviations from normal conditions. Conditions classified as "Operator Aids" include; channel bypass conditions, approach to interlocks, and equipment status change permissives. Note that "Operator Aids" for the Nuplex 80+ control complex are not interchangeable with the term "Job Aids".

The alarm priorities and "Operator Aid" are coded uniquely to allow the operator to quickly distinguish between alarm conditions. Section 18.7.1.5 provides a detailed description of alarm presentation methodology and operator interaction with alarm information. Table 18.7.1-1 provides the complete Nuplex 80+ coding matrix, including alarms and operator aids.

18.7.1.1.5 Information Access

DPS

To perform operations and respond to abnormal conditions the operator needs to easily access information such as data presented on discrete indicators, ~~CRT~~ process mimic representations and information listings. Tasks that are performed frequently or need to be quickly accomplished require minimal operator actions to access supporting information. The primary method of information access in Nuplex 80+ is through touch sensitive targets. This makes use of the operators natural tendency to point to desired information. The following features that enhance information access are a part of the Nuplex 80+ designs.

A. Alarm Tiles

The primary method by which alarms are acknowledged is by touching a flashing alarm tile. Touching the tile acknowledges the alarm which results in an alarm message being displayed with related targets. Touching an alarm tile that is either in alarm or not in alarm accesses option(s) on the ~~CRT's~~ menu (the ~~CRT~~ on the same panel as the tile) to provide direct access to display pages associated with the alarm tile's descriptions.

DPS SCREEN VDU

B. Display Pages

Touch targets are used to access supportive or diagnostic information associated with a display page's process. Section 18.7.1.3.4 describes display/page information access in detail.

Subsequent sections of Section 18.7.1 provide more details on information access mechanisms within the specific components of the Nuplex 80+ design.

18.7.1.1.6 Data Content/Display Density Guidelines

The Nuplex 80+ information system makes extensive use of ~~CRT~~ VDU and other computer based information presentation devices (e.g., DIAS). This facilitated the need to establish guidelines to provide uncluttered, well organized and easily interpretable displays. The following indicate the major data content and display density guidelines that were followed.

Only data associated with a display process or helpful for the understanding of that process is included. Data to be displayed is selected based on the output of the functional task analysis plant experience, federally mandated requirements and system engineering requirements.

When the operator scans the display for specific information, all other information on the screen is considered background clutter. There is a limit beyond which additional information loading on the screen dramatically decreases the ability of the operator to efficiently obtain the information he needs. Experience has shown and HFE criteria indicate that the display loading (the percentage of potentially active screen area) should not exceed 25 percent. The inactive area constitutes "white space" that is essential for clarity in any display. The amount of potentially active data on a display does not exceed 50 percent of the total screen area, not including demarcation lines. However, organizing related data into many screens requires extensive screen switching, and should be avoided.

18.7.1.1.7 Size Criteria for Labels and Information

Operator data collection for both monitoring and control requires that some data be readable from a distance, and other data be readable while at a given panel. The following sections provide information size criteria for information in the control room. The sizes of characters meet the guidelines of the HFESGB (Reference 2). Apparent character height at expected reading distances subtends at least 12 minutes of arc.

A. Data To Be Viewed From the Shift Supervisors Office

The Integrated Process Status Overview (IPSO) information is provided with a letter height sufficient to allow readability of information from the shift supervisor's office (i.e 40 feet), in accordance with the HFESG. IPSO information provides the highest level information to the operating staff and therefore needs to be visible from any controlling workspace panel, as well as the shift supervisor's office.

B. Data To Be Viewed Within the Controlling Workspace

The control panel identifying labels have a letter height sufficient to allow the operator to determine what panel information is associated with from any location in the controlling workspace. For example, if the operator observes a flashing indication on a panel, the operator will know with which panel the information should be associated. This allows the operator to obtain the exact information associated with the indication by accessing the data on the ~~CRT~~ DPS at his present location. This may be particularly useful as an aid to alarm response.

C. Data To Be Viewed Across the MCC

Since a design bases of the MCC is to allow one person to conduct normal operations at the MCC, certain data on the MCC is readable while the operator is at any other MCC panel. This data includes:

1. Group/Subgroup Labels

   These labels allow the operator to distinguish in which group/subgroup information is changing. If the operator observes an indication such as a valve repositioning (shown by both red/green status lights illuminated) the operator will be able to distinguish in which group/subgroup the valve is located.

2. Alarm Group Labels

   These labels allow the operator to distinguish what group or system is in alarm. For example, the RCS panel has alarm groups for RCPs, seal/bleed, and RCS.

3. Dedicated Parameter Discrete Indicator Labels (e.g. Pzr Pressure)

These labels allow the operator to identify what information is displayed on the associated discrete indicator.

The data that falls into the above categories (1, 2, and 3) on the MCC is of the same size on the ACSC panels to assure useability of information throughout the control room. Additionally, this ACSC information allows an operator to monitor the information associated with an ACSC panel section while seated at a desk in front of the AC or SC, see Figure 18.6.5-4.

D. Data To Be Viewed From an Adjacent Panel

The ~~CRT~~ DPS VDU associated with an adjacent panel may be used by the operator to support monitoring activities associated with his present tasks. For example, the operator may desire a trends format or overview information on the adjacent ~~CRT~~ VDU to aid him in monitoring tasks associated with a process or detailed page on the panel that he is using.

E. Data To Be viewed at a Panel

While performing monitoring and control activities at a panel, the operator observes some information while seated or standing in front of the panel, while other information is only used when performing an action or accessing a display format. Thus, this type of size criteria is divided into two categories as follows:

1. Information Gathering Tasks

The operator needs to view the following information related to the workstation process while in front of the panel:

a. Panel Mimic Diagram Labels (e.g. identification of bypass, recirculation paths).

b. Alarm Tile Descriptors.

c. Existence of alarms on IPSO and location with respect to a system or plant process.

d. Alarm group labels and divisions on panels.

e. Priority coding on alarm tiles.

f. Spatial dedication of alarm tiles on panels.

g. Existence and priority of alarm within first level display page categories provided on ~~CRT~~ DPS display page menu options.

This information is sized to be readable by 95th percentile males and 5th percentile females from both standing and seated positions at the MCC or only standing positions at the ACSC.

2. Information to Support Control Actions and Information

This information is used by the operator when performing an action i.e., touching either a control feature or information access feature. To support these tasks the information is sized to allow readability while performing the specific action.

18.7.1.1.8 Information Input

The capability is provided to manually input to the Nuplex 80+ I&C systems component or parameter information unavailable from automated data acquisition means. This will include information such as Bypassed or Inoperable Status manual input and input related to tagged out components. This capability will be provided by DPS controlled access keyboards located outside the controlling workspace (e.g., CRS console, MCR offices) or other system operator interface devices (e.g., Operators Modules).

18.7.1.2 Integrated Process Status Overview (IPSO)

The presentation of plant processes on display page formats has led to a generally expressed concern that the presentation of information on separate, relatively small formats which must be viewed independently might prevent the operator from gaining an overall "feel" for plant status. In a typical nuclear power plant the understanding of the whole plant process performance is gained by parallel processing of an array of conventional instrumentation, i.e., by means of a sweeping glance around the control room.

In the Nuplex 80+ control room a large panel overview display provides the information that the operator requires for quickly assessing overall plant status. This panel, known as the Integrated Process Status Overview (IPSO), see Figure 18.7.1-2, is a continuous display visible from any panel in the controlling workspace, control room offices, and the Technical Support Center. The IPSO is centrally located relative to the MCC. The IPSO also exists as a DPS display page that is available on any control room ~~CRT~~. It is also available at remote facilities such as the Technical Support Center and Emergency Operations Facility. As a plant overview/top level display page, IPSO allows the operator or other plant personnel to interrogate the

DPS VDU

D. Critical Function Parameters (e.g., RCS Temperature, Pressurizer Pressure and Level, Reactor Power, Plant Power Output) to improve the operator's and supervisor's awareness of plant conditions.

DPS

The IPSO uses the same HF criteria for display design that are used on the ~~CRT~~ process display pages. IPSO uses the dynamic symbols, color code, highlighting, blinking, graphic layout and information coding features described in Section 18.7.1.1. DSER Open Item 18.8.2 2 a. (Section 18.4, Reference 11) provides additional information on the usefulness of a large overview display (IPSO).

18.7.1.2.2 Plant Functional Information on IPSO

A primary operational benefit of IPSO is the use of IPSO information to support operator response to plant disturbances, particularly when a disturbance effects a number of plant functions. IPSO information supports both the operator's ability to respond to challenges in plant power production and plant safety.

To that end, IPSO allows the operator to assess the overall plant's process performance by providing information to allow a quick assessment of the plant's critical safety or power production functions. The concept of monitoring plant power and safety functions requires a categorization of the power and safety-related plant processes into a manageable set of information that is representative of the various plant processes.

The critical functions pertaining to the System 80+ plant are:

	Function	Critical To: Power	Safety
1.	Reactivity Control	X	X
2.	Core Heat Removal	X	X
3.	RCS Heat Removal	X	X
4.	RCS Inventory Control	X	X
5.	RCS Pressure Control	X	X
6.	Steam/Feed Conversion	X	
7.	Electric Generation	X	
8.	Heat Rejection	X	
9.	Containment Environment Control		X
10.	Containment Isolation		X
11.	Radiological Emissions Control	X	X
12.	Vital Auxiliaries	X	X

A 3x4 alarm matrix block containing a box for each critical function exists in the upper right hand corner of IPSO. The matrix provides a single location for the continuous display of the presence of alarms that jeopardize the specific critical function. Above the box is the identification of the emergency procedure currently selected by the operator.

The 3x4 matrix representation is an overview summary of the 1st level critical function display page information. The operator obtains the details associated with Critical Function in the Critical Function section of the display page hierarchy (see Section 18.7.1.3).

18.7.1.2.3 Systems Represented on IPSO

The systems represented on IPSO are the major heat transport path systems and systems that are required to support the major heat transport process. These systems include those that require availability monitoring per Regulatory Guide 1.47, and all major success paths that support the Plant Critical Functions.

The following systems have dynamic operating status representations on IPSO. The identifiers for the systems used on IPSO in Figure 18.7.1-2 are provided below.

CC	-	Component Cooling Water
CD	-	Condensate
CI	-	Containment Isolation
CS	-	Containment Spray
CW	-	Circulating Water
EF	-	Emergency Feedwater
FW	-	Feedwater
IA	-	Instrument Air
SC	-	Shutdown Cooling
RC	-	Reactor Coolant
SI	-	Safety Injection
SW	-	Service Water
TB	-	Turbine Bypass
CH	-	Charging
LD	-	Letdown
DG	-	Diesel Generator
SD	-	Safety Depressurization

System information presented on IPSO includes system operational status, change in operational status (i.e. active to inactive, or inactive to active) and the existence of alarms associated with the system. Alarm information on systems also helps inform an operator about success path related Critical Function alarms.

18.7.1.2.4 Alarms Presented on IPSO

IPSO displays the following types of alarms:

A. The presence of alarms that jeopardize critical functions are displayed in the IPSO alarm matrix boxes. Each box identifies the presence of alarms that jeopardize the specific critical function. The display format for the box indicates the highest priority of all related alarm conditions;

B. Success path availability alarms using system symbols and descriptors;

C. Success path performance alarms using system symbols and descriptors;

D. Key critical function process parameter alarms using IPSO process representations.

18.7.1.3 ~~CRT~~ DPS Display Pages

The Nuplex 80+ ~~CRT~~ display pages contain all the System 80+ plant information that is available to the operator, in a structured hierarchy. The ~~CRT~~ pages are useful for information presentation because they allow graphical layouts of the plant and processes in formats that are consistent with the operator's visualization of the plant. In addition, ~~CRT~~ formats are designed to aid operational activities of the plant by providing trends, categorized listings, messages, operational prompts, as well as alert the operator to abnormal processes.

The primary method that the operator navigates on the Nuplex 80+ ~~CRTs~~ is through touch screen interface. Keyboards are not used for information access on the MCC, AC, or SC panels. Manual entry of information into the DPS is provided via controlled access keyboards outside the controlling workspace (e.g. CRS Console, MCR offices). Messages and supporting display page option touch targets can be accessed on ~~CRTs~~ by touching other control panel features, (see Section 18.7.1 4 and 18.7.1.5).

The Nuplex 80+ ~~CRTs are driven by the~~ Data Processing System (DPS). ~~This system~~ is described in Section 7.7.1.7. The IPSO display page forms the apex of the Nuplex 80+ ~~CRT~~ display page hierarchy. Three levels exist below IPSO, where each level of the hierarchy provides an information content designed to satisfy particular operational needs (see Figure 18.7.1-3). The structure of the hierarchy is based on supporting the operator in the performance of his tasks as well as providing quick and easy access to all information displayed via the ~~CRTs~~. The display formats on the top level provide information for general monitoring activities, while the lowest level displays contain information that is most useful for supporting diagnostic

performance changes, degradation or improvement. An example of a level 3 display page is provided by Figure 18.7.3-3.

18.7.1.3.4 Display Page/Information Access

VDU-B&W50

The operator's ability to acceptably access information and diagnose operational concerns with a ~~CRT based~~ information system is dependent on his ability to access the appropriate display pages. Display page access in Nuplex 80+ is fast, simple, consistent among the various display stations, and easy to use.

Nuplex 80+ display page access is accomplished primarily through the use of menus located at the bottom of the display pages. A Nuplex 80+ ~~CRT~~ DISPLAY PAGE menu is shown on Figure 18.7.1-4. Each display page in the Nuplex 80+ design contains a standard menu format that provides: direct (i.e., single touch) access to the last page viewed and the display page directories (Critical Functions, Primary, Secondary, Power Conversion, Electrical Systems, Auxiliary Systems, and Other Systems/Features for all display pages (see Figure 18.7.1-4).

A. Display Page Access Using the Display Page Directory

There is one display directory for each hierarchy under a 1st level display page (i.e. Critical Functions, Primary, Secondary, Power Conversion, Electrical, and Auxiliary Monitoring). Additionally there is a directory labeled "Other" which contains display pages or information that does not fall into the categories of the previously mentioned directories. The Other category includes the following types of display pages; Radiation Monitoring/ Control, Data Base Information, Maintenance Information, and Historical Data Retrieval Information. Additionally each directory provides access to the Prioritized Alarm List, and Time Sequential Alarm List; see Section 18.7.1.5.3.

Directory Format

There are a total of seven (7) directories which exist: Critical Functions Monitoring, Primary, Secondary, Power Conversion, Electrical, Auxiliary, and "Other".

The Primary, Secondary, Power Conversion, Electrical and Auxiliary Directories are laid out in a format where the display page options are grouped with the control panel they are associated with. For example on Figure 18.7.1.-5 there are four groupings of display pages for pages associated with the following four control panels; Engineered Safety Features (ESF), Reactor Coolant System, CVCS, and Plant Monitoring & Control. The first row of page options for a panel grouping provide access to 2nd level pages, where the page options below these provide access to 3rd level pages.

The "Critical Function Monitoring Directory" and "Other Directory" are presented using a different directory format. The directory formats are different because these directories are not structured based on plant system, thereby not relating to panel groups. The Critical Function Directory is described in Section 18.7.1.8.2. The "Other Directory" pages are grouped by the display page categories described earlier.

B. Accessing Information Using Point Poke

Process parameter labels (alpha-numeric designators) and labels for component symbols of a mimic diagram provide, upon request, access to more detailed information. To obtain more information about a process parameter or component, the operator touches the associated descriptor. Upon touching the descriptor it is highlighted in white to confirm the operator's selection. When the operator lifts his finger from the screen, operational information associated with that parameter is placed on the message line and the menu as follows:

1. Message Area

   The message area contains the parameter's descriptor, data base point I.D., and current value.

2. Dynamic Display Page Options

   Display-page options, that contain the most likely options to provide more information about the parameter such as process control and diagnostic display pages, appear as shown in Figure 18.7.1-6. A maximum of three display pages will be provided.

   Descriptors are also used for alarm acknowledgement on the ~~CRTs.~~ DPS VDUs

   Many display page symbols on IPSO provide a representation of system status. Touching the symbol's descriptor, on the ~~CRT~~ version of IPSO, provides menu options that allow access to display pages associated with the system and an appropriate message in the message area. VDU

18.7.1.3.5 Historical Data Storage and Retrieval (HDSR)

All alarm information will be collected and stored by this system. Alarm activity i.e. time in, priority, time acknowledged, time cleared and time reset, will be stored along with the description of the alarm and any pertinent information that may be required by the operator or the technical support center. It will also store a record of trends for particular data points within the plant.

selection, the field with "fault sel" and tag number reads "op sel" and tag number in reverse image with no flash. When the validation algorithm can validate the data, "op sel" is automatically replaced with the validated information. An example of a typical discrete indicator for process representation parameters is provided in Figure 18.7.1-7.

DPS

~~CRT~~ DISPLAYS:

On any display page that displays a validated parameter on the ~~CRT~~, a fault selected value is indicated by an asterisk placed before the value, e.g.,

DPS VDU

* 2250 psia

VDU

The asterisk remains on the ~~CRT~~ after the operator reviews available sensors and makes a selection on the discrete indicator. This informs the operator that this parameter value is not validated.

VDU

Similarly if a parameter displayed on the ~~CRT~~ is not PAMI validated, it is preceded by an asterisk. The asterisk again indicates to the operator that something is questionable about the particular value. This prompts him to review the value on the level 3 ~~CRT~~ pages or on a discrete indicator before he uses it in calculations or diagnosis.

B. Trends

Trends are particularly useful for observing deviations in processes and the diagnosis of those problems. Discrete indicators have a trend format in addition to the digital and analog values when task analysis indicates that trend information is required for:

1. Routine monitoring or control, or

2. Abnormal event diagnosis.

Figure 18.7.1-7 shows a typical trend format on a discrete indicator.

C. Groups of System/Process Related Parameters - Parameters that allow continued operation without the DPS available include information to monitor Technical Specifications, information required to assess major equipment damage or personnel hazard alarms, and information to monitor Reg.

Guide 1.97 Category 1 and 2 parameters (Types A-C) (not already on single parameter displays). An example of a typical discrete indicator for a process multi-parameter display is provided in Figure 18.7.1-21.

INFORMATION ACCESS

Each discrete indicator contains a menu(s) option that, when requested, replaces the normally displayed digital value and analog bar graph with a menu of parameters that can be monitored on the discrete indicator. The menu is activated by touch.

18.7.1.5 Alarm Characteristics

The Nuplex 80+ annunciator system incorporates the following features:

A. Alarms are presented on grouped alarm tiles or ~~CRT~~ DPS VDU representations with dynamic messages used to inform operators of specific conditions in alarm.

B. Alarms are based on applicability for plant operating mode. Alarm logic and setpoints are specific for each of the following alarm modes:

1. Normal operation.

2. Heatup/cooldown.

3. Cold shutdown/refueling.

4. Post-trip.

Mode change is automatic with respect to the DPS. When the DPS detects that a mode change is appropriate, the system will initiate the change and prompt the operator to do the same to DIAS which is manually changed. The change to post-trip mode is automatic for both systems. Mode dependent alarms significantly reduce nuisance alarm generation.

C. Alarms are acknowledged either individually or within small groups that can be viewed by the operator; global acknowledgement is not used since this tends to mask important alarms. The Nuplex 80+ alarm system aims at trying to make the operator aware of all conditions that are unacknowledged. The alarm system has provisions such as momentary audible tones, reminder tones and flash suppression that make unacknowledged alarms less distracting. Acknowledgement of alarms is done using:

1. Individual annunciator tiles.
2. ~~CRT~~ DPS VDU interface features.

D. Alarm logic and setpoints are based on equipment status; e.g., low discharge pressure is only applicable when a pump is supposed to be running. This approach helps to significantly reduce the number of nuisance alarms.

E. Alarms are partitioned by location with respect to control room panels and operator functions to help provide the operator with discrimination among systems containing process deviations.

To adequately respond to an alarm condition(s) there needs to be an efficient means of identifying the exact nature of the alarm and accessing the most useful information for diagnosing the alarm condition. Alarm information in Nuplex 80+ is presented through the use of the IPSO, discrete annunciators, alarm information display pages, and alarm information on process display pages. Each of these sources of alarm information provides an important role in responding to and diagnosing unanticipated conditions. In the Nuplex 80+ design, alarms are grouped into three priorities, so the operator can determine what the relative importance of each alarm is, as follows:

Priority 1
Priority 2
Priority 3

Section 18.7.1.1.4 describes the alarm conditions within each of these priorities.

In addition to these alarm priorities, there exists a separate category called "Operator Aids". Operator aids provide operational guidance information that is not representative of an undesirable process or component condition. These are discussed further in Section 18.7.1.5.6.

Priority 1, 2, and 3 alarms are processed and displayed independently through both the Discrete Indication and Alarm System (DIAS) and the Data Processing System (DPS). Priority 3 alarms that do not degrade to priority 2 and 1 conditions, and operator aids are processed and displayed only by the DPS. The IPSO panel described in Section 18.7.1.2 is driven by the DIAS and DPS and only provides indication of critical function and success path related alarms. Critical function alarms are displayed on IPSO critical function parameter descriptors and the IPSO critical function alarm matrix. System alarms related to success path availability and performance are displayed on IPSO system descriptors.

DIAS annunciator tiles in the Nuplex 80+ design may be driven by a number of individual alarm conditions. For example: a tile descriptor stating RCP1A pump/motor trouble provides for 11 different RCP1A alarm conditions. In general alarm groupings within an alarm tile are based on alarm response strategies to support operational understanding of what components and systems are affected by disturbances. Message windows and ~~CRTs~~ provide access to the specific alarm conditions. Reducing the number of annunciator tiles helps reduce the amount of data displayed to the operator, and thus the size of control panels. This permits the operator to monitor and control a given amount of equipment with less movement between locations. Fewer annunciator tiles allow the operator to distinguish important alarms during transients.

The operator's ability to control plant processes is dependent upon notification of process performance changes and his ability to efficiently access supporting information for decision making. In the Nuplex 80+ control room much of the plant process information is contained on ~~CRT~~ pages. Emphasis has been placed on the operator's ability to locate the ~~CRT~~ page(s) that most effectively support his alarm handling needs. The Nuplex 80+ design accomplishes this by:

A. Minimization of operator/~~CRT~~ interactions required to access a display page(s) by providing direct access to supporting information via touch targets.

B. Minimization of memory requirements on the operator by providing alarm priority coding on menu sectors in alarm, alarm priority coding on display page directory selections in new and cleared unacknowledged alarm states, supporting diagnostic information related to the condition in alarm via the alarm message (e.g. present process value, setpoint, etc.), and identifying ~~CRT~~ pages containing information related to the alarm condition. These features direct the operators attention to ~~CRT~~ pages containing supporting information related to unacknowledged alarms.

C. Flexibility to provide different information to support different needs and different user preferences via presentation of alarms in many formats including the following: 1) on associated ~~CRT~~ page descriptions of process parameters or components, 2) on ~~CRT~~ alarm lists including prioritized, hierarchical, and time sequential lists, 3) on annunciator tile representation for single unacknowledged alarms, and 4) on the ~~CRT~~ unacknowledged alarm list.

18.7.1.5.1 Alarm Status and Representation

A. Alarm status in the Nuplex 80+ alarm system is provided by DIAS and ~~CRT~~ alarm indications using the following four states which are grouped into UNACKNOWLEDGED and ACKNOWLEDGED alarms: DPS

Unacknowledged Alarms

1. New Alarm (alarm setpoint exceeded, condition not acknowledged)

   If there is a new alarm associated with an alarm tile, the DIAS alarm tile and/or ~~CRT~~ display representation will flash at a fast rate (using a 50/50 duty cycle) with an accompanying audible tone. This condition takes precedence over all other alarm tile states for group alarm displays. This condition requires acknowledgement by the operator. DPS

2. Cleared Alarm (process value returned to within alarm setpoint, condition not acknowledged)

   When an alarm condition clears, the corresponding alarm tile and/or ~~CRT~~ display representation flashes at a slow rate (using an uneven 25/75 duty cycle), again accompanied by an audible tone, until this condition has been acknowledged. This condition takes precedence over the remaining two states for grouped alarms. DPS

Acknowledged Alarms

3. Existing Alarm (alarm setpoint exceeded, condition is acknowledged)

   If an alarm condition exists and alarm states 1 and 2 above do not exist, then the alarm tile or ~~CRT~~ display representation is lit. DPS

4. No Alarm/Reset (alarm setpoint not exceeded/value returns to within alarm setpoint condition acknowledged)

   If state 2 is acknowledged or if there is no alarm condition associated with an annunciator tile, then the alarm tile or ~~CRT~~ display representation is not lit. DPS

alarm hue coding. On the ~~CRT~~ the descriptor is presented grey for static data and in blue for dynamic data to provide good contrast for readability. In addition, the alarm tile and alarm list status fields on the ~~CRT~~ use the same representation.

2. Priority 2 alarms

   Alarm tiles, mimic diagram parameter descriptors, component descriptors, and menu/display page options have a thin box using the alarm hue code around their descriptor.

3. Priority 3 alarms

   Alarm tiles, mimic diagram parameter descriptors, component descriptors, and menu/display page options have brackets around their descriptors.

18.7.1.5.2 Accessing/Acknowledging Alarm Information Using the Alarm Tiles

Alarm tiles for each panel are implemented on a flat panel video display unit. Each alarm tile representation can present either priority 1, 2, or 3 conditions. Each tile can notify the operator of one or more possible alarm conditions relating to a system, component, or major process problem. To quickly determine the actual alarm condition, a message area is provided at the bottom of each alarm display device. By touching an unacknowledged alarming annunciator tile the tile is acknowledged while simultaneously an English description of the specific alarm condition is provided in the message area (see Figure 18.7.1-10).

At the same time that a message appears on the DIAS message area, an alarm message line is also presented on the bottom of the display page on the panel's ~~CRT.~~ If only one alarm condition caused the activation of the tile, a description of the alarm is displayed on the ~~CRT~~. The ~~CRT~~ alarm message contains the following information: Time-in, Priority, Severity (e.g., Hi, Hi-Hi), descriptor, setpoint, real time process value and data base point I.D. In addition, a representation of the alarm tile is provided to the right of the message area (see Figure 18.7.1-6), and menu options/fields on the display page menu provide direct access to the display pages that can be used to obtain supporting or diagnostic information on the alarm condition.

If an alarm tile contains more than one unacknowledged alarm condition, touching the alarm tile representation on DIAS provides a listing of the new alarm conditions associated with that tile in list display format, see Figure 18.7.1-11. This display provides the priorities and messages of the new alarms. An alarm status tile is provided with this display to allow the operator to be aware of any outstanding alarm conditions on the alarm tile matrix format. The operator is made aware that additional alarms exist which he can subsequently access.

At the same time a tile containing more than one unacknowledged alarm is acknowledged on DIAS the operator would see a message in the ~~CRT~~ message window indicating that the alarms behind that tile had been acknowledged, e.g. "RCP 1A TROUBLE (Priority Box) Multiple Alarms Acknowledged". Additionally, the display page menu option is provided to the right of the message area.

The alarm tiles that are in alarm can be accessed and acknowledged on any ~~CRT~~ in a mechanism similar to accessing and acknowledging the alarms via the alarm tiles. A graphic representation of any alarm tile in alarm or cleared/return to normal condition status can be requested on any ~~CRT~~. The operator can quickly select unacknowledged ~~CRT~~ alarm tiles and obtain the same information as described above within the ~~CRT~~ message and menu areas. This means of responding to alarm conditions eliminates the need to traverse the control room to acknowledge alarms while maintaining a consistent method of acknowledgement. This is fully described in the next section.

Priority 3 Alarms and Operator Aids

Alarm information for priority 3 alarms that do not degrade to priority 2 or 1 conditions and operator aids are only available from the DPS and only appear on ~~CRT~~ alarm formats. The operator response to these conditions do not require immediate response since they represent low priority conditions.

The ~~CRT~~ page's menu in the Nuplex 80+ design provides the operator with an overview of the existence of unacknowledged alarms and cleared/return to normal conditions.

18.7.1.5.3 Alarms Presented on ~~CRTs~~

Alarm information is presented on the ~~CRTs~~ by 1) alarm coding the descriptors of the representative features on the process mimics, 2) alarm tile representations and 3) alarm lists. The multiple methods of ~~CRT~~ alarm presentation allow the operators to utilize alarm information in the most meaningful manner for a given function or task.

~~CRT~~ alarm information allows the operator to efficiently access, acknowledge, and diagnose any alarm from any of the control panel ~~CRTs~~. This permits the operator to remain at a panel when an alarm comes in on another panel. Alarm priority and status coding, as described in Section 18.7.1.5.1, is applied when alarms are present on component labels, symbol labels, process parameter labels, directory options, and menu options.

DPS VDUs

18.7.1.5.4 Alarm Access via ~~CRT~~ Menu and Directory Pages

DPS

The menus located at the bottom of each ~~CRT~~ screen (see Figure 18.7.1-5) in the Nuplex 80+ design provides the operator with an overview of the existence of any unacknowledged alarm conditions and a general overview of where they exist by plant sector. If an alarm exists in a plant sector, the corresponding menu option flashes. This is the sector of the hierarchy where the display page can be found that would best allow the alarm to be acknowledged.

DPS

The menu option will reflect the priority associated with the alarm. The operator will be guided to the appropriate display page in this way. When the operator chooses, by touch, the menu option that is flashing, the associated sector directory is shown and the display page that is associated with the alarm, will be flashing. The operator can then access this page by touch and acknowledge the alarm in the most appropriate context. In the case of more than one alarm on the same page, the display page option for that page will reflect the highest priority of unacknowledged alarm. The same coding applies to the directory menu options, in that they depict the highest priority unacknowledged alarm condition of the alarms on display pages that may be accessed within that branch of the hierarchy.

18.7.1.5.5 Alarm Acknowledgement

The Nuplex 80+ ~~CRTs~~ allow significant flexibility in alarm acknowledgement to accommodate varying numbers of alarms (single and multiple) and various methods by which the operator can acknowledge them.

DPS

The following means of alarm acknowledgement are provided through the ~~Nuplex 80+ CRTs:~~ DPS VDUs

SINGLE ALARMS

1. Alarm acknowledgement via the annunciator tile representations -

   When a single unacknowledged alarm condition exists, an alarm tile representation is displayed on the lower right

corner of the ~~CRT~~ screen (see Figure 18.7.1-6). The tile representation corresponds to the DIAS alarm tile for priority 1, 2 and 3 alarms and appears independent of the current display page being presented. Alarms may be acknowledged by touching the ~~CRT~~ alarm tile representation. This action changes the alarm tile representation from a flashing high intensity yellow condition to a medium intensity yellow condition and silences the periodic momentary audible sound associated with the alarm condition. Specific alarm condition messages are viewed on the ~~CRT~~ message window. This message contains: tile name, priority, message, setpoint, real-time process value, time-in and database point I.D. Also display options will appear to provide access to display pages with more information about the descriptor that was touched (see Figure 18.7.1-6). The alarm tile will remain in the medium intensity yellow state until another new alarm comes in or the operator presses the "CLR" button.

2. Alarm acknowledgement using display page descriptors -

Alarm priority and status is displayed, when alarms are present, on component labels and process parameter labels. Touching unacknowledged alarm coded descriptors on process display pages acknowledges the alarm and accesses the following information, displayed in the message area: DIAS tile name, priority, message, setpoint, real-time process value, time-in and database point I.D. Also, as described previously, display page options would appear to give the operator access to more information with respect to the descriptor that had been touched.

3. Alarm acknowledgement using UNACK. ALARMS list

If more than one alarm comes in, such as in post trip conditions, the operator needs a fast effective method to review and acknowledge multiple alarms. This is allowed by providing an UNACK. ALARMS target, for multiple alarms, in the same place as the alarm tile representation for single alarms. When selected, a snapshot of the current new and cleared alarms is displayed on a list format. No individual alarm tile representation is provided when multiple alarms exist. This snapshot will only represent the alarms that existed at the time the target was selected and none that occur after.

Four modes have been selected which correspond to significant changes in the alarm logic based on the plant state. These modes are:

1. Normal operation

2. Heatup/cooldown

3. Cold shutdown/refueling

4. Post-trip

Mode change is discussed in Section 18.7.1.5.

B. Audible alarm information in Nuplex 80+

Distinct sounds/tones are provided in the Nuplex 80+ control room to indicate the following alarm information:

1. New Priority 1 or 2 Alarms

2. Reminder Tone for unacknowledged Priority 1 or 2 or Cleared Conditions (periodic while unacknowledged)

3. Cleared Priority 1 Alarms, or Cleared Priority 2 Alarms (upon becoming cleared)

An audible alarm, tone 1 or 3, is only present for 1 second and tone 2 will repeat periodically, once every minute, until all alarms are acknowledged. If a new alarm condition comes in before the first alarm condition has cleared, an audible tone is presented at that time.

C. Flash Suppression Feature in Nuplex 80+

In situations where multiple unacknowledged alarms exist the operator needs to direct his attention to the highest priority conditions. In this situation all other unacknowledged alarms, i.e. new priority 2, 3, and all cleared alarm conditions, are added noise that distracts the operator from the most important alarm conditions. In the Nuplex 80+ control room a "stop flash" and "resume" button exists on each console. When the "stop flash" button is depressed the alarm system's behavior exhibits the following characteristics:

1. All new priority 2 and 3 alarms change to existing alarms i.e. tiles and ~~CRT~~ DPS representations.

DIAS

2. Any cleared alarm conditions are not presented as alarm conditions.

3. Any new alarm priority 2 or 3 alarm condition coming in after the "stop flash" button has been activated is presented to the operator, however the operator may redepress the stop flash button to suppress these conditions.

The reminder tone informs the operator that unacknowledged or cleared alarm conditions exist. This also serves to remind the operator that the alarm suppression feature is engaged. To reinstate normal alarm features the operator actuates a "resume" button which returns all unacknowledged and cleared conditions to their normal representational alarm status (i.e., fast and slow flashing respectively). The alarm suppression button is backlit after actuation to indicate that the feature is active.

D. Operator Established Alarms

In addition to preestablished alarms the Nuplex 80+ alarm handling system allows the operator to establish his own alarm conditions that can notify him of changes in equipment performance, continued degradation of processes, or other changes in process performance. The operator is able to establish a new alarm associated with any DPS data base point. A display page listing is available for the operator to review the operator established alarm setpoints.

E. Operator Aids

Operator aids consist of information that is helpful to the operator for plant control, but does not represent an undesirable condition in a process or component. Examples of Nuplex 80+ operator aids are:

1. Main turbine turning gear engaged.

2. Low pressurizer pressure trip bypass enabled.

Operator Aid information is presented on ~~the CRT~~ DPS. Operator Aid information is presented using a orange underline of the text of the information it applies to. The operator aid information flashes when unacknowledged and then may be acknowledged by the operator, however there is no cleared state.

Motor Operator isolation valves are provided with mid-travel reversing capability which allows control errors to be corrected immediately upon detection.

C. Modulating/Throttle Valves

Modulating components are classified into four categories that are associated with their operational/control characteristics.

1. Motor-Operated Throttle

These valves are modulated by holding the open or closed switch in the desired direction of travel. Analog position indication is provided on a ~~CRT~~ display DPS page and where appropriate on a discrete indicator. The physical representation of the discrete controls are different than an open/closed isolation valve to allow the operator to easily distinguish the valve's function. When the valve is in a throttled position (i.e. not full open or full closed) both indicator lights are lit.

2. Electro-Pneumatic Modulating Open

These valves are modulated open by pneumatic/air inlet and modulate closed by bleeding off air. Modulating control of this valve type is accomplished on a process controller. Discrete red/green pushbuttons engage or disengage the process controller as follows:

CONTROLLER PERMISSIVE

The red pushbutton is on a split screen switch with a blue permissive indicator with the blue located above red. Selecting this mode permits operation of the valve from the process controller. After selecting this mode, if the process control signal is engaged, the blue status light is lit. The red status lamp lights when the controller, either manual or automatic, modulates the valve off the closed position. Both the red and green switches are lit in addition to the blue/permissive when the valve is in the intermediate position. If the green/close discrete switch is selected, process control is disengaged and the valve returns to the closed/fail condition by bleeding off air, usually assisted by a spring.

The same design is used with multiple components and the signals are cascaded in the same manner.

18.7.1.6.2.8 Process Signal or Component Selection

There are many control designs that permit the selection from redundant process instrumentation channels (e.g, X or Y) as input to a (or a set of) component control logic(s).

If one or multiple components are to be controlled by a selectable process control signal, then there is one switch and status indicator for each available process instrumentation channel.

The standard switch configuration for two channels: (X or Y-not both, but always at least one) is two switches interlocked so the selection of "X" resets the selection "Y" and vice versa. For additional channels, switches are added one per channel interlocked in the same manner.

18.7.1.6.2.9 Component Discrepancy

The DPS and DIAS normally display abnormal component conditions via ~~CRT~~ VDU and alarm features described in previous sections. In addition a component discrepancy operator aid occurs when the demanded state of a component (demanded by remote, automatic control action) is found to be different from that of the component. This operator aid is also displayed as a flashing status indication provided on the component switch backlights to aid the operator in identifying these same abnormal conditions.

The control switch flashing status may be deactivated. This prevents the operator from having to walk around the control room to acknowledge each flashing switch. Acknowledgement is through the ~~CRT~~ VDU or alarm tiles when the control switch flashing status is deactivated.

DPS Component discrepancy Operator Aids have the following properties:

1) Operator Aids coding of the descriptor for the component

2) When acknowledged, displays the message "Component discrepancy: Re-arm control logic at the switch"

3) When the clear Op Aid signal comes in, due to re-arming of the logic, the Op Aid resets.

3. Subloop Operating Mode Selection

Figure 18.7.1-19 shows a typical operating mode selection display. The operator selects the OUTPUT target in the letdown section revealing the dynamic section display as shown. A label above the dynamic section identifies the current selection (LTDN FLOW OUTPUT DEMAND). The current selected option (Manual) is highlighted by "selection" coding. The current output (40%) is also displayed. In the manual mode, the output is varied using the UP or DN touch targets and an arrow with scale is included to indicate the rate (slow or fast) of manual output variation.

4. Subloop Component Selection

Figure 18.7.1-20 provides an example of a typical component selection feature using the letdown control subloop. The component selection target (CH-201P/CH-201Q) is selected in this section revealing the component display as shown. This display replaces discrete control switches on the control panel and mimics their operation for components controlled by the subloop. In this example, CH-201P is selected and CH-201Q is not as exhibited by SELECT target selection coding. Component status is displayed via the component symbol (filled = closed, partial filled = intermediate position, hollow = open). This symbology is consistent with that used for DPS displays. Touching the SELECT target arms the components for controller operation based on subloop demand while touching the CLOSE target causes the component to close.

The selection examples described above are similar for other selectable process controller functions.

18.7.1.8 Safety-Related Information in NUPLEX 80+

Safety-related information is integrated into the control room to allow its use by the operator, where possible, during normal operation.

The following is a summary of safety-related information in Nuplex 80+. Details concerning specific presentation methods (e.g., DIAS) are presented in earlier Sections of 18.7.1.

T2+

18.7.1.8.1 [Safety-Related Data]

Section 7.5 provides a complete discussion of the Nuplex 80+ approach to providing safety-related display instrumentation including compliance with Regulatory Guide 1.97. In many situations, safety-related parameters are only a subset of the

parameters that monitor a particular process. Operators of present control room designs use control or narrow range indications during process control and use separate safety related indications when monitoring plant safety concerns.

For Nuplex 80+ the same indicators used for normal operations are used for monitoring and control of safety-related situations. These indications are validated for accuracy against the safety-related parameters. If a process representation value deviates excessively from the associated PAMI Channel data, a validation alarm is generated. In response to an alarm condition, the operator can review the individual channels associated with the parameter on either a diagnostic CRT page or the discrete indicator displaying that parameter. At this time he can select the indication from the most appropriate sensor for display, including that from post accident monitoring instrumentation. The operator is informed when the validation algorithm is not able to validate the data via the alarm system. The resultant output of the validation algorithms are used on IPSO, the discrete indicators, and the higher level display pages that contain the parameter.

In addition to the CRT and discrete indicator displays integrated into each panel, the Regulatory Guide 1.97 Category 1 information is also displayed by an independent discrete indication or channel at a single location on the safety monitoring panel.

Nuplex 80+ complies with all NUREG-0737 Supplement 1 requirements. The following is a summary of how Nuplex 80+ complies with the eight primary supplement 1 requirements:

1. The Nuplex 80+ Advanced Control Complex provides a concise display of critical function and success path performance indications to control room operators via the Data Processing System (DPS), i.e., the plant computer.

2. Critical function information is provided through a dedicated DPS critical function display page hierarchy and is available on all CRTs in the Nuplex 80+ control complex. There is a CRT on every panel section in the controlling workspace (e.g., RCS, CVCS, ESF, etc.).

3. The IPSO big board display is a dedicated display which continuously shows all critical function alarms and key critical function and success path parameters to the control room operators.

4. The DPS system, which provides the Nuplex 80+ SPDS function, has a reliability of greater than 99.99%

parameters that monitor a particular process. Operators of present control room designs use control or narrow range indications during process control and use separate safety related indications when monitoring plant safety concerns.

For Nuplex 80+ the same indicators used for normal operations are used for monitoring and control of safety-related situations. These indications are validated for accuracy against the safety-related parameters. If a process representation value deviates excessively from the associated PAMI Channel data, a validation alarm is generated. In response to an alarm condition, the operator can review the individual channels associated with the parameter on either a diagnostic ~~CRT~~ page or the discrete indicator displaying that parameter. At this time he can select the indication from the most appropriate sensor for display, including that from post accident monitoring instrumentation. The operator is informed when the validation algorithm is not able to validate the data via the alarm system. The resultant output of the validation algorithms are used on IPSO, the discrete indicators, and the higher level display pages that contain the parameter.

DPS DISA

In addition to the ~~CRT~~ and discrete indicator displays integrated into each panel, the Regulatory Guide 1.97 Category 1 information is also displayed by an independent discrete indication or channel at a single location on the safety monitoring panel.

DPS

Nuplex 80+ complies with all NUREG-0737 Supplement 1 requirements. The following is a summary of how Nuplex 80+ complies with the eight primary supplement 1 requirements:

1. The Nuplex 80+ Advanced Control Complex provides a concise display of critical function and success path performance indications to control room operators via the Data Processing System (DPS), i.e., the plant computer.

2. Critical function information is provided through a dedicated DPS critical function display page hierarchy and is available on all ~~CRTs~~ in the Nuplex 80+ control complex. There is a ~~CRT~~ on every panel section in the controlling workspace (e.g., RCS, CVCS, ESF, etc.).

DPS VDU
DPS VDU

3. The IPSO big board display is a dedicated display which continuously shows all critical function alarms and key critical function and success path parameters to the control room operators.

4. The DPS system, which provides the Nuplex 80+ SPDS function, has a reliability of greater than 99.99%

5. The DPS accommodates the failure of any single hardware element so that no single failure will disable any of its functions. The DPS is fully isolated from all safety systems.

6. The DPS HSI design is developed according to a comprehensive set of Human Factors Standards and Guidelines for System 80+.

7. All five (reactivity control, reactor core cooling and heat removal from the primary system, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions) of the safety function elements are included in the DPS Critical Functions Monitoring hierarchy which forms the basis of the Nuplex 80+ SPDS function.

8. The System 80+ Critical Functions Monitoring function (SPDS) is being developed in a complementary (parallel) fashion with the development of System 80+ Emergency Procedure Guidelines. Generic emergency procedure guidelines are used during the design process.]

Attachment 2 of Reference 2 provides a more detailed explanation of how Nuplex 80+ complies with NUREG-0737 Supplement 1 requirements.

18.7.1.8.2 Critical Function and Success Path Monitoring

Critical Function and Success Path (availability and performance) information is integrated throughout the Nuplex 80+ information hierarchy. The critical function and success path monitoring application programs in conjunction with the continuous IPSO display and the DPS CRTs meet SPDS requirements for Nuplex 80+ without using stand-alone monitoring and display systems. Alarms provide guidance to unexpected deviations in critical functions as well as success path unavailability or performance problems.

Alarm priorities are assigned based on the proximity of the alarm setpoint to a significant operator action condition. Section 18.7.1.1.4 provides a more detailed explanation of alarm priorities.

IPSO continuously provides overview information that is most useful for operator assessment of the critical functions, see Section 18.7.1.1. Each box within the matrix highlights the presence of alarms that threaten the specific critical function. The display format for the box indicates the highest priority of all related alarm conditions. Supporting information relating to critical function alarm conditions is available by using the alarm tiles on the critical functions section of the CRT display page hierarchy.

5. The DPS accommodates the failure of any single hardware element so that no single failure will disable any of its functions. The DPS is fully isolated from all safety systems.

6. The DPS HSI design is developed according to a comprehensive set of Human Factors Standards and Guidelines for System 80+.

7. All five (reactivity control, reactor core cooling and heat removal from the primary system, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions) of the safety function elements are included in the DPS Critical Functions Monitoring hierarchy which forms the basis of the Nuplex 80+ SPDS function.

8. The System 80+ Critical Functions Monitoring function (SPDS) is being developed in a complementary (parallel) fashion with the development of System 80+ Emergency ~~Procedure~~ Guidelines. Generic emergency procedure guidelines are used during the design process.

Attachment 2 of Reference 2 provides a more detailed explanation of how Nuplex 80+ complies with NUREG-0737 Supplement 1 requirements.

18.7.1.8.2 Critical Function and Success Path Monitoring

Critical Function and Success Path (availability and performance) information is integrated throughout the Nuplex 80+ information hierarchy. The critical function and success path monitoring application programs in conjunction with the continuous IPSO display and the DPS ~~CRTs~~ meet SPDS requirements for Nuplex 80+ without using stand-alone monitoring and display systems. Alarms provide guidance to unexpected deviations in critical functions as well as success path unavailability or performance problems.

Alarm priorities are assigned based on the proximity of the alarm setpoint to a significant operator action condition. Section 18.7.1.1.4 provides a more detailed explanation of alarm priorities.

IPSO continuously provides overview information that is most useful for operator assessment of the critical functions, see Section 18.7.1.1. Each box within the matrix highlights the presence of alarms that threaten the specific critical function. The display format for the box indicates the highest priority of all related alarm conditions. Supporting information relating to critical function alarm conditions is available by using the alarm tiles on the critical functions section of the ~~CRT~~ display page hierarchy.

	Operator Interface Feature	Information
1.	IPSO	Priority 1, 2, 3 Critical Function/Success Path alarm indication; Safety Function Status Check selected
2.	ESF Monitoring Module (ESF Monitoring Panel)	Safety Parameter status by train (for safety systems encompassed by Reg. Guide 1.47)
3.	DIAS Displays	Alarm information depicting critical function and success path parameter problems
4.	~~CRT~~ DPS VDU Displays	Critical Function section of Information hierarchy and alarm information in lower level pages (i.e., 2nd and 3rd level) depicting success path problems and critical function parameter problems.

18.7.1.9 Operators' Modules

Operators' Modules are provided in Nuplex 80+ for operator interaction with specific I&C systems or functions (e.g., PPS, MDS, CPC, CCS, Control Element Drive Mechanism System). These modules and features are not included in the six standard HSI monitoring and control design features described in Section 18.7.1 because the functional requirements are unique for each system. They will be designed in accordance with the standard Nuplex 80+ information and control system conventions and the criteria specified in the Human Factors Engineering, Standards, Guidelines, and Bases for System 80+ (Section 18.4, Reference 6). A suitability verification will be performed on each system or function operators' module in accordance with the HFE Verification and Validation Plan (Section 18.4, Reference 3). Other as yet unspecified features will be developed using this same process.

TABLE 18.7.1-1 (Cont'd)

(Sheet 2 of 2)

NUPLEX 80+ CODING MATRIX

	CODE																													
	SHAPE CODES												COLOR CODING																	
													HUES								INTENSITY						FLASH RATE		SWITCH POSITION CODES	
	PROBLEM SHAPE	EQUIPMENT/COMPONENT STATUS			DIRECTION SHAPES			ALARM & OP AID SHAPES				TARGET SELECT SHAPE									TEXT		ALARM & OP AID			ALARM & OP AID		(RELATIVE TO EACH OTHER)	
PROPERTY	ASTERISK (1,2,4)	CROSS HATCHED (1,4)	HOLLOW (1,2,4)	FILL (1,2,4)	UP ARROW (1,4)	DOWN ARROW (1,4)	OTHERS + , -,DOT (1)	REV VIDEO (1,2,4)	BOX (1,2)	BRACKETS (1,2)	UNDERLINE (1)	BUTTON (1,2,4)	RED (1,3)	GREEN (1,3)	BLUE (1,3)	YELLOW (1,2)	CYAN (1)	WHITE (1)	ORANGE (1)	PURPLE (1,2)	HIGH (1)	MED (GRAY) (1)	HIGH (1,2)	MED (1,2,7)	LOW (1,2)	FAST (1,2,3,4)	SLOW (1,2)	TOP (3,4)	BOTTOM (3,4)
CONTROLLER STATUS																														
AUTO															X															
ABNORMAL MANUAL CONTROL																			X											
DATA																														
DYNAMIC																		X			X									
STATIC INFORMATION																		X				X								
SUSPECT	X																		X											
DYNAMIC DATA LABELS																	X													
RG 1.97 CAT.1 LABELS																				X										
INCREASING VALUE					X																									
DECREASING VALUE						X																								
ABOVE, BELOW OR AT TARGET VALUE							X																							

NOTES:
(1) ~~CRT~~ DATA PROCESSING SYSTEM
(2) Discrete Indication & Alarm System
(3) Switches
(4) Process Controllers
(5) Instrumented Component (Dynamic Data)
(6) Non-Instrumented Component (Static Data)
(7) Medium intensity yellow is desaturated (dulled with gray) to enhance its absolute discriminability from

Amendment W
June 17, 1994

The sequence of the steps listed above looks first at what is required functionally by the operator. Following specific criteria, the control room configuration as a basis, the functions required to be performed in the control room are placed on the control panels. The second portion of the effort involves determining and categorizing all control and indication devices required in the control room. The control and indication devices are assigned to the selected functions. The third and final portion involves arrangement of these devices within the functional groups according to specific criteria for detailed panel layout. Evaluation of the design is performed in the first and third step. In the first step a high level operational analysis is performed, based on function only. A full operational analysis is performed using procedures and operational, engineering and human factor personnel in the third step.

18.7.2.1 Part I: Determination of Functional Groups and Assignment to Respective Control Panels

The first step in arriving at main control panel layouts involves four basic tasks.

A. Based on the functional task analysis, Emergency ~~Procedure~~ Operations Guidelines (EDG) ~~(EPG)~~ and plant operating sequences, functions performed by the operator during various operating modes are determined.

B. These functions are assigned to the main control panels based on the configuration defined in Section 18.6.5.

C. The functions are arranged on the assigned panels.

D. A high level operational analysis is performed based on the functional arrangement.

18.7.2.1.1 Nuplex 80+ Control Room Organization

Prior to the development of control panel layouts it is necessary to establish the NUPLEX 80+ control room functional organization, (see Section 18.6.5 for a more complete discussion of the panel configuration within the control room).

The Nuplex 80+ controlling workspace consists of two main operational areas, the MCC and the ACSC. The MCC is the area where normal operations take place. The controls and indications located on these panel sections provide an operator with the capability of maneuvering the plant from hot shutdown to full power operation and return to hot shutdown. The MCC is designed

18.7.2.2.1 Criteria for Determination of Required Devices and Assignment of Devices to Functional Groups

The controls and indications required to perform the operator functions determined in Section 18.7.2.1 are obtained from the functional task analysis (Information and Control Requirements), Federally mandated information and control requirements, and System I&C Inventory (from the system cognizant engineering organization). It is then determined how the information is displayed and how the controls are implemented based on the System Description for Control Complex Information System (Section 18.7, Reference 2). The following criteria are used to determine the methods of providing control and information.

A. All control devices for plant components in critical function main flow paths and the minimum inventory of fixed location controls needed to accomplish credited safety function success path tasks identified in EPGs and Probabilistic Risk Assessment are assigned to fixed position discrete switches (e.g. CCS Switch Configuration).

B. Other process controls (e.g. process controllers, switches) may use touch screen (soft) controls that use VDU devices (e.g., CCS Process Controller Display) or other control devices (e.g., CCS Switch Configuration, Operators Modules). Each device is limited to control loops within a related functional group.

C. The DPS ~~CRT~~ displays are an operator information display interface for all functional groups. The ~~CRTs~~ display essentially all plant information sent to the main control room.

VDU
DPS VDU

D. Discrete indicators are used primarily to display frequently monitored data to enhance overview comprehension of system level performance. This data include the major/representative process parameters such as system flowrate or controlled parameters, i.e., temperature for a cooling system. In addition, discrete indicators are provided to meet redundant display requirements for the following information:

1. Information required for maintaining power production without the DPS (including plant investment protection) for up to 24 hours.

2. Display of plant safety related parameters for normal and post-accident monitoring, including continuous display of Regulatory Guide 1.97 Category 1 parameters and display of the minimum inventory of dedicated information needed to accomplish the EPG.

DIAS

E. Alarms are provided on alarm tiles as well as the ~~CRT~~ DPS display system. See Section 18.7.1.5 for a description of alarm features and characteristics.

18.7.2.2.2 Procedure for Determination of Required Indication and Control Devices and Assignment to Appropriate Functional Groups

A. Step 1

Obtain the applicable documentation that indicates the information and controls that are to be located on the main control room panels. This information is determined by the System I&C Inventory from the system cognizant engineers and the Procedure Guideline Information and Control Requirements from the FTA.

B. Step 2

List the operational mode being considered and the function to be evaluated.

C. Step 3

Review the documentation obtained in Step 1 to determine the controls and indications necessary to perform the function. At this point the Nuplex 80+ methodology for display or control is selected according to the criteria in the System Description for Control Complex Information System (Section 18.7, Reference 2).

D. Step 4

List the devices required in the appropriate area. This step includes determining parameter grouping on discrete indicators, alarm grouping, switch grouping, and process control loop grouping for display on one device.

E. Step 5

After all devices have been assigned, review the assignments to determine if any devices have been assigned to more than one functional group. If this is the case, review the task analysis data and operating guidelines and sequences to determine the functions that are performed sequentially or most frequently, and assign the device to that functional group.

F. Step 6

Review the data obtained in Step 1 to assure that all information and controls required are provided by the display and control devices identified in this part of the procedure.

1. System Flow Path

For functional groups that are primarily associated with one system, information gathering tasks are made easier if the information is presented in a format that is similar to the operator's mental image of the system. For a fluid system that contains a number of components the operator's mental image is typically related to a process mimic diagram. The mimic diagrams reflect those used during training, if appropriate, or are designed specifically to reflect operators concerns. The control panel device layouts reflect these mimic diagrams. This technique for device layout is consistent with the associated system layout mimic on the ~~CRT~~ display pages. DPS

Functional groups arranged by system flow path should mimic the associated process on a left to right, or top to bottom basis. Parallel rows are used where parallel process paths are encountered. Bold lines are placed on panels to connect component controls when they effectively enhance the representation of the process.

Flow path arrangements are not always appropriate as is the case when several controls are associated with a single component or the functional group contains devices in a number of systems. The alternate layouts described below are used when device layouts cannot be arranged to resemble mimic diagrams.

2. Sequential

Sequential layouts are typically used for multiple controls associated with large components or other situations that require device operation in a designated sequence.

Sequential arrangements are configured in the sequence most frequently used by the operator. Controls are arranged in rows, left to right, and columns top to bottom (i.e., the same as a page of type).

3. Related Function

These indications and controls are arranged in groups based on the related function. Some functional groups do not fit into the flow path or sequential arrangement methods. An example of related function is containment isolation. Containment isolation valves are extracted from many systems so there is no relationship by flow or sequence. The relationship that is common to all is that they perform the same function: isolate the

containment. Note that ~~CRT~~ process mimics also show these valves as part of the individual system flowpaths. DPS

18.7.2.3.2 Criteria For Spacing of Indications and Controls

The criteria for spacing of indications and controls is contained in the Human Factors Engineering Standards, Guidelines and Bases for System 80+ (Section 18.4, Reference 6).

18.7.2.3.3 Criteria for Device and Functional Group Identification

Techniques enabling the operator to easily obtain information are implemented by the use of the following human engineering design principles. Four types of techniques are employed:

A. Alpha-numeric Labels

B. Graphic Symbology

C. Color coding

D. Demarcation

Identification using labels on the control panels help establish a hierarchy for the control panel information. Guidelines on label sizes are established to reflect the hierarchy as well as provide readability from various locations in the controlling workspace. The criteria for letter height is provided in the Human Factors Engineering (HFE) Standards, Guidelines and Bases for System 80+ (Section 18.4, Reference 6). The size requirements for readability is discussed in Section 18.7.1.1.7. The labeling hierarchy used within the Nuplex 80+ control room is in accordance with the HFE Standards, Guidelines and Bases for System 80+ (Section 18.4, Reference 6).

Display device and panel information labels conform to the Nuplex 80+ coding/conventions indicated in Section 18.7.1.1.2.

Functional Group Identification

In addition to a label, functional groups are identified by the use of panel demarcations. A group align stripe outlines all components within the group. The information on the label indicates the function, major component or system controlled by the group. Panel space required for name tags is reduced by providing system or functional level information only and using legends on switches whenever possible to describe the purpose of the components within the group.

1. Related Component.

2. Related Function.

3. Related System.

M. Systems Engineers, a Human Factors Engineer and a Senior Reactor Operator reviewed and modified the list as necessary to meet the Nuplex 80+ alarm philosophy.

N. Compiled a composite list of annunciators. This list is contained in Section 18.7.3.2.3.

The above steps identify all indication, alarm and control devices required for the RCS panel. This focuses on those needed for maneuvering the plant from hot shutdown to full power operation and return to hot shutdown. Additionally, devices are identified to provide all RCS indication, alarms and controls necessary for reactor trip recovery, emergencies, maintaining plant availability and investment concerns. Although not identified in the design criteria for layout of the MCC, indications and alarms for RCS parameters used for Heatup, Cooldown, Cold Shutdown and Refueling are included on this panel to provide a single system oriented location for all RCS instrumentation.

The following three sections identify specifically the results of this part of the RCS panel design effort. Section 18.7.3.2.1 details the indication required for the RCS panel through both discrete indicators and ~~CRT~~ displays. Section 18.7.3.2.2 describes RCS process and component controls with individual sections for ~~CRT and~~ alarm ~~system~~ controls. Section 18.7.3.2.3 describes in detail the RCS panel alarms. Each of these sections assigns its RCS instrumentation to one of the three functional groups identified in Section 18.7.3.1.

DPS

DPS VDU & DIAS

18.7.3.2.1 RCS Panel Indication

RCS panel indication is provided by the DIAS flat panel/indicators and DPS ~~CRT~~ displays. The general descriptions of these Nuplex 80+ information systems are provided in Section 18.7.1.4 and 18.7.1.3, respectively. The design integrates the information presentation of these two systems. The following two sections identify the discrete indicators and ~~CRT~~ display pages that exist for the RCS panel. Subsequent sections identify the specific information that exists for these devices and assigns them to functional groups.

VDU

DPS

18.7.3.2.1.1 Discrete Indication

The DIAS is an important Nuplex 80+ presentation system containing frequently used process parameters that help an operator's overview of the plant condition and other parameters needed when the ~~CRT~~ DPS display system is unavailable. Many individual parameters have been identified in these categories relating to the RCS. In a conventional control room, each of these parameters is assigned to an individual indicator on the panel. The operator is required to scan a panel containing over 100 indicators, in order to locate the small number of parameters he uses on a frequent basis. As discussed in Section 18.7.1.4, discrete indicators provide the operator with concise processed information related to components, systems or plant processes in a variety of display formats.

The following steps were taken to determine which RCS parameters are continuously displayed, those that require access when the DPS is unavailable, and on which indicator these parameters are displayed.

A. Review the generated list of indicators and their characteristics.

B. Review Instrument and Control Design Requirements for System 80+ and the P&IDs for System 80+ to determine available sensors and range.

C. Consolidate the available sensors using validation and menuing techniques based on one or more of the following criteria:

   1. Frequency of use (based on the number of times a function and its associated parameters are identified in the functional task analysis).

   2. Functional Group on the RCS panel.

   3. Operational Importance by identifying parameters that have a major impact on plant process such as those that control power, inventory, pressure, level, temperature.

D. Identify the discrete indicators and the parameters that may be viewed on each. There are ten indicators identified for the RCS panel. The indicators are:

1. RCP1A

2. RCP1B

3. RCP2A

4. RCP2B

5. RCP Seal/Bleed

6. RCS

7. T_{hot}

8. T_{cold}

9. Pressurizer Pressure

10. Pressurizer Level

With these ten indicators, the operator has continuous display of all frequently accessed plant process parameters related to the RCS panel and easy access via menu to all other RCS parameters required for operation when the DPS is unavailable. The 10 indicators provide RCS Regulatory Guide 1.97 Category 1, 2 and 3 parameters, other parameters needed for operation due to inaccessibility of local gages and parameters, plant process parameters, and indication required for surveillance. The displays for these indicators and the parameters indicated on each are described in Sections 18.7.3.2.1.3, 18.7.3.2.1.4 and 18.7.3.2.1.5.

18.7.3.2.1.2 ~~CRT~~ Displays

The Nuplex 80+ ~~CRT~~ displays ~~and~~ driven by the DPS ~~and~~ contain essentially all System 80+ information that is available to the operator. The information is presented on display pages contained in a structured hierarchy (see Figure 18.7.1-5). Process related displays are primarily mimics based on the Nuplex 80+ conventions (Section 18.7.1.1). The detailed characteristics of the ~~CRT~~ display system are provided in Section 18.7.1.3.

This section describes the RCS-related ~~CRT~~ display pages in keeping with presenting the RCS panel design. It is noted, however, that in the Nuplex 80+ control room any DPS ~~CRT~~ page relating to any system or function can be accessed from the RCS panel ~~CRT~~. The RCS-related displays are contained in the hierarchy shown in Figure 18.7.1-5 under the primary systems level 1 display page.

These ~~CRT~~ pages present graphical layouts of the Primary Systems information that is consistent with the operator's system visualization. This format cannot be accomplished with discrete indicators. Figures 18.7.1-5 and 18.7.3-1 through 18.7.3-10 illustrate the CRT pages for the primary systems and controls associated with the RCS panel. Figure 18.7.3-1 is a level 1 overview display for monitoring the Primary Systems, including the Nuclear Steam Supply Systems. Figure 18.7.3-2 is the level 2 display used for control of the RCS. Figures 18.7.3-3 through 18.7.3-6 are the level 3 display pages used for RCS diagnostics: Pressurizer Pressure, Pressurizer Level, RCS/Vessel and RCS Temperature. Figure 18.7.3-7 is the level 2 page used to control RCPs 1A and 1B; RCPs 2A and 2B have similar pages. Figures 18.7.3-8 and 18.7.3-9 are the level 3 diagnostic pages for RCP 1A; RCPs 1B, 2A and 2B have similar pages. Figure 18.7.3-10 illustrates the diagnostic page for the Seal/Bleed Subsystem of the CVCS. This page is included because the Seal/Bleed portion of the CVCS is controlled from the RCS panel.

The RCS information presented on these eleven CRT pages is defined in the following three subsections for the three RCS panel functional groups identified in Section 18.7.3.1.

18.7.3.2.1.3 RCS Functional Group Indication

A. DIAS Displays

As outlined in Section 18.7.3.2.1.1, an evaluation was performed identifying the DIAS indicators that are provided for the RCS functional group. This includes parameters that are accessible on each, display characteristics and whether the display is continuous or accessible by use of a menu. Based primarily on frequency of use and operational importance in identifying both primary and secondary system changes and problems, the following parameters are selected for continuous display on the RCS panel: pressurizer pressure, pressurizer level, RCS T_h and RCS T_c. The discrete indicator for the RCS displays other RCS less frequently accessed parameters. The five DIAS indicators for the RCS functional group and the sensor readings that may be accessed by each indicator are listed below. Note that the validation algorithms providing the valid parameters are discussed in Section 18.7.3.2.1.6. Specific sensor ranges are provided in Table 7.5-1 for safety-related plant process display instrumentation.

DPS VDU

B. ~~CRT~~ Displays

The RCS-related ~~CRT~~ pages are identified in Section 18.7.3.2.1.2. These pages are shown in Figures 18.7.1-5, 18.7.1-7 and 18.7.3-1 through 18.7.3-10. All of the above information displayed on the discrete indicators for the RCS functional group is also contained in one or more of these pages. The following additional information, not provided on a discrete indicator, is also provided on the RCS-related ~~CRT~~ pages: DPS DISPLAY

DPS DISPL

1. Steam Generator No. 1 Differential Pressure (PDI-115A, 115B, 115C, 115D, Valid)

2. Steam Generator No. 2 Differential Pressure (PDI-125A, 125B, 125C, 125D, Valid)

3. RCP 1A and 1B Spray Line Temperatures (TI-103, 104)

4. Pressurizer Surge Line Temperature (TI-105)

5. Reactor Vessel Differential Pressure (PDI-124W, 124X, 124Y, 124Z)

6. Pressurizer Reference Leg Temperature Sensors

7. Indication of all RCS control devices contained on the RCS panel:

   a. Auxiliary Spray Isolation Valve (CH-205)(Position)

   b. RCP 1A and 1B Spray Isolation Valve (RC-100E, 100F)(Position)

   c. Pressurizer Pressure Controller (Setpoint, Selected Channel and Process Value)

   d. Pressurizer Level Controller (Setpoint Selected Channel and Process Value)

   e. Pressurizer Backup Heaters (On, Off, Status)

   f. Pressurizer Proportional Heaters (On, Off, Status and Output)

   g. Letdown Isolation Valve (CH-515) (Open, Closed Position)

4. Oil System

Figure 18.7.3-24 illustrates the Oil System menu page for RCP 1A (other RCP oil system menus are similar).

a. Lube Oil Cooler Temperature (T-158, 168, 178, 188)

b. Pump Bearing Oil Reservoir Level (L-107, 117, 127, 137)

c. Motor Lower Oil Reservoir Level (L-108, 118, 128, 138)

d. Motor Upper Oil Reservoir Level (L-109, 119, 129, 139)

e. Oil Lift Tank Level (L-131, 141, 151, 161)

The operator may select any of these twenty four parameters for continuous display. He would normally select a parameter that is representative of the general state of each RCP. This parameter would likely be seal pressure, since seal failures are the most common problem with RCPs. Monitoring a single seal pressure helps the operator detect problems with any of the three RCP seals. For diagnostic and surveillance tasks, the operator would select the parameter requiring the most frequent monitoring.

B. ~~CRT~~ DPS Displays

The ~~CRT~~ display pages related to the RCP functional group were identified in Section 18.7.3.2.1.2. The RCP indication is organized into the ~~Nuplex 80+ CRT~~ DPS DISPLAY PAGE hierarchy with plant overview information (i.e., RCP pump status) provided on a level 1 page, control information provided on level 2 pages (i.e., RCP motor current), and detailed diagnostic information provided on level 3 pages (i.e., motor lower journal bearing temperature). The RCP-related pages and the corresponding figure illustrating them are: Primary Systems (18.7.3-1), RCS Control (18.7.3-2), RCS/Vessel (18.7.3-5), RCP 1A, 1B Control (18.7.3-7), RCP 1A Seal/Cooling (18.7.3-8), and RCP 1A PP/Motor/Oil (18.7.3-9). Note that corresponding pages for the other RCPs are provided for the last three pages.

All of the above information displayed on RCP discrete indicators is also provided on the RCP functional group ~~CRT~~ DPS display pages. The following additional information is also provided on these pages:

5. Seal Injection Heat Exchanger Inlet Temperature (T-231E)

The operator has the option of selecting any one of these five parameters for continuous display. If the plant is at power with the RCP seals performing normally, none of these parameters need continuous display. However, if the operator is starting a RCP or a seal problem exists with a particular RCP, the operator would select Control Bleed Flow for that RCP.

B. ~~CRT~~ DPS Displays

The ~~CRT~~ DISPLAY pages related to the RCP Seal/Bleed functional group were identified in Section 18.7.3.2.1.2. The pages containing RCP Seal/Bleed information are identical to those identified for the RCPs in Section 18.7.3.2.1.4 with the addition of a dedicated RCP Seal/Bleed page (Figure 18.7.3-10). All of the above information displayed on RCP Seal/Bleed discrete indicators is also provided on the RCP Seal/Bleed functional group ~~CRT~~ DPS display pages. The following additional information is also provided on those pages:

1. Indication of all Seal Injection Control Devices contained on the RCS panel:

   a. RCP (1A, 1B, 2A, 2B) Seal Injection Flow Control Valves (FIC-241, 242, 243, 244) (Position)

   b. Seal Injection Temperature Indicating Controller (TIC-231) (Position)

   c. Seal Injection Containment Isolation Valve (CH-255) (Open, Closed status)

2. Historical and Trend Data of all RCP Seal/Bleed System parameters.

18.7.3.2.1.6 Sensor Validation

Based on System 80+ system designs, the RCS has many sensors measuring the same parameter (e.g., Pressurizer Pressure, RCS T_{hot} etc.). A review of the Functional Task Analysis for System 80+ indicated that the operator is required to collect, detect, read, compare, copy, compute, compile, analyze, confirm, monitor and/or verify many types of information from multiple indicators during operational tasks. To ensure that human cognitive limits are not exceeded during these tasks,

3. RCP 2A Seal Injection Flow Control Valve (FIC-243)

4. RCP 2B Seal Injection Flow Control Valve (FIC-244)

5. Seal Injection Temperature Control Valve (CH-231)

Automatic or manual control of the five valves in this group is performed by this single process controller.

The Seal Injection controller uses the process controller control philosophy as described in Section 18.7.1.7. The controller provides seal injection temperature control as well as flow control to each of the Reactor Coolant Pumps. The Controller also provides for valve positioning of the Seal Injection Temperature Control Valve CH-231, and Seal Injection Flow Control Valves CH-241, CH-242, CH-243, and CH-244. These valves can be placed in either Open Permissive, Close Position, and Valve Position Status.

The following figures provide examples of different Seal Injection controller display formats:

Temperature Output Demand	-	Figure 18.7.3-32
Temperature Setpoint Control	-	Figure 18.7.3-33
RCP 1A Flow Setpoint Control	-	Figure 18.7.3-34
RCP 1A Flow Output Demand	-	Figure 18.7.3-35

DPS VDU

18.7.3.2.2.4 ~~CRT~~ Controls

A single ~~CRT~~ is provided at the RCS ~~MCC~~ panel. As discussed in Section 18.7.1.3, it has touch sensitive controls for displays and alarms. Additionally, the ~~CRT~~ will have controls for brightness, contrast and power. There are no process or component related controls on the ~~CRT~~. It serves strictly as a monitoring system to observe and help diagnose the process.

DPS VDU
VDU
DPS VDU

18.7.3.2.2.5 Alarm Controls

As discussed in Section 18.7.1.5, RCS panel alarm tiles have touch sensitive switches that acknowledge and reset alarms and activate display of the alarm messages.

18.7.3.2.2.6 Lamp Test

A RCS panel lamp test switch is provided to test RCS panel alarm and control system lights.

Figure 18.7.3-25 illustrates this switch, and Table 18.7.3-2 describes it.

18.7.3.2.3 RCS Panel Alarms

The RCS panel alarms that were compiled, as described earlier in Section 18.7.3.2, are organized and displayed on the RCS panel alarm tiles using the same three functional groups as the discrete indication and controls.

Figures 18.7.3-36 and 18.7.3-37 show the functional grouping for the RCS alarm tiles.

RCP alarms are in one group, RCP Seal/Bleed System alarms in another group and RCS alarms form the third functional group.

The RCS panel has over 200 conditions that can cause an alarm. To assure adequate alarm comprehension, many alarms are grouped into subfunctional groups (i.e., RCP Pump/Motor) in accordance with the Nuplex 80+ alarm philosophy discussed in Section 18.7.1.5. The subfunctional group alarm tiles have a variety of related alarm messages that are read in the message areas ~~of the CRT~~. In cases where key process related parameters (i.e., those identified in Section 18.7.3.2.1.3) are alarmed, there is a single alarm tile alarm (i.e., RCS Pressure Low). This single alarm tile provides for rapid understanding of key process variables.

AT THE POINT OF ACKNOWLEDGMENT

In addition to the alarm tile reduction, the other Nuplex 80+ alarm system features, described in Section 18.7.1.5, are also incorporated into the RCS panel. Priorities have been established for all RCS panel alarms. These are indicated for each alarm in the following subsections.

RCS panel alarms are mode dependent based on the modes described in Section 18.7.1.5. Mode dependency is determined on a case by case basis for each alarm with the focus being on eliminating inappropriate or nuisance alarms. An example of the implementation of mode dependency for the RCS alarms is the low pressurizer pressure alarm. The pressurizer pressure alarm is based on the valid pressurizer pressure indication discussed in Section 18.7.3.2.1.3. Mode dependency is accomplished for low pressurizer pressure by automatic adjustment to the alarm setpoint as the operator selects the plant alarm mode (except for post-trip). During normal operation a fixed setpoint exists. Upon reactor-trip, a lower fixed setpoint is established automatically to prevent nuisance actuation of the alarm. The normal post-trip pressure response would activate the alarm if the normal operation setpoint remained. The post-trip setpoint only allows actuation if an abnormally low post-trip pressure response exists. For the heatup/cooldown mode a manually adjusted setpoint is provided to warn the operator of an

b. RCP_Mtr. Lower Oil Reservoir Level High, Priority 2

c. RCP_Mtr. Lower Oil Reservoir Level Low, Priority 2

d. RCP_Mtr. Upper Oil Reservoir Level High, Priority 2

e. RCP_Mtr. Upper Oil Reservoir Level Low, Priority 2

f. RCP_Oil Lift Tank Level High, Priority 2

g. RCP_Oil Lift Tank Level Low, Priority 2

h. RCP_Oil Lift Pump Flow Low, Priority 2

i. RCP_Oil Lift Pump Outlet Press Low, Priority 2

18.7.3.2.3.3 RCP Seal/Bleed System Functional Group Alarms

The RCP Seal/Bleed functional group alarms were selected by the process defined earlier in Section 18.7.3.2. They are provided in a grouping associated with the following alarm tiles:

1. "Seal Injection Temperature"

   Alarm messages under this alarm tile include:

   a. Seal Inj. Temp Hi-Hi-Seal Isolation, Priority 1
   b. Seal Inj. Temp Lo-Lo-Seal Isolation, Priority 1
   c. Seal Inj. Temp Hi, Priority 2
   d. Seal Inj. Temp Lo, Priority 2

2. "Seal/Injection Flow"

   a. RCP_Seal Inj. Flow Hi-Hi-Cntl Fail, Priority 2
   b. RCP_Seal Inj. Flow Lo, Priority 2

3. "Controlled Bleed"

   a. Cntl Bld Press Hi-Hi-Fail/Bld Isol, Priority 1
   b. Cntl Bld Press Hi-Fail/Bld Isol, Priority 2

18.7.3.2.3.4 Priority 2 Operator Established Alarm

This is an alarm tile that the operator may program from the ~~CRT~~ DPS as discussed in Section 18.7.1.5.6 D. It is provided to allow the operator to program for specific RCS conditions for which he desires an additional prompt. One dedicated operator established alarm tile is provided at each panel (e.g., as shown in Figure 18.7.3-39).

T. Pzr Heater 9 Distribution Panel D04 Overload

U. Pzr Prop Heaters No 1 PPCU High Temp.

V. Pzr Prop Heaters No 2 PPCU High Temp.

W. RCS T_{cold} Sensor Deviation

X. RCS T_{hot} Sensor Deviation

Y. Pzr Level Sensor Deviation

Z. Pzr Water Temp Sensor Deviation

AA. Pzr Pressure Sensor Deviation

AB. DPS/DIAS RCS T_c Calculation Deviation

AC. DPS/DIAS RCS T_h Calculation Deviation

AD. DPS/DIAS Pressurizer Level Calculation Deviation

AE. DPS/DIAS Pressurizer Pressure Calculation Deviation

AF. RCS D/P Sensor Deviation

18.7.3.2.3.6 Operator Aid Information for the RCP Panel

Operator Aid information is only available on the ~~CRT~~ DPS (see Section 18.7.1.5.6 E). The only operator aid information, that exists for the RCS, is a component discrepancy generated by the DPS success path monitoring algorithms (see Section 18.7.1.8).

18.7.3.2.4 Alarms on the ~~CRT~~ DPS VDU

As discussed in Section 18.7.1.5, all conditions that activate the RCS alarm tiles also activate duplicate alarms on the ~~CRT~~ DPS VDU. The alarms for the RCS panel are presented using the following three techniques:

A. Hierarchical Mimic Pages present priority 1, 2, 3 and operator aid alarms.

B. A Time Sequential Listing presents priority 1, 2, 3, operator aid and operator established alarms.

C. A Prioritized Alarm List presents the following categories:

1. Priority 1 Alarms

information size, sample displays are drawn. An area measuring 3.75 inches by 3.75 inches meets the criteria for all DIAS displays on the RCS panel. Thus, the hardware selected for DIAS displays is split into two screens with each screen displaying the parameters for a single discrete indicator. An obvious demarcation line is displayed to visually separate the two displays. The discrete indicator for pressurizer pressure and pressurizer level in Figure 18.7.1-7 illustrates how these two process parameters are displayed on a single display device.

The RCS panel ~~CRT~~ is placed in the center of the panel, as with all panels, to facilitate viewing it adequately from in front of all sections of the panels. After placing the three functional groups and ~~CRT~~, the resulting RCS panel design is shown in Figure 18.7.3-39. The following sections address the detailed layout of each functional group.

DPS VDU

DPS VDU

18.7.3.3.1 RCS Functional Group Layout

As discussed in Section 18.7.3.1, the RCS functional group is the most frequently used on the RCS panel. It is, therefore, placed on the right hand side of the RCS panel (RCS panel section closest to the center of the MCC). All controls and some indication are located on the apron (near horizontal) section of the RCS panel for this functional group. The discrete indicators for the RCS functional group are placed on the vertical section of the RCS panel. There is one discrete indicator for the RCS functional group that is located to the left of the ~~CRT~~. The discrete indicator for infrequently viewed RCS parameters is located to the left of the ~~CRT~~ and not above the RCS functional group based on the following factors:

DPS VDU

DPS VDU

A. The discrete indicators for RCS and RCP Seal/Bleed System are displayed on a common device. With one device providing indication for two functional groups, it made it difficult to place it within both functional groups simultaneously unless the groups are adjacent.

B. Placing the ~~CRT~~ (primary source of information) near the center of the RCS panel is the highest layout priority. This ~~CRT~~ location divided the RCS and RCP Seal/Bleed groups and thus necessitated placing the common indicator at a different location.

DPS VDU

C. Since these parameters are infrequently viewed on this indicator, the discrete indicator location poses little inconvenience. All of its parameters would normally be viewed on the ~~CRT~~. DPS

a. RCS T_{hot} Indicator - Label titled "T_{hot}"

b. RCS T_{cold} Indicator - Label titled "T_{cold}"

c. Other infrequently viewed RCS parameter indicator - Label titled "RCS"

B. Layout of RCS Functional Group

The layout of the RCS functional group indication and controls was implemented using the related function technique identified in Section 18.7.2.3.1. The related function technique is used, because neither a flow path nor sequential layout technique is applicable to the RCS functional group.

The controls and indication for the pressurizer, (pressurizer pressure indicator, pressurizer level indicator, pressurizer sprays, and backup heaters) are also arranged by related function in the PRESSURIZER functional group. The subfunction controls for the pressurizer are also arranged based on related function. The Backup and Proportional Heater subfunction groups, which serve the same function (to increase pressure), are located at the bottom of this group. See Figure 18.7.3-39 for location and arrangement of this group. Similarly, the Pressurizer Auxiliary Spray valve is used as a means of reducing pressure and is placed above the heater controls. The Pressurizer Pressure Controller which controls heaters and sprays is placed above and adjacent to the discrete indicators for pressurizer pressure and pressurizer level which is placed above the Pressurizer Pressure controller (see Figure 18.7.3-39).

The T_{hot} and T_{cold} discrete indicators are placed above the pressurizer functional group to allow viewing the four RCS process parameters (pressurizer pressure, pressurizer level, T_{hot} and T_{cold}) at one panel location (Related function). The RCS discrete indicator for other RCS parameters is located to the left of the ~~CRT~~ DPS VDU, as previously discussed.

18.7.3.3.2 RCP Functional Group Layout

There are four Reactor Coolant Pumps (RCP) for System 80+. Each RCP is operated independently of the other RCPs and has separate indication and controls. The controls and indications for the RCPs are divided into four functional groups corresponding to the individual RCP. These four functional groups are arranged from left to right on the RCS panel as follows: RCP1A, RCP1B, RCP2A and RCP2B. This is shown on Figure 18.7.3-39.

18.7.3.3.3 RCP Seal/Bleed System Functional Group Layout

This functional group of indication and controls is placed near the center of the RCS panel. Most indication and all controls for this group are located in the apron section of the panel. The discrete indicator for the RCP Seal/Bleed System is located on the vertical section of the panel above and to the left of the controls. This location is to the left of the ~~CRT~~. Placing the discrete indicator for the RCP Seal/Bleed System away from the controls was determined to be satisfactory in light of the following considerations: DPS VDU

A. The ~~CRT~~ is the primary source of information for the RCS panel and is placed near the center of the panel. This is the highest priority layout concern. DPS VDU

B. The parameters displayed on the RCP Seal/Bleed System discrete indicator are infrequently accessed.

Figure 18.7.3-39 shows the two RCS panel areas where RCP Seal/Bleed System indication and controls are located. Separate labels identify the functional group of indication and controls on the apron section and the indicator on the vertical section.

Identification of Functional Group

The controls for the RCP Seal/Bleed System are identified on the RCS panel by methods specified in Section 18.7.2.3.3. The following methods are used:

1. Group Align Stripe - A thick line forms an enclosed area around the indicating controller.

2. A label titled "RCP SEAL/BLEED" is placed above the top group align stripe on the controls section, which is located on the apron section of the RCS panel.

3. A label titled "RCP SEAL/BLEED" is placed above the discrete indicator for the RCP Seal/Bleed System.

4. A label titled "INJ FLOW CNTL" is placed above the Seal Injection Flow Controller.

5. A label titled "INJ TEMP CNTL" is placed above the Seal Injection Temperature Controller.

18.7.3.4 Alarm Layout

The alarm tiles for the RCS panel are contained on two flat panel display modules. The module used for the 16 Seal Bleed System alarms is located above the RCP and seal bleed

system functional groups to the left of the ~~CRT~~. Figure 18.7.3-39 illustrates its location, and Figure 18.7.3-37 illustrates the detailed layout of the alarm tiles. This location places the alarms at the highest level within the RCP/Seal Bleed functional groups to enhance its attention getting function. The module used for the RCS and Operator Established, Alarms tiles which is located above the Pressurizer functional group to the right of the ~~CRT~~. Figure 18.7.3-39 illustrates its location, and Figure 18.7.3-36 illustrates the detailed layout of the alarm tiles.

A. Identification of Functional Alarm Groups

The RCP functional alarm group is identified by a label titled "RCP", placed above the RCP/Seal Bleed System Alarm Module. The Seal Injection System functional alarm group is identified by a label titled "Seal/Bleed", placed above the RCP Seal/Bleed Alarm Module. The RCS functional alarm group is identified by a label titled "RCS", placed above the RCS alarm module.

B. Layout of Alarms Within Each Functional Group

The alarms for the RCS are located on the right alarm module and arranged as shown on Figure 18.7.3-36. For cases where high and low alarm tiles exist for the same process (i.e., Pressurizer Pressure Hi and Pressurizer Pressure Lo), the high alarm tile is placed above the low alarm tile.

The alarms for the RCP are located on the left alarm module and arranged as shown on Figure 18.7.3-37. They are placed within functional groups identical to the RCP indication and controls. There are four columns of RCP alarms, RCP1A, RCP1B, RCP2A and RCP2B. These columns of alarms are located left to right, as are the indication and controls. To help identify problems common to more than one RCP, similar alarms (i.e., cooling system) for the four RCPs are located in the same row.

There are three alarm tiles for the RCP Seal Injection System. These are shown in Figure 18.7.3-37.

18.7.3.5 ~~CRT~~ Layout

The ~~CRT~~ is located near the center and close to bottom of the vertical panel section, as specified in Section 18.7.2.3.1 (Figure 18.7.3-39 illustrates its location).

C. Effluent Controls

This group contains the indication and controls for processing the primary fluid removed from the RCS.

Included in the controls mounted on the CVCS panel are process controllers for pressurizer level, letdown/charging, and makeup water. These controllers are designed in a consistent manner as the other process controllers which have been covered in RCS panel details (Section 18.7.3.2.2). The Discrete Indicator and Alarm System (DIAS) provides temperature, pressure, level, radiation and flow parameters via discrete indicators. Alarms associated with the systems are grouped and displayed by the alarm tiles and message windows. The Data Processing System (DPS), via the panel mounted ~~CRT~~, provides general monitoring, system/component level monitoring and detail/diagnostic information on the letdown/charging, makeup water and effluent processing systems. The display page formats and information handling is consistent with the Nuplex 80+ ~~CRT~~ methodology (Section 18.7.1.3), as demonstrated on the RCS panel displays (Section 18.7.3.2.1).

Manual controls which are required for operations of the CVCS are located and functionally grouped on this panel. Control identification, symbology and hue, along with functional grouping of control and indications, group demarcation and labeling are in accordance with the Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.2 Plant Monitoring and Control Panel

The Plant Monitoring and Control Panel contains those systems the operator requires for control and monitoring of core reactivity associated with maneuvering the plant from hot shutdown to full power operation and return to hot shutdown, and additional plant level controls that require a convenient centralized location due to the frequency of their access. A functional layout of the Plant Monitoring and Control Panel is exemplified in Figure 18.7.4-2. The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel, with the following exceptions:

Two Engineered Safety Features Actuation System (ESFAS) modules are provided on the Plant Monitoring and Control Panel. These modules provide pushbutton switches for manual actuation of Containment Isolation, Containment Spray, Main Steam Isolation and Safety Injection Actuation. The modules also provide maintained position switches for Emergency Feedwater 1 and 2 actuation. One of these modules is channelized A and the other is channelized D; B and C modules are provided on the Safety

voltage removal. Reactor power is displayed on a discrete indicator which uses the same DIAS conventions discussed in Section 18.7.1.4. This display also provides CEA motion (as demanded by the RRS) and T_{ave}/T_{ref} indications utilizing signals from the Reactor Regulating System (RRS) portion of the Power Control System (PCS).

A PCS Operators Module is provided primarily for the control of system operating/selection modes as well as the display of system specific data from the Control Element Assembly Motion Control, Reactor Regulation, and Reactor Power Cutback functions of the PCS.

A CEA Position Display Operators Module is provided to present a CEA position overview including indication of associated limits and permissives. The position information is based on accumulation of CEDM motion information obtained from the Motion Sequencing Logic.

A Megawatt Demand Setter (MDS) operator's module (See Figure 18.7.4-2) provides the operator with the means to automatically coordinate turbine generator control with specific plant parameters to prevent exceeding NSSS limits affected by local transients. To accomplish this task, display of plant parameters, variable setpoints, maximum allowable rate change, NSSS limits and operating mode selections are provided. In addition, the capability exists to enter selected setpoints and choose the mode of operation.

Two ~~CRTs~~ are mounted on the panel (see Figure 18.7.4-2). The first provides the normal DPS display hierarchy interface (i.e., Integrated Plant Status Overview, Primary Monitoring or other operator selected displays). The second ~~CRT~~ is dedicated to core monitoring functions such as the Core Operating Limit Supervisory System (COLSS), CEA position and associated displays based on operator selection.

DPS VDUs

VDU

A process controller for the Steam Bypass Control System is located on the panel. It is designed in a consistent manner as other process controllers which have been covered in RCS panel description (Section 18.7.3.2.2).

D. Feedwater/Condensate Train

This group contains those indications and controls associated with the condensate system, including hot well level control, condensate cleanup and storage.

Included in the controls mounted on the panel are feedwater process controllers and switches for each steam generator. This includes pumps, downcomer control valves, and economizer control valves. These are shown on Figure 18.7.4-3. These controls are designed in a consistent manner as other process controllers which have been covered in RCS panel description (Section 18.7.3.2.2).

The Discrete Indication and Alarm System (DIAS) provides steam generator level and pressure, and condensate system parameters, along with the alarms associated with the systems. The Data Processing System (DPS), through the panel mounted ~~CRT~~ VDU, provides general monitoring, system/component level and detail/diagnostic information on the feedwater and condensate systems in the manner consistent with the RCS panel displays (Section 18.7.3.2.1).

Manual controls which are required for starting, stopping and controlling the main feed pumps, booster pumps, condensate pumps, and other components required to be operated during system startup (e.g., emergency feedwater pumps), normal operations and shutdown are located on this panel. Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel section (Section 18.7.3).

The Feedwater and Condensate System controls, which require infrequent operation (e.g., condensate pump, booster pump and main feed pump suction and discharge valves) for system startup and shutdown, are located on the Secondary Cycle panel of the Auxiliary Console.

18.7.4.4 Turbine Control Panel

The Turbine Control Panel has those systems required for control and monitoring of the turbine system during normal operations. The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions as exemplified by the RCS panel. The Turbine Control panel contains no instrument channels which are required for post-accident monitoring. Additionally, the system itself is not required for plant safety. The Turbine Control panel is divided into a primary functional group relating to the turbine, and two smaller functional groups relating to

turbine support components and the generator. A functional layout of the Turbine Control panel is exemplified in Figure 18.7.4-4.

Included in the Turbine Control functional group is the turbine EHC module which is provided by the turbine vendor. This panel insert contains those controls and indications required for normal turbine operations. Turbine test functions are provided on a turbine test panel insert which is located on the Auxiliary Console Secondary Cycle panel.

Space has been allocated on the panel for inclusion of some controls for turbine support systems (see Figure 18.7.4-4). Selections of those controls is derived based on the turbine vendor's EHC panel and the operator's needs for normal operations. Other turbine support system controls are located on the secondary cycle panel of the AC.

The Discrete Indication and Alarm System (DIAS) provides for monitoring generator and turbine parameters, along with providing alarm functions for both. The Data Processing System (DPS), via the panel mounted ~~CRT~~ VDU, provides for general monitoring, system/component level monitoring and detailed/diagnostic information on the turbine and generator systems, in a manner consistent with RCS panel displays (Section 18.7.3.2.1).

Controls which are mounted on this panel have control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling that are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description (Section 18.7.3).

Controls and indications for turbine support systems and the generator which require infrequent operation (e.g., turbine oil pumps, oil lift pumps), are located on the AC Secondary Cycle panel.

18.7.4.5 Safety Monitoring Panel

The Safety Monitoring Panel is used by the operator to primarily monitor the Reactor Protective System (RPS) and Engineered Safety Features Actuation System (ESFAS). It provides continuous display of the availability of ESF systems and continuous display of Regulatory Guide 1.97 Category 1 variables. In addition, the Safety Monitoring Panel contains backup controls for the, Process-CCS and the ESF-Component Control System, and Diverse Manual ESF Actuation Switches.

The Safety Monitoring Panel controls and indication have been separated by channel and function. The Safety Monitoring Panel controls and indication consist of the following:

A) Channel A, B, C, D Plant Protection System (PPS) operators modules,
B) Channel A, B, C, D Core Protection Calculator (CPC) operators modules,
C) Channel A, B, C, D ESF-CCS operators modules,
D) Two Discrete Indication and Alarm System, (DIAS-P) discrete indicators,
E) Channel X, Y Process-CCS Operators Modules,
F) B and C Channelized Pushbutton Switches for manual initiation of reactor trip and ESF actuation signals,
G) Diverse Manual ESF Actuation Switches,
H) A Radiation monitoring indicator,
I) A ESF status monitoring module,
J) Alarm Tiles,
K) ~~CRT.~~ DPS VDU

A functional layout of the Safety Monitoring Panel is exemplified on Figure 18.7.4-5.

The PPS operators modules provides pre-trip, trip and bypass indication of the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). Bypass error indication and a bistable reset indicator are also provided. The PPS operators module also provides indication of linear power and variable setpoint resets for pressurizer pressure and steam generator pressure.

The CPCS operators module provides CPCS Trip Logic Calculator (TLC) and CEAC parameter indication, function enable, TLC trip bypass, and TLC and CEAC status indicator lights.

The ESF-CCS operators modules provides access to all ESF-CCS controls and indication. These features are used in the event of failure of any discrete controls or process controllers located on other control room panels. ESF selective group testing is performed at the A, B, C, and D operators module (see Section 7.3 for details). Each module also provides system status for equipment failure.

The DIAS-P discrete indicators provide continuous display of all Regulatory Guide 1.97 Category 1 signals. These displays are redundant to DIAS-N and DPS displays located at other panels. These DIAS indicators are designed in accordance with the standard Nuplex 80+ discrete indicators described in Section 18.7.1.4.

The Process-CCS operators modules provide access to all Process-CCS controls and indication. These features are used in the event of failure of any discrete controls or process controllers located on other control room panels. (See Section 7.7 for details).

B and C channelized pushbutton switches are located on the panel for manual initiation of reactor trip and interface with their respective ESF actuation signals. Pushbutton switches A and D are located on the Plant Monitoring and Control Panel of the Master Control Console.

A single safety grade channel is provided as a backup (via Diverse Manual ESF Actuation Switches) to ESF actuation via the ESF-CCS and PPS. These switches provide for system level actuation of two trains of safety injection, and one train each of containment spray, feedwater, closure of main steam isolation valves, closure of containment air purge valves, and closure of a letdown isolation valve (See Section 7.3).

A radiation monitoring module is located on the panel. It is part of the radiation monitoring system and is used to monitor the radiation levels in and out of the plant.

An ESF status monitoring module is located on the panel. This module displays high level indication of abnormalities in ESF performance and ESF availability. This function is described in Section 18.7.1.8 and the module is shown in Figure 18.7.1-12.

The alarm tiles display alarms associated with the performance of the PPS, CPC, and CCS. In addition, the alarm tiles display the Critical Function alarms, the radiation monitoring alarms, and the ESF performance and inoperability alarms.

The ~~CRT~~ DPS VDU provides direct access to the DPS.

Control identification, symbology and color, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.6 Engineered Safety Features Panel

The Engineered Safety Features (ESF) Panel contains those controls and indications that are required for the control and monitoring of the following safety related systems:

A. Shutdown Cooling

B. Emergency Feedwater/Atmospheric Dump

C. Safety Depressurization

D. Safety Injection Tanks

E. Safety Injection

F. Containment Spray

G. Cavity Flood

In addition, indications are continuously available to allow the operator to assess the status of Containment Isolation and Steam/Feedwater Isolation to each steam generator. The controls and indications provided are consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel. The systems whose component controls are mounted on this panel, are safety-related systems. Discrete Indication displays are provided with each of the functional groups to monitor the system/equipment performance associated with the group. The safety systems on the ESF panel support Plant Safety Function (e.g., Emergency Feedwater supports RCS heat removal via the steam generators). The effect that a safety system has on a plant safety function is monitored on this panel's ~~CRT~~, IPSO or the Safety Monitoring Panel, which is directly to the left of the ESF Panel. DAS VDU

The controls and indications on the ESF panel are broken down into functional groups as follows (see Figure 18.7.4-6):

A. Shutdown Cooling

Each of 2 shutdown cooling trains is layed-out on the panel using a system flow path mimic arrangement. A discrete indicator is provided for monitoring shutdown cooling process parameters.

B. Emergency Feedwater/Atmospheric Dump

Each of 2 emergency feedwater trains and atmospheric dump valves is layed-out on the panel using a system flow path mimic arrangement. A discrete indicator is provided for monitoring emergency feedwater process and steam generator parameters. Two process controllers are provided for control functions associated with steam supply to the steam-driven pumps and feedwater flow control. Switches provide control of the atmospheric dump valves.

C. Safety Injection/Safety Injection Tanks

Each safety injection train and safety injection tank is arranged on the panel using a system flow path mimic layout. Discrete Indication is provided for monitoring the parameters associated with these systems.

D. Containment Spray

Each of the containment spray trains and associated component controls are layed-out on the panel using a system flow path mimic arrangement. Discrete indication is provided for containment spray related parameters.

E. Safety Depressurization

Safety depressurization component controls are provided for Pressurizer and Reactor Vessel depressurization in a single location.

F. Containment Isolation

Containment isolation valves functional group control and indication, providing continuous display of containment isolation status and performance, exist at one location on the ESF panel. The controls for these valves are also distributed throughout the control panels in their appropriate flowpaths. The ESF panel provides a second source of valve indication and close only control.

G. Cavity Flood

Cavity flood component controls are provided for to accommodate cavity flood during a severe accident.

I. In-Containment Refueling Water Tank component controls are provided to accommodate operation of (IRWST) components.

Process controllers, which are mounted on the ESF Panel, are designed in a consistent manner as other Nuplex 80+ process controllers, as discussed in RCS panel description (Section 18.7.3.2.2).

Discrete indicators provide display of those parameters associated with each ESF system that provide overview indication of system performance. In addition, these indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ displays. The DIAS also provides the alarms associated with the systems. The DPS panel mounted ~~CRT~~ provides general monitoring, system/component level and detail/diagnostic information on the ESF systems in a manner consistent with RCS panel design (Section 18.7.3).

VDU
VDU

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description (Section 18.7.3).

18.7.4.7 Cooling Water Panel

The Cooling Water Panel contains those controls and indications that are required for control and monitoring of the Ultimate Heat Sink (UHS), Station Service Water System (SSWS) and Component Cooling Water System (CCWS) non-safety cooling water systems. The CCWS has safety-related and non-safety-related subsystems.

The controls and indications provided are consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel.

The component controls associated with each cooling water system are layed out on the panel using a system flowpath mimic format. The panel is divided into functional groups pertaining to Component Cooling Water and Station Service Water/Ultimate Heat Sink System. The functional layout of the Cooling Water panel is exemplified by Figure 18.7.4-7.

Process controllers, which are mounted on the Cooling Water Panel, are designed in a consistent manner as other process controllers which are covered in Section 18.7.1.7, Process Controllers.

The DIAS provides display of those parameters associated with the Cooling Systems to provide overview indication of system performance. In addition, these indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ VDU displays. The DIAS also presents alarms associated with the cooling water systems. The DPS panel mounted ~~CRT~~ VDU provides general monitoring, system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3).

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.8 Secondary Cycle Panel

The Secondary Cycle Panel has those systems required for control and monitoring of feedwater and condensate, turbine, auxiliaries, excitations and other miscellaneous secondary support systems. These systems are required to be operated infrequently during normal operation, or are required to be operated only during plant startup, shutdown, or testing. The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel. The systems whose components are mounted on this panel are not required for plant safety; however, the discrete indicator displays contain instrument channels, such as for steam generator (SG) 1 and 2 level, which may be utilized for post-accident monitoring. The display of these instruments on this panel is provided as operator convenience following the standard Nuplex 80+ information display philosophy that instruments used normally are also used during accident conditions. Non-safety and PAMI displays for SG 1 and 2 level and other parameters are also provided on the Feedwater and Condensate Panel on the MC and Engineered Safety Features Panel of the Safety Console.

The DIAS provides display of those parameters associated with the secondary cycle that provide overview indication of system performance. In addition, these indicators provide overview indication of system performance. In addition, these indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ displays. The DIAS also presents alarms associated with the Secondary Cycle systems. The DPS panel mounted ~~CRT~~ provides general monitoring, system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3).

VDU

VDU

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.9 Electrical Distribution Panel

The Electrical Distribution Panel has those systems which provide control and monitoring of the auxiliary power distribution, the emergency diesel generators and alternate AC power source. The controls and indications on this panel require infrequent monitoring or operation by the operator during normal plant operation. The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel. The emergency diesel generators and the auxiliary power distribution are Class 1E systems serving electrical trains A and B which are required for plant safety. The Alternate AC Power Source is not a safety-related system.

The controls and indication on this panel are broken down into functional groups (exemplified on Figure 18.7.4-9).

A. Auxiliary Power Distribution

   Contains those controls and indication associated with the onsite distribution of the major normal and emergency power.

B. Alternate AC Source

   Contains those controls and indications for controlling and monitoring the plant specific alternative AC power supply.

C. Diesel Generator 1

   Contains those controls and indications for controlling emergency diesel generator for train A electrical busses.

D. Diesel Generator 2

   Same as diesel generator 1, except generator 2 serves train B electrical buses.

Individual synchroscopes are mounted in the diesel generator and the alternate AC source functional groups. This is a departure from the Nuplex 80+ standard indication and monitoring techniques. The approach of using standard, commercially available synchroscopes is necessary, because the Nuplex 80+ discrete indicator and ~~CRT~~ technology is not technically appropriate for this application. This results from the real-time concerns associated with developing a synchroscope utilizing multiplexed inputs and outputs.

The DIAS provides display of those parameters associated with the emergency power sources and site electrical distribution and provides overview indication of system performance. In addition, those indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ displays. The DIAS also provides the alarms associated with the above systems. The DPS panel mounted ~~CRT~~ provides general monitoring, system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3.2.1).

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.10 Switchyard Panel

The Switchyard Panel has those systems required for control and monitoring or the main generator and site power connections to the electrical grid. These are required to be operated infrequently during normal operation or are used only during plant startup, shutdown, or testing. The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions, as exemplified by the RCS panel. The systems whose components are mounted on this panel are not required for plant safety.

The controls and indications on this panel are broken down into functional groups (exemplified on Figure 18.7.4-10):

A. Generator Excitation

Contains those controls and indication associated with the electrical excitation and control of the main generator (e.g., manual voltage regulation, generator field and exciter breaker controls).

B. Generator Auxiliaries

Contains miscellaneous component controls associated with the generator (e.g., main seal oil pump, stator coolant pumps).

C. Hydrogen Supply

Contains the controls associated with the hydrogen cooling gas supply to the main generator.

D. Core Monitor

Is a vendor supplied insert used for monitoring various parameters of the generator (e.g., temperatures within various stator locations).

E. Switchyard

Contains the controls and indications for the various breakers connecting the site and main generator to the electrical grid.

An individual synchroscope is mounted in the Generator Excitations functional group. This is a departure from the Nuplex 80+ standard indications and monitoring techniques. This approach of using a standard commercially available synchroscope is necessary, because the Nuplex 80+ discrete indicator and ~~CRT~~ DPS DISPLAY technology is not technically appropriate for this application. This results from the real-time concerns associated with developing a synchroscope utilizing multiplexed inputs and outputs.

Space provisions are made on the panel section for a handset for operator communications with the load dispatcher.

The DIAS provides display of those parameters associated with the main generator and switchyard electrical that provide overview indication of system performance. In addition, those indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ displays. The DIAS also VDU provides the alarms associated with the switchyard systems. The DPS panel, mounted ~~CRT~~ provides general monitoring, system/ VDU system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3.2.1).

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.11 Heating, Ventilation, and Air Conditioning Panel

The Heating, Ventilation, and Air Conditioning (HVAC) Panel contains those controls and indications that are required for monitoring and control of System 80+ HVAC systems. The controls and indications on this panel are broken into functional groups (exemplified on Figure 18.7.4-11):

A. Nuclear Annex Ventilation

B. Control Complex Ventilation

C. Fuel Building Ventilation

D. Diesel Building Ventilation

E. Annulus Ventilation

F. Containment Cooling & Ventilation

G. Turbine Building Ventilation

H. Station Service Water Pump Structure Ventilation

I. Radwaste Building Ventilation

The controls and indications provided are consistent with Nuplex 80+ standard techniques and conventions as exemplified by the RCS panel. HVAC systems A, B, C, D, and H above as well as the Containment Isolation Functions associated with HVAC systems E, and F above are safety-related. The remainder of the HVAC indications and controls are not related to safety.

Process control modules, which are mounted on the HVAC Panel, are designed in a consistent manner, as other process control modules, which are covered in RCS panel description (Section 18.7.3.2.2).

The DIAS provides display of those parameters associated with the HVAC systems that provide overview indication of system performance. In addition, these indicators provide access to all information required for continued plant operation after loss of the ~~Data~~ DPS ~~CRT~~ displays. The DIAS also provides the alarms associated with the HVAC systems. The DPS panel mounted ~~CRT~~ provides general monitoring, system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3.2.1).

Control identification, symbology and hue, along with functional grouping control and indication, group demarcation and labeling, are in accordance with panel layout Nuplex 80+ criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.12 Fire Protection Panel

The Fire Protection Panel contains those controls and indications that are required to:

A. Alert the operator to the existence of fires.

B. Monitor the performance of fire protection equipment.

C. Provide manual back up for the automatic fire suppression systems.

The controls and indications are provided consistent with Nuplex 80+ standard techniques and conventions, as exemplified on the RCS panel.

The controls and indications associated with the fire protection panel are grouped into functional groups (exemplified on Figure 18.7.4-12):

A. Fire Protection water supply source, pumps, and headers.

B. Nuclear Annex fire protection equipment.

C. Administration, Service Office building, and other buildings and structures outside the Nuclear Island fire protection equipment.

D. Plant exterior area fire protection equipment.

E. Turbine area fire protection equipment.

F. Diesel area fire protection equipment.

The DIAS provides display of those parameters associated with the Fire Protection systems that provide overview indication of system performance. In addition, these indicators provide access to all information required for continued plant operation after loss of the DPS ~~CRT~~ displays. The DIAS also provides the alarms associated with the fire protection systems. DIAS alarm tiles, located on the upper panel section, are provided to notify the operator of the existence of fires within the plant. The DPS panel mounted ~~CRT~~ provides general monitoring, system/component level and detail/diagnostic information on the systems in a manner consistent with RCS panel design (Section 18.7.3.2.1).

VDU

VDU

Control identification, symbology and hue, along with functional grouping of control and indication, group demarcation and labeling, are in accordance with Nuplex 80+ panel layout criteria (Section 18.7.2) and exemplified by the RCS panel description.

18.7.4.13 [Deleted]

18.7.4.14 Control Room Supervisors Console

The Control Room Supervisors (CRS) Console and Desk provide a workstation from which the Control room supervision can coordinate and monitor plant operations. The SROs workstation is made up of two sections, the CRS Console, and CRS Desk, as exemplified in Figures 18.7.4-13 and 18.7.4-14.

The CRS Console sections allows the CRS to face into the controlling workspace and view the IPSO, MCC and ACSC panels. In addition, the console has two DPS ~~CRTs~~ VDUs to allow the CRS to access plant information. The DPS ~~CRT~~ DISPLAY pages are the same format as utilized throughout the Nuplex 80+ Advanced Control Complex, and have the same capabilities (e.g., alarm acknowledgement via touch targets). In addition, a keyboard is provided to allow data entry by the CRS that may be time consuming with the touch screens.

Provision is made on the console for providing various communication interfaces, which the CRS needs to access (e.g., paging system, intercom, sound powered and the phone circuits).

The following communication features are provided on the CRS console:

A. Intra-plant System Telephones

These telephones provide independent communication throughout the plant and plant site. To ensure its functional operability, a switching feature is provided to allow switchover to redundant circuit electronics, controls, and power supplies. Emergency power is provided from a standby diesel generator, which will automatically start and accept load should normal power be lost.

B. Intra-plant Public Address Telephones

These telephones provide two independent channels of communications throughout the plant and plant site. These independent channels are page and part line. The page channel provides communications over loud speakers with integral amplifiers. Page channel speaker-amplifiers are ring-wired to preclude loss of system function in the event of a single cable failure. Paging is accomplished via the use of either dedicated PA party-line handsets, or via the use of Inter-plant telephone handsets. The connection between the Inter-plant and PA systems is through an isolation device to preserve the independence of the two systems.

C. Intra-plant Sound-powered Telephones

Intra-plant sound-powered telephones, independent of the Inter-plant and PA systems, are provided on the communications panel to provide the following communications during normal and abnormal/accident conditions:

Additional communication features are provided at other panel locations within the control room to allow operations personnel to communicate with maintenance, auxiliary operations, and administrative personnel.

Storage provisions are made at the console in two forms:

A. Drawers - located under the DPS ~~CRT~~ sections. VDU

B. Bookcases - located in the lower section of the console and accessible from the controlling workspace.

Sufficient desk space has been provided at the console to allow the CRS to layout procedures and paperwork, as maybe required in his plant monitoring activities. These features are shown on Figure 18.7.4-13.

By swiveling his chair around, the CRS is facing the desk section of his workstation. This desk is used by the CRS as laydown space and to interface with maintenance and other personnel, while limiting their access to the controlling workspace. Storage space in the form of drawers and bookcases are also provided at this desk. The CRS design is shown in Figure 18.7.4-14.

The arrangement of the CRS workspace provides sufficient space for two persons to utilize the DPS ~~CRTs~~ for information access without overcrowding. VDUs

18.8 CONTROL & MONITORING OUTSIDE THE MAIN CONTROL ROOM

18.8.1 REMOTE SHUTDOWN PANEL

18.8.1.1 Design Description

The Remote Shutdown Panel (RSP) is designed to provide an alternate control station which can be used to shutdown the plant in the unlikely event that the main control room becomes uninhabitable. [Sufficient safety grade instrumentation and controls are provided to perform the following operations:

A. Achieve prompt hot shutdown of the reactor, subsequently referred to as hot standby per standard technical specifications (reactor subcritical at operating pressure and temperature).

T2*

B. Maintain the unit in a safe condition during hot standby.

C. Achieve and maintain cold shutdown of the reactor from the RSP.

Damage to equipment in the control room does not preclude operation of any required equipment at the RSP and a single failure in an active safety train does not preclude a safe plant shutdown from being accomplished.]

The Nuplex 80+ design provides switches near each MCR exit for transfer of control from the MCR to the RSR. See Section 7.4.1.1.10 for additional detail on transfer of control.

The RSP design is based on the standard Nuplex 80+ indication and control methodologies, discussed in Section 18.7.1. It applies, the human factor design criteria described in Section 18.7.2, in a manner consistent with the RCS panel design (Section 18.7.3). Although it implements many of the same features as incorporated in the RCS panel, some specific features address the RSP's unique function and its' qualification as a safety system.

The Nuplex 80+ remote shutdown panel includes all divisions of safe shutdown controls (as indicated in Table 7.4-1 of Section 7.4.2.5), each isolated from the main control panels. Sufficient information is provided for each safe shutdown system to maintain hot standby. The man-machine interface for this instrumentation is consistent with the main control room. The Nuplex 80+ RSP also provides indication and control for the normal control system used for maintaining hot standby. The RSP instrumentation provides centralized controls and indications necessary for achieving cold shutdown. Sufficient communications and indications exist to achieve and maintain cold shutdown using suitable procedures and local control stations. The indication and control at the Nuplex 80+ RSP are physically separated and electrically isolated from the Nuplex 80+ main control room.

The RSP provides controls for plant shutdown operations using either normal systems or safe shutdown systems. The safety grade controls required for achieving and maintaining hot shutdown are identical to those used in the main control room. Also, control of normal process control systems that provide significant benefit to operator convenience in achieving and maintaining hot standby are identical to those in the main control room.

Control of other safety systems and normal components are performed at the RSP using a Component Control System (CCS) operator's module or a Plant Protection System (PPS) operator's module. One CCS operator's module is provided for each safety channel and for each normal control channel. Also, one PPS operator's module is provided for each safety channel. These CCS and PPS operator's modules are the same as those located on the Safety Monitoring Panel and described in Section 18.7.4.5.

Section 7.4.2.5, Table 7.4-1 lists the controls and instrumentation to be provided on the RSP.

18.8.1.2 Functional Grouping and Panel Layout

The RSP design applies the same criteria for human engineering and for information display and control allocation as used for the main control room. It is a sitdown panel similar to the MCC in the main control room (see Figure 18.6.5-11) with a hierarchy of alarms, indications and controls consistent with that used at the master control console. The instrumentation and controls are grouped according to their functional roles supporting the operations to be performed at the RSP, with a similar left to right orientation as the MCC.

Figure 18.8-1 typifies the panel configuration. A central panel is flanked by two wings. The left wing provides controls and indications for the primary systems controlling RCS inventory and pressure and PPS operator's modules. The significant normal controls are inboard on the panel, while the associated safety system controls are located farther out on the left.

The right wing provides controls and indications for the secondary systems controlling RCS heat removal. The normal controls for feedwater flow and steam release are inboard on the panel. The safety system controls for emergency feedwater, main steam isolation and atmospheric dump valves are located farther out on the right.

Alarm tiles are provided in the upper section of each wing, consistent with the master control console design. Alarm tiles are provided for significant alarms related to operations to be performed on the RSP. These are discussed in Section 18.8.1.4. Other alarms are provided through the ~~CRT~~ using the Data Processing System in the same manner as in the main control room. DPS VDU

The central panel contains the ~~CRT~~ and ESF-CCS operator's modules which are used to augment the dedicated indication and controls on each wing panel. One operator's module is provided for each of the four ESF-CCS safety channels. They access the component control system for safety grade controls not included in the dedicated controls. An additional operator's module is available for each of the two normal control channels. Reactor trip push buttons are also provided on this panel. These provide access to the component control system for all normal controls. DPS VDU

The operator's modules provide displays and system controls in the same format as the operator's modules provided in the main control room at the Engineered Safety Features panel. The ~~CRT~~ provides the same display system as available in the main control room. DPS VDU

18.8.1.3 Additional Features Specific to the RSP

The lower section of the center panel provides an open area for spreading procedure documents. It also provides a phone for communication to operators located at local component control stations.

18.8.1.4 Dedicated Alarm Tiles on the RSP

The dedicated alarm tiles selected for the RSP are a subset of those used in the main control room. Alarms are selected only if they are pertinent to carrying out the operations for which the RSP is designed. Specifically, these are operations associated with achieving and maintaining hot standby or cold shutdown, with the assumption that a reactor trip is performed prior to control room evacuation.

The RSP alarm requirements will be identified as part of the Functional Task Analysis and detailed panel design.

18.9 VERIFICATION AND VALIDATION

The verification and validation of the Nuplex 80+ human system interface demonstrates operator task performance capabilities and the capabilities to perform operator functions in the control room. All Nuplex 80+ verification and validation activities are performed under the conditions specified in the Human Factors Engineering Verification and Validation Plan (Section 18.4, Reference 3).

The Human Factors Engineering (HFE) Verification and Validation Plan for Nuplex 80+ describes how the HFE verification and validation is managed, administered, and performed. Additionally, the verification and validation analysis criteria, methodology, required resources (e.g. Emergency ~~Procedure~~ Operations Guidelines, normal and abnormal operating sequences, I&C design requirements, HSI hardware, etc.), schedule for activities, and milestones are provided. Specifically, the HFE Verification and Validation Plan meets the design process requirements and criteria for availability verification, suitability verification, and validation of the ensemble as defined in Sections A-3.6, A-3.7, and A-3.8 of the HFE Program Plan (Section 18.4, Reference 4).

The HFE V&V Plan applies to all Human System Interface (HSI) and workspace environment in the Main Control Room (MCR), Remote Shutdown Room (RSR) and those control stations specified in the Emergency ~~Procedure~~ Operations Guidelines ~~(EPG)~~ EOG.

There are three distinct types of verification and validation activities: 1) Availability Verification, 2) Suitability Verification, and 3) Validation.

18.9.1 AVAILABILITY VERIFICATION

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

The purpose of Phase 1 (Availability Analysis) is to assure the following:

1. System I&C Inventory meet the following requirements:

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

   b. Federally mandated indication and control requirements and,

   c. Fixed position MCR HSI is provided for credited safety function success path tasks identified in the Probabilistic Risk Assessment (PRA) and ~~EPG~~ EOG.

ATTACHMENT 4

TABLE 1.6-1

Remove from all pages

(Sheet 7 of 7)

REFERENCED MATERIAL PREVIOUSLY SUBMITTED

Topical Report No.	Title
LD-93-080	Common Mode Failure Evaluation for Limiting Fault Events, May 1993
NPX80-IC-RR790-01, Rev. ~~0~~ 01	Operating Experience Review for System 80+ MMI Design, LD-93-090, June 1993
NPX80-IC-VP790-03, Rev. ~~0~~ 02	Human Factors Engineering Verification and Validation Plan for NUPLEX 80+, ~~February 1994~~ October, 1994.
NPX80-IC-~~RR~~DP790-01, Rev. ~~3~~ 04	Human Factors Program Plan for the System 80+ Standard Plant Design, ~~February 1994~~ October, 1994.
LD-94-012, Rev. 02	System 80+ Fire Hazards Analysis, August 1993
NPX80-IC-RR790-02, Rev. ~~0~~ 02	Human Factors Evaluation and Allocation of System 80+ Functions, March 1994
NPX80-IC-DB790-01, Rev. 01	NUPLEX 80+ Advanced Control Room Complex Design Bases, September 1994
NPX-TE-790-01	NUPLEX 80+ Verification Analysis Report, April 1992
NPX80-IC-DP790-02, Rev. 01	System 80+ Function & Task Analysis Report, April 1989
NPX80-IC-DP790-03, Rev. 01	Functional Task Analysis Plan, November 1993
NPX80-SQP-0101.0, Rev. 02	Software Program Manual for NUPLEX 80+, February 1994
NPX80-IC-QP790-2	NUPLEX 80+ Software Safety Plan Description, January 1993
NPX~~-~~IC-QG790-00, Rev. ~~01~~ 02	Qualification Guidelines for Instrumentation and Controls Equipment for NUPLEX 80+, ~~February 1994~~ October, 1994.
NPX80-QPS-0401.1 Rev. 01	Requirements for the Supply of Commercial Digital Computer Hardware and Software Components to be used in NUPLEX 80+ Safety Systems, ~~April 1992~~ October, 1994.

REQUIREMENTS FOR THE SUPPLY

OF

COMMERCIAL DIGITAL COMPUTER HARDWARE AND SOFTWARE COMPONENTS

TO BE USED IN

NUPLEX 80+™ SAFETY SYSTEMS

NPX80-QPS-0401.1

Revision ~~00~~ 01

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

This document is the property of ABB Combustion Engineering, Inc. (C-E), Windsor, Connecticut, and is to be used only for the purposes of the agreement with C-E pursuant to which it is furnished.

Prepared by M. S. Novak Date 5-7-92
~~M. S. Novak, Supervisor, Process Information Systems~~ J.K. [illegible]

Reviewed by M. S. Novak

Approved by K. Scarola Date 5-7-92
~~K. Scarola, Manager, Advanced I&C Engineering~~
W J Gill [illegible] Engineering Manager

Approved by J. P. Pasquenza Date 5-7-92
J. P. Pasquenza, Director, Quality Assurance

Issue Date May 7, 1992

RECORD OF REVISIONS

NO.	DATE	PAGES INVOLVED	PREPARED BY	APPROVALS
00	May 7, 1992	All	M. S. Novak	K. Scarola J. P. Pasquenza
01		3, 5, 18, 19	J. K. McNally	

01 all pp

TABLE OF CONTENTS

1. **Purpose** 4
2. **Scope** 5
3. **References** 5
4. **Manufacturer Controls for Computer Hardware Components** 6
   - 4.1 Component Service 6
   - 4.2 Identical Components 6
   - 4.3 Component Identification 6
   - 4.4 Documentation Control 7
   - 4.5 Reproduction of Documentation 7
   - 4.6 Hardware Testing 7
   - 4.7 Problem Reporting 8
   - 4.8 Notification of Manufacturer Changes 9
   - 4.9 Replacement or Repair 10
5. **Manufacturer Controls for Computer Software Components** 11
   - 5.1 Component Service 11
   - 5.2 Identical Software Media 11
   - 5.3 Software Version Control 11
   - 5.4 Software Virus Protection 12
   - 5.5 Documentation Control 12
   - 5.6 Reproduction of Software and Documentation 12
   - 5.7 Software Development Process 12
   - 5.8 Software Testing 13
   - 5.9 Software Problem Reporting 14
   - 5.10 Manufacturer Software Change Control 15
   - 5.11 Discontinuation of Support 15
6. **Administrative Requirements** 16
   - 6.1 Right of Access 16
   - 6.2 Stop Work Authority 16
   - 6.3 Document Submittal (RAR) 16
   - 6.4 Deviation from Contract Requirements (DCR) 16
   - 6.5 Technical Change Request (TCR) 16
   - 6.6 Certificate of Conformance (CofC) 17
   - 6.7 English Language 17

2 USNRC Restrictions on Revisions to the Commercial 10 Dedication Program

1. Purpose

In order for ABB Combustion Engineering Nuclear Systems (CENSYS) to produce nuclear safety systems, CENSYS procures some commercial grade items that will be employed in these systems. Since these items may not generally conform to nuclear industry safety related standards, CENSYS performs a process on these components called dedication, which upgrades these components to the extent required for the safety application. Sections 4 and 5 of this document provide requirements that are imposed on commercial grade component manufacturers in order that procured computer hardware or software can be accepted into a dedication program for Nuplex 80+™. For the purposes of this document, a component is any individually procurable item, including hardware, software and services.

When CENSYS dedicates components, additional seismic, environmental and system qualification, type testing, and software verification and validation is generally performed, beyond that which is performed by the manufacturer. In general, CENSYS only tests one of each component. The goals of this program are to assure that:

- the Nth component supplied on the same order is identical to the unit(s) tested;
- failed components are repaired or replaced such that they are identical to the original components;
- additional components that are supplied, subsequent to the initial order, are identical to the tested components;
- additional components, as may be required for the same or a new project, can be procured, subsequent to the initial order, that are identical to the tested components.

The degree to which a component must be identical and the term of manufacturers' commitments to produce identical components are discussed in this document. The requirements in this document are to assure that:

- the overall qualification performed by CENSYS is not compromised by variations or changes in the supply or subsequent replacement of the components by the manufacturer;
- problems with the supplied products are reported to CENSYS.

The manufacturer's non-compliance with requirements in this document may invalidate the qualification to be performed by CENSYS, and/or previously qualified systems may require requalification. Therefore, the manufacturer may not deviate from these requirements without written authorization from CENSYS. To obtain such authorization, the manufacturer may be required to

submit information needed by CENSYS to determine that the cost or quality of the system produced by CENSYS is not adversely impacted by the authorization.

2. Scope

This document applies to commercial, non-safety computer hardware and software components that are procured for dedication to nuclear safety systems in Nuplex 80+™ and related devices such as power supplies, input/output modules, and data communications modules. Sections 4 and 5 of this document define requirements that must be met by manufacturers of these components, before and after shipment to CENSYS.

In order to utilize a commercial grade component in a nuclear safety application, CENSYS performs a dedication process in three phases:

(1) A technical evaluation of the commercial grade component, based on requirements in this document and other specific requirements developed for the target application;

(2) Following procurement, an acceptance process is conducted, verifying that the received components meet the requirements in this document and other requirements of the order developed specifically for the component to be dedicated.

(3) Additional modifications, testing, analysis and controls are performed as needed for the specific nuclear safety application.

This document does not address the CENSYS portion of the above three phases. For software components, generic requirements are specified in the Nuplex 80+™ Software ~~Quality Assurance~~ Program Manual (reference 3.1). Hardware requirements and any additional software requirements for this process are developed for each specific target application, and are specified in separate design documents.

3. References

3.1 ~~Software Quality Assurance Program~~ for Nuplex 80+™ ~~Systems, NPX80-IC-QP790-01~~ Software Program Manual, NPX80-SQP-0101.0

3.2 Request for Approval or Review (RAR) form

3.3 Deviation from Contract Requirements (DCR) form

3.4 Technical Change Request (TCR) form

3.5 Certificate of Conformance (CofC) form

4. Manufacturer Controls for Computer Hardware Components

4.1 Component Service

Supplier shall provide evidence that the component has been in service by the supplier for at least 3,000 operating years and at least one calendar year.

4.2 Identical Components

The manufacturer shall assure that components provided for a single dedication program are identical, except for changes specifically authorized in writing by CENSYS. To be considered identical, components must consist of identical subcomponents from the original subsuppliers, and the processing, manufacturing and assembly by the manufacturer must not be different from component to component.

The manufacturer shall submit a TCR form (see section 6.5) describing each change to be authorized by CENSYS.

The manufacturer must provide evidence of an internal QA program that assures components provided are identical. The components may be spread over several orders and over a period of time identified in the initial order.

The manufacturer shall provide CENSYS a controlled copy of the QA program and a list showing each part and its subsupplier. If any part has more than one potential subsupplier, or if the subsupplier changes, the manufacturer shall provide a TCR form with information sufficient for CENSYS to determine if the CENSYS qualification is invalidated or questionable by differences between components. CENSYS shall have the right to disapprove multiple suppliers or supplier changes unless CENSYS determines that the qualification remains valid.

4.3 Component Identification

Identical components must be marked with the same version, batch and/or part number assigned by the manufacturer. This number must be different for components that are not identical. Additionally, each shipped component must be marked with a unique serial number or identifier.

Passive components (cables, connectors, etc.) do not require the above identification markings as long as the component is clearly identifiable through inspection or measurement performed by CENSYS.

4.4 Documentation Control

Documentation that is supplied shall correspond to the version or batch of the supplied components. The version or part number, as marked on the components, shall be marked on the documentation.

All documentation shall be submitted for CENSYS approval using the RAR form (see section 6.3).

4.5 Reproduction of Documentation

The manufacturer shall assure that, for at least ten years after initial product delivery, the originally supplied version of the documentation can be supplied as needed at the original quality. The manufacturer may discontinue production of the documentation before the ten year period is elapsed if

- one year advance written notification is given to CENSYS

-and-

- CENSYS has non-exclusive rights to reproduce the original documentation.

4.6 Hardware Testing

The manufacturer shall provide evidence that a formal, first of a kind hardware testing program has been performed on hardware similar to that supplied for a dedication program. The manufacturer shall identify which of the manufacturer's published specifications are also reverified during Nth of a kind manufacturing testing. The manufacturer shall identify its use of the following types of testing techniques:

- diagnostics
- performance testing
- environmental testing
- functional testing
- noise and hazard testing

The manufacturer shall make all testing records available to CENSYS for evaluation.

4.7 Problem Reporting

The manufacturer shall have a procedure in place which is available to all customers for reporting problems to the manufacturer. The problems may be specific to a component or generic to the design. The manufacturer shall maintain records of all reported problems from all sources, including problems reported by the manufacturer, subsuppliers and from other customers.

Within three months after a problem is reported to the manufacturer, the manufacturer shall determine if the problem is applicable to components supplied to CENSYS. If the problem is applicable, the manufacturer will identify the problem to CENSYS, along with either

- the resolution of the problem;

- or -

- the status and schedule of the manufacturer's effort to resolve the problem; to be updated monthly until the problem is resolved.

- or -

- the manufacturer's justification for not resolving the problem, subject to CENSYS approval. The manufacturer shall submit the justification using the RAR form (see section 6.3).

The manufacturer shall identify the procedure followed in its organization to support timely record keeping and correction of problems through 10 years after initial product delivery for a contract (excluding spare parts).

CENSYS will be responsible for determining the nuclear safety significance (if any) of the problem and its application within the CENSYS systems. CENSYS will be responsible for reporting any significant nuclear safety problem to the appropriate licensing authorities. This assignment of responsibility to CENSYS does not prevent the manufacturer from making its own assessment or report to a licensing authority.

4.8 Notification of Manufacturer Changes

Manufacturer must maintain records of changes, such as Engineering Change Orders (ECOs) that are applicable to any shipped component. These records must identify specific shipped components and which ECOs have been and have not been implemented. ECOs must be distinguishable, as in the following example:

- Safety hazard (Personnel, UL) correction
- Design fault correction
- Design improvement or product modification

Through 10 years after initial product delivery, CENSYS must be notified of any safety hazard or design fault corrections that have not been implemented in components after shipment.

On new orders, replacements or repairs, the manufacturer shall supply any components with the same ECOs as the original components. Other ECOs may only be incorporated if

- the manufacturer has provided sufficient information to CENSYS to evaluate the impact of the specific ECOs on CENSYS qualification;

- and -

- CENSYS has determined that the impact on the CENSYS qualification is acceptable and has notified the manufacturer in writing.

The manufacturer shall submit a TCR form (see section 6.5) describing each change to be authorized by CENSYS.

4.9 Replacement or Repair

Through 10 years after initial product delivery, the manufacturer must be able to either repair or replace (manufacturer's discretion) failed components, maintaining them identical to the original shipped, unless specific changes requested by the manufacturer are submitted under TCR (see section 6.5) and approved by CENSYS in advance. The manufacturer shall make its technical records and evaluations available to CENSYS as required to support the approval process.

Concurrent with initial product delivery, the supplier shall escrow (store a copy of) its design documentation of the product with an independent agency. Following the minimum period of ten years after shipment of the component, the manufacturer may, at its own option, cease identical component repair or replacement with one year notification and release of escrowed design documentation to CENSYS. At CENSYS's option, all manufacturer's fabrication plans shall be provided to CENSYS, and CENSYS shall be authorized to use such plans to allow another manufacturer to produce or repair identical components.

The escrowed design documentation will also be immediately released to CENSYS if the manufacturer is unable to fulfill any requirements in this document without CENSYS authorization.

5. Manufacturer Controls for Computer Software Components

5.1 Component Service

Supplier shall provide evidence that the component has been in service by the supplier for at least 3,000 operating years and at least one calendar year.

5.2 Identical Software Media

Manufacturer must be able to assure that multiple copies of software (or firmware) provided for a dedication program are identical to the originally delivered product.

Two software media (disks, tapes, PROMS) are considered identical if

- the media type is the same;

-and-

- the byte in each logical location is the same in both media.

In file oriented media where the physical characteristics of the media are not important, two media are considered identical if the directory and file contents are the same and all files compare byte-for-byte to be the same.

5.3 Software Version Control

All software magnetic media (disks, tapes, PROMS) shall identify the software contained on it according to the manufacturer's version numbering scheme.

Two software media may be assigned the same version number only if they are identical.

The manufacturer shall provide evidence that the configuration control used by manufacturer assures that only identical software is assigned the same version number.

Additionally, each software media item must be marked with a unique serial number or identifier.

5.4 Software Virus Protection

The manufacturer shall assure that the delivered software is virus-free by all of the following practices:

- Software that is of questionable origin (e.g. shareware) is not used in the deliverable software, or in its development and testing.
- Access to the manufacturer's deliverable, development or testing systems is secure and limited to the manufacturer's personnel.
- The manufacturer permits its deliverable, development or testing systems to be interconnected only with systems that are approved by and controlled by the manufacturer.
- For software media where virus protection programs are available, the software is checked using two such programs before shipment.

5.5 Documentation Control

Computer software documentation that is supplied shall correspond to the version or batch of the supplied media. The version or batch number, as marked on the media, shall be marked on the documentation.

All documentation shall be supplied under RAR (see section 6.3) and subject to CENSYS approval.

5.6 Reproduction of Software and Documentation

The manufacturer shall assure that, for at least ten years after initial product delivery, this version of the software and documentation can be supplied as needed at the original quality. The manufacturer may discontinue production of the documentation before the ten year period has elapsed if

- one year advance written notification is given to CENSYS

-and-

- CENSYS has non-exclusive rights to reproduce the original documentation.

5.7 Software Development Process

The manufacturer shall demonstrate that the software has been developed using a quality assurance program that assures conformance with original design requirements. These QA methods must include the identification and tracking of errors during development.

5.8 Software Testing

The manufacturer shall demonstrate that a formal, software testing program has been applied to all software supplied for a dedication program. The manufacturer shall identify its reliance on the following types of testing techniques:

- code inspections
- incremental testing
- functional testing
- system testing
- beta testing

The manufacturer shall make all testing records available for CENSYS's inspection at the manufacturer's facility.

5.9 Software Problem Reporting

The manufacturer shall have a procedure in place which is available to all customers for reporting problems to the manufacturer. The problems may be specific to a software component or generic to the design. The manufacturer shall maintain records of all reported problems from all sources, including problems reported by the manufacturer, subsuppliers and from other customers. The manufacturer shall maintain such records for a period of 10 years after initial product delivery to CENSYS.

Within three months after a problem is reported to the manufacturer, the manufacturer shall determine if the problem is applicable to software components supplied to CENSYS. If the problem is applicable, the manufacturer will identify the problem to CENSYS, along with either

- the resolution of the problem;

- or -

- the status and schedule of the manufacturer's effort to resolve the problem; to be updated monthly until the problem is resolved.

- or -

- the manufacturer's justification for not resolving the problem, subject to CENSYS approval. The manufacturer shall submit this justification using the RAR form (see section 6.3).

The manufacturer shall identify the procedure followed in its organization to support timely record keeping and correction of problems.

CENSYS will be responsible for determining the nuclear safety significance (if any) of the problem and its application within the CENSYS systems. CENSYS will be responsible for reporting any significant nuclear safety problem to the appropriate licensing authorities. This assignment of responsibility to CENSYS does not prevent the manufacturer from making its own assessment or report to a licensing authority.

5.10 Manufacturer Software Change Control

Software that is supplied subsequent to the initial order shall be identical to the originally supplied software except for changes that are authorized by CENSYS in writing. To obtain such authorization, the manufacturer may be expected to submit to CENSYS justification or design information regarding the change using the TCR form (see section 6.5).

Through 10 years after initial product delivery, manufacturer shall maintain records that identify changes that the manufacturer has made against the originally shipped versions. These change records shall identify

- serious design error corrections
- minor design error corrections
- design enhancements and product improvements
- other modifications and workarounds

Manufacturer shall assign a new version number to any software that is modified as above and subsequently shipped under an order by CENSYS.

5.11 Discontinuation of Support

Concurrent with initial product delivery to CENSYS, the supplier shall escrow (store a copy of) all source code used in the deliverable software that is the supplier's property. Following a ten year period after escrow, problem reporting and software change control may be terminated by the supplier provided one year notification is provided and escrowed software is released to CENSYS.

The escrowed software will also be immediately released to CENSYS if the manufacturer is unable to fulfill any of the requirements in this document without CENSYS authorization.

6. Administrative Requirements

6.1 Right of Access

The supplier shall grant access for representatives of CENSYS and/or its client to those facilities and shops of the supplier and subsuppliers as appropriate to the work performed therein for CENSYS. The supplier shall make objective evidence of quality conformance readily available to CENSYS/client representatives. The supplier will provide suitable work space and such incidental support services as may be required.

CENSYS and/or its client will perform such surveillance and conduct such quality audits as may be deemed necessary to confirm the acceptability of supplier and subsupplier activities relative to work performed for CENSYS. While supplier will be notified of planned visits, the depth of investigation, including in-process audits, will not necessarily be limited to the originally planned purpose of the visit.

6.2 Stop Work Authority

CENSYS reserves the right to order the supplier to stop all or a portion of the work for noncompliance with procurement document requirements or upon discovery of a condition adverse to quality which, if uncorrected, could affect safety or operability.

6.3 Document Submittal (RAR)

The supplier shall submit documents (including records packages) for review and approval of information as required by procurement documents using a CENSYS Request for Approval or Review form (reference 3.2).

6.4 Deviation from Contract Requirements (DCR)

The supplier shall complete and submit a CENSYS Deviation from Contract Requirements form (reference 3.3) to describe and request acceptance of any condition which does not fully comply with procurement document requirements.

A DCR is used in place of a TCR (section 6.5) where an exception to the specification is a one time occurrence and not desired to be a generic change.

6.5 Technical Change Request (TCR)

The supplier may request changes to procurement document technical requirements by submitting a CENSYS Technical Change Request form (reference 3.4) to the Buyer. The TCR shall be completed with sufficient detail and justification to enable evaluation. If a change is approved as a permanent change or altered design, the supplier must revise affected supplier drawings and/or other technical documents.

6.6 Certificate of Conformance (CofC)

Upon completion of the work, or a deliverable portion thereof, shipment shall be accompanied by Certificates of Conformance (reference 3.5) as follows:

(1) The supplier shall provide a signed Certificate of Conformance to attest that the equipment supplied to CENSYS has been constructed and tested and is in conformance with the requirements of the procurement documents. The certification shall identify the supplier quality assurance program documentation, including revision or date of issue, utilized during the performance of the work.

(2) Where shipment is to be made directly from supplier to the CENSYS client, a CENSYS Certificate of Conformance will be provided for inclusion with the shipment. The CENSYS Certificate of Conformance is evidence of CENSYS acceptance of the item or service.

6.7 English Language

All submittals to CENSYS required by the procurement documents and this specification shall be in the English language. If a conflict exists between the English language version and the supplier's native language version, the English language version shall take precedence.

9.0 USNRC RESTRICTIONS ON REVISIONS TO THE ~~SOFTWARE PROGRAM MANUAL~~ COMMERCIAL DEDICATION PROGRAM

The United States Nuclear Regulatory Commission (USNRC) staff has determined that the certain sections of the ~~Software Program Manual~~ Commercial Dedication Program cannot be changed without prior USNRC approval, ~~because these sections contain basic information relied on by the staff for its safety determination.~~ prior to implementing the change.

Within the following major section:		Modifications to following sections not allowed without ~~prior~~ USNRC approval prior to implementing the change
1.0	~~Introduction~~ Purpose	1.1 ~~Purpose~~ all 1.2 Scope 1.3 Overview 1.4 General Requirements
3.0	~~Software Quality Assurance Plan~~ 2.0 Scope	3.1 Purpose all 3.2 Management 3.3 Documentation 3.5 Renew Requirements 3.6 Problem Reporting and Corrective Action 3.8 Code Control
4.0	Software Verification and Validation Plan	4.1 Purpose 4.2 Overview of V&V 4.8 System Validation Testing
5.0	Software Configuration Management Plan	5.1 Introduction 5.2 Management
6.0	Software Operations and Maintenance Plan	6.1 Purpose
7.0	Documentation	7.1 General Requirements 7.2 Functional Requirements Documents 7.3 Software Design Requirements 7.4 Software Design Description 7.6 Software Verification & Validation Documentation 7.9 Computer Code Certificate
8.0	Problem Reporting and Corrective Action	8.1 Classification System 8.2 Problem Reporting 8.3 Corrective Action
9.0	USNRC Restrictions on Revisions to the Software Program Manual	9.0 USNRC Restrictions on Revisions to the Software Program Manual

Copy add'l section from next page

Any changes to the commitments identified in the sections above, except for editorial changes and layout, could involve an unreviewed safety question, and therefore will require USNRC review and acceptance prior to implementation. Any requested changes to these commitments shall be specifically described in the Combined Operating License (COL) application or submitted for license amendment after COL issuance.

TABLE OF CONTENTS

1. Purpose 4
2. Scope 5
3. Refrenees 5
4. Manufacturer Controls for Computer Hardware Components 6
   - 4.1 Component Service 6
   - 4.2 Identical Components 6
   - 4.3 Component Identification 6
   - 4.4 Documentation Control 7
   - 4.5 Reproduction of Documentation 7
   - 4.6 Hardware Testing 7
   - 4.7 Problem Reporting 8
   - 4.8 Notification of Manufacturer Changes 9
   - 4.9 Replacement or Repair 10
5. Manufacturer Controls for Computer Software Components 11
   - 5.1 Component Service 11
   - 5.2 Identical Software Media 11
   - 5.3 Software Version Control 11
   - 5.4 Software Virus Protection 12
   - 5.5 Documentation Control 12
   - 5.6 Reproduction of Software and Documentation 12
   - 5.7 Software Development Process 12
   - 5.8 Software Testing 13
   - 5.9 Software Problem Reporting 14
   - 5.10 Manufacturer Software Change Control 15
   - 5.11 Discontinuation of Support 15
6. Administrative Requirements 16
   - 6.1 Right of Access 16
   - 6.2 Stop Work Authority 16
   - 6.3 Document Submittal (RAR) 16
   - 6.4 Deviation from Contract Requirements (DCR) 16
   - 6.5 Technical Change Request (TCR) 16
   - 6.6 Certificate of Conformance (CofC) 17
   - 6.7 English Language 17

7. USNRC Restrictions on Revisions to the Commercial Dedication Program 18

7900001A.WPD

MASTER

QUALIFICATION GUIDELINES

FOR

MILD ENVIRONMENT

INSTRUMENTATION AND CONTROLS EQUIPMENT

FOR

NUPLEX 80+

NPX80-IC-QG790-00

REVISION ~~01~~ 02

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

This document is the property of ABB Combustion Engineering Nuclear Systems, Windsor, Connecticut and is to be used only for the purposes of the agreement with ABB-CENS pursuant to which it is furnished.

Prepared by T. Barry Date 2-15-94
~~T. Barry, Cognizant Engineer~~ J K McNally

Reviewed ~~Approved~~ by [signature] Date 2-15-94
~~G. D. Altenhein, Supervisor, Electrical Systems~~

T. Barry

Approved by Paul L Yanosy Date 2/15/94
~~P. L. Yanosy, Manager, I&C Protection Systems Engineering~~
W J Gill, NUPLEX 80+ Engineering Manager

Issue Date 2/15/94

RECORD OF REVISION

Rev.	Date	Pages Involved	Prepared By	Approved By
00	11/9/90	Original	G. D. Altenhein S. J. Wilkosz	K. Scarola W. J. Gill
01	2-15-94	1,5-7,10-14,16-19, 21-22,24-26,30,34	T. Barry	G. D. Altenhein P. L. Yanosy

02 2, 6, 10, 11 J K McNall T Barry
26, 34 W J Gill

TABLE OF CONTENTS

1.0 PURPOSE 4

2.0 SCOPE 5

3.0 REFERENCES 7

4.0 METHODS OF QUALIFICATION 8
- 4.1 TYPE TESTING 8
- 4.2 OPERATING EXPERIENCE 8
- 4.3 QUALIFICATION BY ANALYSIS 9
- 4.4 COMBINED QUALIFICATION 9
- 4.5 ON-GOING QUALIFICATION 9

5.0 QUALIFICATION REQUIREMENTS 10
- 5.1 ENVIRONMENTAL QUALIFICATION PROGRAM 10
- 5.2 SEISMIC QUALIFICATION PROGRAM 16
- 5.3 EMI QUALIFICATION PROGRAM 22
- 5.4 SWC QUALIFICATION PROGRAM 24
- 5.5 FAULT ISOLATION QUALIFICATION PROGRAM 25

6.0 DOCUMENTATION 28
- 6.1 EQUIPMENT SPECIFIC QUALIFICATION DOCUMENTATION 28
- 6.2 QUALIFICATION DATA SUMMARY AND EVALUATION 30

7.0 QUALITY ASSURANCE 31

8.0 ADMINISTRATIVE PROCEDURES 32
- 8.1 EQUIPMENT SPECIFICATION 32
- 8.2 DESIGN AND QUALIFICATION PROGRAM 32
- 8.3 QUALIFICATION TASK 32
- 8.4 QUALIFICATION DOCUMENTATION AND APPROVALS 32

10 USNRC RESTRICTIONS ON REVISIONS TO THIS DOCUMENT 34

LIST OF TABLES

Table No.	Title	Page No.
1	List of Abbreviations and Acronyms	34

LIST OF FIGURES

Figure No.	Title	Page No.
1	Generic Module Required Response Spectrum	35
2	Generic Floor & Wall Required Response Spectrum	36

1.0 PURPOSE

The purpose of this document is to discuss the methods to be used in the Qualification of Instrumentation and Control Equipment for Nuplex 80+ (NPX80+). This document will acquaint the reader with various qualification activities and approaches. It will be used by the equipment designer in establishing specific qualification plans and procedures.

2.0 SCOPE

This document discusses qualification of instrumentation and controls equipment for NPX80+. It addresses those areas for which equipment is to be qualified; Seismic, Environmental, Life Expectancy, Electromagnetic Interference (EMI), Surge Withstand Capability (SWC), and Fault Isolation; Qualification Methods; Type Testing, Operator Experience, Analysis, On-going and Combined Methods; Qualification documentation; Quality Assurance; and Administrative Procedures.

The qualification requirements described herein apply to all safety related instrumentation and control systems and equipment with the exception of those which are subject to design basis accident environmental conditions. In general, these include:

- Plant Protection System (PPS) including the Plant Protection Calculator (PPC) and Core Protection Calculator (CPC).
- Engineered Safety Feature - Component Control System (ESF-CCS).
- Discrete Indication and Alarm System (DIAS) N and P Channels.
- Safety related process instrumentation signal conditioning devices.
- Post Accident Monitoring Instrumentation (PAMI) processors and data acquisition equipment.
- Electrical Inverters.

In addition, Seismic Category II requirements apply to non-safety related equipment that is in the control rooms or in close proximity to safety-related equipment. This includes:

- Data Processing System (DPS) CRT's and Keyboards.
- Process-Component Control System (Process-CCS) Controls.
- Operators Modules for all systems.
- Sequence of Event (SOE) Recorders mounted in Auxiliary Process Cabinets (APC) A, B, C and D.

For environmental qualification this document is concerned only with the instrumentation and control equipment in mild environments. A mild environment is an environment where the normal service conditions and extremes (abnormal) in service conditions are not significantly affected by the design basis accident (DBA) and where seismic is the only design basis event (DBE) of consequence.

Environmental qualification of electrical equipment located in harsh environments will be in accordance with methodologies outlined in

3. 3.

Reference 11. Reference 11 has been reviewed and approved by the NRC as an acceptable methodology for environmental qualification of nuclear steam supply system safety related electrical equipment. Refer to CESSAR-DC, Section 3.11 for additional instrumentation and control equipment harsh environment qualification requirements. A harsh environment is an environment expected as a result of the postulated service conditions appropriate for the design basis and post design basis accident of the station. Harsh environments are the result of a loss of cooling accident (LOCA)/high energy line break (HELB) inside containment and post-LOCA or HELB outside containment. For harsh environments, it is anticipated that equipment which has previously been qualified in accordance with the requirements of Reference 3.1, 3.3, 3.4 and 3.5 will be utilized. It is expected that no new harsh environment equipment will be required for SYS80+ beyond that which has previously been qualified for the parameter envelop of the SYSTEM 80 design. If necessary, previously qualified harsh environment equipment will be re-qualified by previous methods (or to requirements of References 3.6 and 3.7 when seismic requalification is involved) to plant-specific parameter envelopes for situations where the plant envelope is not bounded by the previous qualification envelope.

3.0 REFERENCES

3.1 IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations".

3.2 IEEE Std 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations".

3.3 Reg. Guide 1.89, Rev. 01, June 1984, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants".

3.4 IEEE Std 344-1975, "IEEE Recommended Practices for Seismic Qualification of Class IE Equipment for Nuclear Power Generating Stations".

3.5 Reg. Guide 1.100, Rev. 01, August 1977, "Seismic Qualification of Electric Equipment for Nuclear Power Plants".

3.6 IEEE Std 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations".

3.7 Reg. Guide 1.100, Rev. 02, June 1988, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants".

3.8 ANSI C37.90a-1974 (IEEE Std 472-1974), "Guide for Surge Withstand Capability (SWC) Tests".

3.9 MIL-STD-461C, 1986, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference".

3.10 IEEE Std 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits".

3.11 CENPD-255-A, Revision 3, "Qualification of Combustion Engineering Class 1E Instrumentation", Combustion Engineering, Inc., October 1985.

4.0 METHODS OF QUALIFICATION

This section discusses type tests, analysis and other methods of qualification defined in Reference 3.1. These methods are:

Type Testing
Operating Experience
Qualification by Analysis
Combined Qualification
On-going Qualification

4.1 TYPE TESTING

The goal of type testing is to demonstrate that the equipment meets or exceeds the requirements of equipment performance specifications under the normal, abnormal and DBA conditions specified for the equipment. Equipment of the type intended for use will be subjected to design basis conditions and performance demonstrated by test. Manufacturer's test data may be applied if the test(s) encompass design basis conditions which apply.

4.2 OPERATING EXPERIENCE

Electric equipment that has operated successfully can be considered qualified for equal or less severe service conditions. Operating experience can provide information on limits, failure modes and failure rates. The validity of operating experience as a means of qualification shall be determined from the type and amount of documentation supporting the service conditions and equipment performance. Both nuclear and non-nuclear related operating experience can apply to this method.

4.3 QUALIFICATION BY ANALYSIS

In general, qualification analyses will consist of mathematical or logical proof that performance of the equipment to be qualified meets or exceeds its specified requirements when subjected to specified normal and design basis event environments. Analysis will be based on established principles, operating experience data, partial type test data, or combinations of these. The analysis will be of a form that can be readily understood and verified by people qualified in the pertinent discipline of engineering or science.

4.4 COMBINED QUALIFICATION

Equipment may be qualified by type test, operating experience, analysis or any combination of these methods. Partial type tests with extrapolation or analysis, operating experience with extrapolation or analysis, and type tests supplemented with tests of components and analysis are examples of the use of combined qualification.

4.5 ON-GOING QUALIFICATION

The qualification methods described above may result in a qualified life of equipment that is less than the required installed life of the equipment. On-going qualification is a method which can be used to extend the qualified life of the equipment for situations where equipment is installed and operating. Examples of on-going qualification methods are:

1) Aging and testing of identical equipment may continue during the qualified life period of the installed equipment.

2) Replacement equipment may be installed and the original equipment removed before the end of the qualified life period. The removed equipment may then be type tested to determine its additional qualified life.

5.0 QUALIFICATION REQUIREMENTS

This section provides method, requirements, general guidance and acceptance criteria for Seismic, Environmental, EMI, SWC, and Fault Isolation qualification.

The following qualification sequence will generally be followed for mild environment equipment.

- Pre-Test Inspection
- Baseline Performance Testing
- Aging Analysis or Accelerated Age Conditioning
- Performance Testing (As Required)
- Normal and Abnormal Environmental Performance Verification
- Performance Testing (As Required)
- Seismic Testing
- Performance Testing
- EMI, SWC and Fault Isolation Testing
- Performance Testing (as required)
- Post Test Inspection

Performance testing and/or monitoring of test unit operability status during environmental and seismic tests will be performed to the extent practicable.

EMI, SWC and Fault Isolation tests may be performed at any point in this sequence. However, the other activities and tests must be performed in sequence as shown to establish susceptibility and allow preconditioning of qualification equipment as applicable.

5.1 ENVIRONMENTAL QUALIFICATION PROGRAM

The objective of this section is to provide guidelines for environmental performance verification of Class 1E instrumentation and control equipment located in mild environments. Environmental qualification of Class 1E equipment located in harsh environments is addressed by other methods as defined in Section 2.0.

Environmental performance verification will be demonstrated by system, cabinet or component - level test, analysis or combined methods as described in Section ~~5.1.1.1~~ 5.0 and documented as defined in Section 6.0. Prior performance of suitable type tests by the equipment suppliers may be applied for environmental performance verification. Independent review of test procedures, data and results will be performed to ensure that test acceptance criteria is met. The detailed steps and results of the independent review process will be documented as defined in Section 6.0.

5.1.1 Environmental Verification Sequence

5.1.1.1 Pre-Test Inspection

Inspection will be performed to ensure that a test unit has not been damaged after manufacture and to identify basic dimensions.

5.1.1.2 Baseline Performance Testing

The equipment will then be operated under normal conditions (e.g., nominal temperature, humidity ... etc.) to provide a data base for comparison with performance under more highly stressed conditions. Measurements such as rate of change, stability, accuracy, response time, data throughput, ... etc. will be established at this time.

5.1.1.3 Aging Analysis and Conditioning

Experience in aging analysis of instrumentation and control equipment in mild environments has shown that most materials and equipment exhibit no significant aging mechanisms that affect susceptibility to failure in a seismic environment with the exception of electromechanical aging.

Arrhenius Methodology aging analysis of I&C equipment has shown that materials and equipment in mild environments have predicted lives greater than to much greater than the 60 year service life goal of the plant. For this reason Arrhenius Methodology aging analysis is not required for mild environment equipment.

Electromechanical aging analysis will be performed on equipment such as relays, switches and like equipment. Age conditioning will be required prior to DBE testing (seismic) if the cyclic operations that a device will experience during its service life in the plant approach the manufacturer's cycle life rating. A guideline threshold for a need for age conditioning is the device service life exceeds 25 percent of manufacturer's cycle life rating. Electromechanical devices requiring age conditioning will be aged by cyclic operation while electrically loaded to the manufacturer's full rated loads for the expected service life number of operations. The expected radiation exposure of 1000 rads TID or less for mild environments is far below the threshold damage level of typical materials and components used in I&C equipment. Thus, no significant degradation due to radiation is expected during the 60 year life goal. Therefore, radiation simulating service life exposure will have no affect on results of subsequent seismic testing and will not be required.

Dust aging will not be requird because dust accumulation will be limited over the service life of the equipment through normal housekeeping practices and air intake filtering of the equipment.

In addition to aging analysis, manufacturers equipment data sheets

will be reviewed for specified lives. If the specified life is less than the equipment's service life the information will be incorporated into a periodic parts replacement program.

Performance testing will be repeated after accelerated age conditioning and before any subsequent testing to verify continued component operability.

5.1.1.4 Normal and Abnormal Environmental Performance Verification

Equipment will be subjected to environmental performance verification in accordance with Reference 3.1 and 3.3. Verification will consist of analysis of equipment manufacturer's environmental test data or rating to ensure that requirements are met. Supplemental environmental testing will also be performed where manufacturers testing is not bounding for the intended normal and abnormal plant service conditions.

In general, environmental service conditions for ABB-CE instrumentation and control equipment located in mild environment are defined as follows:

Main Control Room
Cabinet or Panel
Ambient Conditions

Environmental Parameter	Normal Min.	Normal Max.	Abnormal Min.	Abnormal Max.
Temperature	73°F	78°F	73°F	85°F(3)
Humidity(2),RH	20%	60%	20%	60% (1)
Pressure	Atmospheric		Atmospheric	
Radiation	[1000 Rads or less, 60 year Total Integrated Dose]			

Equipment Room/Remote Shutdown Room
Cabinet or Panel
Ambient Conditions

Environmental Parameter	Normal Min.	Normal Max.	Abnormal(3) Min.	Abnormal(3) Max.
Temperature	65°F	85°F	65°F	104°F
Humidity(2),RH	40 %	60 %	40 %	90 % (1)
Pressure	Atmospheric		Atmospheric	
Radiation	[1000 Rads or less, 60 year Total Integrated Dose]			

Plant Field Locations
Cabinet or Panel
Ambient Conditions

Environmental Parameter	Normal Min.	Normal Max.	Abnormal Min.	Abnormal Max.
Temperature	32°F	104°F	32°F	122°F(3)
Humidity(2),RH	20 %	90 %	20 %	90 % (1)
Pressure	Atmospheric		Atmospheric	
Radiation	[1000 Rads or less, 60 year Total Integrated Dose]			

Notes:
(1) At or above 80°F, the moisture content is that which produces 90% RH at 80°F. (dewpoint of 77°F).
(2) All humidity conditions are non-condensing.
(3) Parameters can occur for an 8 hour period.

These normal and abnormal temperatures reflect equipment cabinet or panel ambient conditions. An additional heat rise will be measured and added to normal and abnormal temperatures to address cabinet or panel internal temperature rise for internally-mounted subassemblies.

Additional margin will also be applied to the verification of electrical Class 1E equipment in accordance with Reference 3.2.

Environmental influences such as chemical spray, submergence and abrupt pressure changes will not be addressed under environmental performance verification since mild environment equipment will not be subject to these influences.

The methods and results of environmental performance verification will be documented as defined in Section 6.0.

5.1.2 Acceptance Criteria

Acceptance criteria for environmental performance verification is established prior to start of type testing and is included as part of the test procedure document. The following is a list of typical acceptance criteria:

A. Test environments are at least as severe as, and representative of, the required environmental profile.

B. Operation of the equipment under normal environmental conditions to the extremes of performance and electrical characteristics is within the limits of accuracy required in the equipment specifications.

C. Equipment has been aged, as appropriate, prior to design basis accident testing.

D. Operation of the equipment in its Class 1E functions, while exposed to the design basis event environment is within the limits of accuracy required in the equipment specifications.

E. Equipment has been subjected to seismic DBE testing.

F. Post-test examination of the equipment reveals no conditions which might have interfered with the ability of the equipment to perform its Class 1E functions.

G. Typically, instrument accuracy requirements are established from the assumptions used in the particular Safety Analysis for which the equipment performs its Class 1E function. These requirements are reflected where applicable, in the equipment specifications and in the safety system setpoints. The most conservative limits on time and accuracy requirements are used for qualification. However, the same model instrument may be qualified to various levels based on the particular application.

5.1.3 Test Anomalies

In the event that anomalies are observed during testing that violate defined acceptance criteria, the following actions will be taken as appropriate, prior to further testing to ensure complete and satisfactory resolution:

A. Document the anomaly;

B. Verify operability status of monitoring and data acquisition equipment involved;

C. Establish the type of failure (random or common-mode);

D. Re-evaluate acceptance criteria requirements, if appropriate;

E. Define, review and approve recommended corrective action before continuation of testing.

5.1.3.1 Random Failures

If it is determined that the failure was random, appropriate corrective action will be taken to eliminate the problem.

Replacement parts may be utilized to replace those that have failed. All replacement parts so used will have experienced the same accelerated age conditioning and testing as the original failed part did prior to continuation of the program. All corrective actions taken will be documented and fully justified.

5.1.3.2 Common-Mode Failures

If it is determined that the failure was common mode, appropriate corrective action will be taken to eliminate the problem.

Possible corrective action may include equipment/component redesign, part replacement, equipment relocation, additional analysis and/or any combination thereof. All corrective actions taken will be documented and fully justified.

Part replacement or redesign will meet the pre-conditioning requirements previously defined before continuation of testing.

5.2 SEISMIC QUALIFICATION PROGRAM

The objective of the seismic qualification program is to demonstrate the ability for continued functioning and physical integrity during and after dynamic motion loading due to normal operating, transient, seismic and accident conditions, of the instrumentation equipment associated with the Reactor Protection System, Engineered Safety Features Actuation System, and Post-Accident Monitoring System. Independent review of test procedures, data and results will be performed to ensure that test acceptance criteria is met. The detailed steps and results of the independent review process will be documented as defined in Section 6.0. The seismic and dynamic qualification program conforms to the requirements of Reference 3.6 and 3.7. The seismic and dynamic testing portion of the qualification program is performed in a sequence consistent with the requirements Reference 3.1.

5.2.1 Equipment Classification

Equipment is divided into two seismic categories in accordance with the criteria defined below. The categories are Seismic Category I and Seismic Category II.

Seismic Category I

Those plant features defined as seismic category I are safety-related; in particular those which are necessary to assure: (1) the integrity of the reactor coolant boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100.

Seismic Category II

Seismic Category II equipment is defined as non safety related equipment whose failure can prevent the satisfactory accomplishment of safety functions or reduce the performance of safety related equipment.

Seismic Category I and II equipment may be qualified to the generic Required Response Spectrum (RRS) shown in Figures 1 and 2. As an alternative, this equipment may be qualified to plant-specific RRS levels in lieu of generic RRS levels.

5.2.2 Equipment Performance Requirements

The following requirements are guidelines for acceptable performance criteria which must be met for seismic and dynamic qualification.

5.2.2.1 Seismic Category I

The safety-related features of Seismic Category I equipment must operate as necessary to perform the intended task(s). In general, proper operation is verified by monitoring all facets of the equipment operation; primarily outputs and inputs. Where possible intermediate parameters, such as setpoints, are also monitored. Usually the monitored information is permanently recorded. If the equipment has a change-of-state safety function (e.g., reactor trip), then the equipment will be exercised to verify correct state change. If the equipment has more than one safety operating mode, the additional modes are also verified. This may require repeating the simulated SSE for each mode.

In summary, analog circuits are monitored to verify proper transmission accuracy. Relay circuits are monitored to verify required change-of-state, and to assure that unauthorized state change (e.g., unacceptable relay chatter) does not occur. In addition, no loss of physical integrity, such as yielding or loosening which could impede proper system (safety) functioning, is permitted in Seismic Category I equipment.

5.2.2.2 Seismic Category II

The physical integrity of Seismic Category II equipment must be maintained to the extent of ensuring non-interference with nearby Seismic Category I equipment or operating personnel.

5.2.3 Equipment Seismic Qualification Methods

The following methods are used to demonstrate satisfactory equipment performance for seismic qualification. All significant in-service operating conditions, such as mounting and loading, are simulated for testing and addressed for analysis. Where similar equipment is concerned, analysis may be used to qualify variations from qualified equipment.

Seismic Category I

Seismic Category I equipment is tested (vibrated) in such a manner to generate an effect on the equipment that is at least equal to the effect which would result from exposure to the specified seismic environment. Equipment supports are tested, analyzed, or qualified

by combined test and analysis, to demonstrate the physical integrity of the supports and to determine the seismic environment of the supported equipment.

Seismic Category II

This equipment is tested or analyzed to show that its mounting, fasteners and restraints are sufficient to prevent interference with the surroundings (equipment falling off mounts, parts falling off equipment that could damage Class 1E equipment in the area).

5.2.4 Seismic Qualification Procedures

5.2.4.1 Testing

Testing is normally done by multi-mode, multi-direction (biaxial) excitation, with seismic motions represented by response spectra, time history, or power spectral density function. To qualify equipment, several techniques are utilized.

Proof Test

The proof test is designed to simulate the seismic environment of the equipment. The proof test will generate the same (or greater) equipment response that would be generated by the earthquake. The motions of the shake table used in seismic simulation are characterized by response spectrum, called the Test Response Spectrum (TRS). For qualification to a particular seismic environment, characterized by Required Response Spectrum (RRS), the TRS must envelop the RRS throughout the frequency range beginning with the first mode (lowest natural frequency) of the equipment and continuing through applicable higher frequencies. When no attempt is made to determine equipment modes, TRS-RRS envelopment must begin at one (1) Hz and continue to applicable higher frequencies. The minimum number of tests for each sequence is 6; at least 5 half level SSE tests with magnitudes equal to or greater than one-half SSE followed by one full SSE test. During the full SSE test, the equipment is functionally exercised to verify proper operation. Upon completion of testing the equipment is inspected and any effects due to testing are documented by methods defined in Section 6.0.

Although not required for qualification, a resonance survey is usually performed before the proof test to determine the equipment resonance modes. The test direction may be biaxial or single axis.

Functional Equipment (Modules and Complete Assemblies)

With the equipment prepared, operating, and mounted to the shake table as intended for service, the table is excited and its motions are analyzed by spectrum analysis to determine the TRS. The excitation wave form can be random multi-frequency or any other applicable form with the strong motion reasonably consistent

throughout the duration. The direction of the excitation is biaxial; one horizontal and one vertical in each test sequence. If the vertical and horizontal excitation components are locked in-phase, four sequences are completed, with the equipment rotated 90 degrees for each sequence. If the two components are phase-incoherent (unlocked), two sequences are completed, with the equipment rotated 90 degrees for the second sequence.

Supports of Functional Equipment

In some cases, it is not possible to test functional equipment and its support as a unit. This is especially true when many electrical devices or modules are contained in or attached to a common support structure, such as a rack or cabinet. In this case the support may be proof tested first. The support will be fully loaded with actual equipment or have dynamically equivalent dummy weights in place of some or all of the actual functional equipment. The dummy weights are representative of or exceed the actual equipment characteristics in regard to mass, mass distribution and mounting. This test is performed as previously described with the following exceptions: (1) Since the support has no function (other than support), no functional monitoring is required, and (2) The seismic environment of the supported devices and modules is determined by monitoring the motions of their mounting locations. These motions are spectrum analyzed to yield the RRS of the devices and modules which are then qualified in accordance with the methods previously described.

As an alternative approach, functional equipment may be tested to the generic module RRS levels shown in Figure 1. These are the maximum levels to which functional equipment may be exposed at its supports. In this case, functional monitoring is required during and after test. The installation of this qualified functional equipment in its support (i.e., cabinet) is then analyzed by the methods defined below to confirm that:

a)installation of functional equipment does not impact the qualified status of its support, and

b)the support does not exceed the RRS levels to which the functional equipment is qualified.

5.2.4.2 Analysis

As a qualification method, analysis without testing is limited to cases where the maintenance of structure integrity is sufficient to show qualification, providing the structure can be adequately modeled. It is difficult for analysis to predict the performance of electrical circuity due to the excessive number of components and considerations which must be taken into account. Only support structures may be qualified by certification of structural integrity alone.

When the equipment to be analyzed serves as a support for seismic

category I devices, the seismic environment, to which the supported devices must be qualified (by testing), can be determined by analysis. The following method is used to show structural integrity, and when required, determine the seismic environment of the supported seismic category I devices.

Dynamic Analysis

The equipment is modeled as a representative number of mass points connected by massless members of given stiffness and damping. The modal frequencies, shapes, and dampings are either tested or evaluated to determine stresses and/or displacements resulting from the specified seismic environment. The calculated stresses are limited to those members, fasteners, and restraints which are responsible for maintaining structural integrity in the manner previously described. The resulting stresses, determined by response spectrum modal, time history, or other analyses, are compared to appropriate allowable stresses to determine qualification.

Combined Testing and Analysis

The following methods are employed for specific circumstances where both test and analysis are required for qualification.

In-Place Testing and Modal Determination

This method is used to qualify supports of Seismic Category I equipment when testing is not practical. In this case, testing accompanies analysis, since the seismic environment of supported equipment is one of the effects to be determined, and the accurate results afforded by testing are desired.

With the structure loaded with functional equipment, or dynamically-equivalent models, and mounted as it would be in-service (not mounted to shake table) either at the place of manufacture or at the plant site, one or more portable exciters are attached to the equipment at various locations which will excite the equipment modes of vibration. Vibration sensors are attached to various locations on the equipment to gather response data. This data is used to determine modal frequencies, shapes, and damping values.

A model of the equipment is made, a dynamic analysis is performed and the results of in-place testing are used to refine the model. The required testing (seismic environment) of the supported devices or modules is then determined. This approach is normally performed during the equipment design phase.

Extrapolation for Similar Equipment

Where equipment under consideration is similar to previously qualified equipment, extrapolation of previous data is used to qualify the new equipment.

Equipment Previously Qualified by Analysis

In cases where previous qualification was based on analysis, the extrapolation consists of making adjustments to the original analysis in accordance with the equipment changes. The documentation reflects the results of the original analysis and is amended as necessary to accommodate the changes in equipment.

Equipment Previously Qualified by Test

For changes of a structural nature only; where the stiffness, damping, or mass distribution of the equipment is affected, an analysis is performed to show how the changes affect the equipment's seismic response.

When the change involves substitution of electrical components, without affecting the dynamic characteristics of the equipment as a whole, an analysis is performed for the substituted component if the variation between components is minimal. If the substituted component is considerably different from the original, the new component is tested to verify qualification. The input test motions are conservatively equivalent to those motions expected at the component mounting locations.

If both structural dynamics and functional components are involved in the change, the variation of the structure response is determined first. The new components are then tested or analyzed with respect to the modified dynamic environment.

Seismic qualification will be applied in accordance with Reference 3.6 and 3.7 requirements. These standards are similar to earlier versions of these standards but include provisions to address the effects of non-seismic loading conditions. These provisions and the methods applied to address them are defined as follows:

- Vibrational Aging. Where equipment is subject to the effects of non-seismic vibrational loads, the characteristic environment is addressed by test and analysis. A resonance survey is typically performed before proof testing to identify equipment resonance modes. The results of the resonance survey is applied to define equipment susceptibility to non-seismic vibration. Installation and operating requirements are then imposed to ensure that the equipment is not exposed to non-seismic vibration in the susceptible ranges during operational service. A site survey may be performed to verify operational service conditions.

- o Hydrodynamic Loads. Where equipment is subject to the vibratory effects categorized as hydrodynamics loads, a combined RRS is typically applied for qualification testing. The combined RRS consists of SSE components combined with vibratory loads.

- o Nonlinear Equipment Response. Nonlinear equipment response such as local vibration of equipment structure is addressed by test where equipment is mounted in a structure (i.e., cabinet). In cases where equipment and structure are tested separately, nonlinear response is characterized during structure testing and applied by test or analysis for equipment qualification.

- o Maintenance. When maintenance is performed during half-level SSE (seismic conditioning) testing, it becomes part of the post earthquake field maintenance checks and procedures for the equipment.

5.3 EMI QUALIFICATION PROGRAM

This section provides guidelines for electromagnetic interference (EMI) qualification of instrumentation and control equipment. EMI includes the effects of conducted and radiated elector-magnetic interference, radio frequency interference (RFI), and electrostaticdischarge (ESD).

EMI qualification will be demonstrated where required by system, cabinet or component-level test, analysis or combined methods and documented as defined in Section 6.0. Independent review of test procedures, data and test results will be performed to ensure that test acceptance criteria is met.

Prior performance of applicable testing by the equipment supplier may be applied to EMI qualification. Independent review of test procedures, data and results will be performed to ensure that test acceptance criteria is met. The detailed steps and results of the independent review process will be documented as defined in Section 6.0. Other applicable EMI standards may be used if equivalence to Reference 3.9 can be demonstrated.

5.3.1 Equipment Applicability

EMI qualification is applied for equipment with known EMI susceptibility based on operating environment and/or inherent design characteristics. This includes but is not limited to power supplies, programmable logic controllers, digital computers, communications interface equipment and input/output equipment.

5.3.2 Qualification Standards

The following standards apply to EMI Qualification. These standards are selected because they invoke test conditions which are considered representative of the anticipated worst-case EMI

operating environment of the equipment. The Reference 3.9 standard applies as follows:

A. MIL-STD-461 RS03

The purpose of test RS03 is to determine susceptibility of the test unit to electric fields of up to 20 v/m and known polarization over the frequency range of 14 KHZ to 10 GHZ. The test shall be conducted in a shielded enclosure and the radiating sources shall be antennas. The electric field strength shall be calibrated and controlled by monitoring field intensity at or near the face of the test unit.

B. MIL-STD-461 RS02

The purpose of test RS02 is to determine susceptibility of the test unit to low impedance magnetic fields generated by the flow of current in nearby power lines. Test signals will be applied to test signal wire routed once over and in contact with the test unit and then parallel to and in contact with bundled interface cables. The test signals will consist of a 10 uSec spike of 100 volts and a 20 amp, 60 HZ power frequency signal applied to the test signal wire.

C. MIL-STD-461 CS01

The purpose of test CS01 is to determine susceptibility of the test unit to conducted emissions in the frequency range of 30 HZ to 50 KHZ. The test signal shall be limited to 5 V(rms) as defined by Figure 2-4 of Reference 3.9. The test signal will be injected on the power lines feeding all ungrounded AC or DC power leads connected externally to the test unit.

D. MIL-STD-461 CS02

The purpose of test CS02 is to determine susceptibility of the test unit to conducted emissions of 1 v from a 50 ohm source in the frequency range of 50 KHZ to 400 MHZ. The test signal will be injected on the power lines feeding all ungrounded AC or DC power leads connected externally to the test unit.

E. MIL-STD-461 CS06

The purpose of test CS06 is to determine susceptibility of the test unit to transients or spikes on the power lines feeding all ungrounded AC or DC power leads connected externally to the test unit. The test signal will be a spike of 100 volts with a pulse width of approximately 10 uSec.

5.3.3 EMI Qualification Test Configuration

The qualification test unit will be set up to reflect a worst-case arrangement for intended service conditions (i.e., equipment cabinet doors will be open to duplicate maintenance conditions, interconnecting cables will be exposed, ...etc.).

Deliverable or functionally representative software will be loaded into the test unit to facilitate functional operation of features during testing. The test unit will be functionally exercised during EMI qualification test signal application while operation and performance are monitored.

5.3.4 Qualification Test Acceptance Criteria

The qualification test unit will be subjected to EMI test signal levels and frequency ranges as specified for the equipment. Proper test unit operation and performance (i.e., software execution, response time, data stability, communication integrity, analog conversion accuracy,...etc.) at the maximum levels defined or the point of discontinuity shall establish the EMI qualification baseline.

Any anomaly or discontinuity observed beyond test unit tolerance limits that would impair the safety related performance of the unit during the application of EMI test signals will constitute susceptibility to the applied EMI test signal. Upon identification of susceptibility, that portion of testing will again be performed to confirm repeatability and the susceptible condition(s) will be documented as the qualification baseline.

Modification may be applied to eliminate the observed EMI susceptibility however, it must be demonstrated by test and/or analysis that the modification does not effect prior EMI qualification results. EMI qualification testing may then be continued to completion.

5.3.5 Site EMI Characterization

A site survey will be performed upon completion of system installation to characterize the installed EMI environment. This characterization will address the synergistic effects of simultaneous operation of multiple systems. EMI characterization is performed to confirm that the EMI operating environment of the equipment is within its qualification baseline.

5.4 SWC QUALIFICATION PROGRAM

This section provides guidelines for surge withstand capability (SWC) qualification of instrumentation and control equipment. SWC qualification will be demonstrated where required by test and

documented as defined in Section 6.0. Independent review of test procedures, data and test results will be performed to ensure that test acceptance criteria is met.

5.4.1 Equipment Applicability

Equipment to which SWC qualification can apply includes power supplies, programmable logic controllers, digital computers, communications interface equipment, input/output equipment and other equipment where a common mode surge is credible and to which either supply voltage or current is applied.

5.4.2 Qualification Standard

Reference 3.8, ANSI C37.90a-1974 (IEEE Sad 472-1974) is applied for SWC qualification. The purpose of the SWC qualification test is to determine susceptibility of the test unit to transients or spikes imposed in the common and transverse modes across all signal & power input and output connections. The SWC test waveform is oscillatory with a frequency of 1.0 MHZ to 1.5 MHZ, voltage range of 2.5 KV to 3.0 KV crest value of the first half cycle peak and envelope decaying to 50% of the crest value of the first peak in not less than 6 uSec from the start of the wave.

5.4.3 SWC Qualification Test Configuration

SWC qualification testing will be performed under normal intended service conditions. Deliverable or functionally representative software will be loaded into the test unit to facilitate functional operation of features during SWC testing. The test unit be functionally exercised during SWC qualification test signal application while operation and performance are monitored.

5.4.4 Qualification Test Acceptance Criteria

The qualification test unit will be subjected to the SWC test waveform as specified in the qualification standard. Proper test unit operation and performance (i.e., software execution, response time, data stability, communication integrity, analog conversion accuracy, ...etc.) will constitute SWC qualification test acceptance.

Any anomaly or discontinuity observed beyond test unit tolerance limits that would impair safety-related performance of the unit during application of the SWC test waveform will constitute SWC test failure. Modification of the test unit (adjustment of impedance,...etc.) as a remedy for SWC qualification failure will require re-test to demonstrate qualification.

5.5 FAULT ISOLATION QUALIFICATION PROGRAM

This section provides guidelines for electrical fault isolation qualification of instrumentation and control equipment. Fault

isolation qualification where required will be demonstrated by test and documented as defined in Section 6.0. Independent review of test procedures, data and results will be performed to ensure that test acceptance criteria is met.

5.5.1 Equipment Applicability

Electrical fault isolation is provided between redundant protective channels through the use of fiber optic technology. Fiber optic technology ensures that an electrical fault in one protective channel can not prevent equipment in any other protective channel from performing its safety function. Fiber optic technology is also applied between Class 1E and non-1E channels to ensure protective channel operability in the event of credible failures within non-1E channels.

Fault isolation qualification testing is not required for equipment which inherently provides electrical isolation (i.e., fiber optic interfaces).

Fault isolation qualification testing will apply where power from one instrument bus is distributed to two independent, redundant loads within the same channel (i.e., through inverters to main control panel and remote shutdown panel devices). Additionally, certain devices are powered by two independent power distribution systems to enhance device availability (i.e., auctioneered DC power supplies). It will be demonstrated that credible electrical faults are not propagated between independent power distribution systems for these configurations.

5.5.2 Qualification Standards

Reference 3.10, IEEE ~~Std~~ Standard 384-1981 as augmented by Regulatory Guide 1.75 will apply to fault isolation qualification. Typical fault test signal levels of 400 VDC and 600 VAC with maximum source current of 50 amps will be utilized for fault isolation qualification testing. These levels are based on credible fault signal exposures of 480 VAC and 325 VDC. A 10% tolerance and 10% margin are imposed and the resultant voltages are rounded up to 600 VAC and 400 VDC respectively. It will be verified in the specific plant design that these are the maximum credible electrical faults to which equipment may be exposed.

5.5.3 Fault Isolation Qualification Test Configuration

Qualification testing will be performed under normal intended service conditions. Test sample devices (i.e., inverter, auctioneered DC power supplies) will be tested under nominal service conditions (i.e., power source voltage, load current, ...etc.). The fault test signal will be applied in the common and transverse mode while the test unit is monitored to ensure that the fault test signal is not propagated through the fault isolation device(s).

5.5.4 Qualification Test Acceptance Criteria

The qualification test unit will be subjected to the fault test signals defined above in the common and transverse modes. The fault test signal will be applied to the line side of the test unit while the load side is monitored for perturbation. Load side perturbations will remain within applicable limits for qualification test acceptance.

6.0 DOCUMENTATION

is section discusses the documentation for qualification. The qualification documentation will verify that the equipment is qualified for its application and meets its specified performance requirements. Equipment specific documentation products and data summary and evaluation forms are discussed. Qualification documentation and supporting test data will be available for audit.

6.1 EQUIPMENT SPECIFIC QUALIFICATION DOCUMENTATION

In order to demonstrate that the equipment qualification program has adequately addressed all pertinent qualification requirements, equipment specific documentation products will be developed, as appropriate. The documentation will be organized in an auditable form and prepared in accordance with the guidelines set forth in Section 8.0 of Reference 3.1.

6.1.1 Aging Analysis Report

The aging analysis report, as discussed in Section 5.1 will contain the following types of information:

A. Overview and Objective;
B. Equipment Description;
C. Bill of Materials;
D. Environmental Service Conditions;
E. Analytical Evaluations and Bases;
F. Age Conditioning Procedures (if required);
G. Component Replacement Intervals (if required);
H. Approval Signature and Date.

6.1.2 Qualification Plan

The qualification plan outlines the necessary testing and documentation activities required in order to demonstrate qualification. The qualification plan will incorporate the results obtained in the aging analysis and any previous qualification testing into the overall qualification plan. The following information will be included in the plan.

A. Scope of Responsibility;
B. Overview and Objective;
C. Equipment Description;
D. Description of Qualification Method (i.e., Prior Test Review, Analysis, New Testing, . . . etc.)
E. Test Sequence and Makeup (Overview);
F. Seismic, Environmental, EMI, Surge and Fault Test Parameters;
G. Acceptance Criteria (Overview);
H. Documentation Submittal Requirements;
I. Approval Signature and Date.

6.1.3 Age Conditioning Report

Where accelerated age conditioning is required, the results of the accelerated age conditioning process will be presented in an age conditioning report either as a separate document or as part of the final qualification test report. The purpose of this report will be to identify and analyze all equipment failures occurring during the accelerated age conditioning process to determine whether the failure(s) were random or common mode. Approval signature, and date will be obtained.

6.1.4 Qualification Test Procedure

Detailed qualification test procedures and associated acceptance criteria will be defined prior to actual qualification testing. The following types of procedural information will be addressed, as appropriate:

A. Overview and Objective;
B. Equipment Description;
C. Detailed Test Sequence;
D. Monitoring and Operability Check Procedures;
E. Baseline Performance Test Procedures;
F. Environmental and Seismic Test Profile Definition and Procedures;
G. Margin Verification;
H. Detailed Test Set Up Schematics and/or Description;
I. Required Test Instrumentation and Equipment;
J. Detailed Acceptance Criteria;
K. Equipment Mounting and Cable Connection Schematics and/or Description;
L. Approval Signature and Date.

6.1.5 Qualification Test Report

Upon completion of qualification testing an equipment specific test report will be prepared summarizing the test results, conclusion, and recommendations. The following types of information will be addressed and included, as appropriate:

A. Overview and Objective;
B. Equipment Description;
C. Description and Justification for All Test Procedure Deviations;
D. Description and Evaluation for All Observed Abnormalities Exceeding Defined Acceptance Criteria;
E. Raw Test Data;
G. Calibration Schedules and Standards for All Test Instrumentation and Equipment;
H. Reference and/or Pointer to all Supporting Qualification Documentation;
I. Approval Signature and Date.

6.2 QUALIFICATION DATA SUMMARY AND EVALUATION

Upon completion of the documentation products defined above a qualification data summary and evaluation package will be prepared.

The purpose of the qualification data summary is to define and list all elements making up the qualification for a particular equipment. The elements within the summary should include qualifications requirements and their sources, methods , plans, analyses, test procedures, test results, test data, test reports and applicable correspondence and references (books, supporting reports, standards etc). The data evaluation portion will summarize the qualification results of the analysis and test reports contained within.

7.0 QUALITY ASSURANCE

Equipment qualified per this report will be in accordance with the following:

A. All vendor and/or test labs directly utilized by ABB C-E for performing Class 1E qualification services will be formally reviewed for their quality assurance practices. Results of this review will be maintained.

B. For qualification tests, ABB C-E group quality control surveillance practices will be applied.

C. ABB C-E standard hardware procurement practices will be applied when procuring test samples.

D. Test procedures and analyses will be prepared to ensure repeatability of the qualification test program.

E. Qualification documentation will be reviewed in accordance with standard ABB C-E review practices and quality assurance requirements.

8.0 ADMINISTRATIVE PROCEDURES

8.1 EQUIPMENT SPECIFICATION

The performance requirements are set forth in the equipment specification which is generally written by ABB C-E. The requirements include normal, maximum and minimum values of performance parameters, and environmental conditions for normal and abnormal operation. The applicable standards for qualification are referenced by the specification. The specification is included in the engineering package which is sent to prospective vendors for bidding.

8.2 DESIGN AND QUALIFICATION PROGRAM

The equipment design and qualification program will be well documented in a traceable manner. The design is reviewed to ensure the equipment is capable of meeting performance and environmental requirements. The qualification program is reviewed for compliance with the requirements of the equipment specification and the referenced standards. In some cases, the qualification program is written by the qualification facility which has been retained by the vendor. In other cases ABB C-E will perform its own testing of vendor's hardware to a qualification program generated by ABB CE.

8.3 QUALIFICATION TASK

The task of qualification is normally performed by a qualification facility. ABB CE follows the progress of the qualification effort and, interfaces with the qualification facility to ensure that the equipment will be exposed to the proper qualification environment. ABB CE is responsible for ensuring that the electrical and operational performance of the equipment meets the acceptance criteria. For the more involved tests, ABB CE may have witnesses present during testing.

8.4 QUALIFICATION DOCUMENTATION AND APPROVALS

Throughout the qualification program various defined documentation products (see Section 6.0) are generated. ABB C-E will review and approve all documentation products to insure proper program definition and control.

In general, qualification documentation will be generated in the following order. The aging analysis report is prepared first defining all aging analyses and part replacement recommendations, as appropriate. Next, the qualification plan is submitted outlining the overall program and verifies to ABB C-E the vendor/test lab understanding of services to be performed. Accelerated age conditioning and its corresponding report is prepared, if required. In parallel with age conditioning, detailed

qualification test procedures and acceptance criteria are developed. After completion of age conditioning and test procedure development, actual qualification type testing is performed.

Upon completion of qualification testing, test reports will be prepared for approval. When a report is approved, it is accepted as a qualification record which contains sufficient information to allow QA traceability and repeatability. Qualification documentation will be available for audit.

Upon approval of all required qualification documentation and supporting test data, a data summary and evaluation package, as discussed in Section 6.2 will be prepared as required and submitted to the customer for his approval. Customer participation in the review and approval cycle for all proceeding documentation is per customer specific contract requirements.

Qualification documentation will be maintained by ABB CE as a qualification record until the time of customer acceptance of the equipment (typically upon commercial operation of the plant). Upon acceptance, the customer will assume the responsibility of qualification record maintenance until such time as the qualified equipment is removed from service.

It will be the responsibility of the qualification record holder to provide qualification records for reference to address post qualification design changes and obsolete component replacement. Modified equipment and/or replacement components will undergo equipment qualification by the methods defined in Section 5.0.

9.0 USNRC RESTRICTIONS ON REVISIONS TO ~~THE SOFTWARE PROGRAM MANUAL~~ THIS DOCUMENT

The United States Nuclear Regulatory Commission (USNRC) staff has determined that the certain sections of the ~~Software Program Manual~~ cannot be changed without prior USNRC approval, ~~because these sections contain basic information relied on by~~ the staff for its safety determination.

prior to implementing the change.

Qualification Guidelines for Digital Equipment for NUPLEX 80+

Within the following major section:		Modifications to following sections not allowed without ~~prior~~ USNRC approval prior to implementing the change
1.0	Introduction	1.1 Purpose 1.2 Scope 1.3 Overview 1.4 General Requirements
3.0	Software Quality Assurance Plan	3.1 Purpose 3.2 Management 3.3 Documentation 3.5 Review Requirements 3.6 Problem Reporting and Corrective Action 3.8 Code Control
4.0	Software Verification and Validation Plan	4.1 Purpose 4.2 Overview of V&V 4.8 System Validation Testing
5.0	Software Configuration Management Plan	5.1 Introduction 5.2 Management
6.0	Software Operations and Maintenance Plan	6.1 Purpose
7.0	Documentation	7.1 General Requirements 7.2 Functional Requirements Documents 7.3 Software Design Requirements 7.4 Software Design Description 7.6 Software Verification & Validation Documentation 7.9 Computer Code Certificate
8.0	Problem Reporting and Corrective Action	8.1 Classification System 8.2 Problem Reporting 8.3 Corrective Action
9.0	USNRC Restrictions on Revisions to the Software Program Manual	9.0 USNRC Restrictions on Revisions to the Software Program Manual

Copy check! section from following page

Any changes to the commitments identified in the sections above, except for editorial changes and layout, ~~could involve an unreviewed safety question, and therefore~~ will require USNRC review and acceptance prior to implementation. ~~Any requested changes to these commitments shall be specifically described in the Combined Operating License (COL) application or submitted for license amendment after COL issuance.~~ ~~Refer to Section 3.5.1 the Design Control Document.~~

TABLE OF CONTENTS

1.0 PURPOSE 4

2.0 SCOPE 5

~~3.0 REFERENCES~~ 7

4.0 METHODS OF QUALIFICATION 8
- 4.1 TYPE TESTING 8
- 4.2 OPERATING EXPERIENCE 8
- 4.3 QUALIFICATION BY ANALYSIS 8
- 4.4 COMBINED QUALIFICATION 9
- 4.5 ON-GOING QUALIFICATION 9

5.0 QUALIFICATION REQUIREMENTS 10
- 5.1 ENVIRONMENTAL QUALIFICATION PROGRAM (environmental service conditions excluded.) 10
- 5.2 SEISMIC QUALIFICATION PROGRAM 16
- 5.3 EMI QUALIFICATION PROGRAM 22
- 5.4 SWC QUALIFICATION PROGRAM 24
- 5.5 FAULT ISOLATION QUALIFICATION PROGRAM 25

6.0 ~~DOCUMENTATION~~ 28
- 6.1 ~~EQUIPMENT SPECIFIC QUALIFICATION DOCUMENTATION~~ 28
- 6.2 ~~QUALIFICATION DATA SUMMARY AND EVALUATION~~ 30

7.0 QUALITY ASSURANCE 31

8.0 ~~ADMINISTRATIVE PROCEDURES~~ 32
- 8.1 ~~EQUIPMENT SPECIFICATION~~ 32
- 8.2 ~~DESIGN AND QUALIFICATION~~ PROGRAM 32
- 8.3 ~~QUALIFICATION~~ TASK 32
- 8.4 ~~QUALIFICATION DOCUMENTATION AND APPROVALS~~ 32

10 USNRC RESTRICTIONS ON REVISIONS TO THIS DOCUMENT

LIST OF TABLES

Table No.	Title	Page No.
1	List of Abbreviations and Acronyms	34

LIST OF FIGURES

Figure No.	Title	Page No.
1	Generic Module Required Response Spectrum	35
2	Generic Floor & Wall Required Response Spectrum	36

TABLE 1

ABBREVIATIONS AND ACRONYMS

APC - AUXILIARY PROCESS CABINET
CPC - CORE PROTECTION CALCULATOR
DBA - DESIGN BASIS ACCIDENT
DBE - DESIGN BASIS EVENT
DIAS - DISCRETE INDICATION AND ALARM SYSTEM
DPS - DATA PROCESSING SYSTEM
EMI - ELECTROMAGNETIC INTERFERENCE
ESF-CCS - ENGINEERED SAFETY FEATURE-COMPONENT CONTROL SYSTEM
PAMI - POST ACCIDENT MONITORING INSTRUMENTATION
PPC - PLANT PROTECTION CALCULATOR
PPS - PLANT PROTECTION SYSTEM
PROCESS-CCS - PROCESS COMPONENT CONTROL SYSTEM
RFI - RADIO FREQUENCY INTERFERENCE
RRS - REQUIRED RESPONSE SPECTRUM
SOE - SEQUENCE OF EVENTS
SSE - SAFE SHUTDOWN EARTHQUAKE
SWC - SURGE WITHSTAND CAPABILITY
TID - TOTAL INTEGRATED DOSE
TRS - TEST RESPONSE SPECTRUM

FIGURE 1
GENERIC MODULE REQUIRED RESPONSE SPECTRUM
HORIZONTAL & VERTICAL OBE & SSE
1% OF CRITICAL DAMPING

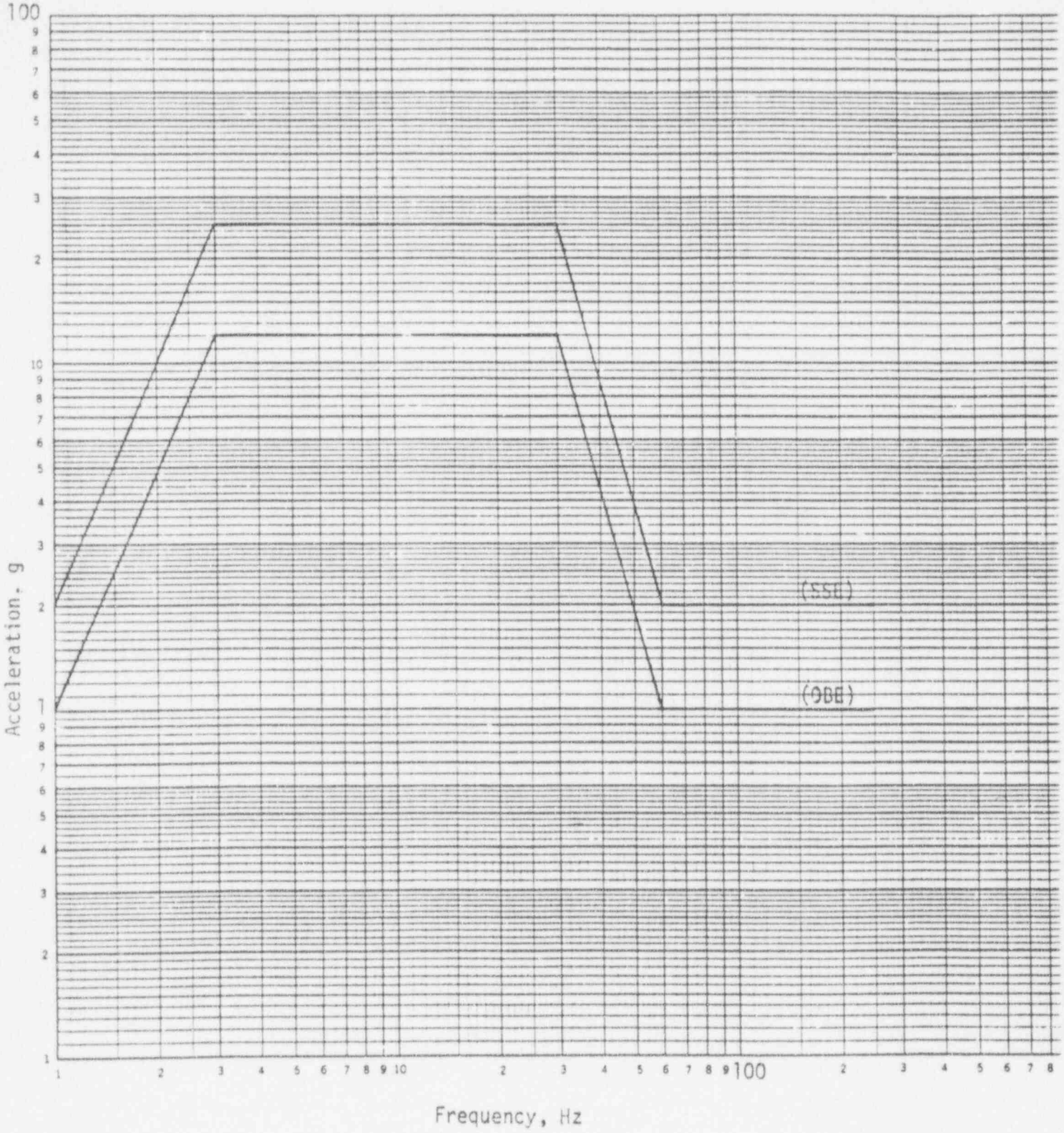
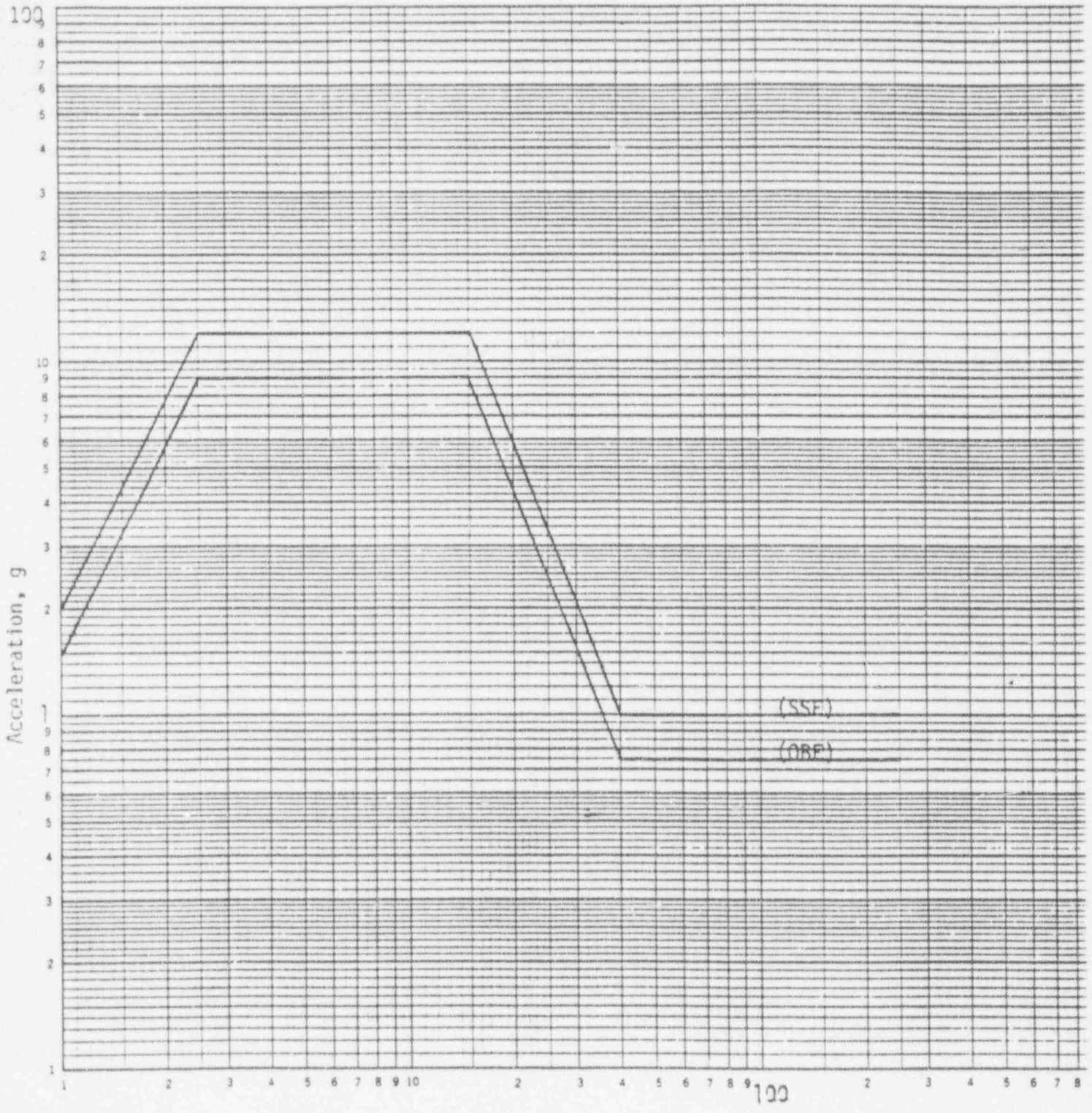


FIGURE 2
GENERIC FLOOR & WALL REQUIRED RESPONSE SPECTRUM
HORIZONTAL & VERTICAL OBE & SSE
1% OF CRITICAL DAMPING



NPX80\DP\7900103.WPD

HUMAN FACTORS PROGRAM PLAN

FOR THE

SYSTEM 80+

STANDARD PLANT DESIGN

NPX80-IC-DP790-01

Revision 04

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

This document is the property of ABB Combustion Engineering Nuclear Systems, Windsor, Connecticut, and is to be used only for the purposes of the agreement with ABB-CENS pursuant to which it is furnished.

Prepared by: _____ Date: _____
R.B. Fuld, Lead Engineer, Human Factors Engineering

Approved by: _____ Date: _____
D.L. Harmon, Supervisor, Control Room Engineering

Approved by: _____ Date: _____
W.J. Gill, Engineering Manager, Nuplex 80+ Project

Issue date _____

A-3 **Element Descriptions**

A-3.1 HFE Program Management[2]

A-3.1.1 Goals

A formal HFE Program is an important component of design team activities to reasonably ensure that 1) HFE input and operations experience is incorporated in system design and development activities to afford usable HSIs to plant operators, that 2) the final HSI design allows operators to sufficiently perform their normal and safety-related operating roles, and that 3) regulatory requirements pertinent to each of the HFE design process elements are satisfied.[3]

*[A-3.1.2 Requirements

A-3.1.2.1 Program Plan

Per the constraints previously defined under **Scope**, a description of the program management plan for HFE activities, herein referred to as the HFE Program Plan, shall be provided prior to certification that includes the following[4]:

A-3.1.2.1.1 **Responsible Management Structure** - The management and organization structure singularly responsible for the direction and integration of HFE in the design and construction of the proposed plant.

---

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

[3] A formal HFE program is recommended as a useful step towards satisfying the requirements of 10 CFR 50.34(f)(2)(iii) to provide a control room whose design reflects state-of-the-art human factors principles.

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

A-3.1.2.1.2 **Technical Resources** - The technical resources (i.e., HFE Specialists, Operations Experts) employed by the applicant to address usability issues in the design.

A-3.1.2.1.3 **Method of Interdisciplinary Interaction** - The manner by which the applicant ensures integration of HFE input and operations experience with I&C and systems design and construction. This shall include, for all incomplete and to-be-performed activities, the details of the methods of interdisciplinary interaction of the design and construction team members, including mechanisms of design tradeoff resolution and design review utilized under A-3.5, HSI Design.

A-3.1.2.1.4 **Method of Design Control** - The details of the method by which design control is exercised among team members.

A-3.1.2.1.5 **Design Process Elements** - Implementation of the following technical HFE elements in the design process:

a) Incorporation of Industry Experience
b) Evaluation and Allocation of System Functions
c) Task Analysis
d) Human-System Interface Design
e) Availability Verification
f) Suitability Verification
g) Design Validation

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

A-3.1.2.2 Responsibility

A-3.1.2.2.1 **Management Structure** - The Responsible Management Structure shall be responsible for a) the implementation of the HFE Program Plan, b) the conformance of the design and construction process and products of all team participants to the program requirements, and c) the resolution of all issues entered in the HFE Tracking System.

A-3.1.2.2.2 **HFE Specialists** - HFE Specialists (as defined in the Introduction) shall be employed by the Responsible Management Structure; the responsibilities of the HFE Specialists shall include the origination of all technical HFE products specified in the HFE Program Plan.

A-3.1.2.2.3 **Operations Experts** - Operations Experts (as defined in the Introduction) shall be employed by the Responsible Management Structure; the responsibilities of the Operations Experts shall include the review of all official milestone HSI design products for usability concerns.

A-3.1.2.2.4 **Interdisciplinary Interaction and Design Control** - All design activities are subject to, and shall utilize the mechanisms and meet applicable requirements, of the overall design team quality assurance (QA) program[5]. However, such compliance shall be the responsibility of the overall design team quality assurance program management structure, and is therefore not governed by the HFE Program Plan.

A-3.1.2.3 Scheduling

For those HFE aspects of the design whose adequacy must be analytically or empirically confirmed to satisfy Verification or Validation requirements, a schedule shall be provided showing that such evaluations will be complete and resulting questions will be resolved at or before the completion of construction of the facility[6].

A-3.1.2.4 Tracking

A-3.1.2.4.1 **Tracking System** - A Tracking-of-Open-Issues (TOI) function shall be provided to ensure the proper disposition of HFE issues formally raised in design and construction analyses and evaluations.

---

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

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

A-3.1.2.4.2 **System Entries** - TOI entries shall include the source and a description of the issue; a Calendar-referenced commitment date for resolution; and a deadline for its implementation.

A-3.1.2.4.3 **Resolution of Entries** - Resolution of TOI entries shall include the source and description of the resolution; and a Calendar-referenced commitment date for its implementation.

A-3.1.2.4.4 **Implementation of Resolutions** - Closeout of TOI entries shall include a description of the final implementation; and verification of the properly completed implementation by a representative of the Responsible Management Structure.

A-3.1.2.4.5 **Unmet Commitments** - Unmet commitment dates shall be responded to with reentry and, if appropriate, an update of the issue/resolution, along with a new commitment date. This process shall be referred to herein as "updating" the entry. The updated issue/resolution shall supersede (equivalent to closing out) the preceding issue/resolution.

A-3.1.2.4.6 **TOI Database Closeout** - Following completion of the design's V&V activities specified by the HFPP, and the resolution of all TOI entries, a TOI database closeout report shall formally verify the closure of all TOI database items.

A-3.1.2.5 COL Applicant Turnover

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

- Task analysis data and reports
- HFE Standards, Guidelines, & Bases
- Verification & Validation plans, data and reports
- Design Validation scenarios & operating sequences
- TOI database and closeout report][7]*

[7] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.1.3 Acceptance Criteria

A-3.1.3.1 Program Plan

A-3.1.3.1.1 **Effective Date** - A formal HFE Program Plan as described in A-3.1.2.1 is in effect.

A-3.1.3.1.2 **Responsible Management Structure** - The Responsible Management Structure presented in the HFE Program Plan a) shows the chain of HFE accountability from the level of technical origination to the representatives of top-level program management, b) is specified by organizational position and primary responsibilities, and c) is supported on request by an official letter or memorandum identifying the individual(s) in each position.

A-3.1.3.1.3 **Technical Resources** - Resumes of all HFE Specialists and Operations Experts that have been employed by the program and for which the program takes credit (e.g., for acceptable origination of HFE products) are retained and available for review; their qualifications meet the definitions and requirements stated in the Program Plan.

A-3.1.3.1.4 **Method of Interdisciplinary Interaction** - The HFE Program Plan provides an explanation of the interdisciplinary design process as described in A-3.1.2.3.

A-3.1.3.1.5 **Method of Design Control** - The HFE Program Plan details or references overall design program procedures for applicable design control methods including review and sign-off of HFE analysis results.

A-3.1.3.1.6 **Design Process Elements** - Criteria for the various DPEs are provided within each Element.

A-3.1.3.2 Responsibility

A-3.1.3.2.1 **Management Structure** - The Responsible Project Office Manager and appropriate discipline managers have reviewed and approved a) the current HFE Program Plan, b) the design and construction products of all team participants for conformance

to these requirements (as indicated by their sign-off per A-3.1.3.5), and c) resolution and implementation of all TOI items.

A-3.1.3.2.2 **HFE Specialists**

a) HFE Specialists (as defined in the Introduction) are Employed by the Responsible Management Structure;

b) HFE Specialists have originated all technical HFE products specified in the HFE Program Plan.

A-3.1.3.2.3 **Operations Experts**

a) Operations Experts (as defined in the Introduction) are Employed by the Responsible Management Structure;

b) Operation Experts have reviewed all milestone HSI design products as documented by official memoranda.

A-3.1.3.3 Scheduling

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

A-3.1.3.4 Tracking

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

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

A-3.1.3.5 COL Applicant Turnover

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

A-3.2 Incorporation of Industry Experience[8]

A-3.2.1 Goals

Many valuable lessons from industry experience in design, construction, operation, incidents, and accidents have been developed and documented. Such material should be considered during the design process, to avoid or mitigate the occurrence of similar problems, and to contribute to producing a more effective final design product.

*[A-3.2.2 Requirements

A-3.2.2.1 Administrative Procedures

Prior to certification, administrative procedures shall be available and be implemented for evaluating operating, design, and construction experience, and for ensuring that applicable important industry experiences will be provided in a timely manner to those designing and constructing the plant, per 10 CFR 50.34(f)(3)(i). A record of resulting transmittals from such provisions shall be maintained to verify implementation.

A-3.2.2.2 References and Studies

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

A-3.2.2.3 Formal Treatment of Safety Issues

A-3.2.2.3.1 All Generic Safety Issues (GSIs) and Unresolved Safety Issues (USIs) shall be evaluated by, and the applicable issues disseminated throughout and receive formal disposition by, the Responsible Management Structure.

---

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

A-3.2.2.3.2 GSI and USI processing shall be controlled by formal procedures, implemented prior to certification.][9]*

A-3.2.3 Acceptance Criteria

A-3.2.3.1 Administrative Procedures

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

A-3.2.3.2 References and Studies

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

A-3.2.3.3 Formal Treatment of Safety Issues

Selective audit of the appropriate records indicates that GSIs and USIs have been evaluated, and are being tracked and dispositioned as required. Controlling procedures appear in official project documents or memoranda.

[9] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.3 Evaluation and Allocation of System Functions[10]

A-3.3.1 Goals

The collective facility systems must ensure the provision of certain operating functions to maintain successful performance, particularly in the area of the health and safety of the public. The human and machine elements within the ensemble should play complementary roles that make the successful accomplishment of these functions highly likely. To pursue this goal, the allocation of functions to the human and machine elements (particularly automated information processing and control) should consider how the facility is to be operated, how plant safety functions are accomplished, and the needs, capabilities, and limitations of the human operator (and the proposed machines.)

*[A-3.3.2 Requirements

A-3.3.2.1 Mandated Allocations

Prior to certification, the design shall incorporate these Federally mandated allocations of function:

a) Automatic indication of the Bypassed and Inoperable Status of Safety Systems; 10 CFR 50.34(f)(2)(v).

b) Automatic and manual initiation of auxiliary (and/or emergency) feedwater systems; 10 CFR 50.34(f)(2)(xii) and 50.62(c).

c) Automatic actuation of containment isolation systems, including all non-essential systems, on high containment pressure; 10 CFR 50.34(f)(2)(xiv)

d) No automatic reopening of automatically isolated containment valves on reset of automatic

---

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

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

e) Automatic isolation of containment system paths to environs on high radiation; 10 CFR 50.34(f)(2)(xiv)(E).

f) Automatic initiation of protective systems including reactivity control (i.e., reactor trip) systems; 10 CFR 50, Appendix A, GDC 20(1).

g) Automatic initiation of systems and components important to safety (i.e., Engineered Safety Features); 10 CFR 50, Appendix A, GDC 20(2).

h) Automatic initiation of turbine trip; 10 CFR 50.62(c).

A-3.3.2.2 Critical Safety Functions

Prior to certification, a description of the plant Critical Safety Functions and the design basis for their implementation shall be documented sufficient to permit understanding of the operator's safety-related role a) as allocated as an integral part of the overall system design, b) as incorporated by the design basis evaluations (which shall be referenced) performed to establish the adequacy of the plant Critical Safety Functions, and c) as evaluated by Task Analysis, Verification, and Validation activities[11].

This may be "in the form of a discussion, with specific references, of similarities to and differences from, facilities of similar design for which applications have been previously filed with the commission"[9]. Alternately, or if no predecessor system is extant, a formal systems analysis may be provided.

---

[11] This requirement is felt to be consistent with the general regulations of 10 CFR 50.34(b)(2) for "A description ... of the facility ... sufficient to permit understanding of the system designs and their relationship to safety evaluations."

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

A-3.3.2.3 HFE Evaluation of Allocations

The Task Analysis (Section A-3.4), Availability Verification (Section A-3.6), Suitability Verification (Section A-3.7), and Design Validation (Section A-3.8) activities shall be sources of feedback on allocation issues. Performance problems thus identified in the design product shall be resolved using TOI system mechanisms per the Requirements of A-3.1.2.4.1*[10]

A-3.3.3 Acceptance Criteria

A-3.3.3.1 Mandated Allocations

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

A-3.3.3.2 Critical Safety Functions

An official project document or memorandum exists which includes a description of the plant Critical Safety Functions and the design basis for their implementation as described in A-3.3.2.2.

[10] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.4 Task Analysis[11]

A-3.4.1 Goals

Task Analysis should identify the human operator's detailed input and output requirements for a representative set of control room, and remote shutdown tasks, and any local control tasks required by the EOGs. Task Analysis (TA) should also evaluate operator loading, to provide assurance that human performance capacities are not grossly or chronically exceeded by anticipated task demands. Task Analysis data can support the development/evaluation of the control room design, operating procedures, and operator training. Satisfactory TA results contribute to the basis for concluding that qualified operators are reasonably able to perform their required tasks, particularly those related to safety[12].

*[A-3.4.2 Requirements

A-3.4.2.1 Operational Basis

Task Analysis shall be based on operational input that provides a reasonable "best estimate" of how the plant will be operated. Source material should include a) operating procedures or operating guidelines for similar existing facilities, b) analyzed operating sequences for proposed new facilities, and c) the input of Operations Experts. The balance of a) and b) utilized should reflect the degree to which the facility is similar to existing designs.

---

[11] This Design Process Element corresponds to Element 5 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[12] The application of task analysis is a basic component of the Control Room Design Review (CRDR) process specified by Section I.D.1 of NUREG-0660. Section I.D.1 is the related post-TMI action plan item referenced (per Footnote 8, "for information only") by 10 CFR 50.34(f)(2)(iii); performance of task analysis may thus contribute to providing "a control room design that reflects state-of-the-art human factors principles."

A-3.4.2.2 Design Basis Task Inventory

The inventory of tasks subject to TA shall include the contents of the emergency operating guidelines, including any local control station tasks, as well as a representative selection of MCR and RSA tasks. Both normal operations and anticipated operating occurrences shall be represented, including startup, design basis load transients, shutdown, and uncomplicated reactor trip. "Worst case" justifications may be used to establish bounding cases and delimit the scope of analysis.

A-3.4.2.3 Level of Detail

The level of detail at which task elements are identified, and task element inputs and outputs are described, shall meet or exceed that embodied in the plant operating procedure steps.

A-3.4.2.4 Methodology

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

A-3.4.2.4.1 **Inputs and Outputs** - The TA data shall provide task element input and output characteristics in a manner sufficient to support the Verification of Availability as described in Section A-3.6.2.3.2.

A-3.4.2.4.2 **Workload Evaluation** - The TA shall incorporate a criterion-referenced method to evaluate operator loading. Analyzed conditions resulting in exceeding the loading criterion shall be entered for tracking as TOI issues per the Requirements of A-3.1.2.4.

A-3.4.2.5 Staffing Assumptions

The Task Analysis shall identify the relationship between the design basis for staffing and the staffing assumptions that are incorporated in the analysis, and shall verify (within the limits of the TA methodology) the acceptability of operator loading in terms of the design basis minimum staffing (as appropriate for the specified scenario).

A-3.4.2.6 Reporting of Results

Task Analysis reports shall provide a) an explanation of the methodology, assumptions, and criteria employed, b) citation of the inputs, bases, and references used, c) the resulting task element specification data, and d) a summary evaluation of the results, including identification of any specific concerns (e.g., cases of excessive loading). Reports shall receive formal interdisciplinary review from the design team.

A-3.4.2.7 Analysis of Human Error

Systematic error analysis is not required as part of the TA effort. While PRA activities may include HRA studies (and thus incorporate some Task Analysis activities) this shall be the responsibility of the PRA program and its associated management structure, and is therefore not governed by the HFE Program Plan or the present Process Element.

A-3.4.2.8 Role in Availability

The TA results, specifically the inventory of task elements and their data, shall serve as input to the Verification of Availability effort in A-3.6.1*[13]

A-3.4.3 Acceptance Criteria

A-3.4.3.1 Operational Basis

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

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

[13] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.4.3.2 Design Basis Task Inventory

A-3.4.3.2.1 The Task Analysis Report(s) describes analyses which include all emergency operating procedure tasks, and an additional selection of control room normal and abnormal operating procedures, including startup, design basis load transients, shutdown, and uncomplicated reactor trip.

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

A-3.4.3.3 Level of Detail

The level of task element detail of the TA is verified in the Task Analysis Report(s) to be not less than the level of detail provided by the plant operating procedure input.

A-3.4.3.4 Methodology

A-3.4.3.4.1 The TA method is demonstrated by example to provide the data required by Section A-3.6.2.3.2.

A-3.4.3.4.2 The TA method provides a criterion, basis, and evaluation of operator loading.

A-3.4.3.5 Staffing Assumptions

A-3.4.3.5.1 The design basis staffing and staffing assumptions incorporated in the analysis have been identified in the TA Report(s).

A-3.4.3.5.2 Operator loadings have been evaluated in the TA Report(s) for the design basis minimum staffing.

A-3.4.3.6 Reporting of Results

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

A-3.5 Human-System Interface Design[14]

A-3.5.1 Goals

The goal of Human-System Interface (HSI) design is to ensure that the final facility provides a thoroughly sufficient HSI, and a control room that reflects the State-of-the-Art in HFE. Stated differently, the aim is for the HSI designer's products to support the HSI user's needs. This is also the overall goal of HFE efforts; the specific efforts identified under HSI Design (the Process Element) focus on the provision and implementation of HFE Design Guidance, to provide criteria for and ensure the Suitability of the components comprising the HSI (e.g., labelling, layout, etc.)[15]

*[A-3.5.2 Requirements

A-3.5.2.1 HFE Design Guidance

A-3.5.2.1.1 **Provision** - Prior to certification, a collection of pertinent Human Factors Principles, as defined in the Introduction, shall be assembled by the design team to be applied to the HSI design as HFE Design Guidance.

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

---

[14] This Design Process Element corresponds to Element 6 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[15] As noted under I.3.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for Task Analysis, HFE design guidelines are a central component of CRDR; presuming sound bases for such guidelines, they may be construed as the required "principles" themselves. Incorporation of sound HFE Design Guidance in the design process thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

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

A-3.5.2.1.3 **Basis** - A technical basis for the HFE Design Guidance shall be provided. This shall include the scientific and/or technical references, studies, or rationale that supports the HFE Design Guidance provided. Justification in terms of juried scientific and technical publications shall be an acceptable basis for HFE Design Guidance; however, this shall not preclude the use of a priori reasoning.

A-3.5.2.1.4 **Content** - The HFE Design Guidance shall include coverage of the following topics:

a) Annunciator Warning Systems
b) Visual and Auditory Indications
c) Controls
d) Process Computers
e) Display-control Integration
f) Panel Layout and Organization
g) Labeling and Locator Aids
h) Workspace Layout and Environment
i) Communications
j) Anthropometry
k) Maintainability

This organization of the topics is provided for information only, and is not itself required.

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

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

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

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

A-3.5.2.2 HFE Design Assumptions

A-3.5.2.2.1 **Workspace Conditions** - The HSI design and the corresponding HFE Design Guidance shall accommodate working conditions imposed within applicable workspaces as assumed in the analysis of SRDBEs, as defined in the Introduction.

A-3.5.2.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the HSI design or HFE Design Guidance shall not preclude the ability of the design to satisfy the requirements of 10 CFR 50.54(m)(2)(i) for minimum staffing.

A-3.5.2.3 Reference Design

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

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

A-3.5.2.3.3 **Mockup Development** - The Reference Design documentation of A-3.5.2.3.1 shall be the basis for corresponding HSI mockups constructed for use in Suitability Verification.]* [16]

A-3.5.3 Acceptance Criteria

A-3.5.3.1 HFE Design Guidance

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

---

[16] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.5.3.1.2 **Applicability** - The HFE Design Guidance, either through its contents or promulgation, formally indicates its applicability as specified under A-3.5.2.1.2.

A-3.5.3.1.3 **Basis** - A technical basis for the HFE Design Guidance has been provided as specified under A-3.5.2.1.3. If original, it has been explained by an HFE Specialist.

A-3.5.3.1.4 **Content** - The HFE Design Guidance includes coverage of the topics specified under A-3.5.2.1.4.

A-3.5.3.1.5 **Promulgation** - The HFE Design Guidance is verified by document distribution forms to have been formally promulgated by the Responsible Management Structure to the design team for implementation in the design.

A-3.5.3.2 HFE Design Assumptions

A-3.5.3.2.1 **Workspace Conditions** - The HSI design and the corresponding HFE Design Guidance shall accommodate working conditions imposed within applicable workspaces as assumed in the analysis of Safety-Related Design Basis Events, as defined in the Introduction.

A-3.5.3.2.2 **Staffing Assumptions** - Staffing assumptions embodied in the HSI design or HFE Design Guidance shall not preclude the ability of the design to satisfy the requirements of 10 CFR 50.54(m)(2)(i) for minimum staffing.

A-3.5.3.3 Reference Design

A-3.5.3.3.1 The Reference Design for HSI systems and equipment documented and reviewed per the Requirements of A-3.5.2.3.

A-3.5.3.3.2 Corresponding mockups are verified to have been constructed for the Reference Design HSI.

A-3.6 Availability Verification[17]

A-3.6.1 Goals

The goal of Availability Verification is to ensure and document the presence, range, accuracy, etc. of the Indication and Control Features (as defined in the Introduction) for required emergency procedure tasks, and required for operators to perform other necessary operating tasks in the main control room and the remote shutdown area, per GDC 13 and 19 of 10 CFR 50, Appendix A.[18]

*[A-3.6.2 Requirements

A-3.6.2.1 Mandated Availability - The design shall make Available the following Federally mandated Indication and Control Features:

a) Integrated display of safety parameter indications; 10 CFR 50.34(f)(2)(iv).

b) Indication of the Bypassed and Inoperable Status of Safety Systems; 10 CFR 50.34(f)(2)(v).

c) Indication of relief and safety valve position; 10 CFR 50.34 (f)(2)(xi).

d) Indication of auxiliary feedwater system flow; 10 CFR 50.34 (f)(2)(xii).

---

[17] This Design Process Element, along with Suitability Verification and Validation, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[18] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for Task Analysis (and as an explicit and objective use of the Task Analysis results), Availability Verification is a central component of CRDR. Verification of Availability thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

e) Control of auxiliary feedwater system initiation; 10 CFR 50.34 (f)(2)(xii).

f) Indication of containment pressure; 10 CFR 50.34(f)(2)(xvii).

g) Indication of containment water level; 10 CFR 50.34(f)(2)(xvii).

h) Indication of containment hydrogen concentration; 10 CFR 50.34(f)(2)(xvii).

i) Indication of containment (high level) radiation intensity; 10 CFR 50.34(f)(2)(xvii).

j) Indication of noble gas effluents at potential accident release points; 10 CFR 50.34(f)(2)(xvii).

k) Indication of inadequate core cooling; 10 CFR 50.34(f)(2)(xviii).

l) Post-Accident Monitoring Indications; 10 CFR 50.34(f)(2)(xix).

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

A-3.6.2.2 I&C Inventory

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

a) that allows the elements of the Task Inventory identified in A-3.4.2.2 (i.e., their inputs and outputs) to be indexed and tracked against it the entries of I&C Inventory, and vice-versa;

b) whose data entries shall include device type, units, and required range, scale precision, and accuracy.

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

A-3.6.2.3 Formal Analysis

Prior to the combined operating license, a formal Availability Analysis will be performed to create the I&C Inventory and test/verify its content against the TA Task Inventory.

A-3.6.2.4 Methodology

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

A-3.6.2.5 Analysis Report

Report(s), explaining the methodology and summarizing the results of the formal Availability Analysis, including all discrepancies between required and actual I&C availability, shall be provided, and receive formal interdisciplinary review from the design team.

A-3.6.2.6 Discrepancies

Discrepancies between required and actual I&C availability specified by A-3.6.2.1 or A-3.6.2.2 shall be entered as TOI issues per the Requirements of A-3.1.2.4.][19]*

A-3.6.3 Acceptance Criteria

A-3.6.3.1 Mandated Availability

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

---

[19] Any change to this information requires NRC Staff approval prior to implementing the change.

A-3.6.3.2 I&C Inventory Database

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

A-3.6.3.3 Formal Analysis

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

A-3.6.3.4 Methodology

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

A-3.6.3.5 Analysis Report

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

A-3.6.3.6 Discrepancies

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

A-3.7 Suitability Verification[20]

A-3.7.1 Goals

The goal of Suitability Verification is to ensure that the HSI's various Indication and Control Features (as defined in the Introduction) afforded by the main control room, the remote shutdown area, and the local control stations required for executing emergency procedures, are Usable designs that will support the operator's successful task accomplishment per the applicable HFE Design Guidance.[21]

*[A-3.7.2 Requirements

A-3.7.2.1 Formal Analysis

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

A-3.7.2.2 Relationship to HFE Design Guidance

Because of the necessarily generic and context-free nature of HFE Design Guidance, and the context-dependent nature of design tradeoffs, conformance to HFE Design Guidance is not itself a requirement.

---

[20] This Design Process Element, along with Availability Verification and Validation, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[21] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for HFE Design Guidance (and as an explicit application of that Guidance), Suitability Verification is a central component of CRDR. Verification of Suitability thus contributes directly to satisfying 10 CFR 50.34(f)(2)(iii).

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

A-3.7.2.3 Fidelity

Suitability Analysis shall utilize mockups or other representations of the completed design that manifest fidelity of the design characteristics being evaluated by the HFE Design Guidance. This may include evaluation of the completed design itself (e.g., a survey of installed lighting levels.)

A-3.7.2.4 Methodology

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

A-3.7.2.5 Analysis Report

Suitability Analysis report(s), explaining the methodology and summarizing the results of Suitability Analysis, including all discrepancies identified between the HFE Design Guidance and the actual design, shall be provided. Reports shall receive formal interdisciplinary review from the design team.

A-3.7.2.6 Discrepancies and Concerns

Discrepancies between the design and the HFE Design Guidance, and other concerns identified in Suitability Analysis reports, shall be entered as TOI issues per the Requirements of I.2.1.2.4.]* [22]

A-3.7.3 Acceptance Criteria

A-3.7.3.1 Formal Analysis

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

A-3.7.3.2 Relationship to HFE Design Guidance

---

[22] Any change to this information requires NRC Staff approval prior to implementing the change.

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

A-3.7.3.3 Fidelity

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

A-3.7.3.4 Methodology

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

A-3.7.3.5 Analysis Report

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

A-3.7.3.6 Discrepancies and Concerns

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

A-3.8 Design Validation[23]

A-3.8.1 Goals

The goal of design Validation is to ensure that the sum of the various HSI design features afforded by the main control room, the remote shutdown area, and local control stations required for executing emergency procedures, provide Usable design ensembles that support the successful accomplishment of the operator's functional role (i.e., as specified by training and procedures) under dynamic, real-time conditions.[24]

*[A-3.8.2 Requirements

A-3.8.2.1 Formal Evaluation

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

A-3.8.2.2 Relationship to Design Basis

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

---

[23] This Design Process Element, along with Availability Verification and Suitability Verification, corresponds to Element 8 of HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors.

[24] As noted under I-2.4.1, 10 CFR 50.34(f)(2)(iii) refers to Control Room Design Review (CRDR) when mandating "state-of-the-art human factors principles" in the control room design. As was true for the Availability and Suitability aspects of Verification, Validation is a central (and the final) component of CRDR. Conduct of Validation exercises thus contribute directly to satisfying 10 CFR 50.34(f)(2)(iii).

safety function limits that will serve as acceptance criteria. The scenarios shall include normal operations (startup, design basis load transients, shutdown, and uncomplicated reactor trip), emergency operations, and all SRDBEs (as defined in the Introduction) which credit operator actions in their analysis.[25]

A-3.8.2.3 Fidelity

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

A-3.8.2.4 Evaluation Report

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

A-3.8.2.5 Discrepancies and Concerns

Failures to meet Validation criteria, and other evaluator concerns identified in the Validation

---

[25] This scope for Validation, one that includes both the intended methods of dealing with emergencies (i.e., the Emergency Operating Procedures) and the design basis emergencies themselves, is felt to provide a reasonable basis in the area of HFE, consistent with the extent and content of actual design basis safety analyses, for reaching "a final conclusion on ... safety questions associated with the design" per 10 CFR 52.47(a)(2).

Reports, shall be entered as TOI issues per the Requirements of A-3.1.2.4.][26]*

A-3.8.3 Acceptance Criteria

A-3.8.3.1 Formal Evaluation

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

A-3.8.3.2 Relationship to Design Basis

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

A-3.8.3.3 Fidelity

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

A-3.8.3.4 Evaluation Report

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

A-3.8.3.5 Discrepancies and Concerns

Failures to meet the Validation criteria, and other evaluator concerns identified in the Validation Reports, have been entered as TOI issues for resolution.

---

[26] Any change to this information requires NRC Staff approval prior to implementing the change.

NPX80\VP\7900301.WPD

HUMAN FACTORS ENGINEERING

VERIFICATION AND VALIDATION PLAN

FOR

NUPLEX 80+

NPX80-IC-VP790-03

Revision 02

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

This document is the property of ABB Combustion Engineering Nuclear Systems, Windsor, Connecticut, and is to be used only for the purposes of the agreement with ABB-CENS pursuant to which it is furnished.

Prepared by _____ Date _____
R.L. Rescorl, Man-Machine Interface Design

Prepared by _____ Date _____
R.B. Fuld, Lead Engineer, Human Factors Engineering

Approved by _____ Date _____
D.L. Harmon, Supervisor, Control Room Engineering

Approved by _____ Date _____
W.J. Gill, Manager, Nuplex 80+ Project

Issue Date _____

2.0 SCOPE

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

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

---

[1] NRC Staff approval is required prior to implementing a change in this information; see the System 80+ Design Control Document.

*[[6.0 V&V TASK METHODOLOGY AND CRITERIA

6.1 AVAILABILITY VERIFICATION

6.1.1 Purpose

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

Phase 1 (Availability Analysis) assures the following:

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

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

   b. Federally mandated indication and control requirements and,

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

   d. Each entry has a specified basis.

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

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

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

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

2. Identifying candidate HSI indications or controls for removal.

6.1.2 Scope

Phase 1 (Availability Analysis)

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

1. Federally mandated indication and control requirements,

2. ICR (from FTA) and,

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

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

6.1.3 Resources

The following resources will be available:

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

- ICR from the FTA;

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

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

- HFE TOI database;

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

6.1.4 Methodology

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

6.1.4.1 Phase 1 Methodology (Availability Analysis)

The following activities are performed (see Figure 7.1):

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

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

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

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

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

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

1. HFE identified requirements (as verified in Phase 1) from the ICR, Federally mandated

requirements, etc. (e.g., display, control or annunciator required, fixed position for a required display, method of display (e.g. analog, time history)).

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

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

6.1.4.2 Phase 2 Methodology (Availability Inspection)

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

6.1.5 Criteria

6.1.5.1 Phase 1 Availability Analysis Criteria

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

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

b) Indication of the Bypassed and Inoperable Status of Safety Systems; 10 CFR 50.34(f)(2)(v).

c) Indication of relief and safety valve position; 10 CFR 50.34 (f)(2)(xi).

d) Indication of auxiliary feedwater system flow; 10 CFR 50.34 (f)(2)(xii).

e) Control of auxiliary feedwater system initiation; 10 CFR 50.34 (f)(2)(xii).

f) Indication of containment pressure; 10 CFR 50.34(f)(2)(xvii).

g) Indication of containment water level; 10 CFR 50.34(f)(2)(xvii).

h) Indication of containment hydrogen concentration; 10 CFR 50.34(f)(2)(xvii).

i) Indication of containment (high level) radiation intensity; 10 CFR 50.34(f)(2)(xvii).

j) Indication of noble gas effluents at potential accident release points; 10 CFR 50.34(f)(2)(xvii).

k) Indication of inadequate core cooling; 10 CFR 50.34(f)(2)(xviii).

l) Post-Accident Monitoring Indications; 10 CFR 50.34(f)(2)(xix) and in accordance with Reg Guide 1.97 (Reference 12; as specitied in CESSAR-DC Section 7.5).

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

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

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

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

6.1.5.2 Phase 2 Availability Inspection Criteria

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

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

6.2 SUITABILITY VERIFICATION

6.2.1 Purpose

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

6.2.2 Scope

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

6.2.3 Resources

The following resources will be available:

- sources for the individual panel I&C features from the individual panel reports as exemplified by the panel mockups or prototypes;

- prototypes of added HSI features;

- HFE Standards, Guidelines, and Bases for System 80+;

- suitability inspection criteria provided in the form of checklists (to be developed as part of the suitability verification process), as exemplified in Reference 4;

- HFE TOI database;

- a qualified HFE specialist and an operations expert to perform the analysis.

6.2.4 Methodology

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

6.2.4.1 Phase 1 (Suitability Analysis) Methodology

Suitability analysis will be performed to cover all indication and control features and environmental conditions in the MCR, the RSR, and local control stations specified in the EPGs. Groups of HSI features (e.g., a particular panel, local control station, etc.) will be subjected to Suitability analysis as they are readied by the design process. All HSI elements (e.g.,

annunciators, displays, controls, etc.) will be included in and reviewed as part of the verification of one or another such groups. New or non-standard features will require the most scrutiny, while standard features will be more familiar.

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

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

6.2.4.2 Phase 2 (Suitability Inspection)

Using the bottom-up approach, the analyst will evaluate the various aspects of the prototype HSI for conformance to applicable portions of Reference 6. Nonconformances to Reference 6 Standards must be documented.

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

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

The checklist includes a place for comments.

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

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

6.2.5 Criteria

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

6.3 VALIDATION

6.3.1 Purpose

The purpose of validation is to ensure that the sum of the various HSI features afforded by the MCR, RSR, and any local control stations specified in the EPGs provide usable work ensembles that support the successful accomplishment of the operator's required tasks (i.e., to validate performance of the integrated Man-Machine system for System 80+). Validation includes exercise of specified scenarios and plant operating sequences (per the Scope in 6.3.2). Validation tests the following objectives:

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

2. Confirmation of Task Analysis results;

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

4. Allocation of functions and operator situational awareness;

5. Operator communication and team interaction;

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

7. Alarm system effectiveness.

6.3.2 Scope

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

6.3.3 Resources

The following resources are required for validation:

6.3.3.1 Facilities

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

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

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

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

These facilities shall conform to the following requirements:

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

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

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

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

6.3.3.2 Operating Sequences

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

1. Technically complete procedure guidance;

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

6.3.3.3 Team Personnel

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

6.3.4 Methodology

6.3.4.1 General Description

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

Validation team personnel, including both observers and performers, will hold a pre-scenario briefing on the purpose and objectives of the exercises. The team will then participate in the planned real-time scenario. Afterwards, observers and performers will hold a post-

exercise evaluation, to complete the subjective data and review the objective results. Walk-throughs or other analyses may be used to supplement these data.

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

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

6.3.4.2 Operating Sequences

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

A. Normal Operation (using Normal Operating Sequences)

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

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

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

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

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

B. Abnormal Operation (using Abnormal Operating Sequences)

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

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

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

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

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

6. Loss of Instrument Air from 100% power

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

8. Stuck open PZR relief valve

9. Loss of Shutdown cooling

10. Loss of Service Water/Component cooling Water

11. Turbine and Main Generator Trips

12. Seismic Event

C. Emergency Operation (using EPGs)

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

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

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

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

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

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

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

D. HSI and I&C Equipment Failure Sequences

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

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

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

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

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

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

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

1. Reactor Coolant System
2. CEDMECS
3. Shutdown Cooling System
4. Safety Injection & Rapid Depressurization Systems
5. Service Water/Component Cooling Water Systems
6. Containment Isolation
7. Containment Spray & Fan Cooler Systems
8. Annulus Ventilation System
9. Hydrogen Monitoring & Control
10. Fuel Pool Purification and Cooling
11. Main Steam System
12. Feedwater Systems
13. Pressurizer Pressure Control

14. CVCS
15. Reactor Coolant Gas Vent System
16. HVAC Systems
17. Instrument Air System
18. Electrical Systems & Emergency Power Sources
19. Nuclear Instrumentation
20. Reactor Protection System
21. Release Path Monitoring, Control, & Isolation

F. Offnormal or Alarm Conditions

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

6.3.4.3 Performance Measures

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

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

Two basic approaches to data generation will be used:

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

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

Scenario-specific objective criteria and subjective evaluation tools will be provided for each scenario. Reference 5 provides relevant guidance on performance evaluation in simulation environments. Specifications for performance measurement must be prepared according to the requirements of Appendix B.

6.3.4.4 Operating Ensemble Validation Activities

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

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

6.3.5 Criteria

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Validate time response for credited operator actions:

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

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

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

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

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

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

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

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

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

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

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

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

   g. Operators can identify automatic actuation of safety systems.

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

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

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

5. Validate operator communication and team interaction:

   a. Operators are able to communicate with each other effectively (e.g. there is no excessive noise, and

tasks requiring coordination were completed without excessive repetition of commands and confirmation).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

l. Alarms are not inadvertently acknowledged.

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

n. Operators can establish an additional alarm setpoint on a condition in alarm.]]*[2]

---

[2] NRC Staff approval is required prior to implementing a change in this information; see the System 80+ Design Control Document.

7.3 VALIDATION SCHEDULE & MILESTONES

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

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

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

To perform the validation exercises the following must be available:

1. Validation facilities per Section 6.3.3.1;

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

3. Validation scenarios and objective plant function limits and criteria for the operating sequences listed in Section 6.2 2;

4. Scenario-specific evaluation tools.

[[The results of validation exercises will be presented in Validation Reports. Closeout of validation (i.e., the final design validation report) shall include an appendix with the resolution for each formal validation finding produced during the process.]][3]

The validation process is illustrated on Figure 7.3.

---

[3] NRC Staff approval is required prior to implementing a change in this information; see the System 80+ Design Control Document.

8.0 HFE V&V ADMINISTRATIVE PROCEDURES

8.1 FINDINGS REPORTING & RESOLUTION

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

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

The Responsible Management Structure of HFE V&V will ensure that all comments related to the findings and resolutions are reviewed by the design team, and any open issues tracked and resolved, per the requirements of Reference 1. The Responsible Management Structure of HFE V&V will also ensure that any finding and resolution requiring a design change is entered into the TOI database.]]*[4]

Availability Verification

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

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

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

---

[4] NRC Staff approval is required prior to implementing a change in this information; see the System 80+ Design Control Document.

APPENDIX B V&V IMPLEMENTATION DETAILS

A. AVAILABILITY VERIFICATION

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

B. SUITABILITY VERIFICATION

1. *[[Prior to suitability verification, a detailed schedule with milestones must be provided.]]*[5]

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

C. VALIDATION

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

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

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

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

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

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

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

---

[5] NRC Staff approval is required prior to implementing a change in this information; see the System 80+ Design Control Document.

ATTACHMENT 5

LIST OF TABLES

APPENDIX 5F

Table	Subject
5F-1	Summary of the Benefits and Limitations of Potential Design Changes
5F-2	Summary of Cases Analyzed for Multiple Steam Generator Tube Rupture
5F-3	System 80+ Secondary System Valves
5F-4	~~Sequence of Events for SGTR~~ This item intentionally blank.
5F-5	Parameter Values for Analyses
5F-6	Summary of Design Features Added to System 80 to Preclude Lifting MSSVs on SGTR in System 80+
5F-7	Sequence of Events for Case 1, Steam Generator Tube Rupture (Base Case for 1 Tube)
5F-8	Sequence of Events for Case 2, Steam Generator Tube Rupture (Base Case for 5 Tubes)
5F-9	Sequence of Events for Case 3, Steam Generator Tube Rupture (1 Tube) with MSIS on High SG Level Bypassed
5F-10	Sequence of Events for Case 4, Steam Generator Tube Rupture (5 Tubes) with MSIS on High SG Level Bypassed
5F-11	Sequence of Events for Case 5, Steam Generator Tube Rupture (1 Tube) with Auxiliary Spray on N-16 Indication
5F-12	Sequence of Events for Case 6, Steam Generator Tube Rupture (5 Tubes) with Auxiliary Spray on N-16 Indication
5F-13	Sequence of Events for Case 7, Steam Generator Tube Rupture (1 Tube) with RCGV Actuated on N-16 Indication
5F-14	Sequence of Events for Case 8, Steam Generator Tube Rupture (5 Tubes) with RCGV Actuated on N-16 Indication
5F-15	Sequence of Events for Case 9, Steam Generator Tube Rupture (1 Tube) with SG Blowdown (High) on N-16 Indication
5F-16	Sequence of Events for Case 10, Steam Generator Tube Rupture (5 Tubes) with SG Blowdown (High) on N-16 Indication

LIST OF FIGURES

APPENDIX 5F

Figure	Subject
5F-1	MSSV Lift Time vs. No. of Tubes Ruptured
5F-2	RCS and SG Pressures vs. Time for 5 Tubes Ruptured and Automatic Rapid Depressurization System
5F-3	RCS and SG pressures vs. Time for 5 Tubes Ruptured and Automatic SG Liquid Blowdown
5F-4	System for Automatic Steam Generator Liquid Blowdown to Condenser
5F-5	RCS and SG Pressures vs. Time for 5 Tubes Ruptured and Automatic SG Liquid Blowdown to Condenser
5F-6	RCS and SG Pressures vs. Time for 5 Tubes Ruptured and Automatic Rapid Depressurization System
5F-7	System for Automatic Steam Generator Liquid Blowdown to IRWST with Design Change
5F-8	RCS and SG Pressures vs. Time for 5 Tubes Ruptured and Automatic SG Liquid Blowdown to IRWST
5F-9	Automatic Atmospheric Dump Valve System
5F-10	RCS and SG pressures vs. Time for 5 Tubes Ruptured and Automatic ADVs
5F-11	Primary System Components
5F-12	Secondary System Components
5F-13	~~CEPAC vs CENTS Comparison, SGTR Event Results~~ This item intentionally blank.
5F-14	RCS and SG Pressures vs. Time, Case 1 for 1 Tube Ruptured and Current System 80+ Design
5F-15	Leak, HPSI and Bypass Flow Rates vs. Time, Case 1 for 1 Tube Ruptured and Current System 80+ Design
5F-16	Steam Generator Level vs. Time, Case 1 for 1 Tube Ruptured and Current System 80+ Design

SGTR events is evaluated. Second, proposed design changes are evaluated to determine their benefit. Third, the Appendix establishes a criterion to use for measuring the benefits of the various design options. This criterion is the length of time from the initiation of the event until the operator must take action to prevent opening of the MSSVs.

1.3 SCOPE

This Appendix identifies the preventative and mitigative features of the current System 80+ design that prevent or limit radiological release following SGTR events. Eleven design changes proposed to enhance the plant response to SGTR are also identified and described. Methods employed to determine the realistic or best estimate responses of the plant are presented. These methods are employed to determine the response for the current plant design and for each of the proposed design changes. The intent is to provide realistic analytical estimates of the actual behavior, given a SGTR, so that valid comparisons may be made among the various proposed changes.

An evaluation of each plant configuration is provided, based upon the design and the plant response. As stated above, a criterion is established as the time to open the MSSVs assuming no operator action. In addition to this criterion, the evaluation bases include other considerations. The economics of the plant response consequences are considered. For example, the extent of cleanup required or the likelihood of significant equipment damage is evaluated. The complexity of the design change is considered along with the complexity of utilizing it during an event.

Proveness of the design change is also considered. This is important in the System 80+ design process since much has been done to confirm the effective integrated behavior of interacting systems and components. Uniqueness of the effects of a proposed change is reviewed to ensure that unexpected equipment responses do not occur during other design basis events or operational evolutions.

A summary of the proposed design changes is given in Table 5F-1 where the significant benefits and limitations are listed for each change.

2.0 SUMMARY OF RESULTS

2.1 DESIGN OF THE SYSTEM 80+ PLANT FOR SGTR MITIGATION

The System 80+ evolutionary ALWR was derived, in part, from design evaluations of the System 80 NSSS over an eight year period. Changes that were incorporated into the System 80+ systems and component configurations have resulted in substantial increases in plant safety. The plant changes that increase safety are evident in the plant design and the verifications of their safety benefit are evident in the increased operating margins~~, and in the PRA evaluations presented in CESSAR-DC~~. Interactions among the plant systems and the control and protection systems have been studied and refined to yield the integrated System 80+ design. Significant changes to accommodate new bases for safety analyses and/or new acceptance criteria for Design Basis Events are thoroughly evaluated to ensure that the effectiveness of the System 80+ integration is maintained.

rejected for various reasons. One particular proposed change discussed in Section 3.10 is the automatic blowdown of steam generator liquid to the IRWST. ~~As demonstrated in Section 3.10~~, this proposed change is rejected because ~~a probabilistic argument demonstrates that~~ the spurious opening of the blowdown system would be ~~about two orders of magnitude~~ more likely than a true demand for the blowdown system.

Table 5F-2 summarizes these evaluations and the following analyses in Sections 3 and 4 of this Appendix demonstrate the sufficiency of the System 80+ design and the improvement in capability relative to the System 80 NSSS Standard Design to avoid containment bypass via MSSVs during a SGTR event.

3.0 DISCUSSION OF DESIGN CHANGES EVALUATED

Analysis and evaluations were performed on the current System 80+ design and on eleven proposed changes to the current design. This section presents a summary of the analytical results and an overview of the evaluation. Detailed analytical results are presented in Section 4.0.

A description of each change is given. These changes have been carried through the design process sufficiently to support the conclusions of the evaluations.

Benefits of each design change are highlighted, followed by the limitations.

3.1 CURRENT SYSTEM 80+ DESIGN

3.1.1 DESCRIPTION OF CURRENT DESIGN

The current System 80+ design provides a number of systems for use in mitigation of a tube rupture event. The design basis of these systems are not typically for the prevention or mitigation of a steam generator tube rupture event, however, their use, whether automatic or manual, decreases the probability of a main steam safety valve from lifting. The following systems will help mitigate the consequences of a tube rupture event:

1. The Turbine Bypass System (TBS) is an automatic system which provides a path to remove steam from the steam generators. In the event of steam generator tube rupture, the TBS will automatically relieve secondary pressure and dump steam to the condenser (See Section 5.5 for more detailed description). This system will regulate the pressure in the secondary system below the MSSV setpoint and remains effective until a MSIS is generated on high steam generator level.

2. The operator has the capability to initiate pressurizer spray if the Reactor Coolant Pumps (RCPs) are operating or auxiliary pressurizer spray if the RCPs are tripped. The pressurizer spray will reduce the primary pressure, thus, decreasing the primary to secondary leakage

3. The operator has the capability to throttle the safety injection pumps in order to lower the primary system pressure. This, if used in conjunction with the main or auxiliary spray, will allow the operator to reduce primary pressure, even to the point where there is almost zero leakage.

In addition, redesign of the control systems for this function may impact the ~~Probability Risk Assessment (PRA) or~~ plant availability. The ultimate configuration will be a first of a kind with unproven performance and additional complexity.

New instrumentation will be a first-of-a-kind design.

3.3 AUTOMATIC INITIATION OF AUXILIARY PRESSURIZER SPRAY

3.3.1 DESCRIPTION OF CHANGE

The Chemical and Volume Control System (CVCS) auxiliary spray is currently designed to provide auxiliary spray for control of pressurizer pressure and to allow for pressurizer cooling during final stages of normal shutdown when the RCPs are not operating to provide main spray capability. The auxiliary spray design consists of a pipe connection from the charging pumps that ties into the main pressurizer spray lines. A normally closed isolation valve prevents flow during normal operation. Operator action is required to initiate auxiliary spray to depressurize the RCS. Auxiliary spray is not required to perform any accident mitigation or safe shutdown functions for design basis events.

A design change considered to mitigate the consequences of a steam generator tube rupture event is to provide a signal to open the auxiliary spray isolation valve based on radiation detection (N-16) coincident with a reactor trip signal. In the event of a tube rupture, the reactor will trip and the N-16 monitor will generate a signal which will open the auxiliary spray isolation valve, start a charging pump if one is not already operating, align a source of water and start to depressurize the RCS. Lower RCS pressures will decrease the primary to secondary leakage and delay or possibly prevent the secondary pressure from reaching the MSSV setpoint.

3.3.2 BENEFITS

This design change requires minimal hardware changes but may require modification of control systems.

3.3.3 LIMITATIONS

In order to maximize auxiliary spray flow to obtain a rapid depressurization, the charging pumps would have to be isolated from the RCS. This would require additional changes to the control system including interfacing safety and non-safety control signals

A similar design has been used in Europe (Reference 6-4) where rapid depressurization minimizes the primary to secondary flow. However, the European design receives a SIAS with a coincident low pressurizer pressure and low pressurizer level. In the System 80+ design a SIAS occurs only on low pressurizer pressure. Therefore, the safety injection pumps will actuate and keep the RCS pressure high effectively defeating the auxiliary pressurizer spray from depressurizing the RCS. If the pressurizer goes solid, there is no benefit for auxiliary spray. Controlling or terminating SI flow using pressurizer level was not considered for System 80+ over concerns for level measurement inaccuracies and increased core damage frequency ~~(PRA)~~.

The benefit of this change must balance the need against the limitation that inadvertent operation of the blowdown system is more likely. Analysis has shown that this system need only be actuated if multiple tubes rupture. ~~The initiating event frequency for a single tube rupture, as presented in the EPRI ALWR PRA Key Assumptions and Groundrules, is 4.5E-03 per year. The NRC uses a value of 1.0E-02 per year as the frequency for SGTR events. There is no calculated frequency for multiple tube ruptures because no multiple SGTR events have occurred. However, in discussions between ABB-CE and the NRC, it has been generally agreed that the conditional probability of a multiple SGTR event involving 5 tubes is on the order of 1.0E-02. The probability that the automatic blowdown system will be required can be estimated as the probability of an SGTR event with multiple (5) ruptured tubes. Using the EPRI initiating event frequency, this probability is 4.5E-05. Using the NRC initiating event frequency, the value would be 1.0E-04.~~

Inadvertent initiation of the blowdown system has the potential to either dry out the affected SG, or overfill the IRWST or both. Inadvertent opening of the blowdown valves could occur due to a failure of both valves, an operator error in which the operator inadvertently initiated the blowdown system or a failure of the control system. The operators inadvertently initiating the blowdown system during normal operation is considered to be remote. ~~NUREG-1638 (NUCLARR) presents a mean failure rate of 1.86E-06 per hour for spurious opening of a motor operated valve. The probability of spurious opening of a single valve, based on a one year mission time, is (1.86E-06)*(8760) which equals 1.63E-02. Spurious opening of both valves is calculated as P(v1)*P(v2) + *P(v) where is the common cause failure factor. The EPRI ALWR PRA Key Assumptions and Groundrules present a value of 5.0E-02 for motor-operated valves. Therefore, the probability of spurious opening of both valves is 1.08E-03. IEEE-STD500, 1984 has a failure rate of 1.19E-06/hour for computation al modules (page 720). This value was used to estimate the failure probability for the automatic blowdown system based on an assumed mission time of one year. The probability of a spurious signal is calculated as (1.19E-06)*(8760) = 1.04E-02. The total probability of a spurious signal is calculated as (1.19E-06)*(8760) = 1.04E-02. The total probability for spurious opening of the blowdown valves is the sum of the spurious signal probability and the probability of the valves failing open. This equals 1.04E-02 + 1.08E-03 = 1.15E-02.~~

~~As calculated above, automatic blowdown system will be challenged at a frequency of 4.5E-05/year if EPRI numbers are used or 1.0E-04/year if NRC numbers are used.~~ The spurious opening of the blowdown valves ~~has an occurrence frequency of 1.15E-02/year. This shows that the spurious opening of the TBS valves~~ is ~~about 2 orders of magnitude~~ more likely than a true demand for the blowdown system.

3.11 AUTOMATIC INITIATION OF THE ATMOSPHERIC DUMP VALVES

3.11.1 DESCRIPTION OF CHANGE

Each main steam line in the current System 80+ design is provided with one manually operated atmospheric dump valve (ADV) to allow cooldown of the steam generators when the main steam isolation valves are closed, or when the main condenser is not available as a heat sink (see Figure 5F-9). The ADVs are designed to maintain the steam pressure below the lowest setting of the main steam safety valves during emergency shutdowns or plant hot standby conditions. Each valve is sized to allow a controlled plant cooldown in the event of a line break or tube rupture, which

4.0 SGTR ANALYSIS AND EVALUATION METHOD

4.1 METHODS OF ANALYSIS

The SGTR events presented in this Appendix were analyzed with best estimate analysis methods and assumptions. In addition, the analysis required the capability to actuate various plant systems/components based on specific conditions being reached in the plant during the transient. For these reasons the CEPAC interactive computer code was chosen to analyze the SGTR events with varying number of tubes being ruptured.

A technical description of the CEPAC code is provided in Reference 6-4. An overview of the primary system components that are modeled by the CEPAC is shown in Figure 5F-11. The code models the key nuclear steam supply system components such as the steam generators, reactor vessel and core, hot and cold legs, pressurizer, and reactor coolant pumps. For the primary system, key safety and control systems/components are modeled. These systems include the pressurizer sprays, heaters, relief and safety valves, safety injection pumps, charging and letdown flows, and reactor regulating and shutdown rods. Initial conditions and other plant design parameters pertaining to these models are provided by the user to initialize the code and to initiate transient calculations.

includes

The secondary system models include key components from the main feedwater valve to the turbine admission valves as shown in Figure 5F-12. The steam generators are modeled to receive feedwater from main and auxiliary feedwater systems and a steam generator liquid blowdown system is included. The main steam lines contain atmospheric dump, main steam safety, main steam isolation, turbine admission, and steam dump valves. Again, initial conditions and other plant design parameters relevant to the secondary system models are provided by the user to initialize and initiate transient calculations.

model

The CEPAC code is an interactive code which allows for inputting equipment and control system disposition as well as specific operator actions. The outputs from the code includes time-dependent graphical display, hard copy printouts of major transient parameter values, and transient parameter plots.

The CEPAC code has been benchmarked against other codes, such as, CESEC (Reference 6-5) and CENTS (Reference 6-6) for various plant transients and accidents including a SGTR. Reference 6-7 contains detailed discussion on these CEPAC benchmark analyses and Reference 6-8 contains comparison between the CENTS code and CESEC, the approved safety analysis transient code. The benchmark analysis results for the SGTR event are briefly discussed below.

The CEPAC bench mark analysis for the SGTR event was performed by comparing CEPAC results against those generated using the CENTS code. These results are presented in Figure 5F-13 and Table 5F-4. The event consists of a single tube ruptured in one steam generator for the 2700 Mwt class plant. As a result of the ruptured tube, Figure 5F-13 shows that the primary pressure initially decreases at a relatively slow rate. The pressurizer heaters automatically turn-on, charging flow is increased, and letdown is decreased as the pressurizer level decreases. The plant is tripped automatically at about 480 seconds as the subcooling margin trip is exceeded. The pressure rapidly

decreases after trip due to shrinkage in the RCS. The upper head begins to show small voiding at a pressure of 1500 psia. At 1300 psia, the operator trips the reactor coolant pumps in opposite loops. All plant safety systems function normally during the event.

A comparison of results between CEPAC and CENTS for the pressurizer pressure and level, steam generator pressure and downcomer levels, and hot and cold leg temperatures is also provided in Figure 5F-13. Generally, the CEPAC calculated results compare very well with CENTS. Both codes calculate the same general system response for this event.

The primary difference in results is in the steam generator pressure. The pressure at the time of reactor trip calculated by CEPAC spiked to a relatively high value and remained higher than the pressure calculated by CENTS. This difference in pressure response was traced to input differences between the two codes. By tuning the bypass valve area and opening time in CEPAC, the pressure response would better match that of CENTS.

The steam generator level response in the ruptured generator calculated by CEPAC is similar but higher than CENTS as shown in Figure 5F-13. These higher CEPAC values are due to the CEPAC automatic feedwater control, which matches the steam flow, compared with the level control used in CENTS analyses.

4.2 ANALYSIS ASSUMPTIONS

4.2.1 INITIAL CONDITIONS

Normal, full power plant conditions are assumed for the analyses (except initial power is 102%). See Table 5F-2 for parameter values used in the analyses.

4.2.2 BEST ESTIMATE ASSUMPTIONS

The following best estimate assumptions are made in the transient analyses presented in this Appendix:

1. Offsite power is available during the transient.

2. All control systems are assumed to be in the automatic mode.

3. No operator actions are included in the analysis.

4. Normal plant protection systems are assumed to be available.

5. Control system actuations during the transient are assumed to be at nominal setpoint values. Table 5F-5 gives the setpoints.

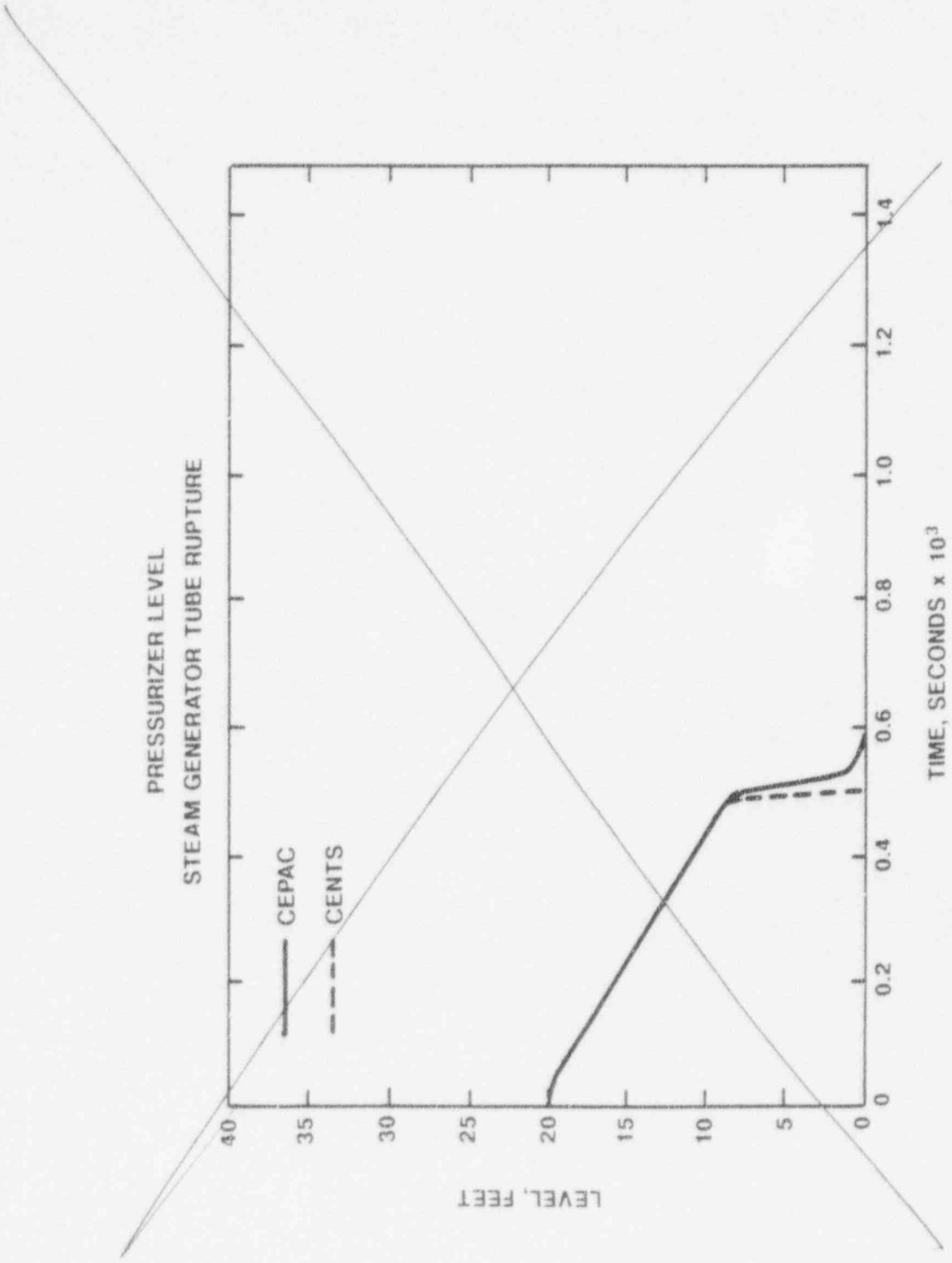
6. The condenser is assumed to be available for receiving steam flowing through the steam bypass valves from the steam generators and steam generator liquid that flows through the blowdown piping.

TABLE 5F-4

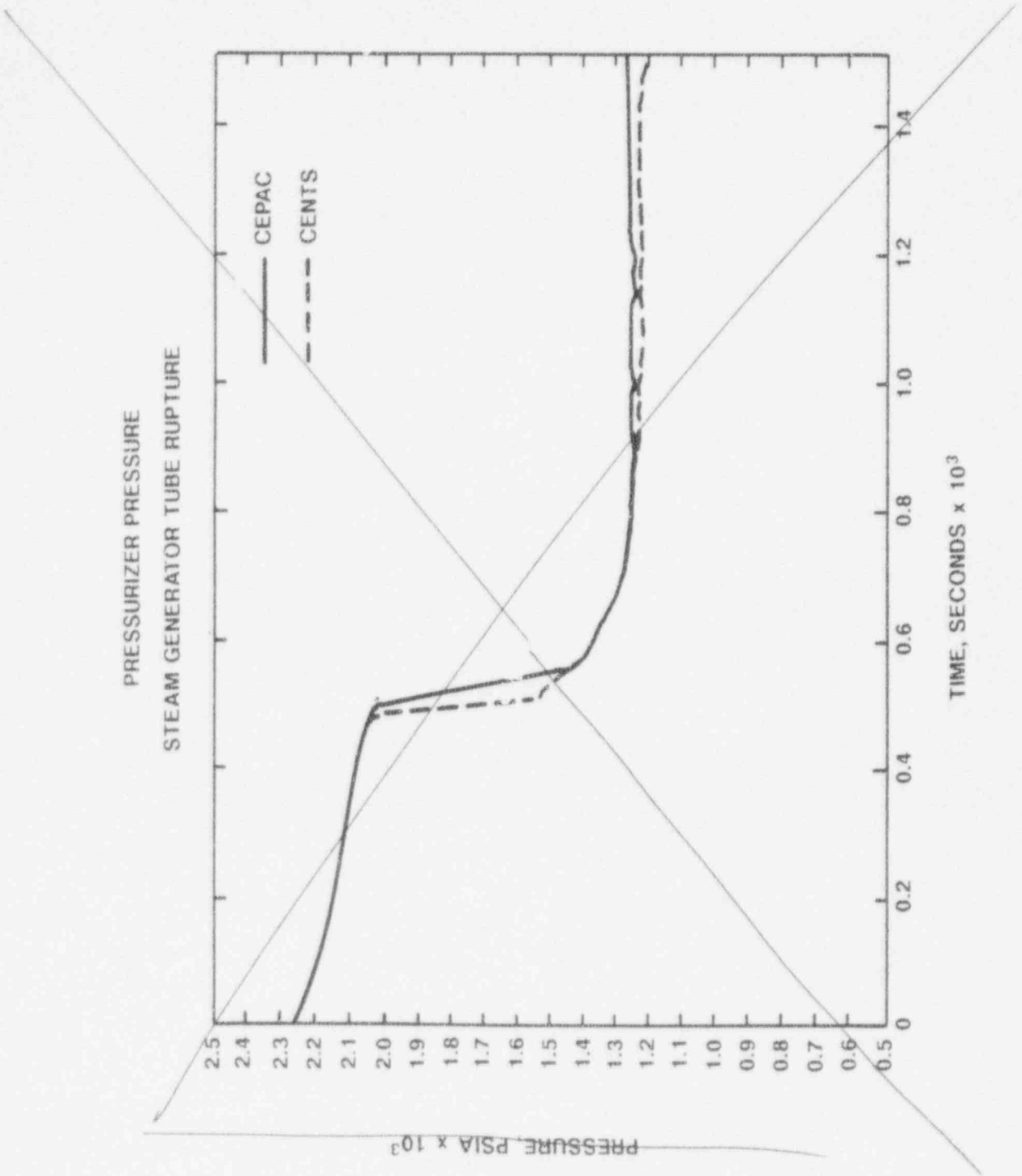
SEQUENCE OF EVENTS FOR SGTR

CEPAC	CENTS	EVENT
0	0	Steady-state 100% power
10	10	Initiation of SGTR (one tube)
80	80	Backup heaters on and full charging
495	480	Reactor Trip on subcooling margin
500	500	Main feedwater manually isolated
535	520	SIAS actuated: charging to max flow, letdown isolated
680	690	Trip two RCPs at 1300 psia
1170	1140	Auxiliary feedwater is automatically actuated with flow diverted to both steam generators

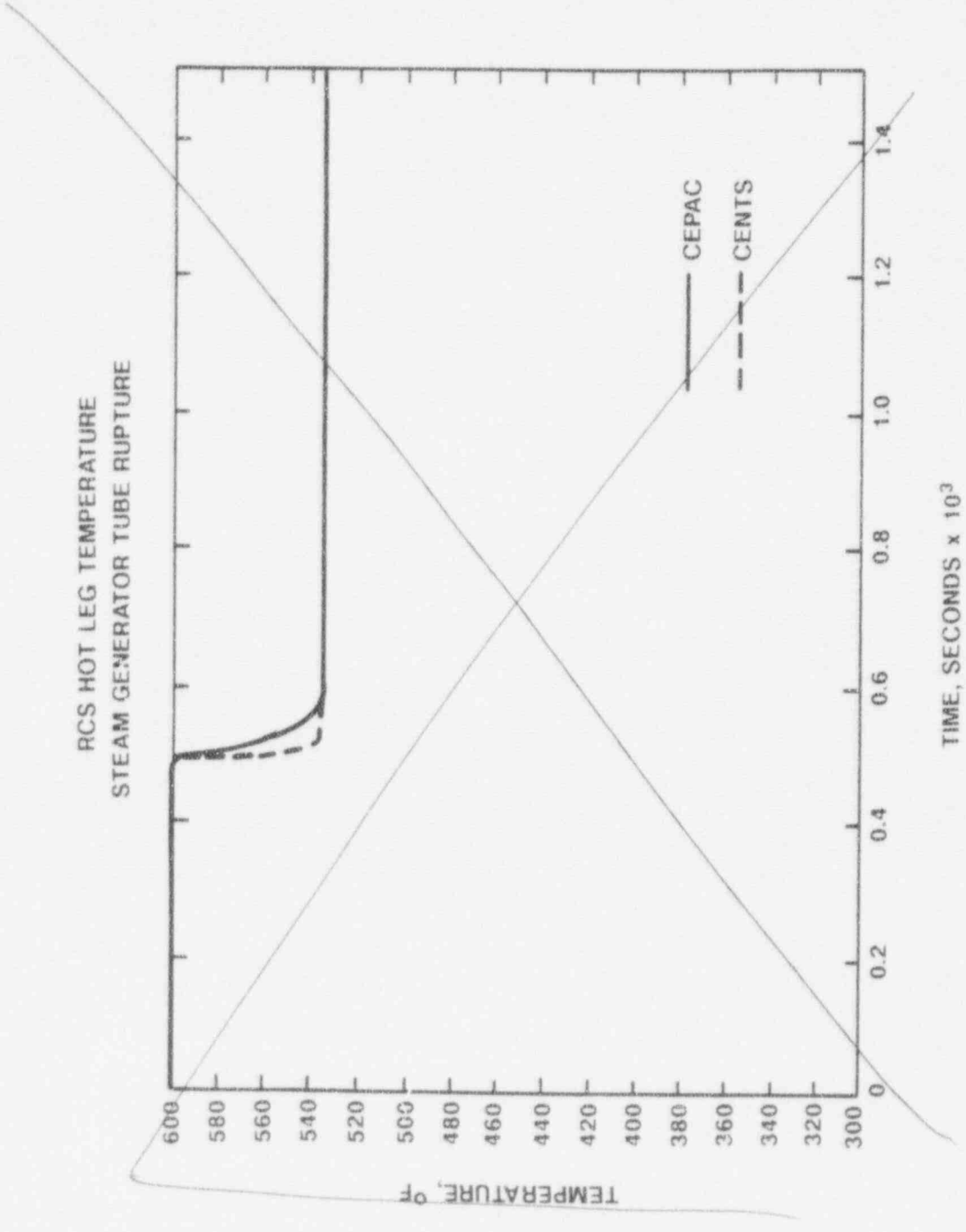
This page intentionally blank.



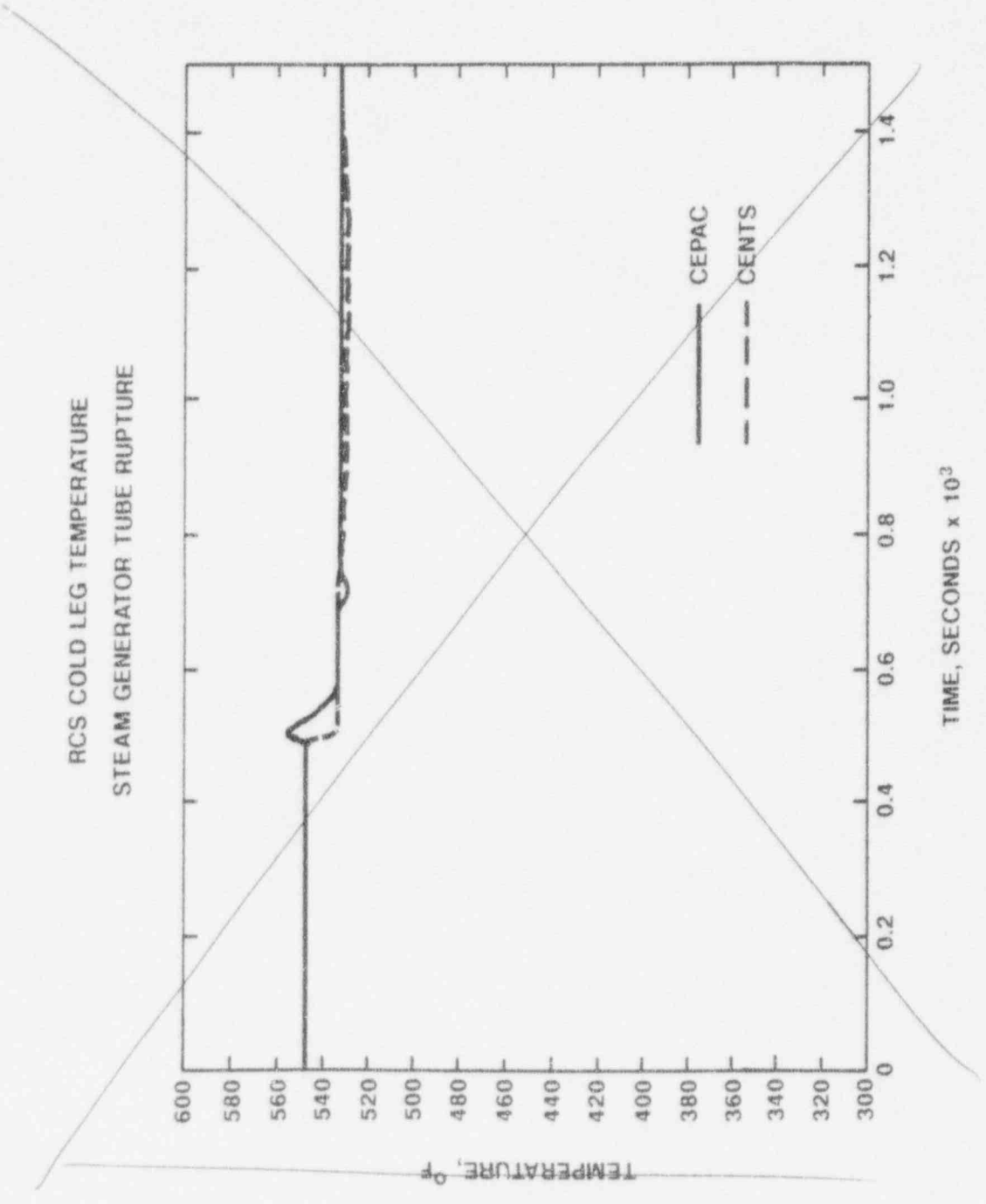
This page intentionally blank.



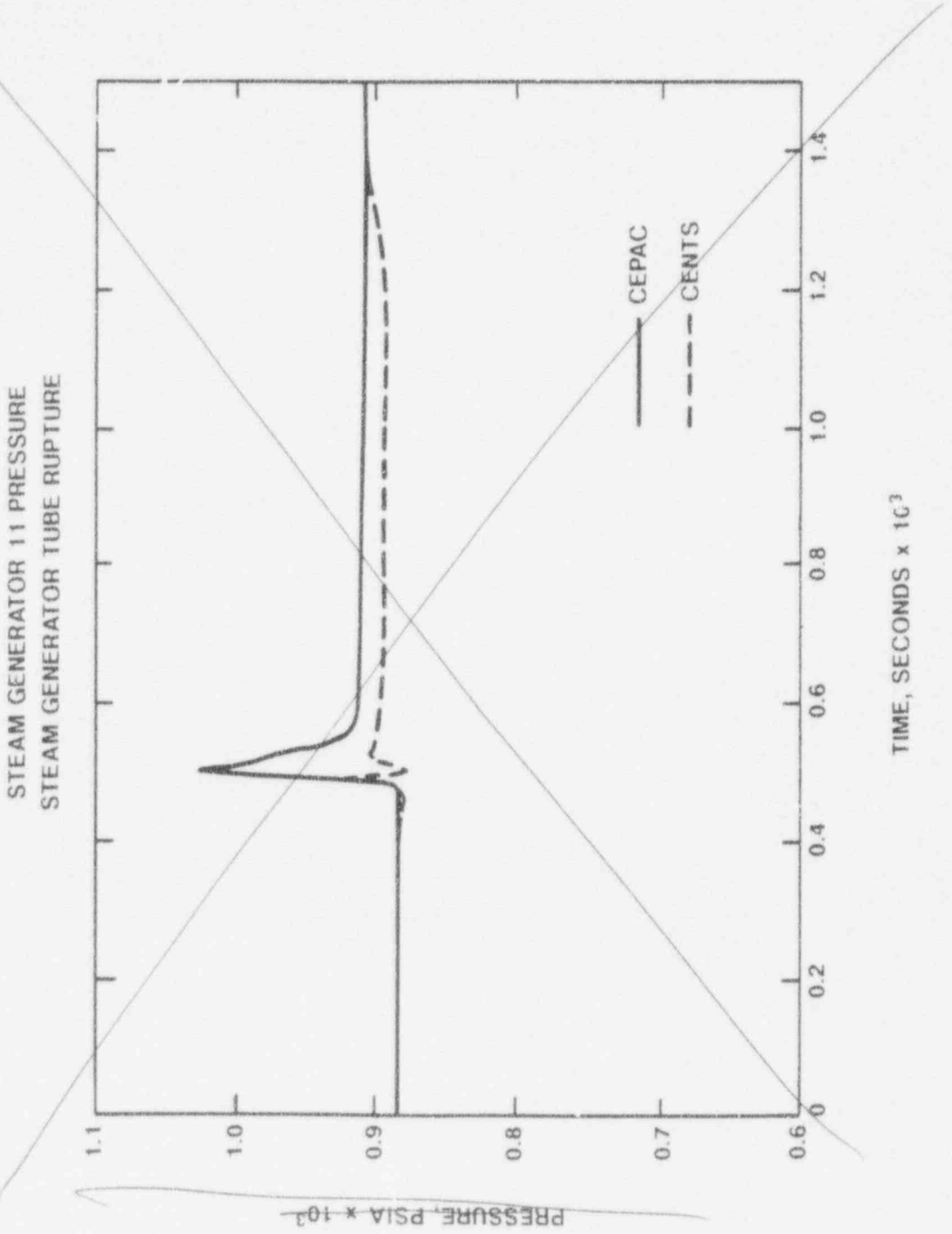
This page intentionally blank



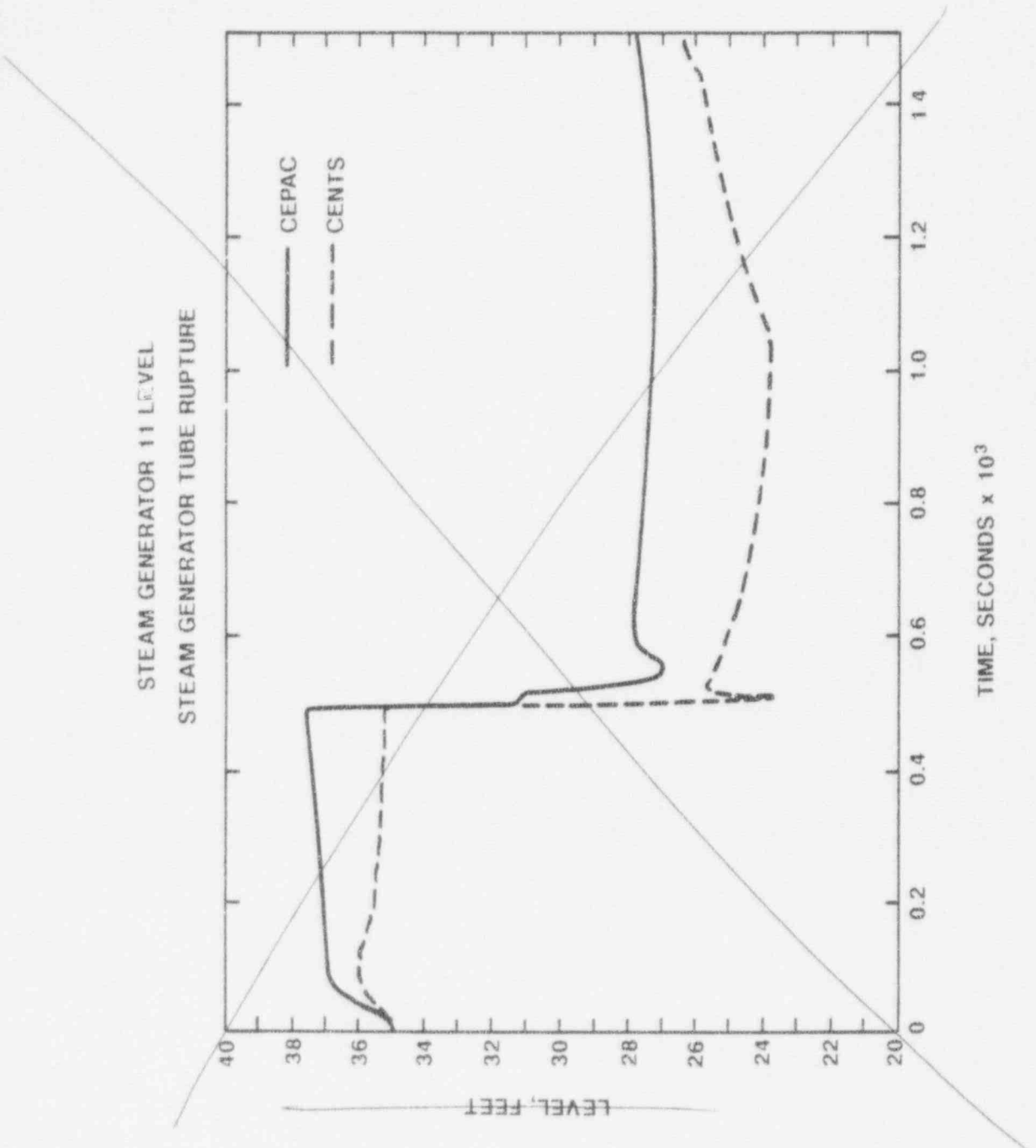
This page intentionally blank.



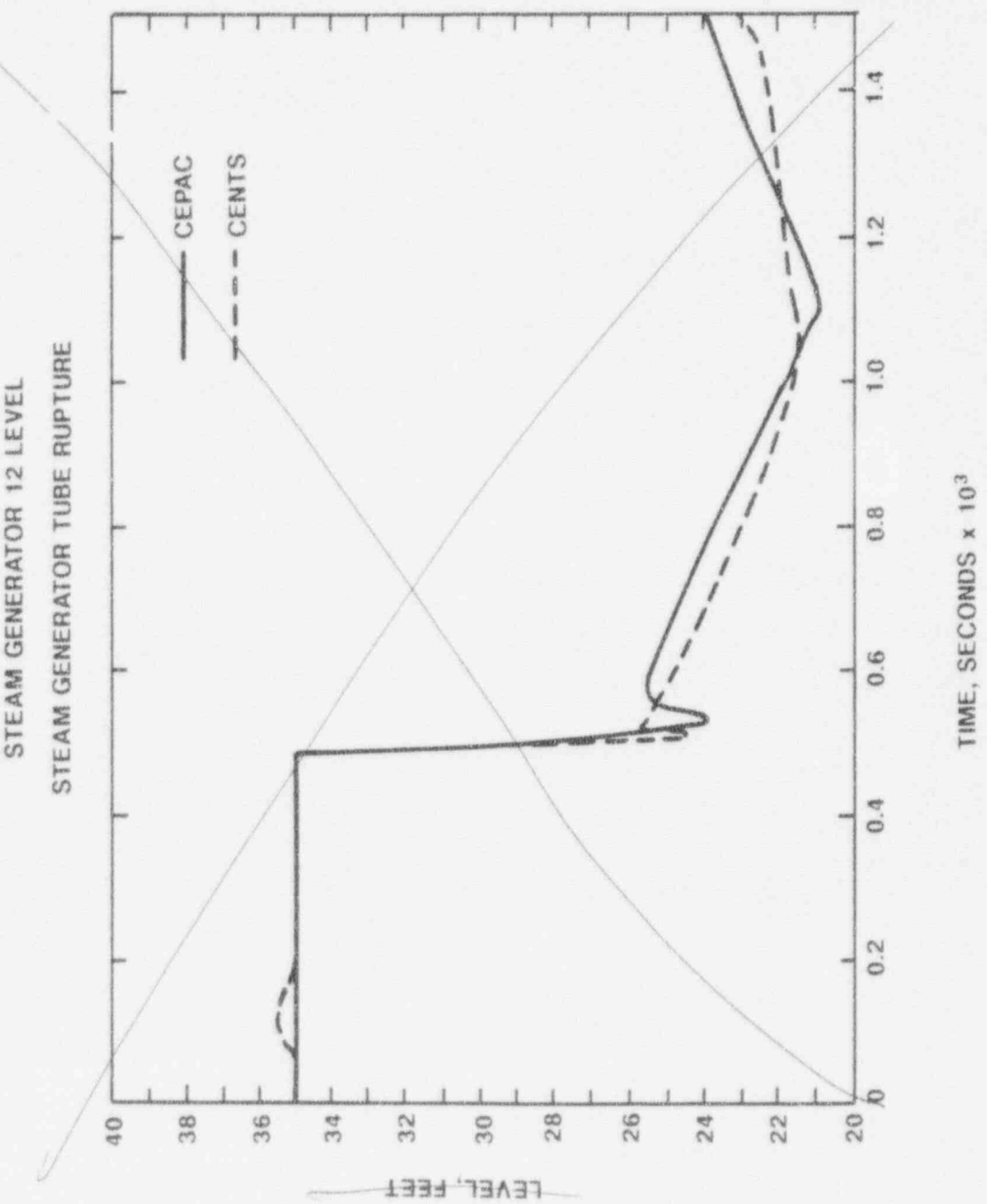
This page intentionally blank.



This page intentionally blank



This page intentionally blank.



This page intentionally blank.

6.5.5 EMERGENCY CONTAINMENT SPRAY BACKUP SYSTEM

The Emergency Containment Spray Backup System (ECSBS) is used as an alternate means of providing containment spray in the event of a beyond design basis accident in which both CS pumps, both SCS pumps, and/or the IRWST are unavailable. The ECSBS pumping device operates independently of the site normal and emergency AC power sources and is capable of being aligned to the spray header of either CSS division; see Figures 6.3.2-1A and 6.3.2-1B.

The ECSBS design includes the following features:

1) an eight inch diameter tee connection to the IRWST recirculation line of each CS pump;

2) an extension of the eight inch diameter Safety Class 2 piping from the tee to the exterior of the Nuclear Annex;

3) external connections, at or near grade level, for the temporary hookup of an external source of water;

4) a portable pumping device (e.g., fire truck) that has a minimum rated flow of 750 gpm;

5) all necessary hoses, fittings, and spool pieces, which would be stored with the pumping device or in the proximity of the piping connection to the IRWST recirculation line.

The ECSBS is assumed to be placed in service 24 hours after a severe accident to prevent a catastrophic failure of the containment. The ECSBS flow rate provides sufficient heat removal to prevent containment pressure from exceeding ASME Code Section III Service Level C limits. [[The design takes into account expected radiation levels and shielding requirements for any required local operator actions. The ECSBS pumping device is beyond the scope of Design Certification and shall be discussed in the site-specific SAR.]]1

19-5

The ECSBS pumping device and the connection to IRWST recirculation line tee will also provide an alternate means of introducing water into the containment, via the IRWST, after a severe accident. By repositioning remote-manual valves in the IRWST recirculation line of either CS pump, the ECSBS equipment and external water source can be used to refill the IRWST to provide long term flooding capability in the event of a severe accident.

1. COL information item; see DCD introduction section 1.8.2.

LIST OF FIGURES

APPENDIX 6C

Figure	Subject
6C-1	Unwrapped Annulus - 4-Pump Operation
6C-2	Unwrapped Annulus - 1-Pump Operation
6C-3	Transient Boron Concentration with 1-Pump Start
6C-4	~~Boron Dilution and RCP Restart Event Tree (Unweighted Estimate)~~ This item intentionally blank.
6C-5	~~Boron Dilution and RCP Restart Event Tree (Overweighted Estimate)~~ This item intentionally blank.

A. Model Assumptions

The analysis provides a reasonable and conservative estimate of the frequency of erroneous RCP restart, given the existence of the physical plant conditions necessary for the event to occur. The following conservative assumptions are part of the model:

- Operating experience suggests that it is unlikely that the operating crew would have reason to restart an RCP after prolonged post-LOCA two-phase natural circulation. However, having such a reason is not necessarily an error, and HRA is thus not an appropriate method for estimating its probability. Therefore, the model conservatively assumes that the control room staff will always want to restart an RCP.

- Other than the lack of 20 minutes of single-phase natural circulation, it is assumed that no plant conditions exist to preclude RCP restart (even though at least 12 conditions must be considered).

- No credit is taken for improved plant or procedure ergonomics.

- Activities required for pump restart are assumed to require no execution time (a potential mitigating factor), and to be 100% successful.

Three other reasonable assumptions have been made to limit the model complexity:

- No single (i.e., random) error will cause an RCP restart.

- If the TSC is asked to consider the RCP restart, it will proactively communicate to the Main Control Room (MCR) if any of the RCP restart criteria are not met.

- The Main Control Room will follow the TSC directions if they are given.

B. Model Structure

Two HRA event trees were constructed to determine the probability of erroneously restarting an RCP ~~(Figures 6C-4 and 6C-5)~~. The event tree ~~of Figure 6C-4~~ determines the lower bound of probability and the ~~event tree of Figure 6C-5 determines the~~ upper bound.

~~There are several decisions/evaluations/actions the operator and the TSC could take. Therefore, the model structure for both trees incorporates the following actions:~~

- ~~In Node A, the MCR staff requests the TSC staff to evaluate the need and acceptability of restarting an RCP.~~

- ~~In Nodes B and E, the MCR staff notes that the criterion for ensuring the establishment of 20 minutes of single-phase natural circulation prior to starting an RCP, is not met.~~

- In Nodes D and E, the TSC staff notes that the criterion for ensuring the establishment of 20 minutes of single-phase natural circulation prior to starting an RCP, is not met.

- In Node C, the MCR staff verifies that the TSC will permit the restarting of an RCP.

Any time movement along the event tree is downward and to the left, the correct actions are being taken. If movement is made down and to the right, errors are being made.

C. Model Quantification

THERP models are highly sensitive to the adjustment of their individual event weights (i.e., performance shaping factors). In addition, decision research has shown that model structure, rather than weighting, is the more frequent strength of "experts" (Dawes, 1979). Thus, two quantifications of the same model were used to provide reasonable limits for discussion and assessment.

The lower limit was obtained by using unweighted nominal HEP values (i.e., 3.0 E-3) for each event in the tree (Figure 6C-4). The unweighted quantification is presented as a best estimate result for this model. This produced a total HEP of 2.7 E-6 for the event tree.

The upper limit was obtained by "overweighting" the model with a set of hyperconservative values (Figure 6C-5). Relatively poor procedure ergonomics were assumed. Therefore, a larger-than-nominal value (1.0 E-2) was used as the basic Human Error Probability (HEP). The effects of stress and dependency were then incorporated at unfavorably high levels. This produced a total HEP of 5.54 E-2 for the event tree.

Finally, the geometric mean of the two values was taken to account for uncertainty as follows:

- Geometric mean is the Nth root of the product of N terms.

  For this case:

  - N = 2
  - A = Lower Bound = 2.75 E-6 (unweighted estimate)
  - B = Upper Bound = 5.54 E-2 (overweighted estimate)

Therefore:

The geometric mean $= (A \times B)^{1/2}$

$= (2.75 \text{ E-6} \times 5.54 \text{ E-2})^{1/2}$

$= 3.91 \text{ E-4}$

The result
This value of 3.91 E-4 is presented as a conservative estimate of the total HEP for this event.

7.0 OVERALL RISK ASSESSMENT

The overall risk associated with boron dilution during a small LOCA is assessed in this section of the report. The assessment involves the description of two potential scenarios of concern, ~~and the quantification of the scenario probabilities. The impact of the scenario probabilities on the Probabilistic Risk Assessment results presented in Section 19.9 is also assessed in this section.~~

7.1 SCENARIO PROBABILITIES

Two small LOCA scenarios were assessed:

1. A small LOCA during which all safety injection pumps operate, and the operator initiates an incorrect restart of a Reactor Coolant Pump (RCP) during the first third of the fuel cycle.
2. A small LOCA during which only two of the four safety injection pumps operate, and the operator initiates an incorrect restart of a RCP during the first third of the fuel cycle.

The probability of Scenario 1 can be expressed as follows:

$$F_{s1} = SLOCA * HEP_{RCP} * X_{cycle}$$

where,

F_{s1}	=	Scenario probability of small LOCA and incorrect restart of a RCP during the first third of fuel cycle
SLOCA	=	Small LOCA initiator ~~(3.0E-03 per year)~~
HEP_{RCP}	=	Human error probability for un-desired restart of a RCP ~~(3.9E-04)~~
X_{cycle}	=	Probability multiplier of a small LOCA occurring during the first third of cycle ~~(0.33)~~

The ~~above~~ frequency of a small break LOCA is used in the System 80+ PRA, ~~and is obtained from Table 19.3.3-2~~. The human error probability (HEP) for incorrect restart of a RCP is based on the procedures for mitigating a small LOCA ~~and is estimated~~ as shown in Section 6.3 of this Appendix. The cycle time reflects the fact that boron is required during the first third of the fuel cycle and the small LOCA must also occur during this time in order for the scenario to be of safety significance. ~~By substituting the values in the above expression, the probability for Scenario 1 becomes:~~

~~F_{s1} = 3.0E-03 * 3.9E-04 * 0.33~~

~~= 3.9E-07 per year.~~

The probability of Scenario 2 can be expressed as follows:

$$F_{s2} = SLOCA * SI_2 * HEP_{RCP} * X_{cycle}$$

where,

F_{s2}	=	Scenario probability of small LOCA, failure of two of four safety injection pumps to operate, and incorrect restart of a RCP during the first third of the fuel cycle
SLOCA	=	Small LOCA initiator ~~(3.0E-03 per year)~~
SI_2	=	Failure probability of 2 of 4 safety injection pumps to operate ~~(2.2E-04)~~
HEP_{RCP}	=	Human error probability for un-desired restart of a RCP ~~(3.9E-04)~~
X_{cycle}	=	Probability multiplier of a small LOCA occurring during the first third of cycle ~~(0.33)~~ .

The frequency of a small LOCA, the HEP for incorrect restart of a RCP, and the probability multiplier for the cycle time are the same as described for Scenario 1. The dominant contributors to the probability of 2 of 4 safety injection pumps failing to operate include common cause failure of the pump breakers to close, common cause of the pumps to start, and common cause failure of the pumps to operate. Simultaneous independent failures of the pumps are not significant contributors to the overall failure probability of the pumps. ~~The failure probability of 2 of 4 safety injection pumps to operate is 2.2E-04 per demand. This probability is based on failure rates used in the System 80+ PRA. By substituting the values in the above expression for Scenario 2, the probability becomes:~~

~~$F_{s2} = 3.0E-03 * 2.2E-04 * 3.9E-04 * 0.33$~~

~~$= 8.5E-11$ per year.~~

7.2 IMPACT ON PRA RESULTS

~~The PRA results presented in Table 19.9-1-4 show that the core damage frequency of internal events is 1.67E-06 per year. If~~ Scenario 1 described in Section 7.1 is ~~assumed~~ more likely than to cause core damage, ~~the overall core damage frequency for internal events would increase. The core damage frequency for internal events would increase from 1.67E-06 to 2.06E-06 per year.~~ Scenario 2 ~~would have no impact on the core damage frequency for internal events~~. Therefore, from a deterministic standpoint Scenario 2 ~~this scenario~~ is not considered.

If the worst case conditions are assumed and boron mixing is ignored, the outcome of the limiting small LOCA boron dilution event is a damaged but otherwise coolable core. Core recovery is considered likely because of (1) the availability of safety injection, (2) the short duration of the induced core power spike, (3) the RCS pressure relief through the existing hole in the RCS, and (4) the pressure absorption capability in the partially voided upper portions of the RCS when the reactivity insertion event takes place. Severe accident analyses, as well as experience with TMI-2, indicate that adequate core cooling can be established even in the presence of severely damaged core.

provided an adequate internal water supply is available. As long as the RCS pressure does not produce material stresses that exceed the ASME Service Level C limits, emergency core cooling system integrity is expected. As a consequence of items 2, 3, and 4 above, pressurization of the RCS to levels that exceed Service Level C stresses is highly unlikely.

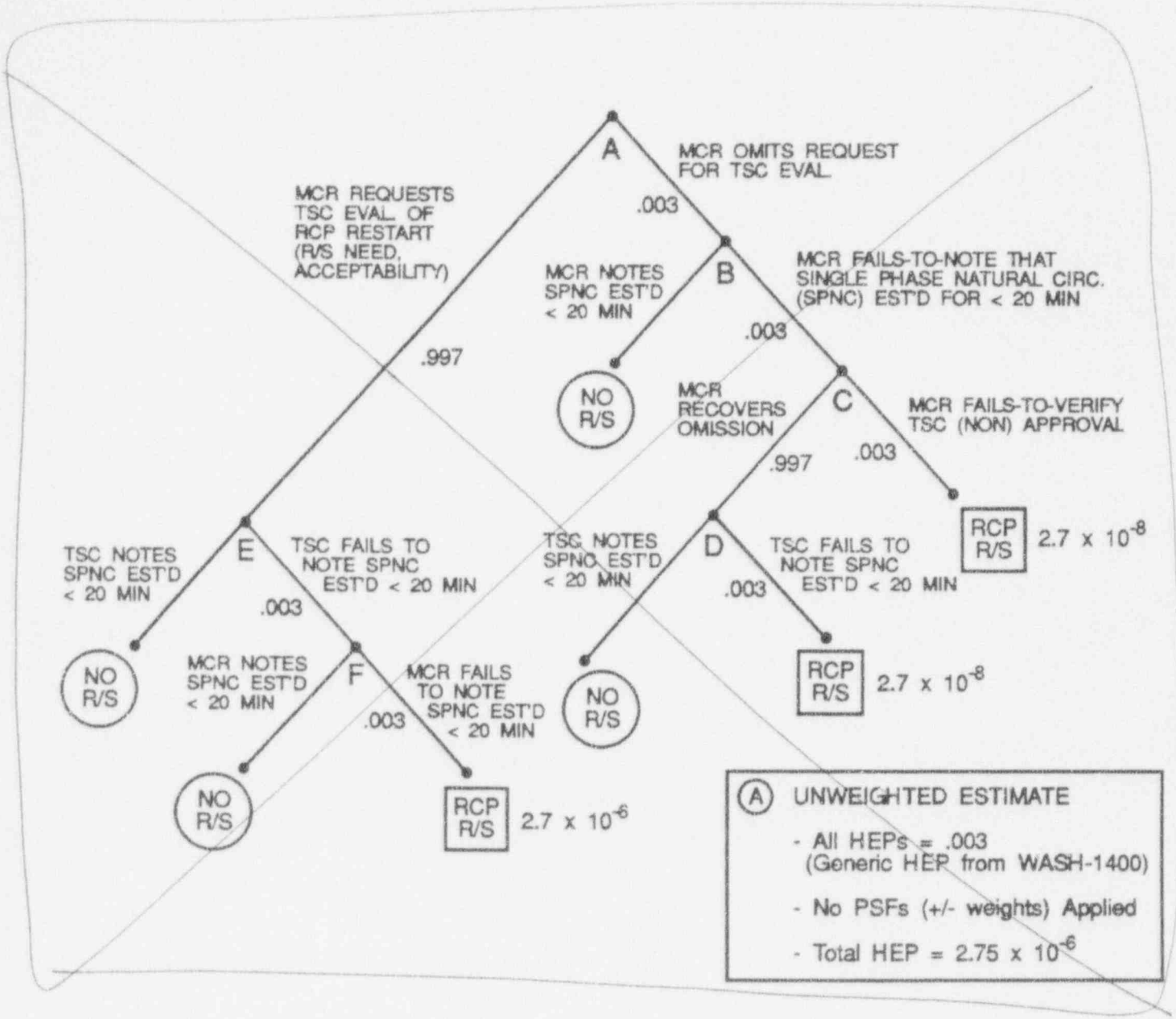
In the event that an unrecoverable core damage event occurs, containment spray and cavity flooding systems would be capable of arresting the event within the intact containment. Since the systems required to mitigate the post-vessel breach corium progression are not influenced by the small LOCA boron dilution event, and both AC power and component cooling water are available, at least one train of the containment spray system will be available and containment integrity will not be compromised.

~~Based on the guidelines and requirements of the Advanced Light Water Reactor (ALWR) Utility Requirements Document, the industry has established a mean core damage frequency goal of 1.0E-05 per year. Even if Scenario 1 causes core damage, the increased core damage frequency is well within this goal.~~ Since in-vessel recovery of the scenario will occur if the RCS pressure remains below the Level C stress limits, and since essential containment safeguard systems are available even if the RCS pressure exceeds the Level C stress limits the increase in overall plant radiation releases will be negligible. ~~The PRA conclusions are preserved even when the worst case boron dilution scenario is considered~~.

8.0 CONCLUSION

Although there is a potential to produce some unborated condensate during some small break LOCAs, this condensate will be mixed with highly borated water in the RCS upon the onset of single-phase natural circulation. Appendix 6B provides a very conservative core coolability assessment of the natural circulation case assuming no mixing of the condensate.

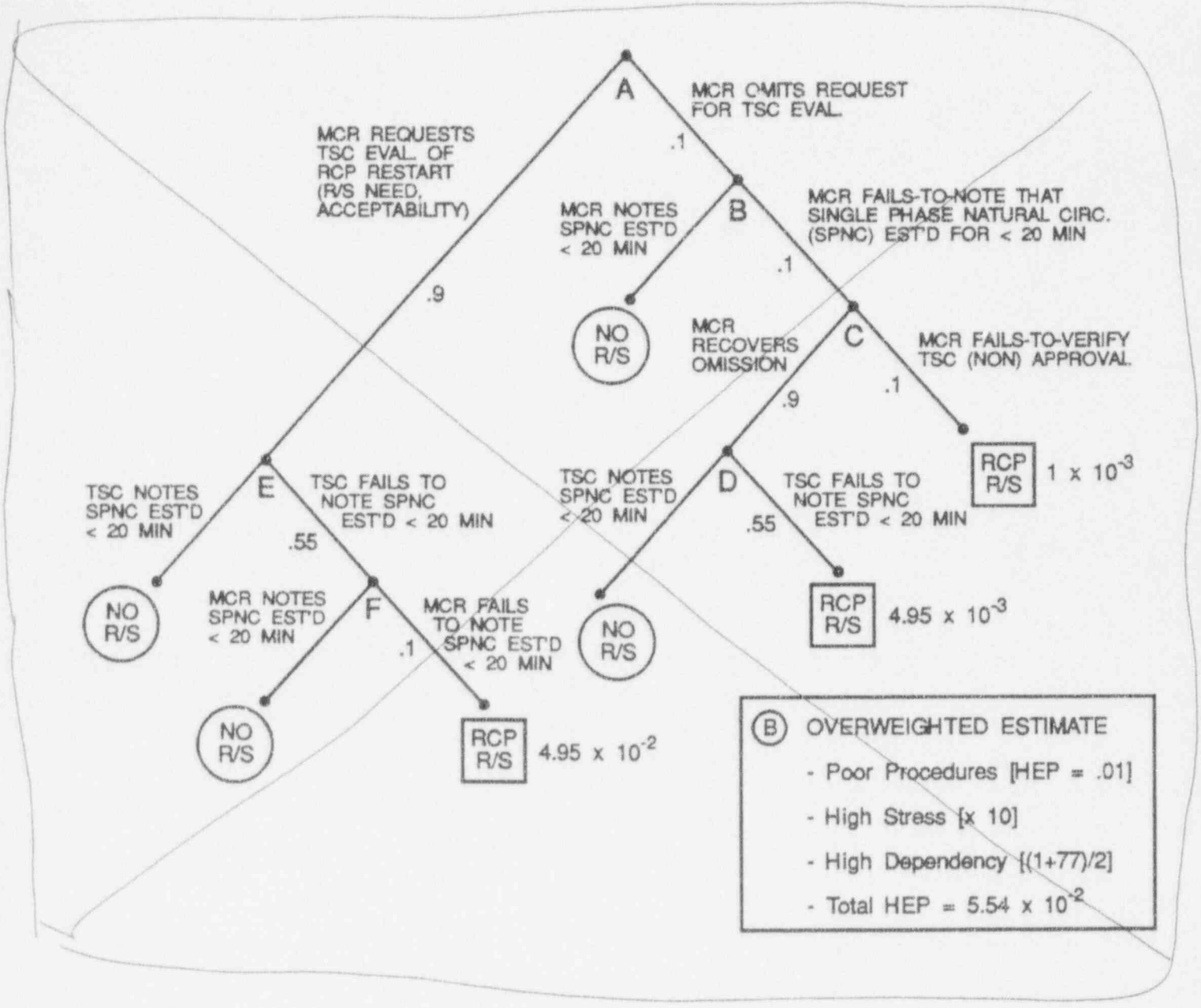
This appendix provides Emergency Operating Guideline (EOG) modifications which significantly reduce the probability of RCP restarting prior to achieving adequate mixing by natural circulation. It also provides a demonstration that, even if RCP restart is assumed to occur at the worst time, sufficient mixing occurs to ensure the core remains subcritical and adequately cooled.



This page intentionally blank.

Amendment V - 4/29/94

SYSTEM 80+™	BORON DILUTION AND RCP RESTART EVENT TREE - UNWEIGHTED ESTIMATE	Figure 6C - 4



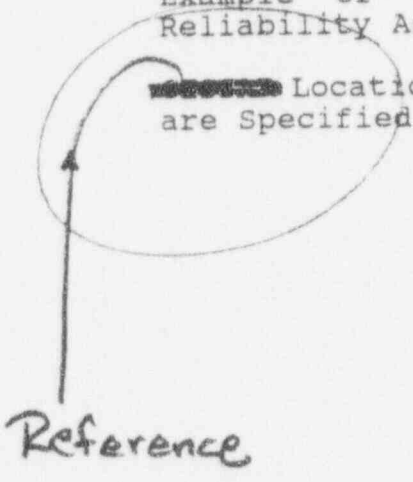
This page intentionally blank.

SYSTEM 80+™	BORON DILUTION AND RCP RESTART EVENT TREE - OVERWEIGHTED ESTIMATE	Figure 6C - 5

LIST OF TABLES

CHAPTER 17

Table	Subject
17.3-1	Example of Component Importance for an ALWR for Internal Events
17.3-2	Example of Risk-Significant Ranking of SSCs for the CCWS Train 1
17.3-3	Example of CCWS Failure Modes & Operations Reliability Assurance Process Activities
17.3-4	[redacted] Locations Where D-RAP Systems and Equipment are Specified



17.0 QUALITY ASSURANCE PROGRAM

17.1 QUALITY ASSURANCE DURING THE DESIGN PHASE

The ABB-CE Quality Assurance Program is described in the topical report CENPD-210-A, "Quality Assurance Program." The list of specific equipment covered by this program is contained in Table 3.2-1. ~~of CESSAR DC~~. In regard to Three Mile Island (TMI)-2 Item I.F.2, one part of subpart 3, (inclusion of QA personnel in design activities) is covered by the quality assurance program for the System 80+ design, described in CENP-210-A.

[[The COL Applicant will develop and implement a construction QA program (COL Item 17-1)]]. This will include the site-specific information to address the issues in TMI Action Plan Item II.J.3.1.

17.1.1 VERIFICATION PROCESS FOR DESIGN BASIS EVENTS

The goal of the Design Certification Program is certification of the System 80+ Standard Plant design by the Nuclear Regulatory Commission under Part of the Code of Federal Regulations.

The starting point for the System 80+ Design Certification program was the System 80 design as represented by CESSAR-F (which holds a Final Design Approval from the NRC in conformance with existing regulations) and the Duke Power Company's Cherokee and Perkins (P-81) balance-of-plant (BOP) design. A full complement of final design detail is available for the System 80 Nuclear Steam Supply System (NSSS) and for CESSAR-F. The P-81 BOP design progressed to the PSAR stage and was awarded a Construction Permit by the NRC before the project was canceled.

Certain analyses of design bases events included in ~~CESSAR-DC~~ this document are not intended to be repeated by the COL applicant. Accordingly, such non-repetitive safety analyses have been subjected to design verification prior to an award of a contract. The traditional design verification process for a nuclear power plant, consistent with the requirements of NQA-1, is finished after the detailed design. However, in the design certification process, since a portion of the detailed design is yet to be completed, the design verification process cannot follow this sequence. In order to address the design verification needs for a Certified Design, the scope of the ABB-CE design verification process used for the System 80+ Standard Plant covers all the non-repetitive safety analyses. Specifically, these non-repetitive safety analyses include all the design basis event analyses presented in Chapters 5, 6, and 15; analyses that set safety-related design parameters, including those described in the Certified Design Material (CDM); and an Appendix 6B analysis performed to verify the System 80+ capability to safely handle a hypothetical small break LOCA-boron dilution event. In addition, the work performed outside the traditional NSSS design has been verified.

1. COL information item; see DCD introduction section 1.5.2.

In addition, to provide added assurance that the System 80+ design information is correct and appropriate for intended purposes, the following has been done:

1) multi-disciplinary reviews (Integrated Reviews) were conducted throughout design development by teams appointed by Project Management, and

2) design information provided to the NRC has been reviewed for consistency among relevant ~~CESSAR DC~~ chapters and among other referenced documents.

17.2 QUALITY ASSURANCE DURING THE OPERATIONS PHASE

[[The COL Applicant will develop and implement an operation QA program (COL Item 17-1)]][1] This will include the site-specific information to address the issues in TMI Action Plan Items I.F.2 and II.J.3.1.

1. COL information item; see DCD introduction section 1.5.2.

17.3 RELIABILITY ASSURANCE PROGRAM DURING THE DESIGN PHASE

This section presents the System 80+ Design Reliability Assurance Program (D-RAP).

17.3.1 INTRODUCTION

The System 80+ Design Reliability Assurance Program (D-RAP) is a program that will be performed by the designers during detailed design and specific equipment specification phases to assure that the important System 80+ reliability assumptions of the Probabilistic Risk Assessment (PRA) will be identified and considered throughout the plant life. The PRA evaluates the plant response to initiating events to assure that plant damage has a very low probability and risk to the public is very low. The PRA also evaluates improvements in overall plant safety relative to previous designs, and identifies the relative risk significance of the plant's structures, systems and components (SSCs). Input to the PRA includes details of the plant design and assumptions about the reliability of the plant risk-significant SSCs. The plant owner/operator will complete the site specific D-RAP and will have an operations reliability assurance process. [[The COL applicant/holder should incorporate the operational reliability assurance process objectives into existing programs (e.g., quality assurance or maintenance) that will monitor equipment performance to provide reasonable assurance that the plant is operated and maintained with an acceptably low risk commensurate with PRA assumptions. (COL Item 17-3)]]1.

The D-RAP will include the design evaluation of the System 80+. It will identify relevant aspects of plant operation, maintenance, and performance monitoring of important plant SSCs for owner/operator consideration in assuring safety of the equipment, maintenance of critical functions, and limited risk to the public. The policy and implementation procedures will be specified by the owner/operator (See Section 17.3.13).

Also included in this explanation of the D-RAP is a descriptive example of how the D-RAP will apply to one potentially important plant system, the Component Cooling Water System (CCWS). The CCWS example shows how the principles of D-RAP will be applied to other systems identified by the PRA as being significant with respect to risk.

17.3.2 SCOPE

The System 80+ D-RAP will include the design evaluation of the System 80+, and it will identify relevant aspects of plant operation, maintenance and performance monitoring of plant risk-significant SSCs. The PRA for the System 80+ and other industry sources will be used to identify and prioritize those SSCs that are important to prevent or mitigate plant transients or other events that could present a risk to the public.

1. COL information item; see DCD introduction section 1.5.2.

The Project Director is responsible for the programmatic aspects of the plant design as well as the overall direction of the project, certification and licensing issues. The NSSS Design Manager is responsible for the design of the nuclear steam supply system. The Regulatory Conformance Manager has the responsibility of addressing any regulatory concerns and bringing these concerns to the attention of the Project Integration Manager and PRA and D-RAP Program Manager.

The Nuclear Steam Supply System (NSSS) Design Engineering organization is the core of the RAP and it is responsible for the design of the System 80+ NSSS. It is in this group where the NSSS design and drawings are developed with inputs from the mechanical, Instrument and Controls, Reactor, and Fluid Systems subgroups. It is also in this organization where the PRA models are developed as well as the Technical Specifications and plant procedures.

The PRA and D-RAP Program Manager is responsible for managing and integrating the D-RAP Program and has direct access to the System 80+ Project Integration Manager and is responsible for keeping him abreast of D-RAP critical items, program needs and status. The PRA and D-RAP Program Manager or his designee will attend all of the design review and progress meetings. He has organizational freedom to:

A. Identify D-RAP problems;

B. Initiate, recommend or provide solutions to problems through designated organizations;

C. Verify implementation of solutions; and

D. Function as an integral part of the design team and final design process.

The PRA and D-RAP Program Manager is in the ~~Reliability Analysis Services~~ department which performs reliability analyses, risk assessments and PRAs. This group ~~is part of ABB-CE Nuclear Services and~~ reports to the NSSS Design Manager, through the PRA and D-RAP Program Manager (Figure 17.3-1). The PRA input to the D-RAP and any of the System 80+ reliability analyses will be performed in this ~~organization~~ group and will be integrated into the ~~System 80+ design.~~ design organization.

The Quality Assurance organization provides quality control by performing regular audits and participating in the scheduled meetings to discuss System 80+ issues.

[[The COL applicant completing detailed design and equipment selection during the design phase, should submit its specific D-RAP organization for the NRC to review ~~(See Section 17.5.13)~~ (COL Item 17-2)]].

1. COL information item; see DCD introduction section 1.5.2.

the System 80+ PRA.

17.3.6 SSC IDENTIFICATION/PRIORITIZATION

The PRA prepared for the System 80+ will be the primary source for identifying risk-significant SSCs that should be given special consideration during the detailed design and procurement phases and/or considered for inclusion in the operations reliability assurance process. The method by which the PRA is used to identify risk-significant SSCs is described below. The PRA insights are summarized in Section 19.15 and the system and component importance is given in ~~Sections 19.9.4.1 and 19.9.4.2~~. It is also possible that some risk-significant SSCs will be identified from sources other than the PRA, such as nuclear plant operating experience, other industrial experience and relevant component failure data bases.

~~Table 17.3-4 gives the sections in CESSAR DC where systems and equipment are specified to be included in the D-RAP.~~ The primary source for the identification of systems and equipment to be included in the D-RAP is the PRA ~~(Section 19)~~. A Level III Probabilistic Risk Assessment (PRA) has been performed for the System 80+ design. The PRA evaluates the plant response to initiating events to assure that the risk to the public is also very low. Input to the PRA includes details of the plant design and assumptions about the reliability of the plant risk-significant Systems, Structures, and Components (SSCs). The results of the PRA include such things as core damage frequencies and the combination of equipment failures that lead to core damage or large releases.

The primary analytical measure used is the Risk Achievement Worth (RAW). It represents how the Core Damage Frequency (CDF) would increase if the system or component always failed (i.e., failure probability of 1.0/demand). It gives an extreme measurement of how the risk would be affected if a system or component were poorly designed, selected, installed, maintained, or operated. This measure is given in ~~Table 19.9.4-2~~ for internal events. For example, the steam generator atmospheric dump valves have a RAW of 5.14. If these valves were incapable of performing their task, the total core damage frequency would increase by a factor of 5.14.

assume

The ALWRs in general have a CDF that is approximately an order of magnitude lower than the existing plants. For the D-RAP program, risk significant SSCs are those SSCs that have a RAW of five or greater. The equipment not included in D-RAP will have a RAW less than 5. This means that if the excluded equipment is poorly designed, selected, or installed so that it has a near zero reliability, the predicted CDF would still be lower than that of the average existing plant by a factor of two. In the example of the atmospheric dump valves, because of the relative sensitivity (RAW $\geq$ 5), the D-RAP would include them to assure the proper design, selection, installation, and maintenance.

the System 80+ PRA.

Another analytical measure to identify risk significant SSCs is the Risk Reduction Worth (RRW). This is a measure of how the CDF would be reduced if the component had a perfect reliability (failure probability 0.0/demand). The measure given is the ratio of the base CDF divided by the RRW CDF and is greater than 1.0. In the shutdown PRA, the inverse value is given.

The third analytical measure is the Fussell-Vesely Worth (FVW). This gives the fraction of the base CDF that failure of the component contributes to the CDF. It is the best estimate for the importance of a component in the current design.

Risk Significant SSCs are also selected based on regulations and engineering judgment. For example, equipment specified in 10CFR50.62 is considered. Risk significant SSCs as described in Section 3.3.1.4 of ANSI/ANS-51.1 are considered in the equipment classified as QC-2 in Table 3.2-1.

17.3.6.1 Level I Analysis

The Level I analysis follows an accident sequence from an initiating event through failures of various safety functions to an end state which results in core damage. The Level I also predicts the frequency and dominant contribution to core damage.

The System 80+ PRA ~~Table 19.9.4-2~~ gives the component importance for System 80+ for internal events using different importance measurements. As discussed above, components with a RAW (RAW, change in risk if failure rate is 1.0) greater than five ~~have been~~ are selected for the D-RAP program. ~~Table 19.9.4-2~~ highlights the components with RAWs greater than 5.

The System 80+ PRA ~~Table 19.9.4-3~~ gives the Risk Reduction Worth for the components for internal events. The RRWs represent the reduction of risk with a component having a zero failure rate. The components with the RRWs greater than 1.1 ~~have been~~ are selected for the D-RAP ~~and have been highlighted~~. ~~All but four of these components were already included in the D-RAP because of their RAW and the four new components were noted in the table.~~

SSCs with a RAW between 2.0 and 5.0 ~~were~~ are selected if their ~~RAW was~~ RRW is greater than 1.05. ~~There were no SSCs which fell into this selection category.~~

The System 80+ PRA

The Fussell-Vesely Worth (FVW) is a measure of what fraction of the CDF the component failure contributes. ~~Table 19.9.4-2~~ gives the FVW for the components and failure modes. Using a selection criteria of 10%, ~~seven~~ components ~~were~~ are selected for the D-RAP. ~~All seven were already identified using the other two worths.~~

17.3.6.2 Level II Analysis

The Level II analysis predicts vessel failure, the containment response, and ascertains the likelihood, magnitude, and timing of radiological releases to the environment. ~~Sections 19.11 and 19.14~~ describes a containment response and sensitivity analysis for the Level II of the PRA. The containment sprays were added to D-RAP bases on discussions in Section ~~19.11.9~~. ~~Table 19.15.2-12~~ shows the sensitivity of the risk consequences to various Level II assumptions. Only one assumption (failure to isolate containment) showed a noticeable effect (sensitivity case/base case > 5) on releases. ~~Failure to isolate the containment increases the risk consequences by a factor of 8.3~~. The other assumptions increase the risk by ~~a factor of three or~~ less.

17.3.6.3 External Events

External events are ~~described in Section 19.7 of the CESSAR DC~~ and include tornado, fire, flooding, and seismic events.

The CDF due to tornado strike events is calculated ~~to be 2.5E-7/year~~. The event is modeled as loss of offsite power for 24 hours ~~with~~ the alternate AC source also being unavailable. Section 19.15.~~2.2~~ of CESSAR-DC describes the insights from this event. ~~Failure~~ of the diesels is the dominant cause and the designers are reminded of the importance of this safety equipment. Clogging of the SSW intake structure with tornado generated debris was also found to be important and the intake structure design has been included in D-RAP.

The risks associated with fires are discussed in ~~Section 19.7.3 of CESSAR-DC (CDF = 3.1E-8/year).~~ Fires represent a small risk to the plant as long as the three hour fire barriers are designed and maintained between the divisions (Section 19.15.3.2). Fire barrier design has been included in D-RAP.

Flood analysis is ~~presented in Section 19.7.4~~ and the insights are given in Section 19.15.~~3.2~~. In a scoping analysis, the CDF from flooding was estimated as ~~1.1E-8/year~~. The existence of the flood barriers dominates the risk and has been added to the D-RAP.

The seismic analysis is presented in ~~Section 19.7.5 of the CESSAR-DC~~. The first dominant contributor to the plant HCLPF (High Confidence of Low Probability of Failure) is seismically induced gross structural failure due to a seismically induced failure/overturning of the containment vessel, which is assumed to lead directly to core damage and containment failure. The second dominant contributor to the plant HCLPF is a seismically induced LOCA in excess of ECCS capacity caused by a seismically induced failure of the RCP supports.

There are three sequences where the contributor to the plant HCLPF due to "mixed cutsets" is potentially significant. A "mixed cutset" contains both seismic failures and random failures. These sequences are SEIS-SBO, EQA-15 and EQA-9. SEIS-SBO is a seismic induced loss of offsite power with random failures of the diesels and alternate AC source leading to a station blackout and battery depletion. EQA-15 is a seismically induced ATWS early in the core life. The ATWS was assumed to be caused by seismic deformation of the upper guide structure and leads to a small LOCA from failed check valves. EQA-9 is another ATWS sequence with failure of the charging system to provide long term reactivity control. The Safety Depressurization System also fails so that the SIS can not be used for reactivity control. The structures and equipment associated with these external events have been added to the D-RAP.

17.3.6.4 Shutdown Analysis

The shutdown risk assessment ~~is presented in Section 19.0~~ for System 80+ was performed and the insights are presented in Section 19.15 ~~of CESSAR DC~~. An importance analysis ~~(Table 19.0-6-1a)~~ was performed for the branch points of the event trees. The branch points contain initiating events, the operator errors, and the equipment failures (fault tree cut sets) for the systems. The branch points with RAW values greater than five or RRWs less than 0.8 or FVW greater than 0.1 have been included in D-RAP.

17.3.6.5 Other Sources

On October 4-6, 1993, a panel of engineers from ABB-CE met to establish important PRA-based safety insights for System 80+ and recommend at what tier in the licensing environment they should be addressed. Recommendations for D-RAP and operations reliability assurance process were made ~~(see Table 19.15-1)~~.

Design engineers have chosen to place their equipment into the D-RAP program. The references ~~for this equipment~~ are given in Table 17.3-4.

17.3.7 DESIGN CONSIDERATIONS

The reliability of risk-significant SSCs, which are identified by the PRA, will be evaluated at the detailed design stage by appropriate design reviews and reliability analyses. Current data bases will be used to identify appropriate values for failure rates of equipment as designed, and these failure rates will be compared with those used in the PRA. Normally, the failure rates will be similar, but in some cases they may differ because of recent design or data base changes. Whenever failure rates of designed risk-significant SSCs are significantly greater than those assumed in the PRA, an evaluation will be performed to determine if the equipment is acceptable or if it must be redesigned to achieve the appropriate reliability.

operation. Maintenance that will be performed more frequently than refueling outages must be planned so as to not disrupt operation or be likely to cause reactor scram, engineered safety feature (ESF) actuation, or abnormal transients. Maintenance, planned for performance during refueling outages, must be conducted in such a way that it will have little or no impact on plant safety, on outage length, or on other maintenance work.

As plant experience data accumulates, the failure rates and human error rates in the operations reliability assurance process should be updated. These failure rates were used by the designer in the PRA.

[[The COL applicant should provide a complete operations reliability assurance process description to be reviewed by the NRC ~~(see Section 17.5.19)~~ [COL Item 17-3]]].

17.3.10 OPERATIONS RELIABILITY ASSURANCE PROCESS

[[The operations reliability assurance process that is expected to be prepared and implemented by the COL applicant [COL Item 17-3], should make use of the information provided by the designer. This information will help the owner/operator determine activities that should be included in the operations reliability assurance process. Examples of elements that might be included are as follows:

Reliability Performance Monitoring -- Measurement of the performance of equipment to determine that it is accomplishing its goals and/or that it will continue to operate with low probability of failure and high availability. Monitoring should preferably be predictive in nature to prevent loss of critical functions.

Reliability Methodology -- Methods by which the plant/operator can compare plant data to the SSC data in the PRA.

Problem Prioritization -- Identification, for each of the risk- significant SSCs, of the importance of that item as a contributor to its system unavailability and assignment of priorities to problems that are detected with such equipment.

Root Cause Analysis -- Determination, for problems that occur regarding reliability of risk-significant SSCs, of the root causes, those causes which, after correction, will not recur to again degrade the reliability of equipment.

Corrective Action Determination -- Identification of corrective actions needed to restore equipment to its required functional capability and reliability, based on the results of problem identification and root cause analysis.

Corrective Action Implementation -- Carrying out identified corrective action on risk-significant equipment to restore equipment to its intended function in such a way that plant safety is not compromised during work.

1. COL Information Item; see DCD Introduction section 1.5.2.

Corrective Action Verification -- Post-corrective action tasks to be followed after maintenance on risk-significant equipment to assure that such equipment will perform its intended functions.

Plant Aging -- Some of the risk-significant equipment is expected to undergo age related degradation that will require equipment replacement or refurbishment.

Feedback to Designer -- The plant owner/operator should periodically compare performance of risk-significant equipment to that specified in the PRA and D-RAP, and, at its discretion, may send SSC performance data to plant or equipment designers in those cases that consistently show performance below that specified. The plant owner/operator should consider participation in the CEOG.

Programmatic Interfaces -- Reliability assurance interfaces related to the work of the several organizations and personnel groups working on risk-significant SSCs.

Maintenance Rule Integration -- The plant owner/operator should consider the integration or interface of operations reliability assurance process and the requirements of 10 CFR 50.65 which require the operator to develop a maintenance program for risk significant SSCs or SSCs that could produce trips or transients.

The plant owner's operations reliability assurance process should address the interfaces with construction, startup testing, operations, maintenance, engineering, safety, licensing, quality assurance and procurement of replacement equipment[1].

17.3.11 D-RAP IMPLEMENTATION

An example of implementation of the D-RAP is given for the Component Cooling Water System (CCWS). This system was selected as an example because it was a support system and was found in the earlier System 80 PRA to contain risk-significant components. Because of this finding, and through the D-RAP organization described in Section 17.3.5, the design was changed. The design and analytical results, as presented in this chapter, is presented only as a D-RAP example and does not necessarily correspond to the current System 80+ design.

17.3.11.1 CCWS Function

The Component Cooling Water System (CCWS) is a closed loop system that provides cooling water flow to remove heat released from plant systems, structures, and components. The CCWS functions to cool the safety-related and non-safety-related reactor auxiliary loads.

Heat transferred by these components to the CCWS is rejected by the Station Service Water System (SSWS) via the CCWS heat exchangers.

1. COL Information Item; see DCD Introduction section 1.5.2.

17.3.13 COL INFORMATION

A. Policy and Implementation Procedures for D-RAP

[[The COL applicant will specify the policy and implementation procedures for using D-RAP information. (See Subsection 17.3.1) (COL Item 17-2)]].

B. D-RAP Organization

[[The COL applicant completing its detailed design and equipment selection during the design phase, must submit its specific D-RAP organization for NRC review. (See Subsection 17.3.5) (COL Item 17-2)]].

C. Provision for Operations Reliability Assurance Process

[[The COL applicant will implement an operations reliability assurance process, to be reviewed by the NRC in the plant's maintenance program, QA program, or other existing programs. (See Subsection 17.3.9) (COL Item 17-3)]].

---

1. COL information item; see DCD introduction section 1.5.2.

17.3.14 REFERENCES

17.3-1 Lofgren, E. V., et al., "A Process for Risk-Focused Maintenance," SAIC. NUREG/CR-5695, March 1991

17.3-2 ~~Piccinini, P. J., et al~~, "Base Line Level 1 Probabilistic Risk Assessment for the System 80 NSSS Design," ABB-CE, January, 1988.

TABLE 17.3-4

REFERENCE LOCATIONS WHERE D-RAP SYSTEMS AND EQUIPMENT ARE SPECIFIED

SYSTEM OR EQUIPMENT	REFERENCE
FROM PRA	
Risk-Significant SSCs for Inclusion in D-RAP	Table 19.15.6-1
PRA, Level I Equipment	~~Table 19.1.4-2~~ System 80+ PRA
Seismic Fragilities	~~Table 19.7.5.1-1~~ ~~Table 19.7.6.1-2~~ ↓
PRA, Level II, III Equipment	Table ~~19.15.2-13~~ 19.15.L-1
Containment Spray System	Section 19.11.3
PRA, Shutdown Risk	~~Table 19.8.6-1~~ System 80+ PRA ~~Table 19.8.6-2A~~ "
External Events, Diesel Generators	Section 19.15.3.1
SSW Intake Structure	Section 19.15.3.1
Fire Barriers	Section 19.15.3.2
Flood Barriers	Section 19.15.3.3
Significant PRA-Based Safety Insights	Table 19.15-1
Risk Significant SSCs for Consideration in the RAP and Other Activities	Section 19.15.6
FROM OTHER SOURCES	
Equipment Classified As QC-2	Table 3.2-1
Hydrogen Igniters	Section 6.2.5
Cavity Flood System	Section 6.8.2.2.4
IRWST Screen	Section 6.8
I&C Equipment	Section 7.1.3B
Equipment Specified In 10CFR50.62	Section 7.7.1.1.11
Dedicated Seal Injection System	Section 9.3.4.3.1
Containment Cleanliness	Section 13.5

REVISED PAGE OF SECTION 19.1

the deterministic analyses performed in support of the PRA and the insights gained from the PRA.

19.1.0 INTRODUCTION

19.1.1 PURPOSE

One of the requirements of 10 CFR Part 52(1) is that an application for design certification must contain a design specific Probabilistic Risk Assessment (PRA). This section documents the results of the probabilistic risk assessment for the System 80+ Standard Plant Design.

The System 80+ Standard Design PRA has three primary purposes. The first purpose is to identify the dominant contributors to severe accident risk. The second purpose is to provide an analytical tool for evaluating the impact of design modifications on core damage probability and the overall risk to the health and safety of the public. The final purpose is to calculate the core damage frequency and large release frequency for the System 80+ Standard Design.

19.1.2 SCOPE

The System 80+ Probabilistic Risk Assessment is a Level III PRA for the System 80+ Standard Plant Design. This PRA addresses both internal and external initiators of accident sequences which lead to core damage. Bounding plant site characteristics were used for the evaluation of external events such as seismic and tornado strike events and for evaluating public risk.

This section Intentionally blank

19.2 METHODOLOGY

This PRA was performed in two phases. In the first phase, event tree and fault tree models were developed for the System 80 design[3]. These models were used to estimate the baseline core damage frequency for a generic plant with a System 80 NSSS and to identify the dominant core damage contributors. [System 80^R, described in CESSAR-F[4] and approved by the NRC(FDA-2), was the starting point for the System 80+™ PRA.] The second phase was an interactive process in which the system fault tree models developed in phase 1 were modified to reflect proposed system design changes and enhancements. The revised models were evaluated to determine the impact of the design changes on core damage frequency and dominant core damage contributors. This information was fed back to the system designers for consideration in the design process. At the conclusion of the design process, the PRA evaluation models represented the final System 80+ Standard Plant design. The analysis was then extended to a full level III PRA.

Standard methodologies were used in this analysis. The level I (core damage frequency) portion of the analysis is equivalent to the baseline probabilistic safety analysis (PSA) described in the PSA Procedures Guide[5] and the methodologies employed in this analysis are consistent, within the scope and intent of this analysis, with methodologies outlined in the PSA Procedures Guide[5] and methodologies described in the PRA Procedures Guide[6]. The methodologies used in this PRA comply with the recommendations of the "PRA Key Assumptions and Groundrules" in Appendix A to chapter 1 of the EPRI ALWR requirements document[7]. The small event tree/large fault tree approach was used for the evaluation of core damage frequency. The initial external events screening analyses were performed by an independent contractor under the Advanced Reactor Severe Accident Program (ARSAP). The external event evaluation methodology is summarized in Section 19.2.6, and the results are presented and discussed in Section 19.7. The methodologies used for the level II (source term) analysis were consistent with the methodologies used in NUREG 1150[8], the methodologies described in the PRA Procedures Guide[6] and those methodologies recommended in the EPRI ALWR Requirements Document[7]. The level III analyses (consequences) also used methodologies consistent with those described in the PRA Procedures Guide[6] and the methodologies recommended in the EPRI ALWR Requirements Document[7]. Figure 19.2.0-1 shows the major tasks in this analysis. The following sections describe these tasks and associated methodology in greater detail.

REMAINDER OF SECTION 19.2
DELETED

THIS SECTION INTENTIONALLY BLANK

19.3 INITIATING EVENT EVALUATION

19.3.1 MASTER LOGIC DIAGRAM DEVELOPMENT

Following plant familiarization, the first major step in determining the plant core damage frequency is to identify the initiating events for which event trees will be constructed and quantified. To systematize the identification of the initiating events, a master logic diagram was constructed. The master logic diagram (Figure 19.3.1-1) is a high level fault tree model of the potential causes of a postulated undesirable event and the logical relationships between these potential causes.

The top event on the master logic diagram is "offsite release of radioactive material from core". A release of core material will occur if there is an event resulting in severe core damage, and there is a loss of the containment function. The loss of containment function can be caused by containment bypass, consequential containment failures, or containment isolation failures.

Severe core damage can occur due to excess core power or loss of core cooling. In an excess power event, core damage results from energy generation within the fuel at a rate greater than the energy can be transferred to the coolant. Conceptually, excess power events can be initiated by CEA ejections, uncontrolled CEA withdrawals from zero power or a boron dilution event at hot zero power early in core life.

For loss of core cooling events, core damage results from core uncovery due to loss of the primary coolant inventory. Primary coolant inventory can be lost as a result of an unisolable breach of the primary pressure boundary (a LOCA-type event) or as a result of a loss of heat transfer to the secondary side which leads to the primary pressure and temperature increasing to the point where the primary safety valves will lift and discharge primary coolant into the Incontainment Refueling Water Storage Tank (IRWST). Loss of heat transfer to the secondary side can be directly initiated by a loss of feedwater flow, a loss of steam flow or an interruption of the primary coolant flow through the core. Loss of heat transfer to the secondary side can be indirectly initiated by events which result in a reactor trip and turbine trip. The initiators discussed above, and shown on Figure 19.3.1-1, represent unmitigated initiators. Mitigation of these initiators is evaluated in the event tree analysis. Severe core damage actually occurs only if the initiator occurs and the mitigating systems do not function.

REMAINDER OF SECTION 19.3 DELETED

THIS SECTION INTENTIONALLY BLANK

19.4 ACCIDENT SEQUENCE DETERMINATION

19.4.1 LARGE LOCA

The large LOCA event tree, Event Tree 1 (Figure 19.4.1-1), applies to all breaches of the Reactor Coolant System (RCS) inside containment with an effective break area greater than 0.50 ft^2. This includes the design basis accident, a double ended guillotine RCS pipe break, as well as any breach of the reactor vessel itself which is within the capability of the Safety Injection System (SIS) to maintain RCS inventory control and RCS heat removal such that severe core damage does not occur.

Large LOCA is a severe event in which blowdown of the RCS occurs within a very short period of time; from seconds to a few minutes. The safety injection tanks refill the reactor vessel lower plenum and downcomer, and the safety injection pumps restore and maintain water in the reactor vessel. Because of rapid depressurization, the nuclear reaction is quickly shutdown due to voiding in the core region. A reactor trip is not required for this sequence.

After the reflood, the subcriticality is assured by the boron in the injected water. Decay heat is removed through the break. Long term removal of the decay heat from within containment is provided by the Containment Spray System and Component Cooling Water System. Reactor coolant discharged through the break will drain to the holdup sump and then into the In-containment Refueling Storage Tank (IRWST). The containment spray pumps pump water from the IRWST through the containment spray heat exchangers where it is cooled by the Component Cooling Water System and then back to the In-containment Refueling Water Storage Tank. Core inventory is replenished from the IRWST by the safety injection pumps.

The following paragraphs described the individual elements of the Large LOCA event tree.

19.4.1.1 Event Tree 1 Elements

19.4.1.1.1 Large LOCA Initiators

A Large LOCA event tree is initiated by a random Reactor Coolant System break with an effective break area greater than 0.50 ft^2. For reactor vessel breaks of this size to be included in this class of initiators, its location must be within the capabilities of the Safety Injection System. Large LOCAs which create a direct path outside containment are treated as a separate type of event (Interfacing System LOCA). LOCAs arising as a consequence of another type of event are evaluated within the context of that event.

REMAINDER OF SECTION 19.4 DELETED

THIS SECTION INTENTIONALLY BLANK

19.5 DATA ANALYSIS

Fault trees are constructed for all systems that impact the likelihood of core melt. These trees are logic models that combine failures or faults which could render a system unavailable or defeat a necessary function. Systems that impact the likelihood of core melt are defined by the event tree analysis which is discussed elsewhere in this report. In order to estimate the frequency of core melt, fault trees for systems that are included in the core melt accident sequences must be properly linked and quantified. This section presents the data for the various components (or elements) of the fault tree models used in this analysis. These components include:

- Component hardware failures
- Common cause failures
- Maintenance unavailabilities
- Human errors
- Failures of special events

The data for recovery actions that are applied to sequence cut sets to prevent core melt are also presented in this section.

Other types of data such as initiating event frequencies used in the event tree analysis and component fragility curves used in the seismic analysis are presented elsewhere in this report.

A rigorous task to develop component failure rates based on plant operating experience was not possible for this analysis. Instead, generic data from industry generic sources was used. For those instances where special failure rates are used, the approach used to estimate these rates are outlined in this report.

The Advanced Light Water Reactor (ALWR) Requirements Document data base[7] is the primary source of generic data used in this report. The data base presented Reference 7 provides mean failure rates but does not provide error factors. The median and upper bound information in volume 5 of the NUCLARR data base[40] was used to calculate error factors. Other sources such as WASH-1400[14], NREP[28], IEEE-500[29], CEN-327[54], and NUREG/CR-4550[66] are used when component data could not be obtained from References 7 and 40. The SHARP[39] approach as described in Sections 19.2.5 and 19.5.5 was used to determine human error probabilities.

The CAFTA[41] computer code is used in this study to quantify the fault tree models as well as the accident sequences. Failure data required to perform these quantifications are entered and stored in the CAFTA data bases. The .TC file contains the generic component failure rate information. The .BE file contains the failure rate information for specific components. The data is assumed to be lognormally distributed and is represented by appropriate parameters (mean values and error factors). These parameters

REMAINDER OF SECTION 19.5 DELETED

THIS SECTION INTENTIONALLY BLANK

19.6 SYSTEMS ANALYSES

19.6.1 GENERAL PLANT DESCRIPTION

19.6.1.1 Scope and Description

The System 80+ Standard Plant Design includes all buildings, structures, systems and components which can significantly affect safe operation. The primary design characteristics of the systems and components are summarized in the subsections below. Those systems and components that are relevant to this study are described in more detail in Section 19.6.3.

19.6.1.2 Reactor Coolant System

The Reactor Coolant System (RCS) contains two independent, closed primary coolant loops, each of which has two reactor coolant pumps (RCPs), a steam generator, a 42-inch ID outlet (hot leg) pipe and two 30-inch ID inlet (cold leg) pipes. In addition, four safety injection lines are connected directly to the Reactor Vessel. An electrically heated pressurizer is connected to one of the loops of the RCS. Pressurized water is circulated by means of electric motor-driven, single stage, centrifugal RCPs. Reactor coolant flows downward between the reactor vessel shell and the core support barrel, upward through the reactor core, through the hot leg piping, through the tube side of the vertical U-tube steam generators, where heat is transferred to the secondary system, then back to the RCPs. RCPs return the reactor coolant to the reactor vessel. The steam produced in the steam generators is passed to the turbine for driving the plant turbine-generator.

19.6.1.3 Engineered Safety Features

Engineered Safety Features (ESF) equipment functions to prevent the accidental release of radioactive fission products from the plant. These safeguards system and components function to localize, control, mitigate, or terminate postulated accidents to hold the exposure levels below the limits of 10 CFR 100[61].

19.6.1.3.1 Containment Structure

The containment structure or building is a 200-foot diameter spherical steel shell with a wall thickness of approximately one and three-quarter inches. This containment shell is supported by, but not anchored to, a spherical depression in an intermediate floor of the shield building. The shield building is a reinforced concrete cylindrical building with a hemispherical dome which totally encloses the containment. Space below the containment and inside the shield building is occupied by the Engineered Safety Features equipment, e.g., Safety Injection System equipment, Containment Spray System equipment, Shutdown Cooling System equipment and Emergency Feedwater System equipment.

REMAINDER OF SECTION 19.6 DELETED

19.7 EXTERNAL EVENTS ANALYSIS

PRAs for existing plants (References 15, 16, 20, and 42) have shown that external events have made a significant contribution to public risk due to specific plant vulnerabilities. An evaluation of external events was therefore included in the System 80+ PRA to determine if there were any unforeseen vulnerabilities in the System 80+ design. In addition, the mean core damage frequency goal of 1.0E-5/yr promulgated by EPRI[7] specifically includes consideration of contributions from external events.

The external events analyses for the standard System 80+ plant were performed as part of the ARSAP program. These analyses included both qualitative and quantitative analyses. For the quantitative analyses, bounding site characteristics were used in order to minimize potential future restrictions on plant siting. Analysis methodology and results are fully documented in References 91, 92 and 93. The information in the following sections was extracted and condensed from those references.

This section intentionally blank.

19.7.1 QUALITATIVE EXTERNAL EVENT EVALUATION

The qualitative external events evaluation consisted of the following four steps:

1. Initial identification of external events to be considered.

2. Events with similar plant effects and consequences were grouped together.

3. Screening criteria were established to determine which events are risk insignificant and can therefore be excluded from detailed quantitative evaluation.

4. Each event was evaluated against the screening criteria to determine if the event was risk-significant and thus required further quantitative evaluation.

The initial set of external events was taken from the PRA Procedures Guide[5]. This list is based on national standard ANSI/ANS-2.12-1978[95] and represents a consensus listing of external events for nuclear power plant PRAs. Table 19.7.1-1 presents the initial list of external events. Several PRAs (References 15,16,20,42, and 96) for existing plants were also reviewed to ensure that events addressed in these PRAs were covered by the initial list. Next, this list of external events was reviewed,and those events which had similar effects on the plant (e. g. hurricane winds and tornado winds have similar plant effects.) were grouped together as shown in Table 19.7.1-2. The grouped events in Table 19.7.1-2 was then condensed to generate the final list of external events as presented in Table 19.7.1-3.

PAGES 19.7-2 THROUGH 19.7-12
DELETED

This Section Intentionally Blank

19.7.2 TORNADO STRIKE ANALYSIS

As stated in Section 19.7.1.12, the major impact of a tornado strike on a System 80+ Standard Design plant site would be a prolonged loss of off-site power. The evaluation of the tornado strike contribution to core damage frequency consisted of five steps:

A. Identification of key components and vulnerabilities.
B. Determination of the site strike frequency.
C. Development of the core damage event tree.
D. Modification of internal event fault tree models to reflect tornado susceptibilities.
E. Solution and evaluation of the core damage event tree.

Each of these steps are discussed in the following paragraphs.

19.7.2.1 Identification of Key Components and Vulnerabilities

To determine the potential impact of a tornado strike on site; key components, which are vulnerable to tornado effects and are important to plant shutdown, were identified. This identification was based on equipment which were found to be susceptible to tornado effects in the past PRAs. Tornados subject components and structures to three types of challenges. The first challenge is the wind loading produced by the tornado as it passes over the site. The second is the pressure differential as the tornado passes over a specific component or structure. The final challenge is due to missiles generated by the tornado which can strike components or structures. Table 19.7.2-1 presents a list of equipment and structures found to be vulnerable to the various tornado challenges in previous PRAs. As described in the following paragraphs, many of these past vulnerabilities are precluded by System 80+ design features.

19.7.2.1.1 Turbine Building

In previous PRAs, the major contributors to core damage frequency from turbine building failures were associated with consequential failures of safety equipment and loss of off-site power. For System 80+, all safety equipment will be located in the auxiliary building and thus is not susceptible to damage due to failure of the turbine building. Turbine building failure is not the dominant contributor to the tornado induced loss of off-site power. Given that no A-C power recovery is assumed for the 24 hour mission time, the impact of a turbine building failure on loss of off-site power is no different from the other more probable causes and thus can be excluded from evaluation.

PAGES 19.7-14 THROUGH 19.7-24 DELETED

This Section Intentionally Blank

19.7.3 INTERNAL FIRE ANALYSIS

19.7.3.1 Qualitative Fire Risk Assessment

19.7.3.1.1 Overview

The System 80+ Phase I Qualitative Fire Hazards Risk Assessment is a part of the ongoing Fire Hazards Assessment being developed in support of the System 80+ plant design. It builds on the information developed by Duke Engineering & Services, Inc. in Reference 101 (Volumes 1 - 5 of the Fire Hazards Assessment) to provide a preliminary analysis of the risk to safe shutdown capability resulting from fires in areas of the Nuclear Island other than in the Containment or the Control Room. It qualitatively evaluates the risk resulting from a fire in each fire area based on the assumption that the fire causes loss of all active components and functionality in the affected area. Adjacent fire areas are identified which will be necessary for future evaluation of the risk associated with fire propagation into adjacent areas. Due to the current stage of development of the detailed design and the lack of "as-built" data, a quantitative assessment will be deferred until such time as more detailed information becomes available.

In the Fire Barrier drawings, the Containment is not divided into individual fire areas. Rather, it forms one large fire area. A Phase I qualitative analysis of the affects of a fire in Containment which engulfs the entire fire area would not result in useful information since the containment necessarily contains equipment from both divisions. Fire Protection design features of the System 80+ containment include physical separation, intermediate fire barriers, fire detection and suppression, as well as functional redundancy among the required safe shutdown systems and components. A more comprehensive analysis involving the exact location of equipment, combustibles, fire detection and suppression equipment, and intermediate fire barriers will be performed to verify that the ability to achieve and maintain safe shutdown despite the occurrence of a localized fire in the containment will be performed when sufficient design detail is available.

The Control Room has not been analyzed in terms of the affect of a fire which engulfs the entire fire area on the ability to achieve and maintain safe shutdown. The continuous presence of operations personnel in the control room precludes the possibility of a fire in the control room going undetected to the point at which it can spread to engulf the entire control room without some action to suppress the fire and mitigate its effects on the part of operations personnel. The safe shutdown panel, located in a separate fire area, provides an alternate means of accomplishing a safe shutdown and safely maintaining the safe shutdown condition.

PAGES 19.7-26 THROUGH 19.7-34 DELETED

This Section Intentionally Blank

19.7.4 INTERNAL FLOOD ANALYSIS

19.7.4.1 Qualitative Flood Protection Assessment

The System 80+ Standard Plant includes a number of design features which provide flood protection to safety-related structures, systems and components. These flood protection measures are designed in accordance with Regulatory Guide 1.102, "Flood Protection For Nuclear Power Plants".

The System 80+ plant design emphasizes the elimination and minimization of potential flood sources within safety-related areas as a means of flood protection. For example, station service water and component cooling water heat exchangers are located outside the Nuclear Annex. Water-cooled components within the Nuclear Annex are cooled by Component Cooling Water, with the exception of HVAC equipment which is cooled by chilled water systems. These cooling water systems are closed systems with a defined volume of water. Component Cooling Water, Emergency Feedwater, Essential Chilled Water, etc., are separated by division with no open cross connections, thus eliminating the possibility of a single pipe break from flooding one division and the other division being lost due to loss of pressure boundary integrity. Condenser circulating water is also located outside of the Nuclear Annex. These features reduce in-plant cooling water to a limited volume which can be easily accommodated to limit the extent of flooding.

The System 80+ control complex is protected from flooding in that no water lines are routed above or through the control room or computer room. Water lines routed to HVAC air handling units, etc., around the control room are contained in rooms with curbs which prevent any potential water leakage from entering the control room or computer room.

Protection from external flooding is provided by elevated building entrances. Secondary flooding sources located in the Turbine Building are confined to that building. Entrances from the Turbine Building to the Nuclear Annex are sufficiently elevated to allow operator action to isolate a break in the Condenser Circulating Water System before the water level from the Turbine Building flood reaches the Nuclear Annex entrance. Lengths of high energy and moderate energy piping have been minimized by equipment location. Equipment is located in quadrants around the spherical containment to minimize the lengths of piping runs. The subsphere provides further close proximity of equipment to reduce piping runs from containment.

Flood barriers have been integrated into the design to provide further flood protection while minimizing the impact on maintenance accessibility. The primary means of flood control in the Nuclear Annex is provided by the structural wall which serves as a barrier

PAGES 19.7-36 THROUGH 19.7-40 DELETED

19.7.5 SEISMIC MARGINS ASSESSMENT

19.7.5.1 Methodology

A PRA-Based Seismic Margins Assessment (SMA) has been conducted to assess the ability of the System 80+ Standard Design to respond to seismic events beyond the design basis earthquake. In this assessment, High Confidence of Low Probability of Failure (HCLPF) acceleration values were calculated for important accident sequences and the plant as a whole. The HCLPF values are those seismic acceleration values for which there is a 95% confidence that the probability of failure for the specified sequence is less than 5%.

The PRA-based SMA for System 80+ was performed using the approach outlined below:

A. Develop Seismic Initiating Event Trees.
B. Develop initial Seismic Fault Tree Models from internal events fault tree models.
C. Prune the initial seismic fault trees.
D. Solve the seismic event trees and fault trees to generate cutsets for each seismically initiated core damage sequence.
E. Derive HCLPF values for components and structures in the seismic fault tree models.
F. Calculate HCLPF values for the seismic core damage sequences.
G. Determine the plant vulnerabilities.

These steps are briefly discussed in the following paragraphs.

The bases for the SMA are the event trees and fault trees developed for the internal events analyses. The event trees developed for the internal events were reviewed first to identify the types of events that might be expected to occur as a consequence of the seismic event. The impact of a seismic event will vary with the magnitude of the seismic event. Thus, a seismic initiator hierarchy tree was developed to represent the order of impact for the various seismic initiators. The hierarchy in this tree is defined such that if a selected initiator occurs, the occurrence of initiators further down the hierarchy is of no significance with respect to the plant response. Next, an event tree was developed for each seismic initiator based on the event trees for the equivalent internal initiating events. This was done by identifying those portions of the internal initiator event trees that would be applicable for a seismic event and/or a consequential event. Figure 19.7.5.2-1 presents the Seismic Initiating Event Hierarchy Tree and Figures 19.7.5.2-2 through 19.7.5.2-7 present the Seismic Initiating Event Trees.

Next, the fault tree models for the systems used to mitigate internal initiating events were reviewed to determine which components could be affected by a seismic event. For each

component that could potentially be affected by a seismic event, an element representing seismically-induced failure, of that component and all like components in the system were added to the fault tree (for example, seismic failure of a pump or seismic failure of motor-operated valves). This is based on the assumption of "one fail, all fail". That is to say, if one motor-operated pump fails to operate due to a seismic event, all motor-operated pumps in that system would fail and this failure was represented by one basic event in the fault tree model. In addition, if the failure of the structure in which a component is housed could result in failure of that component, then the seismically-induced structural failure was added to that equipment. For example, failure of the structure in which the Station Service Water System pump is housed results in failure of that pump and, therefore, a failure of the structure was added to the Station Service Water System. Furthermore, if a system/component interfaces with the system or component of concern and if seismic failure of the interfacing system or component would affect the system or component of concern, seismic failure of the interfacing system or component was included in the model for the system or component of concern. For example, seismic failure of the spent fuel pool heat exchanger could result in loss of the CCW inventory and failure of the CCW system. Also, some seismically induced failures are recoverable. In the example above, if the seismic event causes the spent fuel heat exchanger to leak, it can be isolated from the Component Cooling Water System (CCWS) so that depletion of the CCW inventory can be terminated. For this type of failure, an additional element was included to represent the operator failing to perform the recovery action.

The next step in the seismic analysis was to prune the initial seismic fault trees. In accordance with guidelines provided by the NRC, all random (independent) component failures with a probability less than 10^{-3} and all human errors with failure probability less than 10^{-2}, except selected human errors with probability in the range of 10^{-3}, were deleted from the fault trees. Components which have been traditionally shown in other seismic PRAs to be seismically robust were deleted from the fault tree models. The modified fault tree models are contained in Appendix 19.7.5A.

Next, each of the seismic event trees was solved via fault tree linking to generate seismic core damage event sequence cutsets. In generating the cutsets, the failure probability for the seismic failure basic events was temporarily set to 0.1 to ensure that the cutsets containing the seismic failures were not filtered out. The sequence cutsets were then reviewed to remove any illogical and duplicate cutsets.

The fifth step was to derive HCLPF acceleration values for the seismic component and structural failures in the seismic event trees and fault trees using System 80+ design specific information.

HCLPF values were computed using the Conservative Deterministic Failure Margin (CDFM) approach presented in EPRI NP-6041-SL[176].

HCLPF calculations were performed with reference to a Review Level Earthquake (RLE) of 0.6g. The CMS3 (modified NUREG/CR-0098[218] spectral shape) was used as the RLE spectral shape. HCLPF computations were performed for rock site conditions since this is one of the governing site conditions for design basis.

HCLPF computations were performed for three groups: 1) buildings and structures, 2) electrical and mechanical components and 3) major NSSS components. HCLPF computations were performed in accordance with the procedures identified in the EPRI seismic margin approach (EPRI NP-6041-SL[176]). This methodology calls for the best estimate of the seismic demand and a conservative estimate of the failure mechanism (hence called the Conservative Deterministic Failure Margin approach). This approach quantifies the differences between the code allowables and a conservative estimate of actual failure by recognizing higher component damping values, energy absorbing factors associated with ductile failure modes as well as potential load re-distribution between various structural elements of a structural system.

The HCLPFs for the following structures/structural elements were determined:

A. Nuclear Island (including the Interior Structure, Shield Building and Steel Containment Vessel).

B. Nuclear Annex (including the Fuel Building, CVCS area, Control Areas, Diesel Generator Areas and the Emergency Feedwater Areas).

The lateral load resisting capacity of the primary elements were determined using the methodology described in Appendices L and N of EPRI NP-6041-SL[176].

The HCLPFs for the electrical and mechanical equipment were determined by reviewing the applicable design basis qualification criteria against those permitted by the CDFM approach. For equipment qualified by testing, the response spectra curves for the 0.3g Design Basis (DB) earthquake were reviewed against the 0.6g CMS3 spectra, the RLE for the seismic margin review. Based

on the ratio of the DB to RLE and the criteria outlined in EPRI NP-6041-SL[176], the HCLPF was determined. Generic Equipment Ruggedness Spectra (GERS) were used where applicable.

Solid state switching devices and electromechanical relays will be used in the NUPLEX 80+ protection and control systems. Solid state switching devices are inherently immune to mechanical switching discontinuities such as contact chatter. Robust electromechanical relays are selected for NUPLEX 80+ applications such that inherent mechanical contact chatter is within the requisite system performance criteria. Therefore, contact chatter has no effect on system operation and was, therefore, not included in the seismic analysis. The COL must confirm the use of seismically robust electromechanical relays in the engineered safety features actuation and control systems. [COL Item 19-10][1].

Similarly, for equipment qualified by analysis, the design basis parameters, including damping and anchorage safety factors as well as response spectra, were assessed to determine seismic margins. For example, a seismic margin exists for an equipment item that is seismically qualified using 3% damping, if a higher 5% damping is permitted in the CDFM approach. Margins for each of the significant parameters were determined, and considered with inelastic energy absorption capability for ductile failure modes, to calculate HCLPFs. Seismic fragilities for equipment items that are inherently rugged were based on available industry data.

The NSSS components that were reviewed include:

A. Reactor Vessel
B. Steam Generators
C. Reactor Coolant Pumps
D. Reactor Internals
E. Pressurizer
F. NSSS Piping

These NSSS components were assessed by reviewing the various design basis parameters to identify seismic margins. The stress margins were determined by comparing the loads from the System 80+ RCS analysis and those in existing stress reports. Load combinations in accordance with Section 6 of EPRI NP-6041-SL[176] were evaluated. The HCLPF values were calculated using the CDFM approach and the equations discussed above.

Table 19.7.5.1-1 lists all components that are in the seismic models and presents either the failure rates for independent failures or the component or structure HCLPF value for seismic failures. Table 19.7.5.1-2 lists the structural fragilities calculated for the System 80+ structures and the NSSS component fragilities. All HCLPF values are presented in terms of peak ground acceleration.

1. COL information item; see DCD introduction Section 1.5.2.

The next step was to calculate the HCLPF values for the seismic core damage sequences for the plant. This was done using the MIN-MAX method. In this method, the HCLPF value for a cutset is the maximum of the HCLPF values of the seismic failures in the cutset. Cutsets which contain both seismic failures and non-seismic failures are called "Mixed Cutsets" in this analysis and are treated separately. "Mixed Cutsets" have both a HCLPF value and an independent failure rate. The HCLPF for a seismic core damage sequence is the lowest cutset HCLPF of the cutsets which comprise the sequence. The plant HCLPF is the lowest sequence HCLPF.

The final step in the analysis is to identify the plant seismic vulnerabilities. This is done by reviewing the seismic core damage sequence cutsets to determine which seismic failures contributed to each sequence. The "Mixed Cutsets" are also reviewed to identify accident scenarios which might have had a lower HCLPF in the presence of a failed component or failure of an operator to take appropriate action.

PAGE 19.7-46 DELETED

This section intentionally blank.

19.7.5.2 Seismic Event Sequences

As stated previously, the impact of a seismic event will vary with the magnitude of the seismic event. The Seismic Initiator Hierarchy Tree presented in Figure 19.7.5.2-1 was developed to represent the order of impact for the various seismic initiators. The hierarchy in this tree is defined from left to right. If a selected initiator occurs, the occurrence of initiators further to the right on the hierarchy tree is of no significance with respect to the plant response.

19.7.5.2.1 Seismically Induced Gross Structural Failure

The first initiator on the hierarchy tree is "Seismically-Induced Gross Structural Failure". For this initiator, the seismic event is assumed to result in a gross structural failure of critical structures in the nuclear annex building, the shield building structure or the containment structure. It is assumed that the structural collapse will result in a transient/accident and disable all safety equipment required to respond to the transient/accident. This initiator is assumed to proceed directly to core damage. Furthermore, failure of the shield building structure and failure of the containment structure are also assumed to result in loss of containment integrity.

Seismic failure of the nuclear annex structure in the subsphere area is presumed to result in the failure of all pumps, valves and controls in this area. These include the CCW pumps, the SI pumps and the EFW pumps. Failure of the CCW pumps is presumed to initiate a transient and failure of the other pumps precludes mitigating the transient. The HCLPF for this structural failure was calculated to be 1.08g.

Seismic failure of the nuclear annex structure in the areas outside of the subsphere region is presumed to result in the loss of the motor control and load centers for the safety related pumps and valves, failure of vital and non-vital control systems and failure of the 125 VDC vital power system. These failures will result in a transient and disable the responding safety systems. The HCLPF for this structural failure was calculated to be 1.12g.

Seismically induced sliding of the entire Nuclear Island structure beyond 3 inches is assumed to result in severing of all piping or cabling into the Nuclear Island. This includes failure of the main steam and feedwater lines, failure of the CCW piping, failure of the diesel generator fuel oil piping, and failure of incoming power lines. This is conservatively assumed to lead directly to core damage. The HCLPF calculated for this seismic failure mode is 0.80g.

Seismic failure of the shield building is assumed to result in significant amounts of falling concrete. It is assumed that

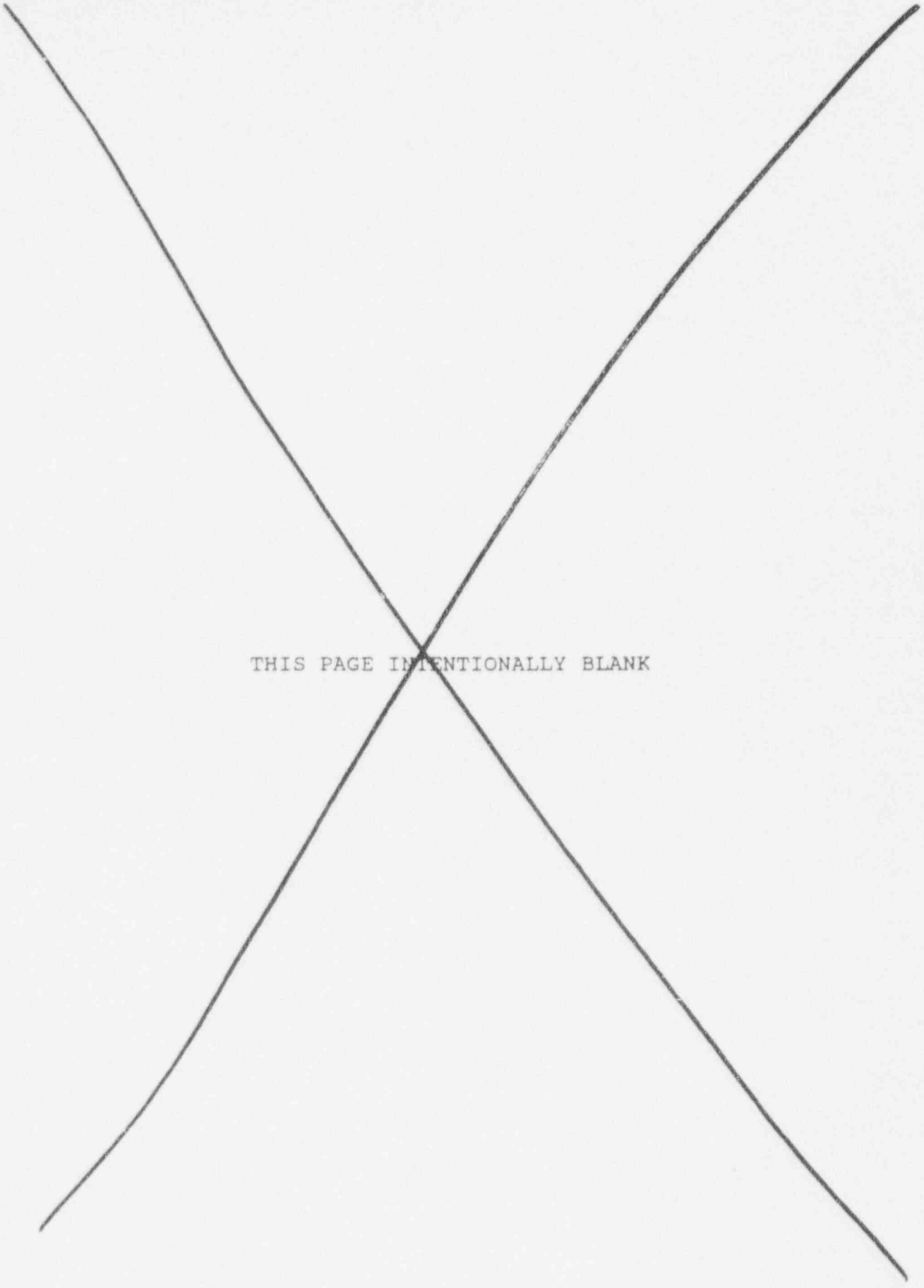
PAGES 19.7-48 THROUGH 19.7-70 DELETED

19.7.5.3 Seismic Margins Results and Insights

Table 19.7.5.3-1 presents the HCLPFs for System 80+ by sequence. The data on this table is sorted in ascending order on the HCLPF values in the second column. As can be seen from this table, the HCLPF for System 80+ is 0.73g. The dominant contributor to the plant HCLPF is seismically induced gross structural failure due to a seismically induced failure/overturning of the containment vessel which is assumed to lead directly to core damage and containment failure. The second dominant contributor to the plant HCLPF, with a HCLPF of 0.86g, is a seismically induced LOCA in excess of ECCS capacity caused by a seismically induced failure of the RCP supports.

There are three sequences where the contribution to the plant HCLPF due to "Mixed Cutsets" is potentially significant. (NOTE: A "Mixed Cutset" is a core damage cutset which contains both seismic failures and random or independent failures.) These three sequences are SEIS-SBO, EQA-15, and EQA-9.

The sequence SEIS-SBO is a seismically induced station blackout. The sequence is initiated by a seismically induced loss of site power, which has a HCLPF value of 0.12g. Failures of the two diesel generators and the standby combustion turbine independent of the seismic event will result in a station blackout. The station batteries and the turbine driven EFW pumps can be used to provide emergency feedwater flow for approximately 8 hours. At this time, the batteries will be depleted and the turbine driven EFW pumps will fail due to loss of control power. This results in core damage. It is assumed that offsite power can not be restored within 24 hours of a seismic event which results in loss of offsite power. Thus, the emergency diesel generators and the standby combustion turbine are important to maintaining the safety of the plant following a seismic event. The diesel generators and the structures in which they are housed are Seismic Category I and are designed to have significant margins over the design basis earthquake. It is also highly desirable that the standby combustion turbine be available to back up the diesel generators for seismic events on the order of the design basis earthquake of 0.3g. As stated in Chapter 6, paragraph 4.6.4.3.5 of volume II of the EPRI Utility Requirements Document[7], practical measures can be taken to exploit the intrinsic seismic ruggedness of the combustion turbine to provide a median seismic capacity of 1.0g. The ARSAP letter report, "Combustion Turbine Generator Seismic Evaluation Guidance WBS 4.1"[219] provides specific guidance on considerations for ensuring the seismic strength of the combustion turbine and the structure in which it is housed.



THIS PAGE INTENTIONALLY BLANK

The structure that houses the combustion turbine must either have a HCLPF value of at least 0.36g, which is consistent with the HCLPF value assumed for the combustion turbine in the seismic margin analysis, or be shown to fail in such a manner that it will not reduce the HCLPF value of the combustion turbine below 0.36g.

Sequence EQA-15 is a seismically induced ATWS early in core life when the MTC is greater than -0.3. The peak RCS pressure for an ATWS with an MTC greater than -0.3 would exceed 3200 psia which would result in failure of the safety injection system check

valves and failure of piping resulting in a small LOCA. This leads directly to core damage. For this sequence, it is assumed that a seismic event initiates a transient that requires a reactor trip but the trip does not occur due to seismically induced deformation or shifting of the upper guide structure preventing the CEAs from inserting. The upper guide structure was determined to have a HCLPF of 0.74g.

Sequence EQA-9 is a seismically induced ATWS later in core life when the MTC is less than -0.3. This sequence involves a seismically induced ATWS with successful operation of the EFW system but failure of the charging system to provide boron for long term reactivity control and failure to depressurize the RCS using the safety depressurization system so that the safety injection system can provide reactivity. As with EQA-15, the seismically induced failure to trip is most likely due to a seismically induced deformation or shifting of the upper guide structure preventing the CEAs from inserting. The primary cause of the failure to depressurize the RCS was failure of the operator to initiate safety depressurization in preparation for feed and bleed cooling. This particular human action has been shown to be important in both the seismic analysis and the internal events analysis.

Four sequences have a HCLPF value of 0.89g. This HCLPF value is associated with a structural failure of the walls between the EFW storage tanks and the diesel generator rooms. The EFW storage tanks are essentially large, steel-lined concrete structures in the nuclear annex. The diesel generator room in each division shares a common wall with the EFW storage tank for that division. If the common wall between the EFW storage tank and the diesel generator room failed, the EFW inventory would drain into the diesel generator room and flood out the diesel generator. This would result in loss of the EFW and the diesel generator. The seismic strength of the wall is a function of the thickness of the wall and the amount of rebar in the wall.

The structure housing the service water pumps and the SSW/CCW heat exchangers is an important structure. A seismic failure of this structure would result in failure of both trains of the service water system. This in turn would lead to failure of the CCW system which would result in failure of the diesel generators, the injection pumps, the containment spray pumps, the shutdown cooling pumps and the motor driven EFW pumps. The design detail needed to calculate the HCLPF for the structure is not currently available. However, the structure is a single story, Seismic Category I structure. The seismic strength of the structure is a function of the wall thickness and the amount and pattern of rebar in the walls and the anchorage of the walls to the basemat. It is expected that it would be as strong as the interior structure of the nuclear annex. Seismically induced sliding of this structure of beyond 3 inches is assumed to result

in failure of the CCW piping between this structure and the Nuclear Island. This would result in a total loss of CCW. A HCLPF of 1.0g was calculated for this failure mode for the most limiting soil site (B3.5). This value was used as the structure HCLPF for the rock and all soil sites.

This analysis was performed in an iterative fashion. During the preliminary analysis, the seismic failure of the CCW surge tanks, with an assumed HCLPF of 0.6g, was found to dominate the HCLPF for several sequences. Failure of these tanks would result in loss of all CCW inventory and failure of the CCW system. This in turn would lead to failure of the diesel generators, the injection pumps, the shutdown cooling pumps, the containment spray pumps and the motor driven EFW pumps. These tanks are located in the upper levels of the nuclear annex at elevation 170+0 feet. The dominant failure mode was overturning of the tanks due to failure of the supports or braces. The seismic capacity of the tanks is a function of the support strength and the strength and location of the braces for the tanks. The final HCLPF for the CCW Surge Tanks was calculated to be 1.10g.

The condensate storage tank provides the water supply for long term (greater than 16 hour) operation of the EFW system following a seismic event. The condensate storage tank is a freestanding metal tank with height less than the diameter. The tank is non-seismic and is located within a seismic Category II dike. The seismic capacity for this type of tank is a function of the number of holddown anchorage bolts. Thus, within certain limits, the capacity can be increased by increasing the number of holddown bolts. Provisions to inhibit lateral slippage of the tank also need to be made. A HCLPF of 0.56g was calculated for the condensate storage tank based on the assumption that 16 hold-down bolts would be used.

Only five human errors appear in the mixed cutset lists presented in Section 19.7.5.2. They are:

1.	AHFFASCSLOCA:	Operator fails to initiate aggressive secondary cooldown for a small LOCA.
2.	VHFFFEEDBLEED:	Operator fails to initiate feed and bleed cooling.
3.	UHFFBORONRCS:	Operator fails to initiate boron delivery to the RCS using the charging pumps.
4.	CHFFISOLATECCWS:	Operator fails to isolate the spent fuel pool heat exchanger before the CCW inventory is depleted.
5.	JHFDRHRI:	Operator fails to align shutdown cooling system for injection operation.

only CHFFISOLATECCWS is unique to the seismic models. Given a seismic failure of the spent fuel pool heat exchanger, this action is needed to isolate the spent fuel pool heat exchanger from the CCW header before the CCW inventory is depleted and the CCW system fails. The calculated failure probability for this human error is 5.60E-02/demand. (See Appendix 19.5E for the calculation sheets for this human error.)

This analysis used the same human error rates for the other three errors as were used in the internal events analysis. All three actions are time-critical actions that would be taken in high stress situations following the failure of normally responding front line safety systems. The fact that the initiating event is a seismic event would not significantly alter the stress level nor the available time in which the actions needed to be performed. Thus, use of the human error rates calculated for the internal events analysis was felt to be appropriate.

The System 80+ Class 1E electrical distribution system is provided with protection schemes which conform to the requirements of IEEE STD-741-1986. The protective schemes are designed to isolate faulted equipment from the rest of the system to minimize the effect of the fault and to maximize the availability of the remaining equipment. The basic schemes consist of ground fault protection, instantaneous overcurrent and timed overcurrent protection. In developing the SMA models, it was assumed that the seismic failure of equipment in the electrical distribution system were "open circuit" failures. Implicit within this assumption is the assumption that if a "hot short" failure were to occur, the appropriate circuit interrupter(s) would open on overcurrent to prevent "backward" propagation of the fault.

Solid state switching devices and electromechanical relays will be used in the NUPLEX 80+ protection and control systems. Solid state switching devices are inherently immune to mechanical switching discontinuities such as contact chatter. Robust electromechanical relays are selected for NUPLEX 80+ applications such that inherent mechanical contact chatter is within the requisite system performance criteria. Therefore, contact chatter has no effect on system operation and was, therefore, not included in the seismic analysis. The COL must confirm the use of seismically robust electromechanical relays in the engineered safety features actuation and control systems.

No formal uncertainty or importance analyses were performed because a seismic core damage frequency was not calculated. However, a set of twelve sensitivity cases were run by changing the HCLPF values for various components or groups of like components and re-evaluating the plant HCLPF and the "Min Sequence HCLPF". The "Min Sequence HCLPF" is defined as the minimum HCLPF for seismic core damage sequences exclusive of the structural failure sequence, and the LOCA in excess of ECCS

capability sequence. The results of these sensitivity analyses are summarized in Table 19.7.5.3-2. This table defines the component or component group for which the HCLPF is being changed, presents the base component HCLPF and the changed component HCLPF, and presents the new "Min Sequence" HCLPF and the new plant HCLPF. These sensitivity analyses basically confirmed the intuitive importance of the component HCLPFs. That is, if the HCLPF for a component that appears as a dominant contributor to a sequence HCLPF is decreased below the plant or "Min Sequence" HCLPF values, the plant and/or "Min Sequence" HCLPF value will decrease to the lower value. On the other hand, if the HCLPF for that component or group of components is increased, the plant and "Min Sequence" HCLPF values do not change.

None of the seismic core damage sequences had a HCLPF less than two times the design basis earthquake. In addition, the dominant sequence is a seismically induced failure of the containment vessel which leads to core damage and containment failure. Therefore, no additional containment isolation failure analyses were performed.

Seismic Margin Assessment

The COL applicant will be required to verify that key assumptions for structures, systems and components considered in the (SMA) are valid for the as-built plant conditions [COL Item 19-4]. This will include evaluation of (HCLPF) values for structures which house non-safety related equipment relied upon in the SMA evaluations such as the combustion gas turbine. The verification process will include a seismic walkdown, including development of detailed procedures, [COL Item 19-4] to ensure that as-built conditions conform to the assumptions used in the SMA and to assure that proper anchorage for equipment has been provided and that the potential for seismic spatial system interaction does not exist. Deviations from assumptions will be evaluated to determine if vulnerabilities have been introduced. Also, if equipment is qualified for site-specific requirements (Appendix 3.9A, Section 1.4.3.2.1.2, Option 4), the impact on the SMA HCLPF will be evaluated.

High Confidence of Low Probability of Failure

The details for verifying that key assumptions for structures, systems, and components considered in the SMA are valid for as-built plant conditions should be modeled after approved NRC SMA procedures and should incorporate insights from SMAs conducted at operating plants. The verification process is expected to consist of the following steps:

1. Preparation for Plant Walkdown

2. Plant Seismic Logic Model Walkdown

3. Assessment of As-Built SMA HCLPF Values

4. Seismic Plant Walkdown

5. Validation of Plant Level HCLPF Calculations

These steps will ensure that as-built plant design characteristics are evaluated; critical component, structural, and sequence HCLPF values are reviewed; and deviations from design assumptions and vulnerabilities which could reduce the plant level HCLPF value below 0.5g are exposed.]!

In Section 19.1.2.2.3 (page 19-149) of the Draft Safety Evaluation Report for CESSAR-DC, it stated:

[["As the seismic analysis is being redone, there is a need to augment the internal events model to the extent possible, by explicit inclusion of structural and other passive failures that were excluded from the internal events model."

This is COL action Item 19-2. As part of the model development for the Seismic Margins Analysis, the internal events model was updated to include structural and passive failures. This completes COL action item 19-2.]!

The Draft Safety Analysis Report for CESSAR-DC contained an additional COL Item, 19.1.2.2.6-1, [[(Item 19-6 in Table 1.10-1) which stated that the COL Applicant should factor site-specific spectra into the analysis and verify the layout and anchorage of critical components. This COL Item is covered by the SMA and the seismic walkdown to be performed by the COL applicant]! as discussed above.

1. COL information item; see DCD introduction section 1.5.2.

This section intentionally blank.

19.7.5.4 Comparison of HCLPF for Rock and Soil Sites

The SMA documented in Sections 19.7.5.2 and 19.7.5.3 is based on a rock site. The rock site was selected because, in general, rock sites are the most limiting. However, component seismic fragilities are a function of the demand spectral frequencies and the natural frequency of the component. Thus, the HCLPF for some components could be lower for some soil conditions than the component's HCLPF for the rock site. To evaluate the potential impact of soil sites on the plant HCLPF, component fragilities were developed for five soil sites that encompass the soil sites used as the design basis for System 80+, and the SMA models were requantified. Table 19.7.5.4-1 presents the component HCLPFs for the five soil sites and the base rock site. Table 19.7.5.4-2 presents the equivalent information for the structures and the major NSSS components. Tables 19.7.5.4-3 through 19.7.5.4-7 present the SMA quantification summary for each of the soil sites. The rock site quantification summary is presented in Table 19.7.5.3-1.

As can be seen by comparing the summary of results for the soil cases on Tables 19.7.5.4-3 through 19.7.5.4-7 with the summary of results for the rock case on Table 19.7.5.3-1, the results for the soil cases are not substantially different from the rock case results. The dominant contributor to the plant HCLPF for all soil cases is the same, sliding/overturning of the containment vessel. The second dominant contributor to plant HCLPF is also the same for the soil cases and the rock case. This contributor is a seismically induced ATWS with an adverse MTC. For the rock case, the third dominant contributor is a LOCA in excess of ECCS capabilities. For the soil cases, the third dominant contributor is a seismically induced station blackout. The seismically induced station blackout is the fourth dominant contributor for the rock site. For lesser contributors, there are some minor changes in specific sequence HCLPFs, but these changes do not affect the overall plant HCLPF. Therefore, it is concluded that the SMA results for the rock site, as presented in Sections 19.7.5.2 and 19.7.5.3 are bounding for System 80+.

This section intentionally blank.

19.8 SHUTDOWN RISK ASSESSMENT

19.8.1 SHUTDOWN PRA SUMMARY AND CONCLUSIONS

A study of the risk associated with the shutdown modes of operation was performed. The scope of this assessment included evaluation of internal events, loss of offsite power and fire and flood during Modes 4 through 6. Since procedures and design details (such as cable routes) were not yet available, the fault trees were not linked and failure of support systems was not included.

Event trees were developed and quantified for loss of decay heat removal (DHR) and loss of coolant inventory for Modes 4 through 6. The risks associated with loss of offsite power and fire and floods were quantified. Criticality events were not quantified after an initial review showed criticality to be a small contributor to risk. In quantifying the core damage frequency (CDF), emphasis was placed on the human errors because earlier studies have shown that these dominate the shutdown risk. The system failure probabilities were evaluated using modifications to the fault trees.

19.8.1.1 Results

Table 19.8.1-1 summarizes the contributors to core damage frequency (CDF) by Plant Operating State (POS) and initiating event. The leading POS in terms of contribution to CDF is the POS for Mode 5R, reduced inventory operation, which accounts for 48% of the internal risk. Loss of DHR is the dominant sequence for this POS. This POS and sequence were also identified in earlier PRAs as being the dominant contributors to CDF. The second leading POS for contribution to CDF is the POS for Modes 6E, and 6I (see Table 19.8.2-1 for definitions). In this POS the IRWST is empty and therefore not available as a source of coolant for any makeup or feed and bleed operation. LOCA is the dominant sequence for this POS because the capability to feed coolant into the core is limited. The third leading POS for contribution to CDF is the POS for Modes 4, 5, and 6F (IRWST full). Loss of offsite power is the dominant sequence for this POS because of the long time interval spent in this configuration and the need to restore AC in about two hours.

The importance of the various internal initiating event types in terms of CDF contribution is also shown in Table 19.8.1-1. Loss of offsite power (LOOP) is the leading internal initiating event in contribution to CDF (39%). Even with requirements for two switchyards and two standby generators to be available during shutdown, the risk was not negligible. Loss of DHR was the second largest initiating event type in terms of contribution to CDF (36% of internal CDF).

Fires account for 36% of the total shutdown CDF. The flooding CDF was calculated to be 8.2E-8/y and was modeled as part of the LOCA risk.

Table 19.8.1-2 lists the dominant sequences leading to core damage. Loss of DHR in reduced inventory accounts for 24% of the internal event CDF. LOOP in Modes 4, 5, and 6F is the second largest sequence. LOCAs in Modes 6E, and 6I when the IRWST and SIS is not necessarily available are the third largest sequence.

Table 19.8.1-3 compares the results of this study with other shutdown PRAs. In all these studies, loss of DHR during reduced inventory is the largest single contributor. The lower total CDF for System 80+ is due to design improvements. The System 80+ has two dedicated Shutdown Cooling Systems (SCS) that can also be used to feed coolant from the IRWST in a LOCA or during reduced inventory operations. The Containment Spray System (CSS) pumps are installed as spares to the SCS pumps. The System 80+ has a four train Safety Injection System (SIS) and a new technical specification requires that two trains be available during most shutdown modes. This coupled with an IRWST gives added LOCA protection and a DHR path using feed and bleed.

This study was performed as a part of the System 80+ design process and had an impact on the design. For example, the cross-connect valves for the CSS were replaced with MOVs which resulted in an improvement in restoration of DHR. This PRA has been used to help develop technical specifications. For example, a new technical specification for two SIS trains to be available in modes when the IRWST is available is being considered.

19.8.1.2 Insights

General

A. The initiating event frequencies are higher than Mode 1 operation because of the greater opportunity for operator errors during outages. Operator training and management control of plant configuration is important to reducing shutdown events and risk.

B. The operation and maintenance personnel must have the procedures, training and spare parts to restore DHR in a timely manner. SCS operation is the true end-state for shutdown sequences.

C. Most systems are manually started or aligned in shutdown modes. Training is especially important because the operator must be able to cope with the plant in an unplanned configuration.

D. The concept of defense in depth applies to shutdown modes as well as Mode 1. The more ways that the operator can maintain coolant inventory and remove decay heat, the lower the risk. The presence of SIS capability in shutdown is an example of added defense in depth.

E. The ability of the operator to be able to align the SIS train for makeup of inventory or to use for a feed and bleed operation is important for defense in depth.

F. There are two trains of SCS and it is important that the COL applicant maintain a configuration management system for maintenance activities on the SCS and its support systems.[1] Configuration control is important because all plant risks, all accidents and incidents, and all accident precursors arise because of critical configurations which have occurred. If configurations were managed so that critical, high-risk configurations did not occur, then the risks would be small and accidents or incidents would occur rarely. Table 19.8.1-4 (developed from the more extended dependency Table 19.6.1-1) is an example of the systems that support each SCS train. The COL applicant should identify the systems, structures and components (SSCs) that support DHR (as well as other safety functions). The COL applicant should consider the overall effect of removing SSCs identified above from service on the DHR safety function. The COL applicant should limit normal maintenance on combinations of equipment so that an additional single or common cause failure would not cause total loss of DHR.[1] A configuration management system should help to insure the availability of the standby SCS.

G. If one train is lost because of fire, flood, or random component failure, it is important that the other train have the highest possible availability. The COL applicant should develop procedures and a configuration management strategy to handle the period of time when one of the two DHR paths is unavailable.[1] In this case (a technical specification violation) the operator should suspend the maintenance and testing activities on equipment that support the operating SCS train. Given failure of one train, the operator should restore any systems that support the other train and are out for maintenance.

H. During plant shutdown, risk can be minimized by appropriate outage management, administrative controls, procedures and operator knowledge of plant configuration. The COL applicant should develop the appropriate administrative controls, procedures and operator training for shutdown operations. (See also insights F and G above.) [COL Item 19-9][1]

---

1. COL information item; see DCD introduction section 1.5.2.

I. During plant shutdown operation, the integrity of fire and flood barriers between areas in the same division, such as quadrants, where systems comprising the alternate shutdown are located should be maintained. [The COL applicant should incorporate in its configuration control program a requirement that, during Modes 4, 5, and 6, the water tight flood doors and fire doors will be maintained closed on at least one quadrant within the subsphere (containing either an SCS or CSS pump) to help prevent common-mode failures from internal floods or fires. The SCS or CSS pump in this quadrant shall be operable. If the flood or fire doors to this quadrant must be opened for reasons other than to permit normal access, a fire watch will be established for the affected door. [COL Item 19-9]].[1]

Loss of DHR Insights

A. Reduced inventory is the most critical operation. The operator should be aware of this and plant activities should be scheduled accordingly. Use of nozzle dams is encouraged as a method of limiting the time spent in this mode.

1. COL information item; see DCD introduction section 1.5.2.

PAGE 19.8-4 DELETED

This Section Intentionally Blank

19.8.2 BACKGROUND

Until recently, emphasis has been on the safety of power plants during power operation. This was due to the fact that the plant is in this configuration most of the time and the core power, decay heat rate and fission product inventory are highest. More recently, people have been investigating the risk of plants during shutdown and refueling. During these modes of operation, the plant has a lower decay heat and fission product inventory. The plant configuration is not as well defined as in full power operation because maintenance and testing is being performed. This section estimates the risk of operation of System 80+ in Modes 4 through 6.

The emphasis on the risks of plant operation during refueling and maintenance outages developed slowly. Although no core damage has occurred during reactor outages, a few events have occurred which could be precursors to more severe accidents. One of the first events to increase the awareness of risks in outages was the loss of the refueling cavity seal at Connecticut Yankee on August 21, 1984. In this event, 200,000 gallons of water quickly spilled into the containment, draining the refueling cavity. This event could have been more severe if the fuel movement had actually started.

Another event which increased the awareness of the risks during outages was the Vogtle 1 event on March 20, 1990. The event started with a truck backing into equipment in a switchyard, causing a loss of power to the first auxiliary transformer. The second auxiliary transformer and one of the diesels were out for maintenance. The second diesel kept tripping due to an instrument failure. This combination of maintenance activities and failures led to a station blackout and loss of Decay Heat Removal (DHR). Under normal conditions, with the vessel filled or with the refueling cavity flooded, the operator would have many hours to restore DHR. In this incident, the plant was in mid-loop operation and the primary inventory was greatly reduced. When DHR was restored in 41 minutes, the primary coolant temperature had risen 46°F to 136°F. This incident illustrates the unusual plant configurations that can exist during an outage and the risks associated with maintenance activities and mid-loop operation.

During 1991, there were several incidents during shutdown. After four events occurred within six days in March, the NRC issued Information Notice No. 91-22 describing these events. One plant had two incidents during the same outage. There were at least seven events where loss of DHR occurred in 1991. All these events increased the emphasis on risks during outages.

The NRC requested additional information from the ALWR participants pertaining to shutdown risk. The EPRI ALWR Requirements Document was modified to include a risk assessment for shutdown modes. This analysis satisfies that requirement. This analysis uses a

PAGES 19.8-6 THROUGH 19.8-8 DELETED

This Section Intentionally Blank.

19.8.3 INITIATING EVENT FREQUENCIES

While the EPRI Key Assumptions and Groundrules Document (KAG)[7] gives initiating event frequencies for performing a PRA at full power for the ALWR program, established frequencies for shutdown modes have not yet been included in this document. The System 80+ analysis has used the frequencies developed in the BNL Coarse Screening Analysis[106]. These frequencies have been developed after an extensive review of operating experience by the BNL staff. The use of these frequencies is quite conservative because these frequencies are based on historical occurrences and do not reflect any lessons learned, procedure improvements, or training improvements. In operating plants, the frequency of automatic trips decreased from about 7/y in the 1970s to about 1.5/y today because of such improvements. With the current emphasis on shutdown risk, initiating events in these modes will also decrease. The use of these frequencies does not take into account System 80+ design changes that could reduce the frequency of certain events. For example, there are four redundant and diverse level measuring instruments for reduced inventory operation which will reduce the frequency of loss of DHR from pump cavitation in that mode.

Table 19.8.3-1 gives the mapping of the BNL Plant Operating States (POSs) onto the System 80+ POSs. While BNL defined POSs for both entering refueling and returning to power, this study used the same POS for the same configuration and assumed that the restoration times reflect the higher decay heats. Table 19.8.3-2 gives the frequencies used in this analysis. The following paragraphs will describe their derivation. The initiating event frequencies are based on an example of the refueling outage given in Table 19.8.3-3. The time spent in each mode was based on the outage task description developed by Duke and reviewed by ABB-CE personnel with operating plant experience. This outage example is not the minimum outage schedule recommended by EPRI (16 days) but is longer to include mid-loop operation and SG and RCP maintenance. The time in unplanned forced outages equals 5 days/year, the forced outage specification in the EPRI URD. The fraction of time in M4, M5, and M5R in the forced outage represents the times needed to change state as presented in the outage schedule. In addition, it was assumed that the plant entered Mode 4 and mid-loop twice a year. The outage schedule assumes that the CL Applicant will use nozzle dams for SG maintenance and minimize their time on reduced inventory operation. It is also assumed that the CL Applicant will use a 18 month refueling schedule. Going to a 24 month schedule will reduce the outage risk.

The initiating event frequencies for Loss of DHR is being taken from the BNL Coarse Screening Analysis. Table 4.2 of that report gives the definitions for the types of DHR losses and Table 4.1-3

PAGE 19.8-10 DELETED

This Section Intentionally Blank

19.8.4 ACCIDENT SEQUENCES

For each of the accident sequences considered in this study, an event tree was developed and evaluated. The event tree starts with the initiating event frequency developed in Section 19.8.3 and describes the sequence of events as discrete events which are completed either successfully or not. Each specific sequence leads to either core damage or a safe plant condition. The following subsections discuss each event tree and their branch points.

The branch points and their supporting fault trees and Human Error Probability (HEP) analysis are given in Section 19.8.5. Earlier shutdown risk studies have identified operator error as a significant contributor to risk. This is because many of the initiating events are caused by operator error and mitigation actions require operator actuation. With emphases being placed on operator error, the Human Reliability Analysis (HRA) trees are also given and discussed in Section 19.8.5. System fault trees for system failures presented in this report, were modified from those presented in the Mode 1 PRA.

A stable endpoint of the event trees is the establishment of a DHR path or a feed and bleed path. Containment heat removal has been neglected because it can be accomplished with the containment coolers or the containment can be vented before over-pressurization.

19.8.4.1 Loss of DHR

NUREG-1449 found that for PWRs, loss of Decay Heat Removal (DHR) represented one of the more serious event types observed in reactor operations. Many shutdown PRAs such as NSAC-84, NUREG/CR-5015, and the Seabrook PRA for Shutdown Operation concluded that loss of DHR was the leading contributor to CDF, being as high as 82% of the CDF in some studies. The System 80+ has two redundant and independent trains in the dedicated Shutdown Cooling Systems (SCS) that do not share pumps with the Safety Injection System as is common in most existing plants. In addition, two Containment Spray System (CSS) pumps are installed to be used as installed spares to the SCS trains. The SCS trains can also be aligned to the IRWST (when available) and be used to remove decay heat in a feed and bleed operation. Also, two SIS trains are available for feed and bleed (when IRWST is available). As a final method of cooling the core, the CVCS system can be used to inject coolant from the boric acid storage tank. During some parts of the outage, the steam generators are available for heat removal. In this analysis, no credit was given for the SGs as a DHR path. Its inclusion would reduce the risk from loss of DHR.

The following subsections address loss of DHR for various modes. Modes were grouped based on the existence of similar equipment to mitigate the transient. A stable endpoint of the event trees is the establishment of a DHR path or a feed and bleed path.

PAGES 19.8-12 THROUGH 19.8-46 DELETED

This Section Intentionally Blank

19.8.5 FAULT TREE ANALYSIS

The accident sequences described in Section 19.8.4 are represented by a series of branch points representing the success or failure of systems to perform their tasks. With few exceptions, the tasks must be started with an operator action (no automatic actuation) and the analysis of the human error probabilities (HEPs) are presented in this section. Two sets of HEPs were evaluated and used. For all the modes except Mode 5R, the HEPs were based on two hours before core damage and the stresses increased toward the latter tasks. No credit was included for the very long sequences. For Mode 5R, higher stresses were used in evaluating the HEPs. Most of the branch points were evaluated with fault trees that are presented in this section. The basic assumptions in the fault trees are that the systems are tested every 30 days and the mission times are 24 hours. The fault trees are modified versions of those used in the Mode 1 PRA and the individual data sheets on all components are presented in that document. The fault trees were not linked in evaluating the event trees. Table 19.8.5-1 summarizes the branch points.

Previous shutdown PRAs have identified human error probability (HEP) analysis as an important part of the overall risk analysis because most of the systems must be manually actuated. For each fault tree or branch point, the Human Reliability Analysis (HRA) input is described below. The analysis is based on the data and methodology of NUREG/CR-1278 [37]. These data and methods have been implemented for specified event-based scenarios, using simple, conservative and defensible assumptions regarding human performance and error in component tasks, to produce a crude best-estimate analysis of anticipated human error probabilities (HEPs) for shutdown operations.

The results are presented in the following format:

A. Basis material provides details and justification for assumptions, logic, etc., to support review and revision.

B. Calculation tables provide values and NUREG/CR-1278 references for the HEP quantifications.

C. Event trees portray the logic of the quantifications graphically.

19.8.5.1 OI, Operator Isolates Leak

A review of the shutdown LOCAs in PWRs identified 51 events. Most events are operator errors in aligning valves. Only one event, the failure of the refueling cavity seal could not be isolated and this

PAGES 19.8-48 THROUGH 19.8-76 DELETED

This Section Intentionally Blank

19.8.6 IMPORTANCE AND SENSITIVITY ANALYSIS

19.8.6.1 System and Branch Point Importance

Table 19.8.6-1 gives the Fussel-Vesely Importance (FVI) for the event branch points for the internal events considered in this analysis. In this analysis, the fault trees were not linked but were used to give point values. Therefore the event sequences and the FVIs are for systems and not specific components. Insights can still be gained from this importance analysis.

The FVI is the fraction of the CDF that a specific system failure occurred in the event sequences. Branch element SCS-F has the highest FVI, 0.45. This means that the sum of the sequences in which failure of the SCS to feed coolant into the vessel from the IRWST (SCS-F) was 2.4E-7/y or 45% of the internal CDF of 5.37E-7/y. SCS-F is used in LOCAs as an alternative charging path. In loss of DHR in reduced inventory, SCS-F is used to makeup inventory if the CVCS fails. Also for LOCAs in containment when the SIS might not be available, the SCS as a feed mode is important. SCS-F requires the operator to align the SCS train to the IRWST and start a pump. The HEP accounts for 14% of SCS-F failure and shows the importance of procedures and training to do this task. MOV failure accounts for most of the system failure and shows the importance on maintaining these valves.

The branch point with the second highest FVI is OR ORL, the restoration of the operating SCS train. OR ORL contributes to 36% of the CDF. NUREG-1449 identified only 16% of the loss of DHR as mechanical failures. The remaining 84% can be restored if the operator has sufficient training and procedures. For LOCAs that are isolated, restoration of the operating SCS train again requires the operator to have an understanding of the SCS.

The use of SIS in shutdown mode is the third highest FVI contributing to 33% of the CDF. The availability of SIS in shutdown is a new technical specification and is made easier because the System 80+ design has four SIS trains. Two trains could have scheduled maintenance while two are available. Placing the IRWST in containment makes feed and bleed more reliable. SIS is used for both LOCAs and heat removal through feed and bleed. Again, procedures and training are important since the operator must manually actuate this process.

REC-L represents the restoration of some DHR capability while the plant is being cooled using the CVCS and BAST inventory. This has the fourth highest FVI contributing to 30% of the CDF. The operator has 12 or more hours to restore one of four potential DHR paths (two in each train). Here, not only is training and procedures important but a spare parts inventory also helps. The

PAGES 19.8-78 THROUGH 19.7-80 DELETED

This Section Intentionally Blank

19.8.7 RADIOLOGICAL CONSEQUENCES

The analysis presented in Section 19.8.4 quantifies the probability of core damage during various shutdown modes. For a Level III PPA this analysis would be continued to quantify the risk to the off-site population from the release of the fission products. The fission product inventory is reduced during shutdown because of two effects. If the accident occurs after the fuel shuffling is completed, one third of the core contains fresh fuel with no fission products. Also, as the outage continues, the nuclear inventory is reduced by fission product decay.

To demonstrate the effects of fission product decay on the radiological consequences, an evaluation of the nuclide inventory was performed starting with the nuclide inventory associated with 4 days after shutdown. This time was selected because it represents the minimum time during which mid-loop operation can be initiated. Tables 19.8.7-1 and 19.8.7-2 illustrate the effects of the fission product decay process on the overall core radioactive nuclide inventory and the concentration of potentially volatile fission products. A review of the radionuclide decay chain indicates that the fission product inventory has decreased by 30% by the end of a 20 day refueling. Furthermore, the concentration of potentially volatile nuclide releases will be reduced by at least a factor of 5. If the shutdown is extended to 40 days, the nuclide inventories would be one half of the four-day level and the concentration of the volatile fission products would be only 6% of that potentially available at 4 days into shutdown.

Radiological consequences are also affected by the containment integrity. Containment integrity is associaced with Modes 4 (Hot Shutdown) and higher. In the literal sense, containment integrity involves "Operable" airlocks, fully scaled and leak-tested equipment hatch and fuel transfer tube. It also mandates closure of Containment High Purge and leak tests of associated valves. Containment integrity, due to its complex nature, is obtained by adherence to procedure.

Containment closure has a less stringent set of requirements. Basically, it consists of reasonable measures taken to limit spread of contamination in a short time frame. Actions such as closure of all penetrations and one door of each airlock, securing equipment hatch with at least four bolts, closure of fuel transfer tube valve (not flange replacement), and shutdown of all containment ventilated into and out of containment would be needed to effect containment closure.

The System 80+ design will provide indication of all containment isolation valves, except those which require manual power to manipulate. Indication will be either a combination of valve switch indication, panel status light or computer point position indication.

REMAINDER SECTION 19.8 DELETED

TABLE OF CONTENTS (Cont'd)

APPENDIX 19.8A

Section	Subject	Page No.
7.0	SYSTEM 80+ DESIGN FEATURES FOR SIMPLICITY OF SHUTDOWN OPERATIONS	7.1-1
7.1	INTRODUCTION	7.1-1
7.2	DISCUSSION	7.2-1
7.2.1	TECHNICAL SPECIFICATIONS FOR REDUCED INVENTORY	7.2-1
7.2.2	SHUTDOWN COOLING SYSTEM	7.2-1
7.2.3	CONTAINMENT SPRAY SYSTEM	7.2-2
7.2.4	COMPONENT COOLING WATER SYSTEM	7.2-2
7.2.5	STATION SERVICE WATER SYSTEM	7.2-2
7.2.6	ELECTRICAL DISTRIBUTION SYSTEM	7.2-2
7.2.7	NUPLEX 80+ ADVANCED CONTROL COMPLEX	7.2-3
7.2.8	REDUCED INVENTORY INSTRUMENTATION	7.2-5
7.2.9	CONTAINMENT	7.2-5
7.3	CONCLUSION	7.3-1
8.0	CONCLUSIONS	8.0-1
9.0	REFERENCES	9.0-1

APPENDICES

APPENDIX A	RESPONSES TO REQUESTS FOR ADDITIONAL INFORMATION	A-1
~~APPENDIX B~~	~~PROCEDURE GUIDANCE TO SUPPORT REDUCED RCS INVENTORY OPERATIONS~~	~~B-1~~

LIST OF FIGURES

APPENDIX 19.8A

Figure	Subject
2.5-5D	MODE 5 LOCA, MPC VS TIME
2.5-5E	MODE 5 LOCA, UTILITY PERSONNEL WHOLE BODY DOSE VS TIME
2.5-6A	MODE 6 BOIL OFF, CONTAINMENT TEMP VS TIME
2.5-6B	MODE 6 BOIL OFF, WHOLE BODY DOSE VS TIME
2.5-6C	MODE 6 BOIL OFF, THYROID DOSE VS TIME
2.5-6D	MODE 6 BOIL OFF, MPC VS TIME
2.5-6E	MODE 6 BOIL OFF, UTILITY PERSONNEL WHOLE BODY DOSE VS TIME
2.7-1	NUCLEAR ISLAND FIRE BARRIER LOCATIONS, PLANT AT ELEVATION 50+0 (See Chapter 9, Figure 9.5.1-2.)
2.7-2	NUCLEAR ISLAND FIRE BARRIER LOCATIONS, PLANT AT ELEVATION 70+0 (See Chapter 9, Figure 9.5.1-3.)
2.8-1	REACTOR COOLANT SYSTEM ELEVATIONS RELATED TO SHUTDOWN COOLING OPERATIONS
2.8-2	DIFFERENTIAL PRESSURE INSTRUMENT TAP LOCATIONS - SCHEMATIC
2.8-3	SCHEMATIC REPRESENTATION OF THE INADEQUATE CORE COOLING, HJTC PROBES
2.8-4	SCHEMATIC REPRESENTATION OF THE NARROW-RANGE HEATED JUNCTION THERMOCOUPLE PROBES
2.9-1	LOCATIONS OF SAFETY INJECTION SYSTEM SUCTION IN IRWST (See Chapter 6, Figure 6.8-1.)
2.9-2	LOCATION OF WING WALL DEBRIS SCREEN ASSEMBLIES

LIST OF FIGURES

APPENDIX 19.8A

Figure	Subject
2.9-3	LOCATIONS OF TRASH RACK AND SPILLWAY FOR IRWST AND HVT
2.10-1	RESULTS OF MODE 6 NATURAL CIRCULATION ANALYSIS OF SYSTEM 80+
2.11-1	CONTAINMENT BUILDING LOAD HANDLING PATHS
2.11-2	FUEL HANDLING BUILDING LOAD HANDLING PATHS
2.12-1	POTENTIAL RCS INTERFACING SYSTEM DRAINAGE PATHS FROM SCS TRAIN NO. 1
2.12-2	POTENTIAL RCS INTERFACING SYSTEM DRAINAGE PATHS FROM SIS/SCS DVI NOZZLE 1A
2.12-3	POTENTIAL RCS INTERFACING SYSTEM DRAINAGE PATHS FROM CVCS
2.12-4	POTENTIAL RCS INTERFACING SYSTEM DRAINAGE PATHS FROM PSS
2.13-1	NUCLEAR ISLAND DETAILED ARRANGEMENT PLAN AT EL. 50+0 (See Chapter 1, Fig. 1.2-4)
2.13-2	NUCLEAR ISLAND DETAILED ARRANGEMENT PLAN AT EL. 70+0 (See Chapter 1, Fig. 1.2-5)
4.0-1	INITIAL CONDITIONS FOR PRESSURE AND TEMPERATURE IN MODES 3 THROUGH 6
4.1-1	MAXIMUM POWER VS STEAM LINE BREAK AREA
5-1	CLAD SURFACE TEMPERATURE, SAFETY INJECTION, INITIATED AT 10 MINUTES, DVI LINE BREAK
5-2	PRESSURIZER PRESSURE, NO SAFETY INJECTION, DVI LINE BREAK
5-3	REACTOR VESSEL MIXTURE HEIGHT, NO SAFETY INJECTION, DVI LINE BREAK

1.2 SCOPE

Sections 2.1 through 2.13 present detailed discussions on specific shutdown issues. ~~PRA results for shutdown are presented in Section 19.8.~~ Sections 4.0, 5.0 and 6.0 of this appendix present an evaluation of the applicability of the analyses in Chapters 6 and 15 to LOCA and accident events that are initiated from shutdown modes. Section 7.0 evaluates the features of System 80+ that simplify shutdown operations and thereby reduce the potential for initiating shutdown events. Conclusions of this appendix are provided in Section 8.0.

Appendix 19.8A also addresses the RAI's from the NRC staff on CESSAR-DC that pertain to shutdown risk. Appendix A to Appendix 19.8A lists the RAIs and provides either the response or a referral to sections of this appendix which encompass the response to each RAI.

2.0 SHUTDOWN RISK ISSUES

Sections 2.1 through 2.13 present detailed evaluations of specific shutdown issues that were identified at the December 18, 1991 meeting with the NRC and that are listed in Reference 2. Each section is subdivided into four subsections. The first subsection states the issue consistent with the interpretation and evaluation in NUREG-1449 and the appropriate RAIs. The second subsection lists the acceptance criteria that are employed to evaluate the System 80+ design to prevent and/or mitigate unacceptable consequences related to each shutdown issue. The third subsection discusses the postulated plant scenarios, the analyses and the evaluations considered by to assure that the shutdown issue is adequately addressed. Finally, the fourth subsection states how the issue is resolved by the System 80+ design. Depending upon each issue and its significance in evaluating System 80+, the content of these subsections varies. Where appropriate, reference is made to RAI's on the issue, both outstanding and previously submitted. Appendix A contains ~~the~~ responses to ~~all the~~ RAI's.

2.1 PROCEDURES

2.1.1 ISSUE

The operational guidance provided by the plant designer to the owner/operator might not be sufficient to ensure that procedures to avoid, detect, mitigate, and/or recover from abnormal events initiated from shutdown operations can be developed by the plant owner/operator.

2.1.2 ACCEPTANCE CRITERIA

The operational guidance provided by the plant designer to the owner/operator shall be sufficient to properly utilize design features that are available to detect, mitigate and assist recovery from abnormal events initiated during shutdown operations.

2.1.3 DISCUSSION

The System 80+ design incorporates advanced features which promote safer and simpler plant operation. The features include redundancy and diversity of components and systems, dedicated and/or permanently aligned systems, and an advanced information system which better informs the operations staff of plant status, potential adverse system interactions, and available recovery paths if an abnormal event occurs. These features also contribute to improved operability and maintainability that should significantly reduce the initiating situations that have contributed to increased shutdown risk.

The plant owner/operator is responsible for preparing detailed procedures for normal, abnormal, and emergency operations using guidance developed by the plant designer and plant site specific information. The plant designer's guidance generally is in the form of suggested operational sequences that preserve the safety bases of the design. Since shutdown operations must be intimately connected to an outage strategy, specific procedures cannot be imposed by the plant designer to cover the array of possible shutdown events. However, the plant designer can provide guides which instruct the plant owner/operator in the use of design features which can detect, mitigate, and assist recovery from abnormal events that can occur during shutdown operations.

The operational guidance contained in this appendix will be provided to the plant owner/operator through the plant designer's Operational Support Information (OSI) program. The intent of the OSI program is to insure that features of the System 80+ design are effectively utilized in the operation of the plant as specified in the plant owner/operator's operations program. The OSI program also provides a formal means to transfer design related bases for operations, regulatory operational commitments and related information that is typically provided to and required by a plant license applicant. The OSI program is staged to develop more detailed information as the plant design matures and is expected to be completed during the

construction and pre-operational phases of a plant project. The OSI program integrates information from various interrelated areas, e.g., the Maintenance Plan, the Reliability Assurance Program and as-procured equipment characteristics, to insure the owner/operator can efficiently operate the plant within the design bases.

A summary of general operational guidance related to shutdown operations is provided in Table 2.1-1. Specific details are contained in the appropriate sections of this appendix.

An outline of the operational guidance developed to support RCS reduced inventory operations is provided in Appendix B. This guidance together with supporting information from this appendix is sufficient for a plant owner/operator to develop an operational guideline for reduced RCS inventory operations. The development of a detailed procedure by the plant owner/operator would require specific equipment characteristics of procured components and results of the pre-operational testing (Chapter 14) to determine system performance values. As an example to support mid-loop operation, the shutdown coolant system flows, suction line vortexing characteristics, level instrumentation calibration, among others, would be measured during plant startup. This data would be used to verify performance as well as to provide operational data. Specific testing requirements for shutdown oriented instrumentation are given in Chapter 14.

2.1.4 RESOLUTION

The issue of procedures for shutdown operation is resolved for System 80+ by providing operational guidance to address use of advanced design features to detect, mitigate, and assist recovery from abnormal events initiated from shutdown operations.

of the Emergency Operations Guidelines

TABLE 2.1-1 (Cont'd)

(Sheet 3 of 6)

SUMMARY OF PROCEDURAL GUIDANCE RELATED TO SHUTDOWN OPERATIONS

TOPIC	PROCEDURAL GUIDANCE	REFERENCE TO REPORT SECTION
	MITIGATION (Immediate Operator Action)	2.3.3.4, 2.12.3, 2.12.4, 2.12.2.3(2) ~~Appendix B~~ stet
	Identify leakage path. Isolate leakage path. Make up losses. a. Safety Injection b. SCS via IRWST c. Containment spray from IRWST via SCS lines d. Charging pumps e. BAST f. Safety Injection Tanks	Emergency Operations Guidelines
Heavy Loads 1) Drop of transported equipment. 2) Drop of fuel bundle 3) Refueling pool seal integrity. 4) Loads over ICI table.	Restrictions specified for: a. Lift Height b. Travel Directions c. Systems Lineup (Specified in, Chapter 9 and Plant Designer's "Heavy Load Guides")	2.11.3

TABLE 2.1-1 (Cont'd)

(Sheet 4 of 6)

SUMMARY OF PROCEDURAL GUIDANCE RELATED TO SHUTDOWN OPERATIONS

TOPIC	PROCEDURAL GUIDANCE	REFERENCE TO REPORT SECTION
Outage Maintenance	Strategy for Shutdown Operations	2.4.3.2.2
	a. Define operating and operational divisions. b. Limit maintenance activities to components and systems not included in a).	Appendix B of Emergency Operations Guidelines
Fire Protection	Administratively require fire protection systems to remain operable in shutdown modes.	2.7.3.2, and 2.7.3.3
	Procedurally Control: a. Combustible materials b. Housekeeping c. Hot work	
	Pre-Fire Plan a. Outline fire fighting strategies b. Monitor status of fire barriers	2.7.3.2

2.2 TECHNICAL SPECIFICATION IMPROVEMENTS

2.2.1 ISSUE

When a plant is operated within the limiting conditions for operation provided by the technical specifications, the consequences of design basis events should be bounded by the results of the safety analyses. However, limiting conditions for operation developed for power operation might not be sufficient to ensure that the consequences of events initiated from shutdown modes are bounded by the analyses. Technical Specification should include the necessary limiting conditions for operation that are applicable to shutdown modes.

2.2.2 ACCEPTANCE CRITERIA

Technical specification shall insure that when the plant is operated within the limiting conditions for operation applicable to the mode of operation, consequences of design basis events shall be bounded by the results of safety analyses for that mode.

2.2.3 DISCUSSION

The System 80+ design incorporates advanced features which promote safer operation and greater margins to operating limits. The features include redundancy and diversity of components and systems and an advanced information system which better informs the operations staff of plant status, potential adverse system interactions, and the recovery paths if an abnormal event occurs. These features also contribute to improved operability and maintainability that should significantly reduce the initiating situations that have contributed to increased shutdown risk.

One objective of the plant designer is to reduce the operational constraints that limit the plant owner's flexibility to operate the plant as efficiently as possible. Another objective is to formally impose the operational constraints required to insure the plant remains within analyzed bounds for operation through the initial set of technical specifications. Overly restrictive technical specifications especially for shutdown modes may unnecessarily complicate operations and may increase risks by prolonging the shutdown period and adding to staff stress. The objective of this assessment of shutdown risk for the System 80+ relative to technical specifications is to ~~modify existing~~ assure that technical specifications ~~to the extent necessary to~~ address event initiators not fully covered by analysis of the traditional design basis events.

A summary of the ~~proposed~~ technical specification modifications is provided in Table 2.2-1. The technical specification modifications and additions reflect:

a. the added redundancy and diversity of the System 80+ design that allows these modifications without affecting operational flexibility;

b. analysis of events initiated during shutdown operations;

c. assessment of the risk of operating in these plant configurations for extended periods, e.g., refueling, unplanned maintenance.

The rationale for the technical specification modifications is contained in the appropriate sections of Appendix 19.8A.

2.2.4 RESOLUTION

The issue of shutdown specific technical specifications is resolved for System 80+ by modifications and additions to the Technical Specifications based upon safety analyses performed for Modes 2 through 6. These modifications and additions provide additional assurance that the consequences of transients and accidents which might occur during shutdown modes of operation are less limiting than those given in Chapters 6 and 15.

and in the Bases of the Technical Specifications in Chapter 16.

A general description of the types of instrumentation which are used for reduced inventory is outlined below.

1. Redundant and independent wide and narrow range level sensors are provided for continuous monitoring of RCS level during draindown operations. The level indicators provide monitoring capability from the pre-drain down normal level in the pressurizer to a point lower than that required for SCS operation. The level indicators are calibrated for low temperature operation and they provide a high degree of accuracy. Indication of levels and low-low, low, high and high-high level alarms are provided in the main control room.

   The wide range level instruments cover draining from the pressurizer to below the bottom of the hot leg and are available with the head on and off the vessel. The narrow range level instruments cover reduced inventory operations, and are also available with head on and off the vessel. The narrow range instruments are accurate for measuring level within the hot leg. During a draindown, level monitoring would be transitioned from the wide range level instruments to the narrow range instruments when the greatest degree of accuracy is required during operations with level within the hot leg region.

2. Several independent diverse temperature measurements representative of core exit temperature are provided during reduced inventory operations. Temperature indication is available when the head is located both on and off the vessel. Since temperature is valuable in guiding SCS restoration actions and in monitoring the success of recovery actions, alarm setpoints are based on integrated response times necessary to support SCS recovery, event mitigation, time to boil, and containment closure.

3. SCS operation monitoring instrumentation is provided that assures precise knowledge of the status of the operating SCS loop; including pressure, temperature, flow and pump performance indicators.

2.3.3.2 SCS Design

~~The functional design of~~ the Shutdown Cooling System (SCS) ~~is substantially complete for System 80+~~. Design features that improve SCS performance during shutdown operation are detailed below.

1. The System 80+ SCS suction lines do not contain any loop seals. An improved suction piping layout allows self venting.

Figure 2.7-1

Nuclear Island Fire Barrier Locations
Plan At Elevation 50+0

Figure 2.7-2

Nuclear Island Fire Barrier Locations
Plan At Elevation 70+0

(For these figures, see Chapter 9, Figures 9.5.1-2 and 9.5.1-3.)

Figure 2.9-1

Locations of Safety Injection System Suction In IRWST

(For this figure, see Chapter 6, Figure 6.8-1.)

Figure 2.13-1

Nuclear Island Detailed Arrangement Plan At El. 50+0

Figure 2.13-2

Nuclear Island Detailed Arrangement Plan At El. 70+0

(For these figures, see Chapter 1, Figure 1.2-4 and Figure 1.2-5.)

4.7 RADIOACTIVE MATERIAL RELEASE FROM A SUBSYSTEM OR COMPONENT

4.7.0 INTRODUCTION

The purpose of this section is to present evaluations which confirm that all radioactive material release from a subsystem or component events postulated to be initiated in a shutdown Mode have acceptable consequences for the System 80+ Standard Design.

4.7.1 RADIOACTIVE GAS WASTE SYSTEM FAILURE

This section of the Standard Review Plan has been deleted (Reference 26 of Section 15.0).

4.7.2 RADIOACTIVE LIQUID WASTE SYSTEM LEAK OR FAILURE

This section of the Standard Review Plan has been deleted (Reference 26 of Section 15.0).

4.7.3 POSTULATED RADIOACTIVE RELEASES DUE TO LIQUID CONTAINING TANK FAILURES

This event has been evaluated in Section 15.7.3 and is not Mode dependent.

4.7.4 FUEL HANDLING ACCIDENT

This event has been evaluated in Section 15.7.4 and is not Mode dependent.

4.7.5 SPENT FUEL CASK DROP ACCIDENTS

This event has been evaluated in Section 15.7.4 ~~of CESSAR-DC~~ and is not Mode dependent.

TABLE 6.1-2

CASES ANALYZED

MODE	LOCA	MSLB
1	102% Power DEHLS, DESLS, DEDLS Chapter 6, Section 6.2 ~~CESSAR DC~~	102%, 50%, 20% Chapter 6, Section 6.2 ~~CESSAR DC~~
2	0% DESLS ~~Current Report~~ This Appendix	0% Chapter 6, Section 6.2 ~~CESSAR DC~~
3	Analysis Not Required Note 1	Analysis Not Required Note 1
4	Analysis Not Required Note 1	Analysis Not Required Note 1
5	Analysis Not Required Since RCS T < 210°F	Case Analyzed With RCS T At 210°F and SG At 350°F ~~Current Report~~ This Appendix
6	Analysis Not Required Since RCS T < 135°F	Analysis Not Required Since Less Limiting Than Mode 5

Note 1: Less NSSS stored energy than Modes 1 and 2. Same ESF available as in Modes 1 and 2.

8.0 CONCLUSIONS

This appendix has provided responses to issues on shutdown risk raised by NRC RAIs. The report shows that the System 80+ design features along with Technical Specifications and operational guidance will result in acceptable consequences from accidents during shutdown.

System 80+ is engineered with features that enhance shutdown safety: 1) by deliberate system engineering, equipment specification and plant arrangements for shutdown operation, 2) by mode dependent control logic that assists and limits operations, 3) by instrumentation, displays and alarms that clearly portray plant status in each mode and 4) by thorough procedural guidance and Technical Specifications that address important shutdown evolutions. Appendix 19.8A shows that these features successfully prevent the occurrence of shutdown risk events or mitigate the consequences of the events.

~~The PRA shows that the core damage frequency for internal events while the plant is in shutdown modes is about the same as the frequency while the plant is at power operation.~~ Evaluations of SAR Chapter 6 and 15 events while in shutdown modes show that all acceptance criteria are met. In addition to the Chapter 6 and 15 analyses, the System 80+ design was reviewed with regard to other issues such as flooding and spills, fires, the dropping of heavy loads, and containment closure times. Again, all acceptance criteria were met.

As a result of the shutdown risk study, several changes to the Technical Specifications have been made. In addition, two design changes will provide improved RCS water level indication during midloop operation. One of these changes is the addition of two narrow range delta P cells between the DVI nozzle and the SDC nozzle at the hot leg. The other change is the addition of two heated junction thermocouple strings to cover the hot leg region. These changes provide a more accurate measurement of the water level in the vicinity of the hot leg elevation.

APPENDIX A

LIST OF TABLES

Table	Title	Page No.
440.129-1	TIMES TO BULK BOILING OF CORE LIQUID AND TO COMPLETE BOILOFF OF LIQUID ABOVE ACTIVE CORE	A-28
440.129-2	HOT-SPOT HEATUP TO 1800°F	A-28
440.154	TECHNICAL SPECIFICATIONS TO ESTABLISH MINIMUM REQUIREMENTS FOR SAFETY FUNCTION CONTROL DURING SHUTDOWN MODES	A-48
440.156	EPRI - URD REQUIREMENTS FOR SHUTDOWN COOLING SYSTEM SUCTION LINE DESIGN AND VORTEX CONTROL	A-54
~~440.176~~	~~ESTIMATE OF CDF FROM LOOP DURING REDUCED INVENTORY MODES~~	~~A-83~~

radiation level. However, if it is necessary to do maintenance on the reactor vessel pool seal, temporary shielding can be placed around the extension shafts to reduce the radiation levels in the work area.

d. The responses to parts a, b, and c of ~~this~~ RAI address the concerns of this question.

*This response was previously transmitted by Reference A-13.

SPLB Question 440.14 : This item intentionally left blank.

~~SPLB Question 440.14~~

~~Table B1.3-1 of Appendix B provides comparisons of severe accident frequency for System 80+ versus System 80. Recent scoping studies have indicated that events when not at power (i.e., shutdown) can provide a significant risk contribution.~~

~~Have these events been analyzed and incorporated into the PRA and if so provide relevant information in the summary table? If not evaluated, provide a schedule for submitting this additional analysis.~~

~~Response 440.14*~~

~~A shutdown risk assessment is being performed for the System 80+ ALWR and will be provided to the NRC by July 31, 1992. This risk assessment includes a Shutdown PRA which is being performed using the methodology described in the revised EPRI PRA Groundrules and Key Assumptions Document. A comparison of the results for System 80+ and System 80 will not be possible because a Shutdown PRA is not available for the earlier plant.~~

~~*This response, and the mentioned risk assessment, supplement the previous response to this RAI in Reference A-15.~~

SPLB Question 440.16(a)

Generic Letter (GL) 87-12 requested information regarding lower RCS inventory operation. Please provide a response to the generic letter with respect to the System 80+.

Response 440.16(a)

Generic Letter 87-12 requested each licensee of operating PWRs and holder of construction permits for PWRs to "provide the NRC with a description of the operation of [the] plant during the approach to a partially filled RCS condition and during operation with a partially filled RCS to ensure [the plant] meet[s] the licensing basis." The description provided in response to Generic Letter 87-12 was to include each of the following nine (9) items, which are in turn responded to.

Generic Letter Item 1

A detailed description of the circumstances and conditions under which [the] plant would be entered into and brought through a draindown process and operated with the RCS partially filled, including any interlocks that could cause a disturbance to the system. Examples of the type of information required are the time between full-power operation and reaching a partially filled condition (used to determine decay heat loads); requirements for minimum steam generator (SG) levels; changes in the status of equipment

1. Limiting whole body dose to utility personnel to < 2.5 rems.

2. Limiting internal dose to utility personnel to < 520 MPC per quarter,

3. Temperature limits inside containment based on a minimum work time of 10 minutes needed to close personnel hatches in Mode 5, at reduced inventory, and Mode 6, and 60 minutes to close the equipment hatch in Mode 5 at full inventory.

For Mode 5, at reduced inventory, the integrated two hour whole body and thyroid doses are below the acceptance limits of 2.5 rem (whole body) and 30 rem (thyroid). In addition, radiation and temperature within the containment are within limits to give utility personnel up to 30 minutes to evacuate and close personnel locks in the containment.

In Mode 5, for full inventory, the integrated two hour whole body and thyroid doses are below the acceptance limits of 25 rem (whole body) and 300 rem (thyroid). Internal radiation levels for utility personnel are within acceptable limits provided either air supplied or self-contained breathing units are used. Whole body dose is also within acceptance limits. Temperature within the containment are at levels that could limit the time available to utility personnel to close the containment equipment hatch within the assumed one hour period. Ways to decrease the time needed to close the equipment hatch and lengthen the work time within containment need to be evaluated: e.g., the use of fan coolers to reduce temperature, improved equipment hatch design to reduce closure time, review of procedures and training to reduce time to evacuate and close the containment.

In Mode 6, the integrated two hour whole body and thyroid doses are below the acceptance limits of 2.5 rem (whole body) and 30 rem (thyroid). Radiation and temperature levels in the containment should provide utility personnel up to 30 minutes to evacuate and close the personnel hatches in the containment.

*This response and the mentioned appendix sections fulfill the commitment in Reference A-14 relevant to this RAI.

SRXB Question 440.131 : This item intentionally left blank.

~~Since the System 80+ no longer has RWST gravity feed capability due to the location of the In-containment RWST, discuss other methods of restoring RCS water during midloop operations via gravity feed. Also, CESSAR-DC page A-45i states that a safety injection pump and "another means would be available during cold shutdown" to add water to the RCS. What is the other means and has this system/method been accounted for in the Technical Specifications?~~

~~Response 440.131*~~

~~The response to this item is contained in Sections 2.3 and 2.4 of Appendix 19.8A.~~

~~*This response and the mentioned appendix sections fulfill the commitment in Reference A-14 relevant to this RAI.~~

Response 440.137*

Section 2.6 of Appendix 19.8A addresses the potential for a consequences of the injection of an unborated water slug into the core. The results, the evaluation indicates that considering the injection of the largest credible unborated water slug, which was determined to be via the DVI lines, the core will remain subcritical.

*This response and the mentioned appendix section fulfill the commitment in Reference A-14 relevant to this RAI.

SRXB Question 440.139 : This item intentionally left blank.

~~As mentioned in RAI 440.109, discuss the potential for boron dilution during the recovering phase following a SGTR when backfill from the secondary system through the ruptured steam generator occurs. This analysis should also be provided in support of GSI-22, Section 15.4.6, etc.~~

Response 440.139*

The issue of a "potential" boron dilution resulting from a SGTR accident was addressed in the response to RAI 440.109.

*This response was previously transmitted by Reference A-11.

SRXB Question 440.140

How will plant instrumentation be designed to operate properly during shutdown operations, and what key parameters will be monitored? The answer to this question should address particularly the issues of instrument availability and appropriate ranges for shutdown measurements, including:

a. A description for any deviations, bases and justifications of the deviations, from the Generic Letter 88-17 recommendations that each plant provide two independent RCS level indications, two independent core exit temperature measurements, the capability of continuously monitoring decay heat removal (DHR) system performance whenever a DHR system is being used for cooling the RCS, and visible and audible indications of abnormal conditions in temperature, level, and DHR system performance.

b. Indicate what instruments identified in resolution of GSI-99 (see Chapter 20) and Section 5.4.7 are classified as safety related and therefore within the scope of environmental qualification and quality assurance criteria. For those that are not so classified, provide a description of the quality assurance program that will be used to provide reliable instruments with accurate information in the expected ranges of shutdown measurements that will be enhance operator confidence in the instrument, and the training program for operators to understand and interpret and the data provided by the instruments.

Response 440.140*

The response to this item is provided in Sections 2.1, 2.2, 2.3 and 2.8 of Appendix 19.8A.

*This response and the mentioned appendix sections fulfill the commitment in Reference A-14 relevant to this RAI.

SRXB Question 440.151 : This item intentionally left blank

~~SRXB Question 440.151~~

Several probabilistic safety assessment studies performed for low power and shutdown conditions for the existing plants indicated that losses of decay heat removal during mid-loop operation of PWRs and operator errors dominate the risk. Your response to RAI 440.14 has qualitatively described a number of System 80+ design enhancements to decrease shutdown risk. However, to demonstrate adequate treatment of the issue, CE should conduct an analysis that provides a structured evaluation specifically identifying the System 80+ design's vulnerabilities to shutdown and low power operations. This evaluation can take the form of a quantitative probabilistic assessment or an appropriately detailed engineering assessment. It is essential that the assessment be of sufficient depth to identify remaining significant shutdown and low power vulnerabilities and identify any potential corrective actions.

Response 440.151*

As noted in the revised response to RAI 440.14, ABB-CE has performed a detailed Shutdown Risk Assessment including both a detailed engineering assessment and a Shutdown PRA. This assessment is included in the Shutdown Risk Evaluation Report, Appendix 19.8A and the PRA shutdown evaluation, Section 19.8. They address both operator actions and reduced inventory operation.

* This response and the mentioned appendix sections fulfill the commitment to Reference A-14 relevant to this RAI.

SCSB Question 720.98 (Tasks 2.1.5, 2.1.8, 2.1.10, 2.1.11) : This item intentionally left blank

~~SCSB Question 720.98 (Tasks 2.1.5, 2.1.8, 2.1.10, 2.1.11)~~

The bottom line core damage frequency estimate for the System 80+ design appears to be very low. Given these low estimates, address how the System 80+ PRA evaluated initiating events that have a lower frequency than those normally postulated, but may have more serious consequences. Examples include the question, "What does a 1E-5/yr steam generator tube rupture initiator look like and how is it handled in the PRA?", "What do various 1E-5 common cause failures look like, and how were they looked for and evaluated in the PRA?", and "What is the effect of multiple failures/equipment outages during modes other than full power?"

Response 720.98

The System 80+ PRA does not address initiating events with very low frequencies, in part because there is little information on what these initiating events might be. ABB-CE is currently updating the System 80+ PRA to reflect some system design changes. ABB-CE is willing to address this type of initiating event in the updated PRA. However, ABB-CE does request that the NRC provide some guidance as to how to identify a reasonable set of such initiators and the level and type of analysis expected. ABB-CE has evaluated the Shutdown Risk potential of System 80+ in response to other NRC requests for additional information (RAI). In that evaluation, equipment not specified to be available in the Technical Specifications was assumed to be out of service. Multiple failures of equipment are addressed in the event trees and fault trees. The results of the shutdown risk analysis show that the risk during shutdown is equal to the risk in normal operation.

SRXB Question 440.157

Section 2.8.3.1 discusses the instrumentation used to measure RCS level. ABB-CE employs dP-based level sensors for wide range and narrow range indication. In addition, ABB-CE also employs heated-junction-thermocouples (HJTCs). Together, ABB-CE indicates that these instruments are able to provide RCS level indication for the System 80+ from normal operating condition to shutdown for refueling. The HJTCs will not be available when the vessel head is removed and it is unclear to the staff that the wide and narrow range dP-based level sensors located at the SCS suction piping will provide accurate level measurement given possible dynamic effects due to fluctuating suction pressures when SCS pumps are in operation. Thus, the RCS level measurement method used during reduced inventory conditions may not be able to provide operators with reliable level readings.

Provide an analysis to show that dP-based level sensors will provide accurate level readings and test results for the RCS level instrument during reduced inventory conditions. In addition, when the reactor vessel head is off, ABB-CE has stated that temperature measurement is provided by using hot leg resistance temperature detectors (RTDs) and core exit thermocouples (CETs) (prior to fuel movement). Provide a discussion on (1) how far from the vessel that the RTDs are located on the hot leg and how accurate is the temperature measured, if SCS pumps are not running, and (2) where are CETs located in order to measure core temperature when the vessel head is off?

Response 440.157

The instrumentation package provided for reduced inventory operations adequately describes the RCS state during mid-loop operations. When the reactor vessel head is on, the heated-junction-thermocouples (HJTCs) and the dP-based level sensors provide RCS level measurements. When the reactor vessel head is off, the dP-based level sensors are the means of measuring RCS level. Since these dP based level instruments are less accurate than the HJTCs, ABB-CE recommends that the reactor vessel head be installed when operating at a mid-loop level condition.

Dynamic effects are acknowledged to affect a dP-based level measurement system if the reference tap is exposed to pressurization effects. Because of this, ABB-CE requires that the pressurizer manway be open during all reduced inventory operations to negate RCS pressurization. Notwithstanding, the level measurements from the dP-based instrumentation are useful during RCS drain down and refueling modes and provide indication of loss of level in the RCS during both planned and unplanned drain down evolutions.

The resistance temperature detectors (RTDs) and the core exit thermocouples (CETs) are discussed in the responses to Questions 2 and 6, respectively, from the Instrumentation and Control System Branch.

SRXB Question 440.158 : This item intentionally left blank.

~~In Section 2.8.3.2.1, ABB-CE has stated that a second HJTC provides narrow range level indication for mid-loop operations via measurement of reactor vessel water level in the hot leg region. The benefit of this design is that it permits very accurate measurement when the reactor vessel level is in the hot legs. Please clarify how this system can provide accurate measurement.~~

Response 440.158

The accuracy mentioned in Section 2.8.3.2.1 of the report is determined by the axial spacing between the HJTC junctions in the hot leg region. The spacing in this region is between two and three inches, which is the accuracy of level measurement.

The HJTC level measurement instrumentation is also addressed in the responses to Question 440.157 and to Questions 1 and 2 from the Instrumentation and Control System Branch.

SRXB Question 440.159

Section 2.8.3.2.2 discusses the RCS temperature measurement methods. ABB-CE has stated that if the SCS is lost, the CETs, the hot leg RTDs, and the HJTCs inputs are available to track the response to the loss of shutdown cooling or the approach to boiling. ABB-CE has also stated that core exit fluid temperature can be measured through the use of hot leg RTDs as long as the SCS is operable. It appears to the staff that the two statements contradict each other. Please explain.

Response 440.159

ABB-CE believes that the RTDs, CETs, and HJTCs will supply adequate information for planned and unplanned recovery actions. During shutdown cooling as well as during a loss of shutdown cooling, the core exit fluid temperature is measured directly by the CETs at the core exit and by the HJTCs at the fuel alignment plate and above. During shutdown cooling, the hot leg RTDs give good indication of the core exit fluid temperature if there is shutdown cooling flow in the hot leg. Following a loss of shutdown cooling, the CETs and the HJTCs are available to accurately track the response to the loss of shutdown cooling and the approach to boiling. The RTDs no longer provide a good indication of the core exit temperature, but provide valuable information which increases the operator's confidence in the thermal hydraulics believed to be developing. Since RTD temperatures are expected to lag the rising temperatures measured by the CETs and the HJTCs, the RTDs are used for trending purposes only. A parenthetical note to this effect has been added to Table 2.1-1.

RTD temperature measurement is also discussed in the response to Question 2 from the Instrumentation and Control System Branch.

SRXB Question 440.160

In Section 2.8.3.2.5.5, the Nuplex 80+ component control features provide operators with the capability to actuate equipment and systems. It is not apparent to the staff that when the operator has selected a SCS cooling mode that the SCS system will automatically align valves to allow cooling. Provide a discussion to show whether or not a manual operator action is needed to align important valves for the selected mode and whether or not the design features will automatically perform important functions to reduce the possible man-machine interface errors.

SRXB Question 440.161 (This item intentionally left Blank.

In Section 2.8.3.2.5.3, the NUPLEX 80+ discrete indicators are used to provide operators with information to support shutdown cooling such as inlet and outlet temperatures, and heat exchanger inlet and outlet temperatures. Please explain the difference between inlet temperature and heat exchanger inlet temperature. Are they supposed to be the same temperature which are used to indicate RCS temperature during shutdown cooling conditions? It appears that the NUPLEX 80+ design features allow heat exchanger inlet temperature readings to be indicated in the control room. However, CESSAR, Section 5.4.7.2.2, SCS component description indicates that the inlet heat exchanger temperatures are indicated at a remote location, and temperatures are recorded in the control room. Please explain the inconsistency as to where the inlet heat exchanger temperature indication is located. It is especially important that the operators have the RCS temperature readings accessible and visible within the visual range indicated in the control room.

Response 440.161

Section 2.8.3.2.5.3 inadvertently listed both "inlet/outlet temperature" and "heat exchanger inlet/outlet temperature". Shutdown cooling system temperatures indicated in the control room include the following:

- heat exchanger inlet temperature;
- heat exchanger outlet temperature;
- shutdown cooling return line temperature (temperature of combined HX and HX bypass flow);

In addition to the listed shutdown cooling temperature channels, indication of RCS hot leg temperature is also provided in the control room using discrete indicators. Use of the RCS hot leg temperature channels is described in Section 2.8.3.2.2 of Appendix 19.8A, along with other RCS temperature measurement channels.

The discrete indicators provided for RCS temperature and shutdown cooling temperature provide indication and recording capabilities in the control room, and indication at a remote location; Section 5.4.7.2.2 has been revised to make this clarification. The discrete indicators and their functional capabilities are described in Sections 7.7.1.4.2 and 18.7.1.4. The indicator locations in the control room are selected, based on task analysis, to be within the operator's visual range.

SRXB Question 440.162

In Section 2.3.3.3, ABB-CE has stated that given a heatup during mid-loop the pressurizer cubicle volume is sufficient for venting the RCS pressure during RCS boiling and preventing steam generator nozzle dam failure. In addition, a conservative RCS equilibrium pressure which is below the assumed steam generator nozzle dam design pressure had been calculated to occur 4 days after shutdown, indicating that the earliest time after shutdown from full power for operating at mid-loop is recommended as 4 days. Please provide the analysis results showing that the pressurizer cubicle volume is sufficient for relieving RCS pressure and preventing nozzle dam failure. Also, provide the sensitivity study results to justify the basis of the mid-loop operation at 4 days after the reactor had been shutdown from full power.

are to be locked closed (Paths #4, #10, #13). The cross connect on the suction side of the CSS (Path #6) is also addressed. The probability of having a draindown through these paths depends strongly on the procedures for entering shutdown cooling. Therefore, the following section describes the assumed procedures for entering shutdown cooling.

ENTERING SHUTDOWN COOLING

The operator is entering shutdown cooling in Mode 4 with the containment closed. He has cooled the plant with the steam generators to 350°F and depressurized to 450 psi. He now will start the SCS trains because cooling through the SGs becomes less efficient and he wishes to quickly cool the plant down. He will be starting up both trains of SCS so that he can cool down the plant more rapidly. After the plant is cooled down, he will secure one of the SCS trains and leave it on standby. The following steps are assumed to be in written procedures with a checkoff list and are applied to both trains. The following description is for one train only.

1) Normal SCS Warmup

- 1A In separate steps, with checkoff, the following valves are to be verified as closed: SI-340, SI-341, SI-657, SI-686, SI-300, SI-310, SI-688, and SI-314.
- 1B Open SI-691 to establish recirculation flow in the SCS train.
- 1C Verify SI-312 is open.
- 1D Turn on SCS pump, check flow and pump characteristics.
  Procedural stop for abnormal pump characteristics.
- 1E Open SI-651, SI-653, SI-655 aligning the suction side of the SCS to the RCS.
- 1F Slowly open SI-601 while closing SI-691 to slowly heat the SCS train.
- 1G Ensure that SI-691 is closed and SI-601 is open after heatup.

At completion, the operator is on SCS.

2) Controlling Cooldown Rate

- 2A The operator must slowly open SI-310 and closes SI-312 to control the amount of bypass around the shutdown cooling heat exchanger to cool the plant down at a desired rapid rate of 50°F per hour (less than the administrative limit of 75°F/hr).
- 2B He will monitor the shutdown cooling exit temperature T-300 and primary coolant temperature to control cooldown rate.

After starting both SCS trains at a coolant temperature of 350°F and pressure of 450 psi, the operator will continue to cool and depressurize the plant. We estimate he will enter Mode 5 (defined as having coolant at 210°F) at an RCS pressure of 350 psi. He continues to cool to a RCS temperature of 135°F and 0 PSIG before opening the system for reduced inventory operation or vessel head removal. This time was estimated at 20 hrs ~~(see Figure 19.8.3-31)~~. The average conditions during this cooldown are 175 psi and 175°F.

QUARTERLY TESTING OF CSS AND SCS

Many components in the CSS trains and SCS trains are tested quarterly. Failure to restore the valves to their correct position after the testing could be a precursor to having a draindown event.

The CSS pump and MOV valves are tested quarterly. The suction line from the IRWST (SI-304) is normally open and discharge lines to the IRWST (SI-657, SI-686, and SI-300) would be opened. SI-657 and SI-686 are in draindown path #10. SI-300 is in drain down Path #10, #4 and #13.

The SCS is also tested quarterly. Valve SI-340 is opened on the suction side. The valves in draindown Path #13 (SI-314, SI-688, and SI-300) are opened to establish discharge flow. The cross connect valve on the discharge side, SI-341, is also tested quarterly. This valve is not used for any normal function of starting SCS or CSS and is only used for cross connecting the two systems. This valve is in draindown Path #10.

These tests are on a safety system and require that the valve position be separately verified by another person before the test is complete. In addition, the valve positions are given in the control room and all but SI-300 are to be locked closed.

The NUPLEX 80 contains the COMAX, a computer aided testing system that compares the desired positions to the actual position for the valves with control room indication. This system verifies the valve test arrangement both before and after surveillance tests on safety systems. COMAX should identify to the operator, valves that were not restored after the above tests were performed. ~~No credit was taken for this system in the risk analysis.~~

ADJUST BORON CONCENTRATION

The operator might have to adjust the boron concentration in the SCS train. This should be required very infrequently because quarterly testing will keep the boron concentration at the IRWST concentration. The operator will align the SCS train to the IRWST and pump borated water through flow Path #13. Again, this is a potential sequence that might lead to a misaligned valve.

PATH #2, LTOP RELIEF VALVES

There are two spring loaded safety relief valves to protect the RCS and SCS from overpressure during Modes 5 and 6. Each valve is taken off of each SCS intake piping and is available whenever the SCS is aligned to the RCS. These valves are available even if the SCS train is on standby. If one of these valves fails to close, it can be isolated from the RCS by isolating the SCS train.

~~Spurious opening of a safety relief valve has rate of 5.0E-6/hr (Ref. EPRI-URD). For Mode 5, it was estimated that it would take 20 hours to cool the plant down in Mode 5 before opening the primary system. Assuming an 18 month refueling and one forced outage per year, the time exposed to this drain path is 33 hrs/yr (20 hrs/refuel * 0.6667 refueling/yr + 20 hrs/outage). We are assuming that the probability of spurious opening of the LTOP valves is negligible after depressurization. Since there are two LTOP valves, the draindown frequency is 3.3E-4/yr (5.0E-6/hr * 2 * 33 hr/y).~~

If an LTOP valve spuriously opened, the best estimate for drain down to the bottom of the hot leg would be 26 minutes. Boiloff to the active core would take another 19 minutes and heatup to core damage would take up to 20 minutes. The operator would have approximately 65 minutes to restore inventory or start a feed and bleed operation before CD. This is sufficient time to close the containment (i.e. greater than 1 hour). Given that there is a draindown, the operator has sufficient alarms to diagnose and take action before the onset of core damage (CD). The operator has low pressurizer level alarms, low RC level alarms, holdup tank alarms, containment temperature and radiation alarms and others. He can also take all necessary actions from the control room. In this analysis, core damage is defined as the onset of clad damage or reaching a temperature of 2200°F.

The operator has approximately 45 minutes to diagnose the transient and start some form of injection before uncovery and up to 20 minutes additional time before core damage. The operator would be assisted by the SRO and the shift supervisor for most of this time (after 5 minutes, S&G, T20-4, #3). The shift supervisor would assist with moderate dependency (MD, HEP = 0.14). The SRO is assumed to have high dependency but no credit was taken for his support. Also, no credit is taken for the STA which could assist after 15 minutes. (S&G, T20-4, #3, and T20-17)

~~The operator's failure to respond in 30 minutes (Table value) is estimated at 0.001/d (S&G, T20-3, #4).~~ Support from supervisor reduces this to HEP = 1.4E-4/d (0.001 * 0.14). If one took credit for the full hour, the HEP is reduced by an order of magnitude. In addition, the stuck open LTOP valve produces a bleed path for feed and bleed and returns the coolant indirectly to the IRWST. The core damage frequency is the product of the draindown frequency times the failure probability of the operators.

~~CDF (path 2) = 4.63E-8/yr~~

PATH #13, FROM THE SCS DISCHARGE THROUGH THE FULL FLOW RETURN LINE

The operator had flow Path #13 (through SI-314, SI-688, and SI-300) open for the quarterly flow tests. In very unusual conditions, he may have this path open for adjusting the boron concentration before using the SCS. Through a pre-existing maintenance error, the flow path could be left open.

~~Pre-existing maintenance error = 1.71E-4/d~~
Pre-existing maint. error SI-314 = 8.73E-4/d (analysis of EFWS valve error in CESSAR-DC, p 19.5E-26)
Pre-existing maint. error SI-688 = 0.14 (mild dep., S&G, T20-17, #3)
Pre-existing maint. error SI-300 = 0.14 (above)

Walkdowns and control room scans = 0.14/d
Walkdowns (0.52/d each of three valves, S&G, T20-27, #1) = 0.14/d
~~Control Room Scanning = 1.0 (not quantified)~~

The most probable cause of the draindown is to have the draindown path left open and enter SCS. This would occur in Mode 4 while the containment would be closed.

Starting up the SCS Train ~~(startup sequence is described on page 1).~~

1A: Check valve alignments, operator should discover the error here. ~~HEP = 0.01 (failure to use check list at all, S&G, 20-6, #3).~~

1B: Open valve SI-691, No effect

1C: Check SCS heat exchanger bypass alignment, no effect.

1D: Start SCS pump for recirculation, Get low pressure alarm on P-300 (suction side of SCS pump), pump cavitation, current indicator is incorrect, Operator given Procedural Stop in written procedures. ~~HEP = 0.025 (S&G, T20-2, #2, error per critical step in~~ procedures)

1E: Open suction side of SCS to RCS pressure causes a rapid draindown through the SCS pump to the IRWST.

~~The combination of the above events estimates the probability of having a rapid draindown event through path #13 during SCS startup, frequency = 6.0E-9/yr.~~

Recovery Actions:

1) The rapid draindown occurred during a change in state while the operator was opening valves, and the operator would tend to close the valves he was opening. This sequence is not a spurious failure.

2) Operator has the necessary alarms for the draindown and could activate SIS, or other makeup operations. ~~The HEP for operator action would be less than that used for Path #2, HEP = 4.62E-4/d, which would be used in this calculation.~~

~~The Core Damage Frequency is the product of the draindown frequency times the recovery actions (6.0E-9/yr * 4.62E-4/d).~~

~~CDF (Path 13) = 2.77E-12/yr.~~

The above discussion addresses a draindown through path 13 caused by a pre-existing maintenance error. This sequence occurs while starting SCS. At the end of the refueling, this path is actually established to pump the coolant back to the IRWST from the refueling cavity. At this time the system is open, depressurized, and of lower decay heat. Draining down beyond the desired level is possible but would be detected by level instruments. If the draindown was continued to the bottom of the hot leg, the operator would have approximately two hours to make up inventory. ~~This sequence has not been quantified because of the operator response time.~~

PATH 4, BACKFLOW THROUGH THE SCS RECIRCULATION LINE

Backflow through the recirculation line requires that valves SI-691, and flow Path #13 be left open. It also requires the SCS pump be off. The risk of this path is contained in the risk of Path 13 which would be the actual draindown path before the SCS pump is secured.

PATH 10, THROUGH DISCHARGE SIDE CROSS CONNECT TO FLOW TEST PIPING

This path requires the misalignment of valves SI-341, SI-657, SI-686, and SI-300. All of these valves have position indication in the control room and all but SI-300 are locked closed. Valve SI-341 is not used for any normal or systems test procedure but is only used when aligning the CSS pump to substitute the SCS pump. The valve itself is tested quarterly. Valves SI-657, SI-686, and SI-300 are opened to flow test the CSS pump.

The risk of a draindown through this path while starting up the SCS train is identical to Path #13 since this path parallels Path #13. It does require the misalignment of one additional valve (SI-341) which is not normally used. This path would also cause SCS pump cavitation during startup, but before aligning to the RCS. The risk would be slightly less than Path #13 and could be conservatively assumed to be the same.

~~CDF (Path 10, Mode 4) = 2.77E-12/yr~~

Draindown through Path #10 is also possible when the CSS pump is used for DHR in Mode 5. This sequence would require:

1) Pre-existing maintenance error on valves SI-657, SI-686, and SI-300 ~~(HEP = 1.71E-4/d, from the Path 13 analysis)~~ and failure to detect with walkdowns and control room scans ~~(HEP = 0.14/d)~~ but SI-341 is correctly closed.

2) Failure to diagnose valve error on SCS startup ~~(HEP = 0.01, step 1A of path 13)~~.

3) Loss of DHR in Mode 5 during the 33 hrs/y of cooldown period ~~(2.2E-3/d, BNL freq. - SCS train 1)~~.

4) Failure to start second SCS train ~~(3E-2/d, Section 10.8)~~.

6) Correctly opening valve SI-341 to use CSS pump ~~(assumed successful)~~.

These sequence of events lead to a rapid draindown through Path 10 during cooldown in Mode 5. ~~The frequency for this draindown is 1.58E-11/yr.~~ The event is similar to the analysis of a draindown through Path 6 where a total loss of DHR occurs with CSS maintenance.

Operator has the necessary alarms for the draindown and could activate SIS, or other makeup operations. ~~The HEP for operator action would be similar to that used for Path #2, HEP = 4.62E-4/d, which would be used in this calculation. The CDF for this sequence is negligible.~~

PATH 6, CSS CROSS CONNECT ON THE SUCTION SIDE

The event sequence starts with the disassembly of one of the CSS trains. While the train is disassembled, the operating SCS train must fail and the second SCS train must fail to start. The operator then tries to cross connect the two systems. If the two systems are already cross connected, the CSS will not drain and disassembly would be impossible. A written step in the maintenance procedures will have the cross connect valve tagged out. In aligning the CSS to the SCS, a step in the written emergency procedure should be to verify that the CSS system is available. This is part of configuration management. Only if all of these events happen will a rapid draindown occur.

Given that a rapid draindown occurs, the operator must quickly diagnose the event and start injection. Failure to take action results in core damage (CD). ~~The following paragraphs quantify the sequence of events.~~

~~CSS-D = 0.2/yr~~

~~The CSS must be disassembled for a rapid draindown through this cross connect to occur. It was assumed that this system is disassembled once every five years (the annual frequency is 0.2/yr). It is further assumed that the system is disassembled for 36 hours for maintenance (4.5 shifts).~~

~~L-DHR = 2.4E-3/D~~

The plant is being cooled by the operating SCS train. ~~Failure to continue to run (Loss of DHR) during the 36 hour window that the CSS is disassembled is estimated at 2.4E-3/d. This is based on the hourly failure rate for loss of DHR of 1.79E-5/hr for Mode 5 from the BNL study.~~

~~F-SCS2 = 3E-2/d~~

The operator will try to start the second SCS train after the first SCS train fails. We are neglecting any recovery of the first train which is usually possible because many of the loss of DHR are operator errors. The operator has about two hours to react at this time in the sequence. Failure to start the second SCS train (F-3CS2) is dominated by failure of MOVs to open. This value is from Section 19.8.

F-TAG = 0.01/d

Failure of the maintenance group to tag out the cross connect valve SI-340 is estimated as 0.01/d. It is assumed that this is a step in the written maintenance procedures. This value is based on Swain & Guttmann (S&G, Table 20-6, #5) for failure to use valve change or restore list. If the valve control is correctly tagged out, the operator will not open the valve since it is the primary boundary.

F-CFG = 0.01/d

The operator will have written procedures to verify the availability of the CSS before aligning the CSS to the SCS for restoration of DHR. It is assumed the procedure is greater than 10 items long and the probability of omission (without checkoff) is 0.01/d (S&G, Table 20-7, #4).

F-LOCA = 0.01/d

The sequence of events described above leads to a rapid draindown with a frequency of occurrence of 1.44E-9/yr. It is assumed that the draindown occurs almost instantly and the coolant is drained to the bottom of the hot leg of the RCS piping. It is further assumed that the decay heat is high and boiling to the top of the active core takes 20 minutes. Heatup to the start of core damage (clad temperature of 2200°F) takes up to another 20 minutes. The operator has alarms on the pressurizer level, reactor vessel level, and sump drains. He should be able to identify the problem and take action. In this short time, the failure rate of the operator to take action was assumed to be 0.001/d. This is taken from S&G, Table 20-3, #4, failure to diagnose within 30 minutes.

Core Damage Frequency (CDF)

The frequency for rapid draindowns was estimated at 1.44E-9/yr. If CD actually occurs in 30 minutes, this is 1.44E-12/yr. If mist cooling of the core or lower decay heat extends the time to core damage by 10 minutes, F-LOCA improves by a factor of ten (S&G, T20-3, #4) and the CDF decreases to 1.44E-12/yr.

STEAM GENERATOR MANWAY

The SG manway was identified as a major draindown pathway because of its size. Draindown through the manway would leave the RCS coolant 8 inches above the centerline of the hot leg and would not cause loss of DHR. It is, therefore, not risk significant.

SG NOZZLE DAMS

Loss of the nozzle dams would cause the coolant to drain to the same elevation as the SG manway and not cause loss of DHR.

SRXB Question 440.171

In Section 2.6.3, Table 2.6-1, ABB-CE has identified the possible non-borated water flow paths for the rapid boron dilution events. ABB-CE has only identified one credible boron dilution event, that is from the direct vessel injection (DVI) lines where the RCS leakage through the first SI check valve with a possible diluted water volume is determined to be 60 ft^3. ABB-CE did not take credit for using the pressure indication in the lines and the possible diverting capability by opening valves SI-648, 638, 628k and 618 to minimize the potential dilution to the DVI injection lines. In addition, ABB-CE has also identified leakage through SIS hot legs injection check valves SI-522 and 532. However, in this scenario, ABB-CE took credit for detecting pressure changes using pressure indication in the lines and the ability to divert water to SIT drain and fill lines. Please provide:

(1) Assumptions made for both scenarios and why credit was taken for using pressure indication and diverting water capability in one situation but not for the other.

(2) Consequences of the rapid boron dilution event from the diluted water leakage through hot legs injection check valves, if pressure indication in the lines and the diverting capability were not used, and

Response 440.173

The BAST tank normally holds 180,000 gallons of borated water. The shutdown to cold shutdown uses approximately 85,000 gallons to make up for RCS shrinkage. Since 15,000 gallons is reserved in the tank bottom, approximately 80,000 gallons is available for boil-off. After 4 days (when reduced inventory operations would commence), the decay heat in the core would result in a boiloff of 109 gpm.

One of the insights, ~~in Section 19.8,~~ is that plant procedures be developed which prevent both boric acid makeup pumps and CVCS pumps from being out of service at the same time during reduced inventory operation. Each boric acid makeup pump is rated at 165 gpm, which provides a conservative flow rate for matching boiloff. Plant procedures would require throttling of the boric acid makeup pump flow rate to more closely match boiloff, thus extending boric acid storage tank inventory availability to approximately 12 hours. ABB-CE feels that this is sufficient time for restoration of SCS pump operation. ~~As discussed in Response 17, although not modeled in the risk assessment~~, using the SIT inventory will further extend the time for SCS restoration.

SRXB Question 440.174

The staff has identified that System 80+ does not have the capability for gravity drain from IRWST to the RCS. Provide a discussion of how CE System 80+ could provide water to the RCS to maintain core cooling in case of station blackout (SBO) and also discuss the reflux cooling capability for the System 80+ design. Discuss what actions could be taken to allow for gravity drains and ABB-CE's plans to incorporate such actions.

Response 440.174

In the event of a station blackout the operator can manually align the alternate AC power source, described in Section 8.3.1.1.5, to provide power to the equipment needed to restore decay heat removal and inventory control. Procedural guidance to support recovery from a station blackout is provided in Appendix B of the ~~Shutdown Risk Evaluation Report~~ Emergency Operations Guidelines,

If inventory control cannot be established using the alternate AC power source and pumped inventory addition, the safety injection tanks (SIT's) may be used to provide a source of gravity feed inventory addition. Use of the SIT's in a gravity feed mode is described in Section 2.3.3.4 of Appendix 19.8A; see also the response to Question 440.135.

SRXB Question 440.175 : This item intentionally left blank.

~~Section 5.3.1 indicates that the limiting break is in a bottom of the hot leg or a lower head instrument line~~ resulting in a loss of DHR in ~~Modes 5 and 6. Provide the basis for the break in a bottom of the hot leg or a lower instrument line as the most limiting condition in comparison to other possible pipe breaks.~~

Response 440.175

The decay heat flow removal path exits from the RCS at the bottom of the hot leg and re-enters the RCS at the DVI nozzle. If a break were at a higher elevation then decay heat removal (DHR) could continue because the flow circuit would not be interrupted. In order to postulate a limiting break, where DHR is interrupted, the break is assumed at the lowest points where a break is credible, which are the bottom of the hot leg or at a lower head instrument line in the reactor vessel.

SRXB Question 440.176 : This item intentionally left blank.

Section 19.8 presents the probabilistic risk assessment (PRA) study for shutdown conditions, including mid-loop operation with the refueling cavity water level less than 23 feet above the vessel flange. It appears to the staff that loss-of-offsite power (LOOP) and SBO situations were not modeled in the event trees. The staff study indicates that LOOP and SBO situations can occur during shutdown conditions. As a result, the probability for core damage frequency during reduced inventory increases. It appears that System 80+ PRA models assumed that off-site power is always available for the entire shutdown conditions. Therefore, the availability of the emergency power is of minimal importance. Provide (1) justification for not modeling LOOP and SBO in your shutdown risk analysis, especially during mid-loop operations with water level less than 23 feet above the vessel flange, and (2) how would core damage frequency change during reduced inventory conditions, including mid-loop operation with water level in the refueling cavity less than 23 feet above the reactor vessel flange.

Response 440.176

A risk associated with SBO is quantified in the revised Shutdown Risk analysis as requested in Question 31 from the Probabilistic Safety Assessment branch. Table 440.176 is an estimate of risk specifically for reduced inventory. LOOP frequencies, and all failure rates are from the EPRI-KAG. System 80+ is designed with two DGs and an alternate AC power source (turbine) and is required to be serviced by two separate switch yards. Revised T/S guides specify that two of the generators are to be available in shutdown. Response 2 gives the fraction of time that the plant is in each mode and we estimate the plant is in Mode 5R (reduced inventory) for 76 hrs/y (64 hrs/y coming down and 12 hrs/y going up). While coming down, core damage is possible in 0.7 hrs and after refueling, CD occurs in 2.3 hrs. The probability of failure to restore AC is a weighted average of these two POS.

~~TABLE 440.176~~

ESTIMATE OF CDF FROM LOOP
DURING REDUCED INVENTORY MODES

EVENT	RATE
LOOP RATE/HR (0.035/y)	4.00E-6/HR
LOSS OF SECOND SWITCH YARD	0.22/D
HRS IN REDUCED INVENTORY	76 HRS/Y
FAILURE OF 1 DG	7.16E-2/D
FAILURE OF TURBINE	2.5E-2
SBO FREQUENCY IN REDUCED INVENTORY	1.19E-7/Y
FAILURE TO RESTORE AC (15.8% 0.40 + 84.2% 0.70)	0.65/D
CDF IN REDUCED INVENTORY	7.8E-8/Y

Response 440.187

The System 80+ Technical Specifications had required two independent sources of AC power to each division and a diesel generator in either division when the plant is in reduced inventory conditions. Technical Specification 3.8.2 is amended to require a diesel generator in each division with the exception that the combustion turbine can replace one diesel provided the combustion turbine has been demonstrated to be operational within the past 7 days. This amendment will solve both of the staff's concerns. During shutdown operations with reduced inventory two onsite AC power sources will be required and if the combustion turbine is credited it will have been demonstrated operable.

SRXB Question 440.188

In Section 5.3, LOCA Analysis for Lower Modes of Operation, ABB-CE assumed different conditions in Mode 4. Please provide:

(1) basis for different conditions in Mode 4, and

(2) results from the sensitivity study to confirm that Mode 4, case 4 is the worst case.

Response 440.188

1) Initial Conditions

The initial conditions assumed in the System 80+ Shutdown Risk Evaluation were selected to maximize the primary system inventory loss for the postulated LOCA and minimize the inventory makeup from the Safety Injection System. That is, the pressure and temperature initial conditions were selected to have both the passive and active SIS components inoperative. The equipment availability was based on the Technical Specification requirements at the time the analysis was performed. These requirements have been changed to have automatic operation of the SIS during Mode 4 operation.

2) Sensitivity Study

The results from the sensitivity study are summarized in Figure 5-6. It shows that neither the cold leg break nor the hot leg break result in core uncovery during the time frame under consideration. Only the DVI line break results in core uncovery prior to operator action. However, with the recent technical specification requirement for SIS operability in Mode 4, operator action is not required due to automatic actuation of the SIS.

SRXB Question 440.189 This item intentionally left blank.

~~Section 5.3 evaluates a postulated LOCA event (break in the bottom of the hot leg) in Mode 5 as a result of a loss of DHR. The postulated LOCA event analysis indicates that the water would reach the top of the active fuel in twelve minutes and the operator would have ten minutes to take actions to prevent core boiling. The Standard Review Plan (SRP), NUREG-0800 Section 6.3.8, item 19, states that operator delay time should be greater than 20 minutes. The ten minutes provided by ABB-CE appears to be too short for preventing core boiling. Provide justification for the shorter operator delay time.~~

Response 440.189

When the plant is in Mode 5, the RCS may either be filled or it may be partially filled up to the mid-height of the main coolant piping. Also, the coolant temperature is less than or equal to 210°F (separately, pressurizer pressure cannot exceed 430 psia in order for the SDC to be in operation). Because mode 5 has lower RCS pressure and temperature than at full power, the likelihood of a LOCA in Mode 5 is less than at full power.

At the fastest rate of cooldown (100°F/hr.), the RCS could be in Mode 5 at about 3.5 hr. (12500 sec.) after the start of cooldown. At that time, the RCS is filled with liquid. The Reduced Inventory Operational Guidance (Appendix B to Appendix 19.8A) indicates that the reactor must be subcritical for greater than 96 hr. (346000 sec.) and that the RCS level, at that time, must be gre... than or equal to a value which corresponds to 3 feet below the vessel head flange.

The present analysis was conservative in that it was based on the assumptions of 3.5 hours after the start of cooldown and an initial RCS level at the bottom of the hot leg. These assumptions maximized the decay heat and minimized the initial RCS inventory at the start of the LOCA.

For the limiting Mode 5 analysis which was based on a time of 3.5 hours after the start of cooldown, additional credit could be taken for:

- A full RCS. Therefore, additional time would be required for the RCS liquid to discharge through the break. This extra discharge time would be at least 3.0 minutes for the 0.4 square foot break considered for the Mode 5 analysis.

- Accounting for the decrease of the decay heat with time (instead of being constant at the time of the start of the accident) would add about 0.1 minute because the decay heat is dropping slowly at that time.

- Accounting for the heatup of the core would add about 0.2 minute to the total time from the start of the LOCA until the core reached the boiling temperature of the RCS water.

- Allowing about 2.3 minutes for the liquid level to drop below the top of the core until such time that the operator must initiate safety injection in order to prevent the peak clad temperature from exceeding 2200°F.

Taking credit for all of the above items would bring the time to boil to about 15.4 min.

The above response was provided as a result of conversations with the NRC Staff. Additional conversations indicated that the SRP 6.3.8, Item 19 is not applicable to this scenario.

SRXB Question 440.190

Section 3.3.1, Description of LOCA Scenario, indicates that a severe LOCA would occur at lower operating modes when the RCS temperature are reduced slightly below the temperature where no SI pumps are required to be on automatic. Provide the RCS temperature at which no SI pumps are required to be on automatic.

SRXB Question 440.192

In Section 5.3.3, ABB-CE has indicated that the Realistic Evaluation Model (REM) was used to study the possible impacts of a small break LOCA in Mode 4. Please, provide (1) detailed description of the assumptions made using the REM version of the CEFLASH-4AS and PARCH codes.

Response 440.192

The assumptions of the analysis methodology are documented in CEN-373. The major assumptions used in the shutdown risk report are:

- 1979 ANS Standard 5.1 Decay Heat with plus 2 sigma uncertainty
- Realistic metal water reaction rate
- Mechanistic clad strain model
- Realistic treatment of heat transfer in primary

SRXB Question 440.193 : This item intentionally left blank.

~~In Section 5.3.4, LOCA Analysis for Mode 4, ABB-CE has used 10 minute time available for operator action to take credit for compliance with ECCS acceptance criteria. This assumed 10 minute time is inconsistent with SRP 6.3.8, Item 19 (See also response to Question 440.190).~~

Response 440.193

~~Discussions with the NRC Staff indicated that SRP 6.3.8, Item 19 is not applicable for the scenario under consideration. Furthermore, the incorporation of automatic SIS actuation in the Technical Specification for Mode 4 makes the operator action requirement moot. The original analysis was performed assuming equipment availability as prescribed in the Technical Specifications at the time of the analysis.~~

SRXB Question 440.194

Section 2.6, Rapid Boron Dilution, discusses some potential boron dilution events. NUREG/CR-0105, Vol. 2, "Seventeenth Water Reactor Safety Information Meeting", identifies several potential PWR boron dilution events that ABB-CE has not discussed in Section 2.6 of the submittal. Please provide the below discussions which emphasis in the use of design features, detection, mitigation, and prevention capability and relate these to resolutions in Table 2.6-1:

(1) addition of diluted accumulator water during shutdown due to slow leakage or blowdown through single valve,

(2) LOCA with diluted ECCS water from more than one accumulator or IRWST,

(3) LOCA with sump water diluted,

Response 1

~~The report was revised and~~ major findings, and insights ~~were added to Section 19.8.1. The insights~~ are repeated below.

General Insights

1. The initiating event frequencies are higher than Mode 1 operation because of the greater opportunity for operator errors during outages. Operator training and management control of plant configuration is important to reducing shutdown events and risk.

2. The operation and maintenance personnel must have the procedures, training and spare parts to restore DHR in a timely manner. SCS operation is the true end-state for shutdown sequences.

3. Most systems are manually started or aligned in shutdown modes. Training is especially important because the operator must be able to cope with the plant in an unplanned configuration.

4. The concept of defense in depth applies to shutdown modes as well as Mode 1. The more ways that the operator can maintain coolant inventory and remove decay heat, the lower the risk. The presence of SIS capability in shutdown is an example of added defense in depth.

Loss of DHR Insights

1. Reduced inventory is the most critical operation. The operator should be aware of this and plant activities should be scheduled accordingly. Use of nozzle dams is encouraged as a method of limiting the time spent in this mode.

2. The operator must have procedures and training to align the SCS train to the IRWST and use it to makeup inventory or do a feed and bleed operation.

3. Failure of the standby SCS train for either DHR or feed operation is dominated by failure of control valves and MOVs. An aggressive valve testing and maintenance program on the SCS and CSS would reduce shutdown risk.

4. The use of the CVCS system to makeup inventory is an important recovery action in reduced inventory operation. It also acts as a temporary (about 12 hours) cooling technique. The operator should have procedures and training on its use.

5. Safety injection for feed and bleed is an important DHR method in shutdown modes. Having two of the four SIS trains available during most shutdown modes is an important new technical specification.

6. The CSS pumps are designed as an installed spare to the SCS. The operator must have procedures and training on its alignment and operation. Again, valve maintenance and testing is important for shutdown risk reduction.

LOCA Insights

1. SCS feed is an important makeup method for a LOCA. Training and procedures are required.

2. The dominant failure mode for SCS feed is failure of control valves and MOVs. A valve maintenance program is important.

3. Safety injection using the SIS is important for LOCAs. Since manual actuation is required, training and procedures are required.

4. The CVCS system is another important makeup method that should be available with training and procedures.

5. For LOCAs located in the containment, the IRWST acts as a sump and makes the coolant available for injection. Procedures are needed to ensure that flow paths are maintained during the outage.

LOOP Insights

1. The technical specification for having two of the three standby and emergency generators available ~~reduces the CDF~~ is important.

2. The reliability of the two switchyards is important to risk reduction from LOOP. The Combined License (CL) Applicant should consider procedures to control maintenance in both these areas at the same time.

3. The CL Applicant should ensure that the utility dispatchers are informed about LOOP events and the importance of restoration of AC in a nuclear facility.

Fire Risk Insights

1. The frequency of fires in outages is high because of the maintenance activities and can be reduced by training.

2. The CL Applicant must maintain a well trained and prepared fire brigade.

3. In order to maintain the validity of the assessment of the level of fire risk associated with the System 80+ design, separation must be maintained between systems comprising the alternate success paths within a quadrant. Separation between systems implies not only separation between their major components but also separation between their power supply and control cables.

Flooding Risk Insights

1. In order to maintain the validity of the assessment of the level of flooding risk associated with the System 80+ design, separation must be maintained between systems comprising the alternate success paths within a quadrant. Separation between success paths implies not only separation between their major components but also separation between the associated power supplies.

SPSS Questions 2 - 33: These items intentionally left blank

APPENDIX B TO APPENDIX 19.8A

PROCEDURAL GUIDANCE TO SUPPORT REDUCED RCS INVENTORY OPERATIONS

(This Appendix is deleted from the DCD. The content has been incorporated into Appendix B of the Emergency Operations Guidelines.)

This Section Intentionally Blank

19.9 ACCIDENT SEQUENCE QUANTIFICATION

19.9.1 SUMMARY OF CORE DAMAGE FREQUENCY

Based on the analysis performed, the estimated core damage frequency attributable to both the internal events and external events for the System 80+ plant is 1.67E-06 and 3.3E-07 (excluding the contribution due seismic events) per year, respectively. The estimated contribution due to shutdown risk is 8.4E-07 per year. Table 19.9.1-1 presents the core damage frequency contributions by initiating events.

The accident sequences of internal initiators leading to core damage were identified using event tree analysis. These sequences are presented in Section 19.4. Each accident sequence leading to core damage consists of an initiating event and one or more additional elements which represent either failure of the front line (or mitigating) system or failure of a special recovery action. Table 19.9.1-2 presents the core damage frequency contributions by the internal event initiators. Accident sequences with occurrence frequencies less than 1.00E-09 per year are excluded from the table. The dominant (i.e., at least 10% of the total) internal initiating events and their percent contribution to core damage are:

- Loss of Feedwater Flow (LOFW) - 27.9%
- Medium Loss of Coolant Accident - 18.5%
- Steam Generator Tube Rupture (SGTR) - 18.0%
- Small Loss of Coolant Accident - 12.4%

A detailed discussion of these dominant and other internal event sequences is presented in the appropriate subsections of Section 19.9.2.

The accident sequences of the external initiators that lead to core damage are presented in Section 19.7. Table 19.9.1-3 presents the accident sequences due to external events. Accident sequences with occurrence frequencies less than 1.00E-09 per year are excluded from the table. The dominant external accident sequences include 3 tornado strike event sequences. Scoping evaluations were performed to estimate the core damage frequencies due to external fires and external flooding. A discussion of the external event contributors to core damage frequency is presented in appropriate subsections of Section 19.9.3.

Table 19.9.1-4 presents a comparison of the core damage frequency contributions by initiating events between the baseline analysis for the System 80 plant and the System 80+ plant. Both intermediate and final analyses with a variety of system configurations for the System 80+ plant are included in this table.

REMAINDER OF SECTION 19.9 DELETED

This Section Intentionally Blank

19.10 SENSITIVITY ANALYSES - LEVEL 1

As discussed in Section 19.2.7, PRAs include a number of data analysis and modelling assumptions. A set of eleven sensitivity analyses were run to evaluate the potential impact of modelling and data analysis assumptions for the System 80+ PRA. The initial quantification of core damage frequency was performed in four steps:

1) The core damage cutsets were generated for each core damage sequence.

2) Recovery analysis was performed for each core damage sequence and the cutsets for each core damage sequence were requantified.

3) All core damage sequence cutsets associated with each initiating event were combined into initiating event core damage cutset files. Each initiating event core damage cutset file was quantified to generate an overall core damage frequency for each initiator.

4) The initiating event core damage cutset files were combined to form a Total Core Damage Cutset File. The cutsets in this file were requantified to generate the total core damage frequency.

Several of the sensitivity analyses were performed by requantifying the Total Core Damage Cutset File with temporary data changes in the data base files. The following paragraphs describe the individual sensitivity analyses and there results. Table 19.10-1 summarizes the results of the sensitivity analyses.

19.10.1 OPERATOR ERROR RATE - GENERAL

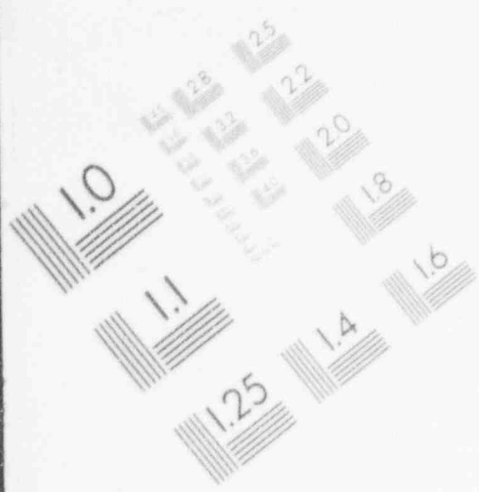
The System 80+ fault trees and event trees include basic events representing failure of the operators to perform specific tasks. The probability that the operator failed to perform the specified tasks was determined using the SHARP[39] methodology as described in Sections 19.2.5 and 19.5.5. There is uncertainty in the quantification of Human Error Probabilities (HEPs) because of the various assumptions that are made in the calculation process. Previous PRAs have shown that the core damage frequency can be sensitivity to the HEPs used in the analysis. A sensitivity analysis was performed to determine the potential impact on the System 80+ total core damage frequency. All operator error rates presented in Table 19.5-5 and the non-recovery probability for recovery action, RCVRMOV, in Table 19.5-7 were increased by one order of magnitude and the total core damage cutset file was requantified. The total core damage frequency increased from 1.67E-06/yr to 9.40E-06/yr, a factor of 5.63 increase in total core damage frequency. This indicates that the System 80+ PRA results

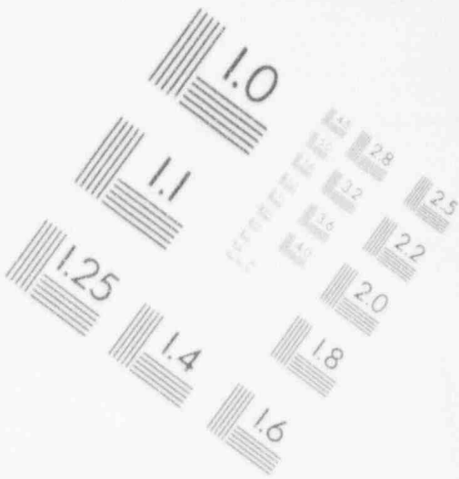
REMAINDER OF SECTION 19.10 DELETED

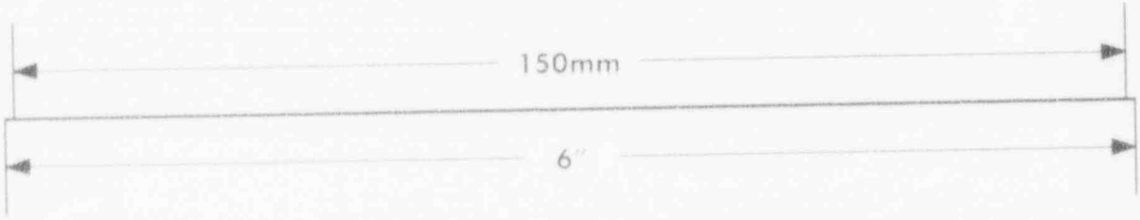
REVISED PAGES OF SECTION 19.11

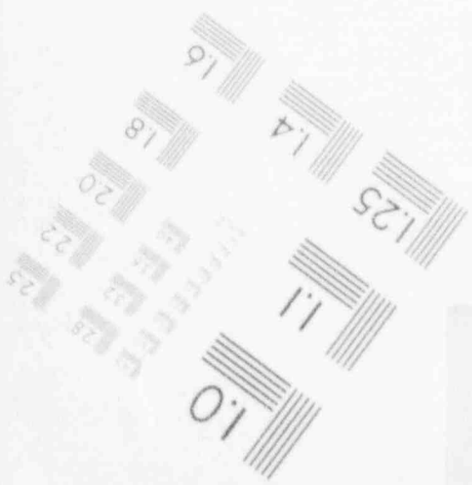
1

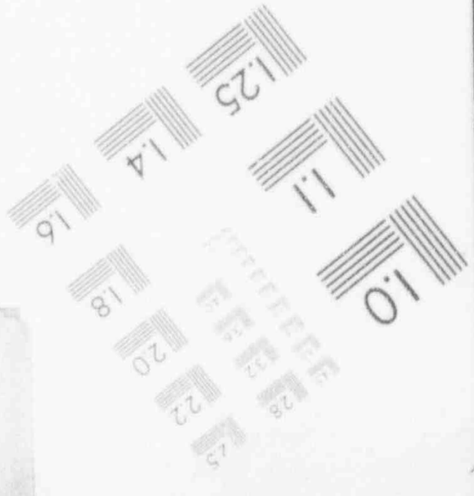
IMAGE EVALUATION
TEST TARGET (MT-3)





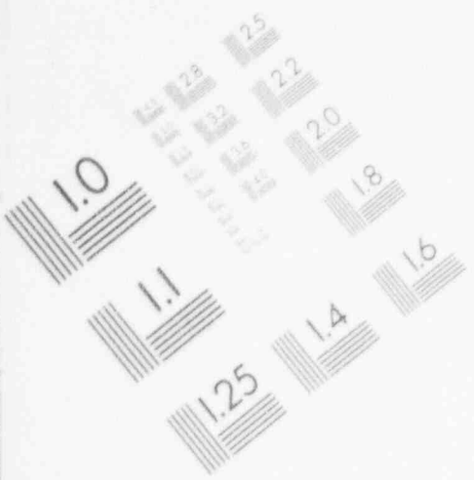


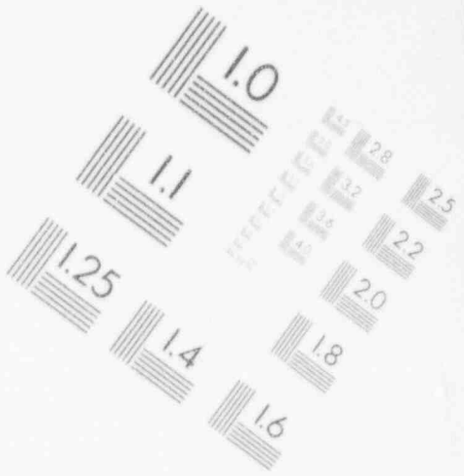


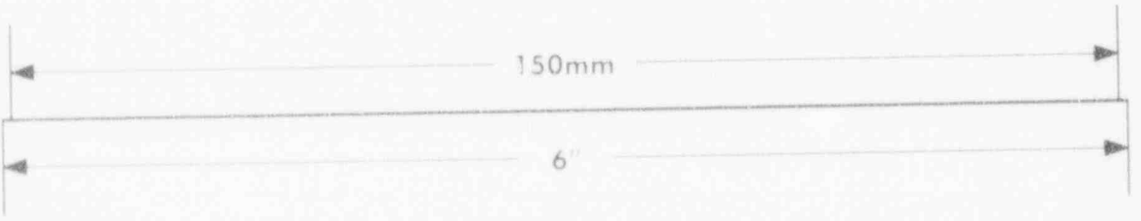


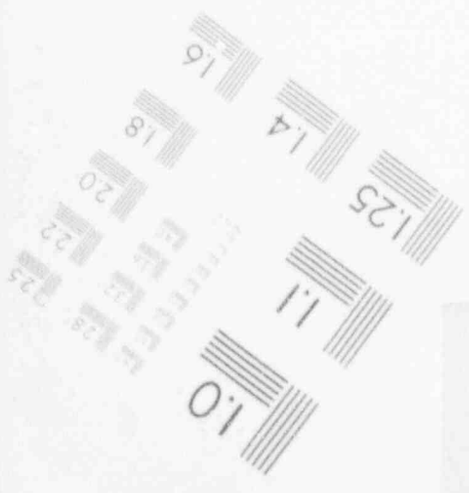
1

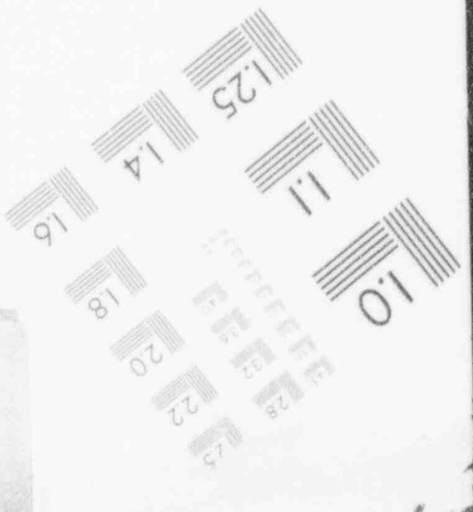
IMAGE EVALUATION
TEST TARGET (MT-3)





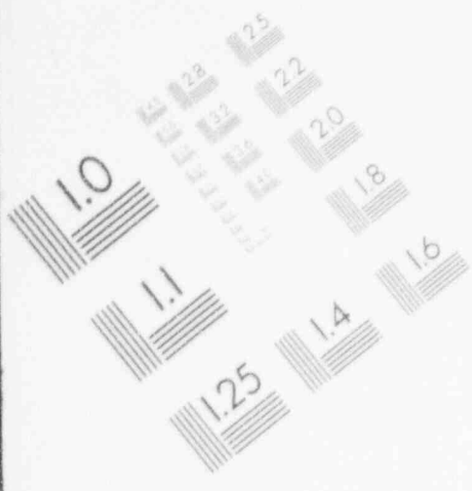


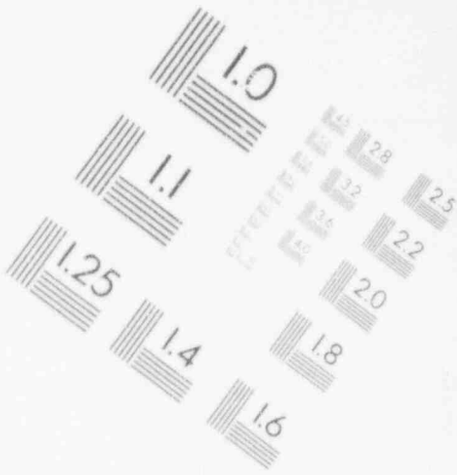


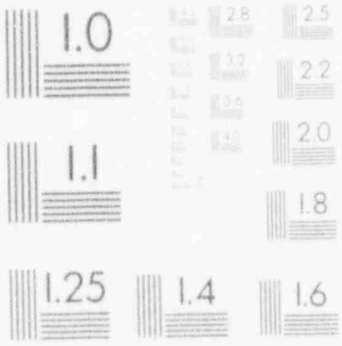


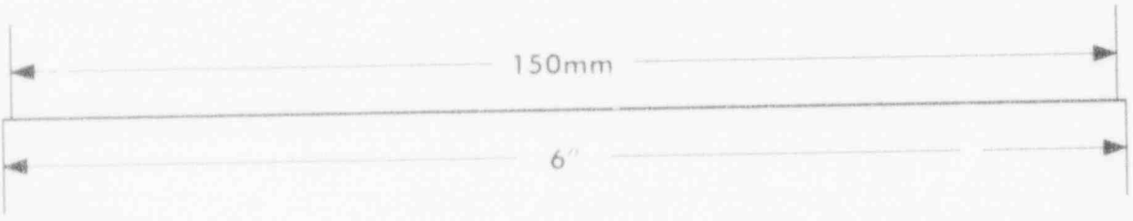
1

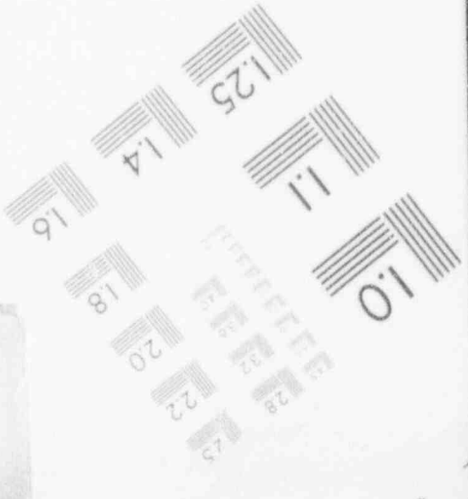
IMAGE EVALUATION
TEST TARGET (MT-3)





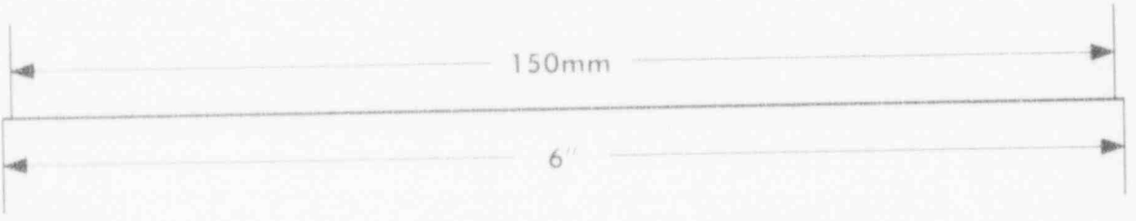






1

IMAGE EVALUATION TEST TARGET (MT-3)



19.11 SEVERE ACCIDENT PHENOMENOLOGY AND CONTAINMENT PERFORMANCE FOR THE SYSTEM 80+ PWR

19.11.1 INTRODUCTION

The PRA indicates that design improvements of System 80+ have decreased the likelihood of core damage by a factor of about 128 over System 80. As a result of this effort a more balanced design has been achieved, and the contribution to severe accident risk from loss of offsite power (LOOP) events (including station blackout) has been significantly reduced. The design enhancements are discussed in response to NRC Requests for Additional Information (RAIs) on CESSAR-DC and are contained within the Level 1 PRA section.

This section provides a description of the severe accident mitigation features of the System 80+ design and provides a technical basis for the severe accident phenomenology modeling assumptions employed in the PRA. In addition it discusses containment performance of the design for selected event sequences leading to severe accidents. It also contains the responses to several RAIs relating to containment performance and establishes a fundamental basis for the interpretation of System 80+ Level 2 PRA.

19.11.2 SCOPE

This section will describe major System 80+ severe accident mitigation features. However, it is not intended to restate the basic design information found elsewhere in CESSAR-DC. Instead, this section will highlight the details of various reactor systems, discuss them from the viewpoint of severe accident mitigation and management and clarify the impact of these mitigation features on the System 80+ PRA.

Section 19.11.3 describes the System 80+ severe accident mitigation design features. The System 80+ design features considered include (1) a large dry steel primary containment, (2) a reinforced concrete secondary containment with an annulus ventilation filtration system, (3) a reactor cavity flooding system, (4) a hydrogen mitigation system to prevent in-containment hydrogen concentration from reaching detonation levels, (5) a safety depressurization system, (6) a large reactor cavity designed for retention and cooling of core debris, (7) missile protection structures, and (8) an integrated shutdown cooling and containment spray system.

Section 19.11.4 provides a concise discussion of severe accident phenomenological issues and a technical basis for their treatment within the System 80+ PRA. Experimental data or analyses used to support PRA conclusions/assumptions and Supporting Logic Model (SLM) structure are identified.

Section 19.11.5 provides representative analytical assessments of the severe accident containment performance of the System 80+ design. Assessments presented in these sections are obtained from analyses performed with an enhanced version of the MAAP 3.0B Rev 16. Enhancements have been included to allow proper representation of unique System 80+ design features. Representative performance of the System 80+ containment to a typical spectrum of severe accidents is provided.

Section 19.11.6 contains the conclusions with regard to the System 80+ design's containment performance under severe accident conditions.

19.11.3.7.5 Application of Missile Generation Within the PRA

While the expectation is that containment failure due to missile impact on the containment structure is highly unlikely, this issue is explicitly and implicitly considered within the System 80+ PRA. Details of the containment failure phenomenology are presented in Section 19.11.4. The containment failure modes that involve missile induced containment failure are summarized below:

A. Alpha mode failure considers the potential for the RV upper head or upper head component to fail the containment via missile generation. The potential for this event has been established based on results of the Steam Explosion Review Group (SERG) to be about 0.001 conditional upon a low pressure core melt failure sequence (See Section 19.11.4.1)

B. An assessment of EVSE is presented in Section 19.11.4.1.2. Results of this assessment suggest that while EVSEs are credible, they will not pose a credible threat to containment integrity via missile generation. Thus, the probability of an induced EVSE containment failure caused by a missile or water slug was therefore assessed as zero. EVSE induced containment failure due to cavity overpressure is discussed in Section 19.11.3.6.3.

C. Detonations are not expected within the System 80+ containment. However, in the highly unlikely event that a detonation does occur in containment, it is conservatively assumed that a containment failure (due to missile generation, etc.) will result.

containment floor they absorb heat until they approach thermal equilibrium with the containment. When the water reaches the containment floor it drains to the holdup volume tank (HVT) and subsequently back to the IRWST.

Following the initiation of a severe accident, the functions of the CSS include, maintaining a low containment pressure and scrubbing fission products from the containment atmosphere. MAAP analyses demonstrate that operation of one CSS train is sufficient to assure containment integrity.

An external source of water to the sprays has been incorporated into the System 80+ containment design since the preparation of the early PRA. The addition of this feature extends containment pressure control for several days. This provides additional time for the plant operators to re-establish containment heat removal and establish long-term containment cooling.

will be limited by availability of debris below the RV and entrainment will be impeded by the presence of corbels, the neutron shield plug (which obstructs more than 50% of the annulus gap) and the hot and cold legs. Initial assessments of upward debris entrainment performed by ARSAP suggested the appropriate upper limit on debris escape from the System 80+ reactor cavity to be 10% of the ejected mass (see Appendix 19.11C).

19.11.4.1.1.6 Significance of DCH Containment Threat to System 80+

As discussed in Section 19.11.3.6, the System 80+ has been specifically designed to mitigate containment threats from HPME and DCH processes. System 80+ mitigation features include from the availability of a safety grade Rapid Depressurization capability within the Safety Depressurization System (SDS) to reduce RCS pressure to below the debris entrainment threshold, a debris retentive cavity configuration with sharp turns, overhangs, flowpath offsets and a "cavity trap", and a convoluted steam discharge path from the cavity which will promote de-entrainment of the core debris within the cavity while allowing adequate cavity steam relief.

In addition to the above features, the System 80+ cavity is designed to be floodable by the operator prior to RV lower head failure. As indicated in the NRC Draft Final Safety Evaluation Report on the EPRI Utility Requirements Document for the Evolutionary LWR, simultaneous dispersal of debris and water should ensure that the containment threat resulting from the HPME is minimal (Reference 161).

Thus, DCH is a credible threat only for those situations where the RCS is at the CRV setpoint prior to VB while simultaneously the reactor cavity is dry. These conditions create a situation where the potential hydrogen combustion associated with the HPME event may be high at a time when all other DCH energy transfer mechanisms are maximized. This set of conditions is limited to about 3.7% of (PDSs). These initiate from high pressure with a CRV RCS leak rate and the CFS system malfunctions or is not actuated prior to VB. Further, this fraction is considerably reduced when one considers that CRV sequences are estimated to have a 0.95 probability of hot leg failure and a 0.65 probability that the failure will be large enough to depressurize the RCS below the DCH entrainment threshold. Furthermore, use of the RD valves also has a high probability of successfully depressurizing the RCS. Based on a current interpretation of DCH containment loading as primarily a hydrogen based threat, blowdown of the RCS prior to VB also implies re-distribution of hydrogen from the RCS into the upper compartment. Based on IET test results, this hydrogen redistribution will reduce the hydrogen available for combustion immediately after VB. Use of the RD valves thus virtually eliminates any credible DCH containment challenge. (Following VB and RCS blowdown, this

hydrogen can potentially burn and challenge the containment as a hydrogen threat.) The percentage of potential DCH threats can therefore be reduced to under 1% of all accident sequences. Furthermore, since the DCH peak containment pressure results in a containment challenge that is below Level C stress intensity, less than 2% of these remaining sequences will proceed to containment failure. Following the preceding arguments one concludes that the conditional containment failure probability given a core melt condition occurs will be less than 0.0002 (See Section 19.11.4.1.1.7).

19.11.4.1.1.7 Application to the PRA

This section discusses the quantification of the DCH induced containment threat for application to the System 80+ PRA.

19.11.4.1.1.7.1 Quantification of RCS Depressurization Parameter RCSHIGH

(1) **High pressure transients with successful operation of SDS or low pressure core melt scenarios.**

For high pressure transients where the SDS is actuated in a timely manner or where RV failure follows low pressure RCS transients, the potential of a DCH induced containment failure will be taken as 0.0. That is, DCH induced containment failures from low RV failures under low RCS pressures is not deemed credible.

(Early containment threats following low pressure RV failure are primarily considered to result from hydrogen combustion or a steam explosion; see Section 19.11.4.1.3 and 19.11.4.1.2.2, respectively.)

(2) **High-Intermediate pressure transient depressurization and the SDS is not actuated.**

Operator actuation of the SDS prior to RV failure is included within the System 80+ Emergency Operating Guidelines (EOG). Consequently, there is a high probability that the RD valves will be actuated in a timely manner so that any DCH threat may be averted prior to significant core uncovery.

However, for high pressure severe accident scenarios where the SDS is either unavailable or not activated, the probability of RCS depressurization caused by induced hot leg failure is ~~assumed to be 0.65.~~ This value represents the probability of an induced DCH failure reducing the RCS pressure to below the DCH core debris entrainment threshold as determined by NUREG-1150. This value is conservatively selected as less

than the RCS hot leg failure probability of 0.95 established in Reference 127 for partial RCS depressurization. Recent information on RCS depressurization imply that the primary contributor to containment threat following HPME is not so much entrained debris as it is an induced hydrogen burn. Failure of the RCS hot leg will allow most of the hydrogen trapped in the vessel to enter the containment and hence substantially reduce any resulting DCH burn. While the lower value is retained for purposes of conservatism, the 0.95 value for DCH mitigation may, in fact, be more appropriate.

The probability of an induced RCS failure occurring as a result of a SG tube rupture in a dry steam generator (allowing potential fission product containment bypass) for sequences at the PSV pressure is estimated to be 0.015. This estimate is based on a review of NUREG-1150 expert elicitations for RV failure phenomena in Zion and Surry and are considered boundary for System 80+.

For intermediate pressure transients, the potential for an induced RCS hot leg failure will be conservatively neglected (See Section 19.11.4.1.1.3). The likelihood of induced steam generator tube rupture is also assumed to be negligible.

19.11.4.1.1.7.2 Quantification of DCHSTREN :DCH Containment Failure Probability

Given a high RCS pressure and that RV lower head failure occurs into a "dry" reactor cavity, the containment failure probability is conservatively based on the results of a high level decomposition of the DCH event into its principal contributors. Peak pressures were established for a variety of conditions and a weighted containment failure probability was established. The process was performed separately for DCH events that are initiated from PDS where the RCS leak rate is governed by a cycling relief valve (CRV) and for the high and intermediate pressure state where a continuous RCS leak is present. Results for this assessment were established using the "two cell" DCH model discussed in Section 19.11.4.1.1.5.2. A description of the decomposition process and the resulting containment failure potentials follow.

19.11.4.1.1.7.2.1 Decomposition of the DCH Pressurization Process

This section utilizes the analytical "Two Cell" DCH method provided in Section 19.11.4.1.1.5.2 and described in Appendix 19.11D to quantify the various outcomes of a DCH containment threat. For purposes of the System 80+ PRA, the DCH event is decomposed into the following major parameters and processes:

1. Fraction of the core oxidized prior to VB (FEOX)
2. Mass of Material Ejected from the RV at the time of VB(MDEB)

3. Fraction of ejected material dispersed from the cavity (FDISP)

4. Fraction of Ejected Metallic Component Oxidized (FDMRC)

5. Fraction of Dispersed Material Ejected into the Upper Containment (1-FA1)

6. Combustion Completeness of the "In-Vessel" hydrogen (EBURNR)

7. Combustion Completeness for in containment hydrogen (EBURNC)

These items are discussed below.

1. FEOX: Fraction of the Core Oxidized Prior to VB

This parameter refers to the level of oxidation in the core prior to VB. Prior to VB the core will undergo considerable oxidation. Analyses and expert judgement suggests that oxidation levels at VB will be between 30 and 60 percent of the total core inventory (See for example Table 19.11.4.1-3). For purposes of this decomposition effort only one "high level" representation (50%) of pre-VB oxidation will be investigated. It is believed that this treatment will contribute to a modestly bounding estimate of containment failure probability.

$$P(FEOX=0.50) = 1.0$$

The oxidation level establishes the maximum amount of zircaloy available for oxidation during ejection and the amount of pre-existing hydrogen available in the RCS and containment prior to VB.

2. MDEB: The Mass of Molten Material Ejected at VB

This parameter represents the mass of molten material ejected into the reactor cavity at VB. This parameter was considered as part of the NUREG-1150 expert elicitation. That investigation concluded that the mass ejected at VB could be bounded between 20 and 60 percent of the total core inventory (see Reference 182). The median value of the ejected mass at VB was only 27% (See Figure 19.11.4.1.1-4). For the System 80+ PRA, this molten mass is conservatively estimated from the SASM study to be in the range of 34 to 40 percent of the initial core inventory. The lower limit is associated with RV failure induced by penetration failure. The higher limit is associated with RV failure induced by global creep of the lower head. This later process typically requires more time to occur and consequently allows more time for molten material to be generated. Analyses performed by Rempe et. al. have generated RV lower head failure maps for typical PWR instrumented lower heads that indicate that lower head creep is the less likely failure mode at RCS pressures below the pressurizer safety valve setpoint (Reference 184). For sequences where the actual failure mode is indeterminate and a non-instrument tube local failure of the lower

head could not be discounted. However, no information on failure size or potential failure dynamics was provided. Since small areas (relative to the total cross sectional area of the lower head) are sufficient to discharge the lower head core inventory in a few seconds (see for example Appendix 19.11F) the actual failure mode may not be of practical consequence. In order to ensure a full bound for this parameter the NUREG-1150 upper limit and cumulative distribution was employed for this assessment.

This issue was quantified as follows:

$$P(0.20 < MDEB < 0.40) = 0.75$$

$$P(0.40 < MDEB < 0.60) = 0.25$$

For the lower range, MDEB was evaluated at its upper limit of 0.40. Similarly, in the upper range of the distribution, MDEB was evaluated at a value of 0.60.

3. FDISP: Fraction of Ejected Material Leaving the Reactor Cavity

The System 80+ reactor cavity is designed to retain core debris. This is accomplished by providing tortuous paths for debris de-entrainment and a chamber for the debris to accumulate. Even if debris pushed towards the collection chamber were entrained it would likely follow the path towards the cavity exit where it will be intercepted by a small relatively enclosed HVAC room which can in effect serve as an alternate debris collection chamber. External structures in this region further support the contention that any debris that may escape this region will be confined to a localized area in the vicinity of the HVAC room. Consequently debris within this flowpath stream is unlikely to directly contribute to containment pressurization.

For purposes of the PRA quantification of this issue, the retention capability of the cavity proper will be considered to be between 10 to 20% at high RCS failure pressures and between 25 and 75% at RCS failure pressures consistent with the small LOCA. These values are highly conservative and take only minimal credit for the debris retention capability of the cavity. These values are qualitatively consistent with small scale test measurements which indicate that cavities with internal structures and exit obstructions can retain a significant fraction of the core debris at moderate RCS pressures (e.g., ~5 MPa) (See for example Reference 216). At high pressures, nearly complete debris entrainment is observed. None of the configurations tested to date is judged to retain debris as effectively as the System 80+ cavity design.

The probability distribution is established as follows:

For CRV/HIGH pressures at VB:

P(0.80 < FDISP < 0.90) = 0.50

P (0.90 < FDISP < 1.00) = 0.50

For intermediate pressure at VB:

P(0.25 < FDISP < 0.50) = 0.50

P(0.50 < FDISP < 0.75) = 0.50

All distributions are quantified at their upper limits.

4. FDMRC: Fraction of the Ejected Corium Debris Oxidized

During the core melt ejection process, the metallic components o the melt will be oxidized by the steam leaving the RV Experimental observations indicate that the oxidation process wil be limited by steam availability and a significant amount oxidatio may occur after the major HPME loadings will be experienced (Se Reference 189). The incomplete steam oxidation during the HPM loading phase arises from the difference between the melt ejectio and steam blowdown times and the short times associated with th debris entrainment process. In System 80+ the debris catcher ma also contribute to reduced oxidation by allowing the debris t accumulate in a central location with limited surface area. It i also expected that because of the limited steam supply in the RC prior to VB (particularly at low pressures) the fraction o material oxidized for intermediate pressure scenarios (most smal and medium LOCAs) will be lower than that possible for hig pressure sequences.

Therefore, FDMRC will be defined as follows:

For PDSs where RCS Leak Rate=CRV, FEOX is assumed to span a rang of 0.50 to 1.0. FDMRC is distributed as follows:

P(0.50 < FDMRC < 0.75) = 0.50

P(0.75 < FDMRC < 1.0) = 0.50

For PDSs which initiate at either a high or intermediate pressur the completeness of the metallic oxidation upon VB is expected t be biased towards lower values (0.25 to 0.75). For these sequence

P(0.25 < FDMRC < 0.50) = 0.50

P(0.50 < FDMRC < 0.75) = 0.50

For conservatism, all distributions were quantified at their upper limits. Furthermore, all the debris retained in the cavity is assumed to oxidize; this assumption is highly conservative.

5. 1-FA1: Fraction of Dispersed Material Which is Ejected into the Upper Compartment

This parameter considers the fraction of the molten material that is dispersed from the RV that ultimately reaches and mixes with the containment atmosphere. Based on extrapolation from results of HIPS experiments this parameter was established to be about 10% (See Appendix 19.11C). The bulk of the debris is expected to be captured within the core debris chamber. This assessment considers the fraction of the material that is released from the cavity that is directly ejected into an open area of the containment. This is restricted to those flowpaths that are initially closed and may or may not create a flowpath during HPME. These dispersal pathways are defined as (1) upwards into the reactor vessel annulus past the RV support corbels, passed the neutron shield plug and through the RV nozzle cavity cutouts and nozzle obstructions and through a passage through (or in the case of failure, around) the permanent refueling pool seal or (2) in the unlikely case of instrument seal table failure, up the instrument chase, past the instrument supports and out the small flow area instrument seal table. For purposes of PRA quantification, a wider range of upward debris dispersal was considered. In this assessment, it was assumed that the upper limit on corium entrainment could be bounded by the ratio (FA1) of the area around the vessel (at the elevation of the corbels) to the total available flow area from the cavity (about 0.25). Full entrainment at this ratio was considered highly unlikely due to the fact that (1) the entrainment process will initiate only after significant quantities of molten material have been driven towards the debris chamber (2) the primary velocities of the steam following VB will laterally move most of the corium away from the RV annulus region (3) the overhanging structures provides considerable obstacles for the entrainment of debris as a film up the annulus, and (4) the de-entrainment of debris which is expected to occur on structures such as the neutron shield plugs and cold and hot leg nozzles. Much of the corium intercepted by the annulus structures will be carried off to the lower compartment via nozzle cutouts.

Thus, 1-FA1 will be quantified as follows:

$$P(\ 1\text{-}FA1 < 0.10) = 0.75$$

$$P(\ 0.10 < 1\text{-}FA1 < 0.25) = 0.25$$

The parameter will be quantified at the upper limit value for each interval. This factor will be applied to all applicable Plant Damage States (PDSs). Dispersal at greater values of 1-FAI was considered negligible and was not considered in this evaluation.

6. EBURNR: Combustion Completeness of "IN Vessel" Hydrogen

This parameter considers the potential for the "in-vessel" hydrogen to contribute to the HPME pressure spike. Hydrogen residing in the vessel prior to VB will be released into the reactor cavity via the blowdown process. This decompression process will require approximately 20 seconds to depressurize the RCS to the SIT setpoint. At that time the hydrogen throughput through the break would diminish as a two phase mixture will cover the lower head. The mechanics of this process suggests that, in practice, all the hydrogen initially in the RCS clearly cannot be involved in the HPME associated combustion processes. First of all, even if the hydrogen were fully mixed in the RCS (which is unlikely) at the time the RCS pressure reaches about 600 psia 20 % of the initial "in vessel" hydrogen will still remain in the vessel. Combustion of this hydrogen in the cooler environment associated with SIT discharge as it leaves the vessel is not likely. Second, hydrogen is expected to collect in the higher elevation regions of the RCS (i.e., the pressurizer and steam generator tubes). This is particularly true if the loop seals remained intact prior to VB, preventing a full RCS natural circulation from developing. Thus, a well mixed discharge will not occur and the amounts of pre-existing "in vessel" hydrogen available during the early portion of the lower head discharge when the exothermic reactions and debris temperatures are the hottest will be limited. Third, even when the hydrogen is discharged, the hydrogen still may not burn in a time frame that will influence the peak DCH pressure. This is particularly possible for the System 80+ cavity design where debris and the flow stream are separated at several locations. The hydrogen in the cavity may be sufficiently steam inerted to prevent complete combustion and some of the hydrogen streams exiting the cavity will be sufficiently cool so as to not auto-ignite in the containment.

The uncertainty associated with the ability of "in-vessel" hydrogen to participate in the DCH pressurization process was reflected as a probability distribution with the level of participation varying from 0.25 to 0.75. The distribution was considered uniform over this range. That is,

$$P(0.25 < EBURNR < 0.50) = 0.50$$

and,

$$P(0.50 < EBURNR < 0.75) = 0.50$$

The lower portion of the distribution was quantified assuming EBURNR=0.50. The upper portion of the distribution was very conservatively treated by considering the maximum value of EBURNR to be 1.0.

This table intentionally blank.

TABLE 19.11.4.1.1-6

CONDITIONAL CONTAINMENT FAILURE PROBABILITY ASSOCIATED WITH DCH

Representative* Transient	DCHSTR1[1]	DCHSTR2[2]
Station Blackout (LEAK=CRV)	.01	0.014
LOCA without CHR (LEAK=NOT CRV, CHR=CHU)	0.0	0.005
LOCA with CHR (LEAK=NOT CRV, CHR=CHA)	0.0	0.001
All Other	0.0	0.000

* For PDS definitions the reader is referred to Section 19.12

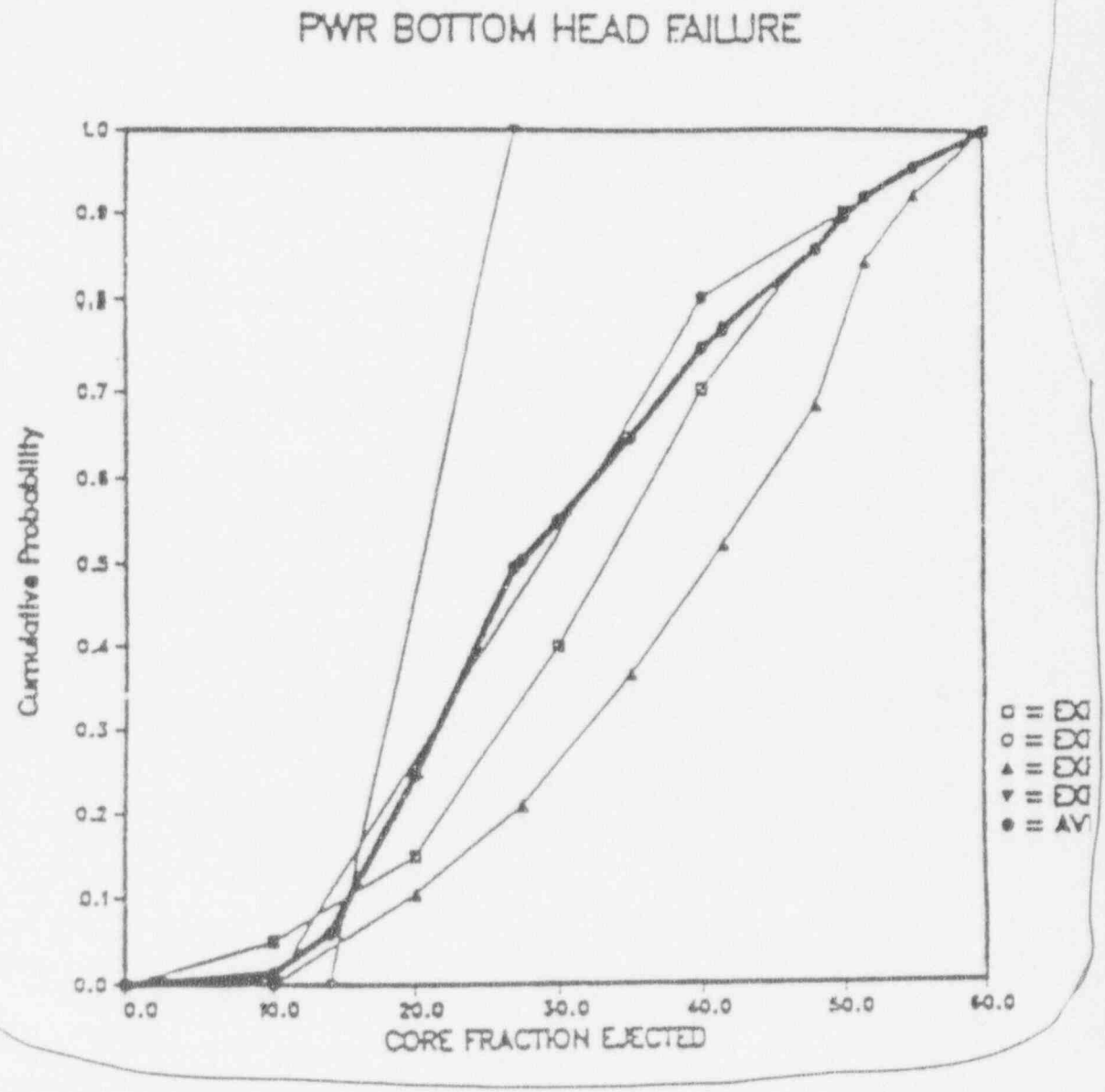
[1]DCHSTR1: Conditional containment failure probability resulting from DCH event with a pre-VB hydrogen burn

[2]DCHSTR2: Conditional containment failure probability resulting from DCH event w/o a pre-VB hydrogen burn

This figure intentionally blank.

FIGURE 19.11.4.1.1-3

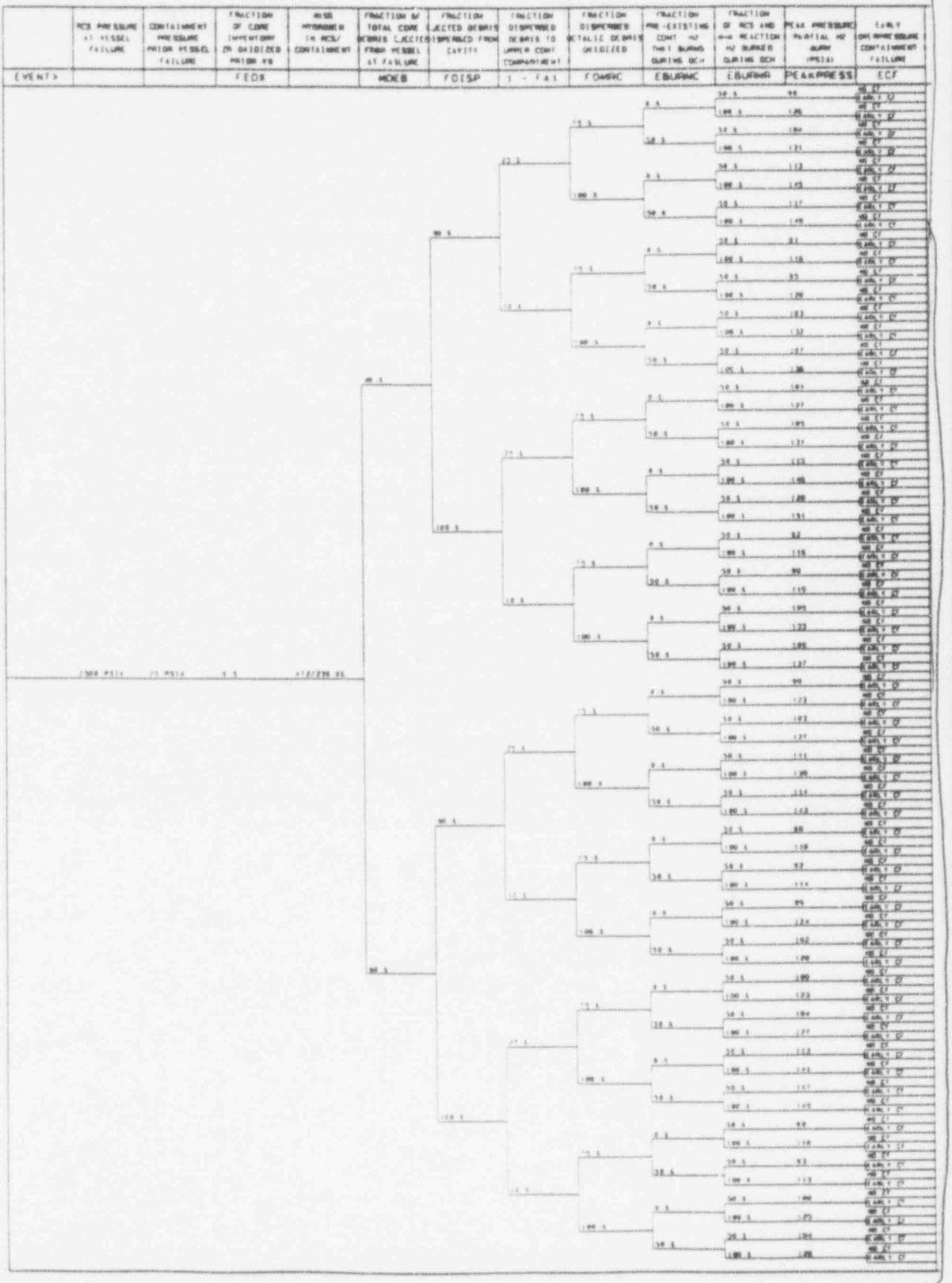
EXPERT ELICITATION QUANTIFICATION
FOR CORE EJECTION FRACTION
(DRAFT B:4551, VOL.2: "IN-VESSEL ISSUES")



This figure intentionally ~~blank~~ blank.

FIGURE 19.11.4.1.1-4A

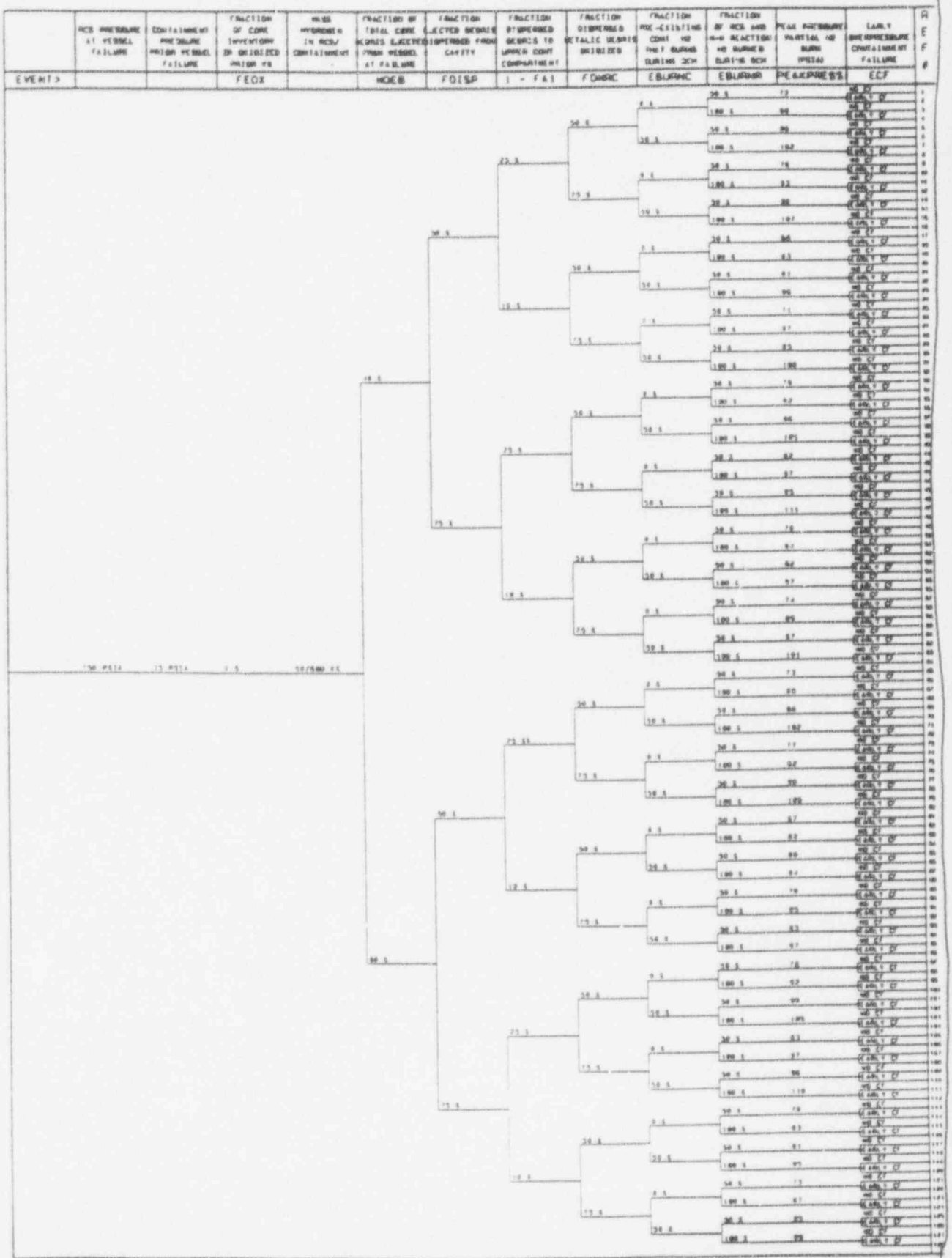
DECOMPOSITION TREE FOR QUANTIFICATION OF DCHSTREN FOR PDSs (LEAK=CRV; CAVT=DRY;CHR={ANY})



This figure intentionally ~~left~~ blank

FIGURE 19.11.4.1.1-4B

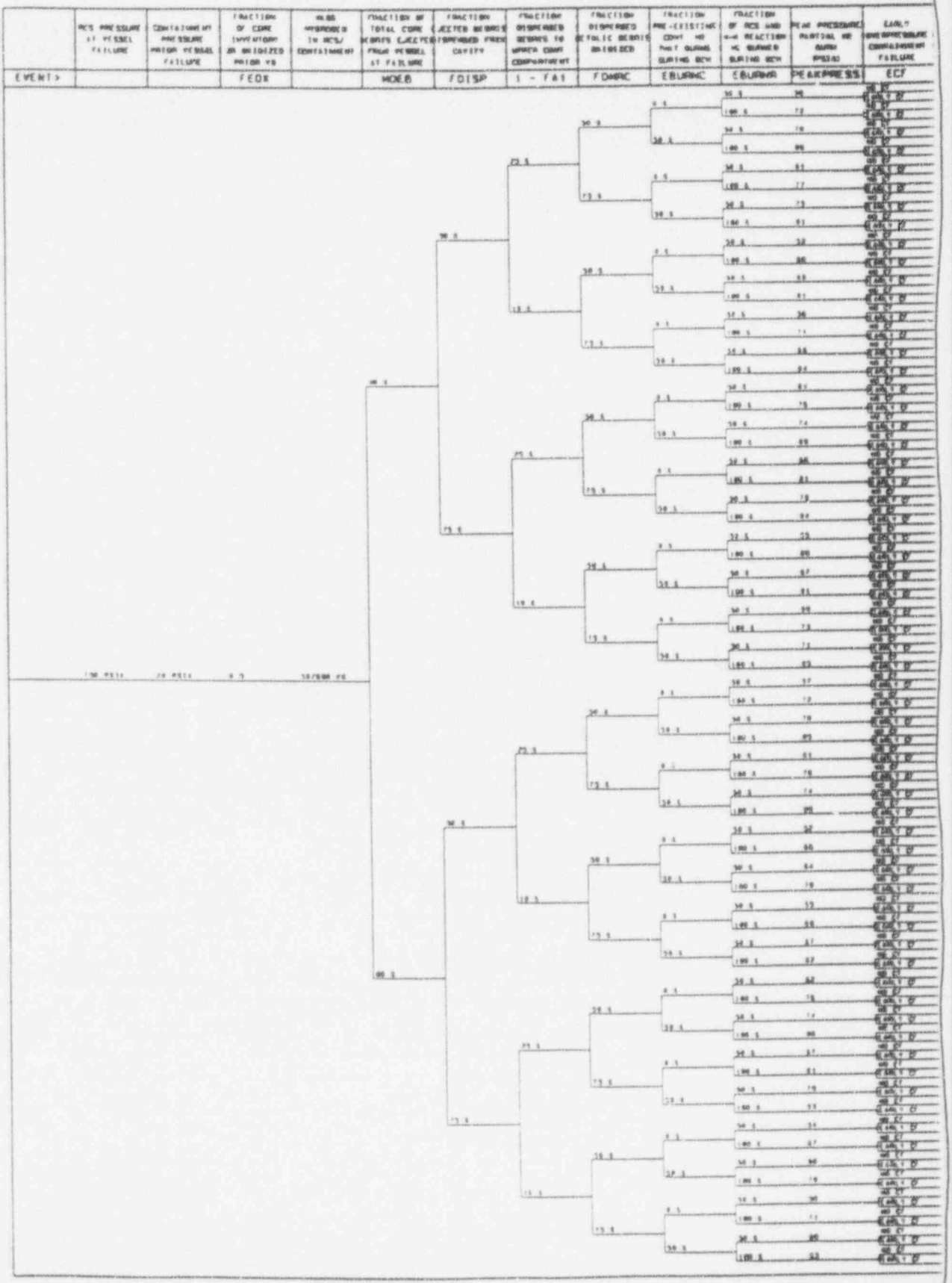
DECOMPOSITION TREE FOR QUANTIFICATION OF DCHSTREN FOR PDSs {LEAK={NOT CRV}; CAVT=DRY; CHR=CSU}



This figure intentionally blank.

FIGURE 19.11.4.1.1-4C

DECOMPOSITION TREE FOR QUANTIFICATION OF DCHSTREN FOR PDS# {LEAK={NOT CRV}; CAVT=DRY; CHR=CSA}



19.11.4.1.2.1.3.3 Ispra High Pressure Experiments

In Reference 126, Dr. Mayinger referred to a steam explosion test program performed by EURATOM to establish the influence of system pressure on steam explosions. While details of this test series are unknown, Dr. Mayinger noted that a general conclusion drawn from these experiments was that initiation of steam explosions at pressures greater than about 300 psia require very strong detonative triggers.

19.11.4.1.2.1.4 Significance of IVSE to System 80+

Based on a review of available steam explosion data and analyses, it appears that sufficient information is available to conclude that the probability of containment failure resulting from a corium-coolant interaction (CCI) event is very low (on the order of 0.001 or less). Much of these assessments considered typical PWR geometries analogous to that of System 80+ and are, therefore, considered applicable to System 80+.

19.11.4.1.2.1.5 Applicability of IVSE to the PRA

The above information is believed to be generally applicable to the System 80+ PRA. Therefore, for the purpose of System 80+ risk assessment, the containment failure caused by an IVSE was taken to have a mean containment failure probability of 0.001 for severe accidents where the RCS fails at pressures less than 250 psig and an order of magnitude lower when the RCS fails at high pressures. This probability is defined in the PRA as variable VB-ALPHA (See Section 19.12).

very small

19.11.4.1.2.2 Ex-Vessel Steam Explosions

19.11.4.1.2.2.1 Description of Phenomena

Steam explosions arise from the generation of steam at a rate faster than can be acoustically or inertially relieved by the surrounding medium. Steam generation occurring at that rate will generate shock waves in the surrounding liquid pool and produce strong impulsive loadings on adjacent structures.

The discharge of molten core debris into the reactor cavity region could potentially result in explosive interactions between the molten core debris and cavity water. The initiation of an explosion, if any, would occur either when the core debris initially contacts the water or when the debris penetrates the water and contacts the concrete surface at the bottom of the reactor cavity. The results of a potential steam explosion would be to generate impulse loads on the reactor cavity walls and in-cavity structures. The resultant damage to important structures was considered negligible for the PWR cavity designs analyzed in NUREG-1150. However, EVSE induced destruction of the reactor

19.11.4.1.2.6 Application of EVSE to the System 80+ PRA

19.11.4.1.2.6.1 Decomposition of the EVSE Process

The System 80+ PRA explicitly considers the potential for Ex-Vessel Steam Explosions and their associated consequences. To establish a median containment failure probability given an EVSE occurs, the EVSE containment failure event was decomposed into the following basic event and parameters:

1. MASS: Mass of Corium Involved in Steam Explosion
2. EFF : Efficiency of Steam Explosion
3. CAVF: Loading Fails Cavity
4. CF : Cavity Failure Induces Containment Failure

This decomposition and quantification is discussed below:

MASS: Mass of Corium Involved in the Steam Explosion

This parameter is highly uncertain. Four participating corium mass ranges were established as follows:

Low (L):	Participating Corium Mass is below 1000 lbm
Intermediate 1 (I1):	Corium Mass is between 1000 lbm and 5,000 lbm
Intermediate 2 (I2):	Corium Mass is between 5,000 lbm and 10,000 lbm
High (H):	Corium Mass is greater than 10,000 lbm

Lower plenum conditions were established prior to VB in Table 19.11.4.1.1-1. Based on this information it is expected that about 120,000 lbms of molten corium mass will be ejected during VB. Estimates of the time dependent discharge mass for a representative lower head failure at high and intermediate pressures are presented in Appendix 19.11 F. These figures show that the corium ejection process requires less than 10 seconds and that the maximum hole in the RV will be about 0.5 ft^2 (See Appendix 19.11F). During this ejection period (Reference 179) steam explosions are possible. For the quantification of the participating mass it was assumed that the EVSE mass could be established by the mass of corium in the jet spanning the height of the water pool. The distribution of masses was directly related to the fractional time that the RV hole was below a specific area. In addition, it was assumed that there was a 10% probability that the total mass participating in the EVSE was above the value that would be calculated using the maximum hole

small

area. The time frame of the steam explosion is on the order of several millseconds. The mass distribution participating in the corium melt is established based on a time-failure area relationship (See Appendix 19.11F).

EFF: Efficiency of steam Explosion

Data from FITS tests indicate that the median steam explosion efficiency is 1.5 % with a range of observed values between 0 and 3%. Two ranges of efficiencies will be considered. These are efficiencies less than 1.5% and efficiencies greater than 1.5%. These groups will be considered equally probable (0.50/0.50) and quantified at the extremes of each range.

CAVF: Cavity Fails due to Loading

This parameter provides the probability that the cavity load condition resulted in containment failure. These conditions are summarized in Table 19.11.4.1.2-3B.

TNT loadings were established using the maximum conversion efficiency identified in each of the Low and High groupings. The failure rates were conservatively established by considering the average failure probability anticipated by the TNT equivalent model predictions.

CF: Cavity Failure Induces Containment Failure

Based on discussions presented in Section 19.11.4.1.2.2.2 above, there is support for the position that the failure of the reactor cavity will not compromise containment integrity. This is due to the fact that adjacent concrete structures, external to the cavity, can provide support to the RV and corbels even if the lower cavity structure carries no load. In addition, the hot and cold legs can provide additional support to the RV. Even if the reactor vessel supports should fail, large RCS motions can be restrained via motion limiting devices on other RCS components. Furthermore, if large RCS motions were to occur, structural analyses indicate that a consequent containment failure is still unlikely. It is our best judgement that for realistic loading conditions, cavity collapse will not occur. However, in the remote possibility of a cavity collapse sufficient structure will still remain, so that a failure of the RV sufficient to induce a subsequent failure of containment integrity is unlikely. In light of this evidence, the probability that cavity failure will cause a consequent failure of containment integrity is conservatively assigned a value of 0.05.

Smith

This section intentionally blank

19.11.4.1.2.2.6.2 Quantification of EVSEFAIL

The event tree resulting from the EVSE decomposition process is presented in Figure 19.11.4.1.2-4. This tree illustrates the potential consequences of an EVSE event occurring in the reactor cavity on the containment integrity. Eight of the outcomes are identified as potentially resulting in containment failure (CF). The resulting conditional containment failure probability was estimated to be <.01. Thus, EVSEFAIL will be set to .01. EVSEFAIL is defined in Section 19.12 as the conditional probability that a containment failure occurs given an EVSE has occurred.

19.11.4.1.2.3 Post-Vessel Breach Steam Spikes

19.11.4.1.2.3.1 Description of Phenomena

Steam spikes following RV breach result from the relatively rapid pressure increase within the containment produced by both (1) the discharge of high pressure water/steam from the reactor vessel and (2) generation of steam associated with the quenching of superheated core debris. These processes can provide a very rapid (occurring in several seconds or less) steam addition to the containment followed by a modest pressure spike. In general, pressure loadings resulting from this process will exceed containment design limits but will be well within ASME Service Level C limits (See Section 19.11.3.1). This containment challenge is discussed in more detail below.

19.11.4.1.2.3.2 Parameters Affecting Post-Vessel Breach Steam Spikes

In the context of the PRA, Post-Vessel Breach Steam Spikes will include both the steam released into the containment following vessel breach (VB) and the vaporization of liquid during the corium quenching process. The impact of these releases are considered along with the pressurization prior to VB to establish the rapid steam generation containment challenge. Consequently, the parameters affecting the magnitude of the post RV failure pressure spike are:

a. Containment pressure prior to VB

b. RCS conditions at VB

c. Mass and Superheat of corium ejected into the reactor cavity

d. Water availability in the reactor cavity.

scenarios. These scenarios include a station blackout, a "V" sequence (interfacing systems LOCA) and a Large LOCA in a containment without availability of containment sprays. These events typically span the range of interest for estimating post VB rapid steam generation pressure spikes. For the first two scenarios, the initial containment pressure will be less than 25 psia, for the last sequence the LOCA was assumed to result in a design basis challenge to the containment resulting in an initial pressure of 67 psia. (This assumption neglects any passive cooling of the containment due to heat transfer to the containment shell and structures within the containment. Design basis analyses and MAAP calculations suggest that these heat sinks will contribute to a reduction in containment pressure of about 20 psi in a three hour time interval prior to VB.) The containment is subsequently pressurized by a combined high pressure steam release and steam generation due to a rapid quenching of the corium debris. For this study the corium mass quenched comprised 65% of the total core mass (including support structure) and was initially discharged into the containment at 2800°K. The mass and mass distribution used for this study were extrapolated from results of the NRC sponsored SASM activity presented in Table 19.11.4.1.1-1 of this report. To ensure that all steam generation modes were accounted for, it was also assumed that 50% of the quenching debris oxidizes during the quenching process. The resulting bounding containment pressures were established for these scenarios. Results of this analysis are presented in Table 19.11.4.1.2-5. Analogous analyses were performed for the Large Break LOCA. However, in this analysis containment sprays were not credited and the mass and energy of steam released from corium quenching at VB was negligible. The peak pressure calculated using this methodology was below 98 psia. While these loadings are above the design basis containment loadings, they are well below the pressure limit determined using the ASME Service Level C criterion.

19.11.4.1.2.3.4 Application to the PRA

Rapid steam generation events (or steam spikes) will not result in a significant challenge to the System 80+ containment. In fact, for scenarios where (1) primary discharge is through the IRWST , (2) the containment is bypassed or the (3) containment heat removal properly functions, the RSG pressures will be below (or slightly above) design pressure limits. These transients will be assumed to have no possibility of failing containment. For transients with direct steam discharge to the containment and without any containment heat removal the final containment pressure following the RSG event will be below 100 psia. This pressure level exceeds the containment design limit by about 50% and is well below Service Level C limits. NRC has indicated that the probability of failing the containment at levels below 1.5 times the design pressure is virtually zero (Reference 127). For purposes of the PRA a failure probability of 0.001 is established for this later condition.

very small

This table intentionally ~~left~~ blank

TABLE 19.11.4.1.2-3A

PROBABILITY DISTRIBUTION FOR THE CORIUM MASS INVOLVED IN EVSE

Low	Intermediate 1	Intermediate 2	High
0.30	0.60	0.075	0.025

This table intentionally ~~left~~ blank.

TABLE 19.11.4.1.2-3B

CAVITY FAILURE PROBABILITY FOR VARIOUS COMBINATIONS OF PARAMETERS MASS AND EFF

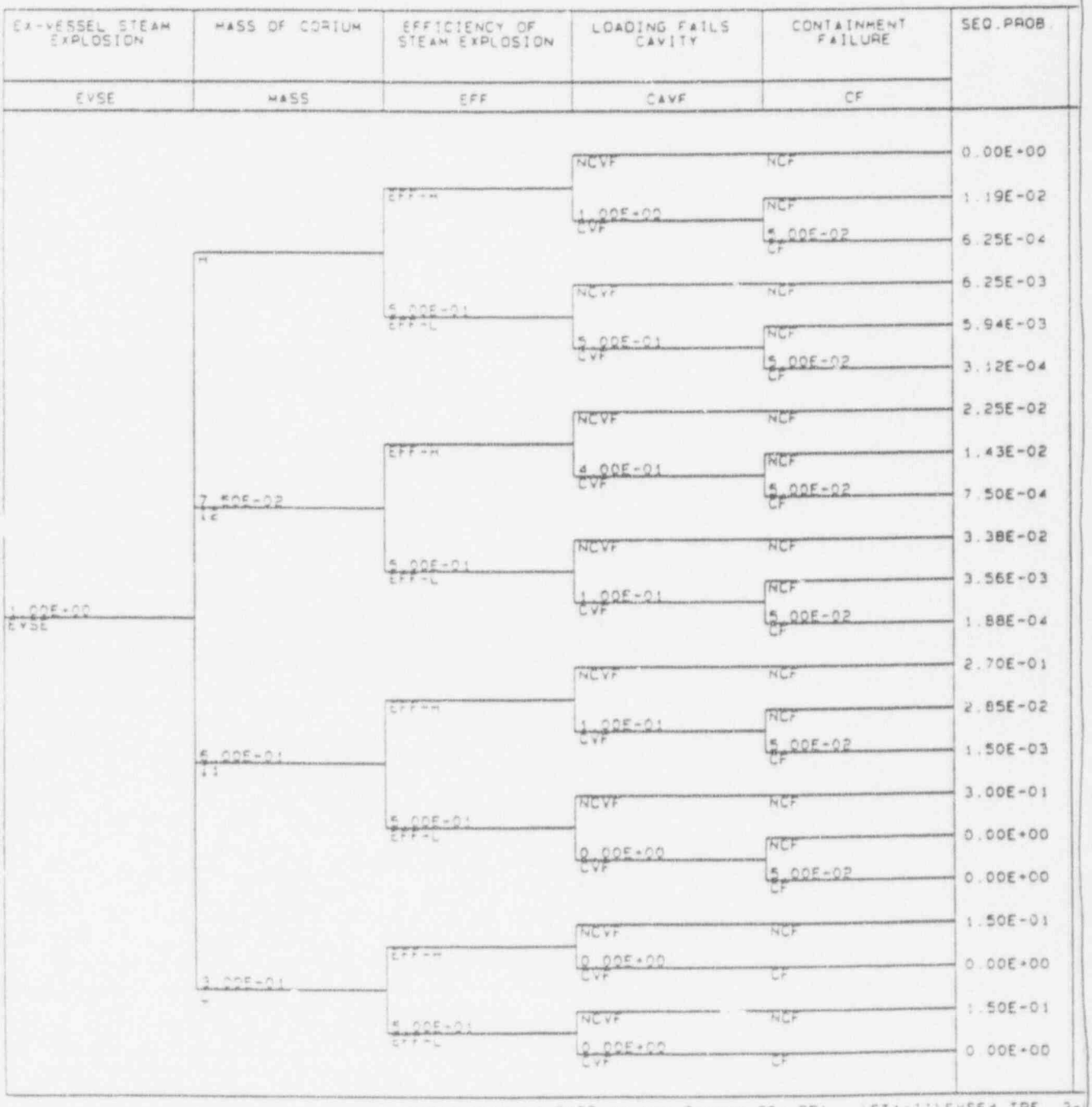
MASS*	EFF+	CAVF
L	L	0.0
L	H	0.0
I1	L	0.0
I1	H	0.10
I2	L	0.10
I2	H	0.40
H	L	0.5
H	H	1.0

* See definitions of parameter MASS
\+ L=LOW (1.5%) ; H=HIGH (3%)

This figure intentionally ~~left~~ blank.

FIGURE 19.11.4.1.2-2

EVSE DECOMPOSITION EVENT TREE



It should be noted that burns occurring below 8 volume percent hydrogen will be incomplete. Furthermore, combustion of hydrogen outside the flammability region is not probable. The conservatism associated with the application of the AICC methodology was established by comparing normalized burn pressure rises predicted using the Appendix 19.11E methodology and results of various hydrogen burn experiments (See Figure 19.11E-1).

Based on the bounding results of the deterministic evaluation of the containment hydrogen threat complete combustion of the hydrogen produced due to 100% oxidation of the zircaloy cladding in the active fuel region will result in a peak containment pressure of less than 103 psia. This value is below ASME Service Level C limits of about 140 psia and are well below the containment ultimate failure pressure of 168 psia (See Section 19.11.3.1).

It should further be noted that the above demonstration ignores the availability of igniters. When igniters are considered, the hydrogen combustion contribution to containment pressure loading will be small.

19.11.4.1.3.1.4.2 Mixing within the System 80+ Containment

The impact of nonhomogeneous hydrogen distributions were established for the ALWR in Reference 149. In this analysis a nodal representation of the ALWR containment was subjected to a forced hydrogen production representing an equivalent 75% clad oxidation during a Station Blackout (SBO). This analysis indicated that the vented IRWST hydrogen concentrations are only 2 v/0 greater than the overall containment concentrations. These results are consistent with predictions of System 80+ mixing analyses presented in Appendix 19.11K.

System 80+ has been designed to facilitate a chimney type natural circulation flow pattern between the steam generator housing "riser" and the containment region outside of the crane wall ("downcomer"), between each floor. This flow pattern promotes containment mixing and will minimize containment concentration gradients.

19.11.4.1.3.1.5 Application to the PRA

In order to establish the probability of a hydrogen deflagration induced containment failure associated with various Plant Damage States (PDSs), the AICC model (Appendix 19.11E) ~~was used, to quantify threats associated with various early containment hydrogen threats.~~

The quantification of the hydrogen containment threat in the PRA is based on best estimate assessments with regard to hydrogen availability and ignition conditions at or prior to vessel breach.

(3) Post-VB Hydrogen Burn Pressures

Post-VB hydrogen burn containment pressures depend upon the following factors:

1. RCS steam discharge path prior to VB
2. IRWST subcooling
3. Availability of Containment Heat Removal Prior to Burn

For transients that discharge steam into the IRWST, or if the RCS inventory is discharged directly into the containment and the containment heat removal (CHR) is partially functioning (at least one containment spray pump and an associated heat exchanger), the hydrogen burn will be assumed to be initiated from the maximum flammability limit (See Figure 19.11.4.1.3-1). This results in initial pressures between 30 and 40 psia.

Transients that result in significant steam discharge into the containment without availability of CHR will be assumed to have an inert hydrogen mixture and will not burn within the early hydrogen burn event. Instead this hydrogen is allowed to accumulate in containment for potential ignition along with additional hydrogen sources during the late hydrogen burn scenario.

These PRA conditions are summarized in Table 19.11.4.1.3-3 along with the resultant containment failure probabilities, based on applying the conservative burn pressure estimates to the System 80+ containment fragility curve (Figure 19.11.3.1-3).

19.11.4.1.3.2 Hydrogen Detonation

19.11.4.1.3.2.1 Description of Phenomena

Detonations are combustion waves in which heating of the unburned gases is caused by compression from shock waves. The pressure loads developed during detonations are essentially dynamic loads (impulses) and can result in very short duration and localized pressure spikes many times greater than that of a deflagration initiated from similar conditions. As a result of these large loadings, detonations, if they should occur, may potentially pose a threat to containment integrity and to the continued operation of mitigative equipment.

19.11.4.1.3.2.2 Parameters Affecting Hydrogen Detonation

Two classes of hydrogen detonations are typically distinguished: (a) detonation via direct initiation by high explosives and (b) Deflagration-to-Detonation Transition (DDT) resulting from an energetic burn in a confined obstructed geometry. Hydrogen detonations are influenced by (1) hydrogen concentration, (2) presence of inertents, (3) the ignition source and (4) system geometry (scale and configuration).

Conditional probability that a hydrogen burn would either be initiated as or become a detonation are defined as follows:

- For accident scenarios where the steam concentration is expected to exceed 30 v/o, detonations are not considered credible. Because of the large steam release associated with the HPME, DCH events are not considered precursors to detonations.

- For hydrogen concentrations below 10 v/o in dry air, detonations within the containment are considered impossible. Thus, detonations are not expected for situations where igniters are functioning and early pre-vessel breach hydrogen burns occur in the containment.

- For conditions where the global hydrogen concentration is expected to be above 10 v/o in dry air and steam concentrations are below 30 v/o steam (i.e containment heat removal is successful), the fraction of hydrogen burns that may become detonations is taken to be 0.01 (highly unlikely to impossible) for sequences which discharge hydrogen directly to the containment.

- For conditions where significant accumulation of hydrogen in the IRWST is expected and steam inerting cannot be guaranteed, the probability ~~for~~ that a potentially threatening detonation ~~was established at 0.05 (unlikely)~~. This is considered a conservative position since detonations in even minimally inerted or sprayed regions are not expected until hydrogen concentrations approach 20 volume percent.

It will be assumed in the PRA that the occurrence of a detonation will fail containment. This is also a **very** conservative position. While the ensuing pressure spike occurring following a detonation is very large compared to a deflagration pressure rise, the detonation spike is nonuniform and of very short duration (typically less than 10 ms) and consequently may not pose a threat to large structural components, and the containment structure. This is particularly true of the IRWST. While the outer walls of the IRWST is defined by the containment walls, the actual containment shell is separated from the water pool and sandwiched in between two layers of concrete each approximately six feet thick. When subjected to large detonation loadings, this arrangement may result in extensive cracking of the IRWST enveloping concrete, however actual failure of the containment is not considered likely. Furthermore, any missiles generated during a hypothetical IRWST detonation will be intercepted by the crane wall and not pose a threat to the containment.

INSERT

① | the probability that a hydrogen burner becomes a detonator is considered to be highly unlikely to impossible.

This table intentionally blank.

TABLE 19.11.4.1.3-3

SUMMARY OF PRA ASSUMPTIONS FOR SYSTEM 80+
EARLY BURN EVENT

Containment Condition	PDS /Basic Event	Fraction of Active Clad (H2 Equivalent)	Peak Pressure	Cont. Failure Probability
1. Igniters on	ANY	0.50	61	0.00
2. Pre-VB Burn	HIGH/MID	0.50	61	0.00
	LOW	0.75	80	0.00
3. Post VB Burn Given Pre-VB Burn Occurs	ANY	0.50	61	0.00
4. Post-VB w/o Prior Burn	ANY*	1.00	103	.006

* See Section 19.12.2.2.6.3.1.2.2

1. For high pressure RV lower head failures, (RCSHIGH) the conditional probability of containment failure due to direct corium impingement was assumed to be 0.0001. (Very Small.)

2. For low and intermediate RV lower head failures containment shell failure due to direct shell attack was not considered credible.

It should be noted that this failure mechanism does not include containment failure via combustion induced missile generation. This failure mechanism is included in the discussion of hydrogen detonation (See Section 19.11.4.1.3).

19.11.4.1.4.2 Cavity Overpressure Failure

19.11.4.1.4.2.1 Description of the Phenomena

Following a HPME, large quantities of steam and corium are discharged into the lower portion of the reactor cavity. This discharge can potentially challenge the integrity of the reactor cavity and thereby threaten containment integrity. Cavity overpressurization can potentially result in a structural failure of the reactor cavity and associated RV supports. Failure of the RV supports can produce excessive motions in the RCS and steam generators potentially failing a containment penetration or producing an unisolable breach in piping exiting the containment.

Potential sources of cavity overpressurization include the EVSE event and the energetic failure of the RV lower head. The EVSE induced failure of the cavity and or reactor internal supports is considered in Section 19.11.4.1.2. This section considers localized cavity pressurization induced by steam pressurization of the reactor cavity space immediately upon RV lower head failure.

19.11.4.1.4.2.2 Significance to System 80+

System 80+ is expected to withstand cavity pressurization events following RV lower head failure. This capability of System 80+ arises from the robustness of the System 80+ reactor cavity design which includes (1) a high reactor cavity wall strength and (2) a large reactor cavity volume.

The post severe accident cavity pressurization performance of the System 80+ design was evaluated analytically for a simulated high pressure superheated steam blowdown following a postulated breach in the RV lower head. Analyses were performed using the ABB-CE DDIF Mod 7 (Reference 141) cavity pressurization computer code. In this analysis a multi-compartment representation (see Figure 19.11.4.1.4-1) was assembled to provide a detailed simulation of the reactor cavity. Pressurizations were established using a spectrum of RV lower head failure sizes ranging from the equivalent of a lower head instrument tube failure to a large creep failure of the RV lower head. Results of these indicate System 80+ cavity loadings to be below 100 psid.

MAAP analyses for similar transients indicates that the cavity pressure rise associated with a best-estimate HPME event caused by a single ICCI failure, will be under 20 psi. For either evaluation, predicted loads are below the cavity wall values of approximately 188 psid (ultimate strength of 235 psid) and consequently will not challenge cavity or containment integrity.

19.11.4.1.4.2.3 Application to the PRA

The cavity overpressurization induced containment failure is not considered a credible threat to containment integrity. However, for the purpose of completeness this failure mechanism has been included in the PRA supporting logic models with a probability of 0.0001.

19.11.4.1.4.3 Rocket Induced Containment Failure

19.11.4.1.4.3.1 Description of Phenomena

The issue of rocket induced containment failure was formally addressed in the Oconee Level 3 PRA performed by NSAC (Reference 216). In this assessment, Battelle Columbus reviewed the potential for containment failure due to an in-containment reactor vessel "lift-off" following the failure of the RV lower head. The rocket analogy resulted in the authors of Reference 216 identifying rocket induced containment failure as the "Saturn V" failure mode. While Battelle Columbus staff does not believe this failure mode to be credible, they could not discount the possible failure mode by way of analysis. However, a low conditional failure probability of about 1.5×10^{-5} was assigned following a high pressure plant damage state (PDS).

Recently, the German evaluation of the rocket containment threat was performed as part of Phase B to the German Reactor Risk Study (Reference 130). The German assessment considered the failure mode of their RV integral lower head to be an instantaneous and complete circumferential failure at the height of the corium upper surface. This results in a RV lower head failure area of approximately 190 ft^2. The RV loading due to this instantaneous failure was established using RELAP 5/MOD 3 calculations (Reference 205). The resulting impulsive loadings were considered sufficiently energetic to propel the RV as a rocket into the wall of the upper containment with sufficient energy to cause a localized containment failure. Specifically, the study concluded that at "internal pressures higher than 8 MPa (1160 psia) it can no longer be excluded that the containment will also be damaged". Based on the probabilities reported in Reference 130 it appears that the conditional containment failure probability associated with RV lower head failure at high pressure was about 0.03.

This section intentionally left blank.

It is interesting to note that this failure mode was included in the German Risk Study whereas the alpha mode failure ("in-vessel" steam explosion induced failure of the containment) was considered incredible and therefore was not.

19.11.4.1.4.3.2 METHODOLOGY

In order to address the Rocket Failure issue, an issue decomposition approach was selected. This method is similar to that employed by Theofoneous (Reference 129) in his quantification of "in-vessel" steam explosion induced containment failure (Alpha Mode). In the decomposition process the phenomenological processes that are involved in leading to containment failure are identified and quantified based on calculations and engineering judgement. In order to assign probabilities to the decomposed events, the following guidelines were used:

Probability	Description
1/2	Behavior is possible and likely but precise value is indeterminate
1/10	Behavior is within known trends but obtainable only at edge-of-spectrum parameters
1/100	Behavior cannot be positively excluded but is outside the spectrum of reason

19.11.4.1.4.3.3 ASSESSMENT OF ROCKET INDUCED FAILURE PROCESSES

In order to proceed with quantification of the rocket induced containment failure scenario it is helpful to decompose the event into its constituent processes so that the various contributors to the event can be independently quantified.

19.11.4.1.4.3.3.1 Event Scenario

In this event scenario it is assumed that either a high pressure (HP) or intermediate pressure (IP) core damage scenario initiates an unrecoverable core meltdown. While the RCS is at pressures above 1000 psia the RV lower head is assumed to fail instantaneously. This results in a short duration (impulsive) pressure load on the RCS. This loading begins to displace the upper portion of the RV and its connective piping and supports upward. After several inches of movement the connecting RCS piping (hot/cold legs) will make contact with the reactor cavity at the top nozzle cutout elevation. Shear stresses within the RCS piping and piping restraints will resist the upward impulsive RV loading. Should the upward RV loads exceed the restraining capability of the RCS piping, a "lift-off" of the RV is possible. The imparted velocity and trajectory of the RV at "lift-off" to a large extent determines the level of the resulting containment threat.

The decomposition of the above event scenario is illustrated in Figure 19.11.4.1.4-2.

19.11.4.1.4.3.3.2 Quantification of Rocket Induced Containment Failure

This section discusses the detailed quantification of this event scenario for high and intermediate pressure plant damage states (PDSs).

19.11.4.1.4.3.3.2.1. Quantification of Issues Relating to the Large Global Failure of the Reactor Pressure Vessel

The potential for a large global failure of the RV lower head to occur considers both the internal RV pressure (which drives the failure dynamics) and the thermal-structural mechanics of the lower head failure process.

The significant contributors to rocket induced containment failure include:

1. RCS pressure prior to VB failure
2. RV Lower Head Failure Size
3. RV failure timing
4. RV restraint capability
5. Kinetic Energy at Vessel Launch
6. RV trajectory

These items are discussed below.

19.11.4.1.4.3.3.2.1.1 RV Pressure Prior to VB (P_{RVHIGH})

The German Risk Study (Reference 130) concludes that if a full circumferential shear of the RV lower head occurs, rocket induced containment threats are credible at RV pressures greater than about 1160 psia. Thus, it becomes an important question to ascertain whether or not a significant RV depressurization (below 1000 psia) occurs prior to lower head failure. Since this issue is of considerable concern to DCH related containment threats, this topic was also considered as part of the NUREG-1150 (Reactor Risk Document) expert elicitation process (See discussion in Reference 115). This information is presented in Section 19.11.4.1. This study concluded that a high pressure melt condition (driven by a cycling PSV) will have a median probability

of not failing the hot leg in time to depressurize the RCS to 600 psi prior to vessel breach of 0.14 with an associated range of (0.00 to 0.28). At intermediate pressures the similarly defined RCS hot leg failure probability was estimated to be 0.83 with a range of (0.5 to 1.0). In addition to induced piping failure, the System 80+ RCS can intentionally be depressurized via use of the RD valves.

In assessing the contribution of pressure of rocket failure it was assumed that (1) PDSs that result in medium or low system pressures or (2) events that are initially at high pressure but induce RCS piping failure or intentional depressurization occurs prior to VB, will not involve sufficient energy to threaten the containment. Consequently, for purposes of quantification, the probability of containment failure caused by these events was taken to be zero.

The combined probability of depressurizing the RCS prior to VB for transients initiating from the PSV setpoint (either via RD valve actuation or creep failure of piping) was conservatively taken to be 0.10. For high pressure transients where the RCS is below the PSV lift point, the probability of depressurization was assumed to occur as a consequence of induced RCS piping failure.

19.11.4.1.4.3.3.2.1.2 RV Failure Size ($P_{RVLARGE}$)

The net upward force on the RV is directly related to the RV lower head failure size. Structural analyses of the integral lower head failure was established as part of the German Risk Study. In this effort the GRS considered that natural circulation currents set up within the RV lower head would cause preferential thinning of the RV walls at point of contact between the corium surface and the RV wall. This mode of attack was postulated to cause an circumferential failure of the reactor vessel, unzipping the RV lower head from the rest of the RV. This leads to a RV failure area of 192 ft^2 for the German PWR. For the System 80+ design the most likely lower head failure area at the time of RCS steam discharge will be about 0.5 ft^2 (See Appendix 19.11F). It is believed this failure will arise from a failure of the lower head ICCI penetration with subsequent hole tabulation. In the extreme, the German approach to defining RV lower head failure based on the unzipping of the RV at the corium-vessel interface, creep failure of the lower head can hypothetically reach 140 ft^2. This later failure is not considered credible however for purposes of quantification of this event the RV failure area was established as a lognormal distribution with a conservatively bounding medium failure area of 1 ft^2 and a maximum RV failure size (conservatively defined with a .01 probability) of 140 ft^2. These large failure sizes were considered for purposes of establishing a quantitative basis for the rocket failure threat only.

A conservative assessment of impulsively loading the RV indicates that under high pressure failure conditions, RV lower head failure areas above 75 ft^2 may be sufficient to cause an impact induced containment failure. Based on this criteria the probability of exceeding a failure area in excess of 75 ft^2 is about 0.013 for PDSs with high pressures prior to VB.

19.11.4.1.4.3.3.2.1.3 Instantaneous RV Failure ($P_{INSTANT}$)

The rate of opening the RV lower head influences the depressurization of the RCS and consequently the RV loading. Analytical calculations of RV loadings resulting from a full circumferential failure of the RV lower head was performed as part of Phase B of the German Risk Study. These calculations were based on a RELAP5 simulation of an instantaneous failure of the RV lower head (Reference 205, See Figure 19.11.4.1.4-3). These calculations suggest that for this instantaneous failure mode the RV pressure loads diminish to low levels in about 0.3 seconds. More gradual RV failures would reduce the net impulse imparted to the RV by effectively area weighing the system pressures. That is small area openings will be associated with the early high system pressures. As the hole in the RV grows the RCS depressurization accelerates. Thus, the large hole areas would be associated with lower system pressures. Analyses of the contribution of hole growth due to ablative considerations (See Appendix 19.11F and Reference 118) suggest this process to take several seconds. Estimated failure times resulting from circumferential failures are believed to be at least as long. Furthermore, since the large failures tend to be induced at the upper portions of the lower head, there exists a significant probability that the steam release associated with the larger hole failures would significantly depressurize the RCS and reduce any Rocket threat. The benefits of a realistic assessment of failure dynamics is considered indeterminate and is assigned a value of 0.5 with an uncertainty of $\pm$ 0.25. This implies that realistic consideration of the pre and post break process would likely reduce the range of failure areas associated with containment failure.

19.11.4.1.4.3.3.2.1.4 Quantification of RV Launch

In order for the RV to rise into the upper containment it must first displace and shear off two hot legs and 4 cold legs while maintaining sufficient kinetic energy to launch the RV into a destructive encounter with the containment. The energy at RV "liftoff" required to turn the RV into a containment threatening missile must exceed 130 million ft-lbf (Reference 206). This estimate is conservatively based on that energy needed to vertically lift the RV and upper internals 100 ft to the containment shell.

19.11.4.1.4.3.3.2.1.5 **RV Not Restrained by RCS Piping ($P_{RESTRAINED}$)**

Approximate structural calculations performed suggest that the median shear strength of the RV piping is sufficient to restrain the RV following a high pressure lower head failure. These calculations were performed assuming RCS hot leg piping at 800°F and RCS cold leg piping at 600°F. Under these conditions, the two hot legs and four cold legs can carry a median dynamic shear vertical loading of more than 84 x 10^{+6} lbf. This capability is more than sufficient to restrain the RV loading associated with lower head failure area in excess of 225 square feet. RV support anchorage provides considerable additional strength. Since the most likely loading associated with System 80+ RV lower head failure is less than 1 ft^2 the probability that the RV is not restrained is considered remote at high RCS pressures and outside the realm of reason at intermediate RCS pressures(about 1200 psia). In order to quantify this feature the restraint capability was established as a lognormal distribution using material ultimate strength and uncertainties associated with carbon steel pipe. This distribution was evaluated against the maximum RV force based on a 140 ft^2 RV lower head instantaneous failure. This resulted in a probability of the RV restraint (hot and cold leg piping) to not restrain the RV from launch to be .002 at high pressure and .0002 at intermediate pressure. Even these values are considered very conservative since in performing the calculations the restraint capability of the piping was reduced by a dynamic loading factor of 2 commensurate with an instantaneous loading.

19.11.4.1.4.3.3.2.1.6 **RV Kinetic Energy at Launch Greater Than Threshold (P_{KE})**

This element considers the probability for a "free" reactor vessel to be propelled through the containment with sufficient energy to cause a breach of containment. Since the actual energy absorbed in the initial RV translation and RCS piping failure has not been considered, this element assesses the potential for energy dissipation to be sufficiently large so as to reduce the RV initial kinetic energy below the containment damage levels. This effect is considered to be a real process which is difficult to quantify. The issue is assigned as indeterminate and is given a probability of 0.5 with a range of 0.0 to 1.0.

19.11.4.1.4.3.4 **Quantification**

The quantification of the Figure 19.11.4.1.4-1 supporting logic model is presented in Table 19.11.4.1.4-1.

This section intentionally ~~left~~ blank.

19.11.4.1.4.3.5 Significance to System 80+

A review of the System 80+ reactor cavity and lower head design suggests that this failure mechanism is not viable for the this plant design. This conclusion is based on the fact that (1) the RV lower head failure mode will be predominately governed by instrument tube failures or modest creep RV failures and (2) the likelihood for transients with a cycling relief valve at the onset of core damage, that the RV will depressurize well below 1000 psia prior to VB was very high.

19.11.4.1.4.3.6 Application to the System 80+ PRA

For completeness the rocket failure mode will be included in the supporting logic model for the System 80+ PRA with a corresponding probability based on Table 19.11.4.1.4-1. For purposes of quantification the RV rocket failure probability was artificially increased to .0001 for PDSs initially at high pressure and .00001 for PDSs initially at intermediate pressures.

19.11.4.1.4.4 Synergistic Issues

Many early containment failure mechanisms are a result of several containment threatening processes occurring simultaneously. For the System 80+ PRA synergistic effects are typically considered under the umbrella of Direct Containment Heating (See Section 19.11.4.1.1).

Synergism between the hydrogen burn and steaming following VB can be established by estimating Hydrogen burn pressures at the uppermost de-inerted steam pressure (see Section 19.11.4.1.3).

Missile threats to the containment are considered under the phenomenological source of the missile. For example missiles generated by hydrogen burns / detonations, IVSE and EVSE are considered within their respective phenomenological section.

19.11.4.1.4.5 Loss of Containment Isolation Prior to Core Melt

19.11.4.1.4.5.1 Description of the Phenomena

During power operation, the containment is required to be closed. However, in rare instances procedures may be violated or common cause valve failures may result in loss of containment isolation during plant operation. Severe accidents initiated from this condition progress in the presence of a compromised final fission product barrier and may release considerable quantities of fission products early into the environment.

radionuclide releases are relatively low), the operation of containment heat removal using containment sprays will ultimately condense the containment steam, and cool the containment atmosphere. Since the containment has a smaller and cooler non condensible gas component, a partial vacuum is created within the containment. This vacuum, while not indefinite, can retain fission products without any leakage into the environment for about 48 hours depending on the initial scenario (see also Section 19.11.5).

19.11.4.1.4.6 Containment Bypass

19.11.4.1.4.6.1 Description of the Phenomena

NUREG-11 (Reference 142) identified containment bypass as an important contributor to the large, early releases of radionuclides for the Zion and Surry PWRs. The principal contributors to these severe accidents are steam generator tube ruptures (SGTRs) with stuck open MSSVs or ADVs and interfacing-system LOCAs (ISLOCAs). Should these events progress into severe accidents, the radiation releases to the environment would be large and energetic and would pose a significant radiation exposure to the general public.

19.11.4.1.4.6.2 Significance to System 80+

19.11.4.1.4.6.2.1 ISLOCAs

Very small.

The core damage frequency associated with System 80+ intersystem LOCA failures is estimated to be about 3×10^{-8} per reactor year. The low probability of these events is associated with the fact that the System 80+ design incorporated much of the EPRI URD guidance in designing to limit ISLOCAs. In particular, much of the connecting piping for the RCS has been designed to meet the ultimate rupture strength criteria required in SECY-90-016 and considerable piping that was previously routed outside of containment is now within the containment envelop. To further reduce the possibility of ISLOCA, interfaces between the RCS and connecting systems include, as appropriate, design features to leak test valves, indicate valve position and alarm high pressure in low pressure lines.

A detailed investigation of the sources of ISLOCAs has been reported to NRC in Reference 145. This report investigated the source of potential ISLOCAs from the System 80+

- Safety Injection System
- Shutdown Cooling System
- Chemical and Volume Control System
- Process Sampling System

19.11.4.1.4.6.3 Application to the PRA

19.11.4.1.4.6.3.1 ISLOCAs

The dominant ISLOCA sequence involves the combined failure c check and isolation valves in the RHR line resulting in catastrophic failure of this line outside of containment. Th ISLOCA will typically deposit RCS inventory into a watertight ar of the auxiliary building. Sufficient RCS inventory will be lo to the auxiliary building prior to substantial core damage so th the ISLOCA break location will be covered by several feet of wate This water will serve to scrub fission product releases from t ruptured safety injection pipe prior to entering the environmen The PRA assumes a decontamination factor consistent with the po scrubbing correlations developed by Powers (Reference 192).

19.11.4.1.4.6.3.2 SGTR

The PRA considers SGTRs due to both SGTR initiating events a thermally induced SGTRs. The consequences of SGTR events resulti from an initial SGTR will be established based on details of t plant damage state (PDS) prior to core damage. Induced SGTRs c only occur when the RCS is at the CRV setpoint with the SG tub uncovered and water inventory in the steam generator. Induced SG would represent ~~less than 0.2%~~ a very small fraction of the PDSs and was therefore n explicitly considered in the baseline PRA.

This table intentionally left blank

TABLE 19.11.4.1.4-1

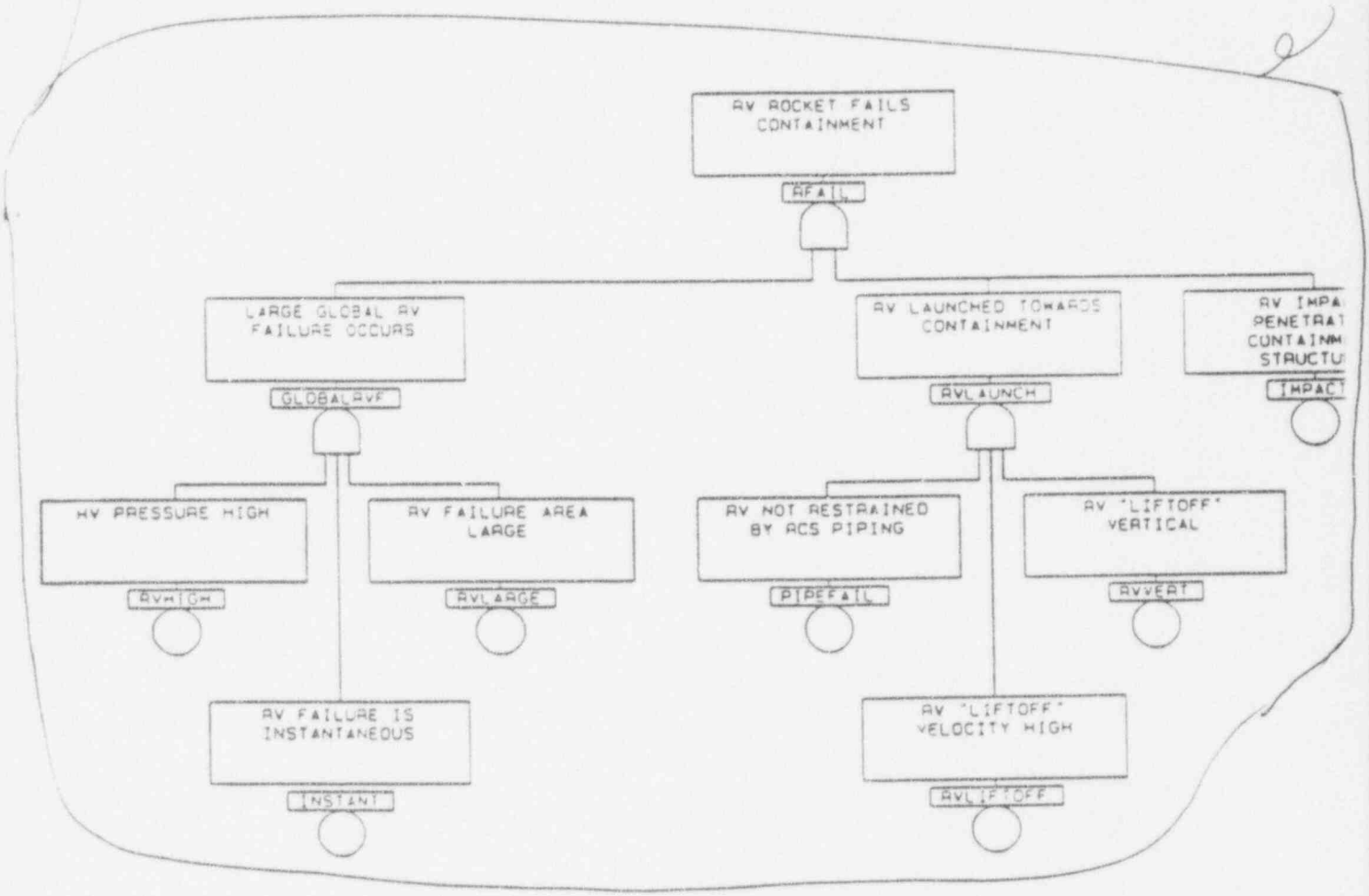
ROCKET INDUCED FAILURE PROBABILITY FOR HIGH AND INTERMEDIATE PRESSURE SEQUENCES

Probability	HP Plant Damage State	IP Plant Damage State
P_{HP}	0.10	0.87
P_{RVSIZE}	0.013	0.001
$P_{INSTANT}$	0.50	0.50
$P_{RESTRAINED}$	0.002	0.0002
P_{KE}	0.50	0.50
P_{FAIL}	$6.5X10^{-7}$	$4.35X10^{-8}$

This table intentionally blank.

FIGURE 19.11.4.1.4-2

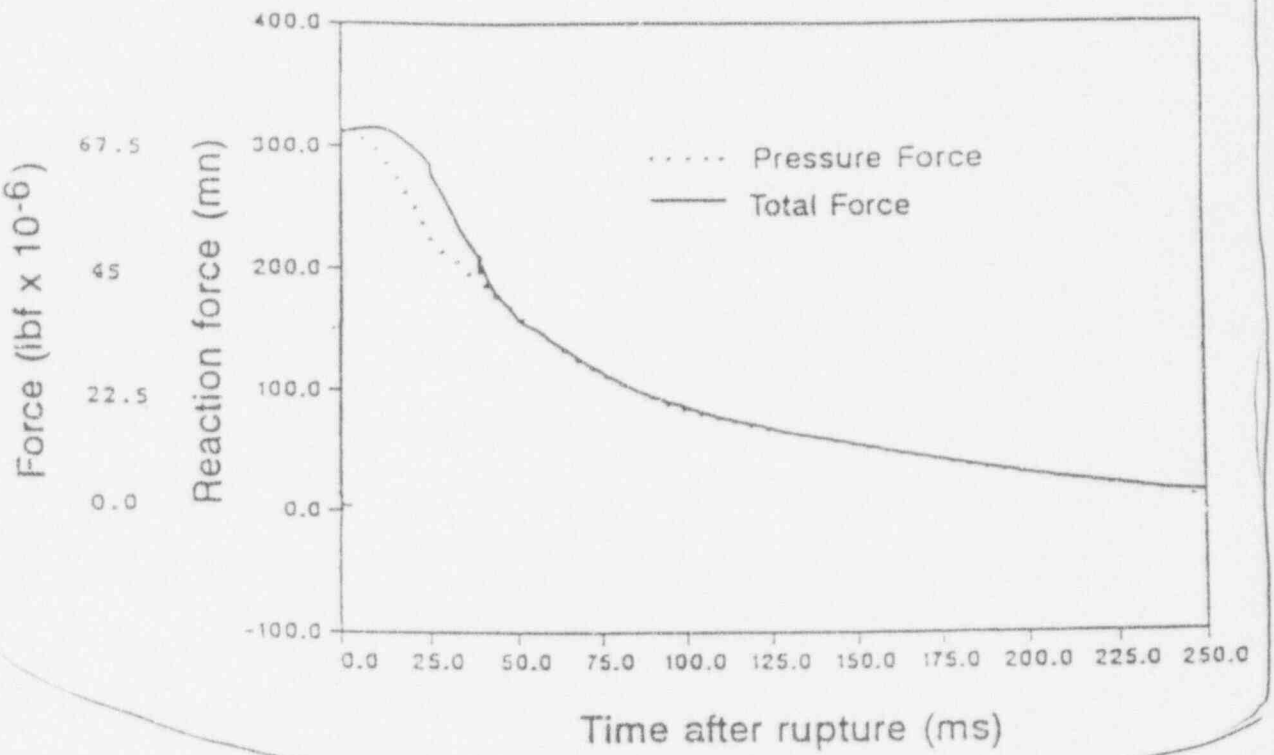
SUPPORTING LOGIC MODEL FOR ROCKET INDUCED CONTAINMENT FAILURE



This figure intentionally blank.

FIGURE 19.11.4.1.4-3

RV LOADING DUE TO INSTANTANEOUS DECOMPRESSION OF A GERMAN-PWR



19.11.4.2.1.1 Steam Overpressurization

19.11.4.2.1.1.1 Description of the Phenomena

19.11.4.2.1.1.1.1 Containment Failure Before Vessel Brea

This category of containment failure arises when the containm heat removal function is irrecoverably lost and cooling of the with a breach (either due to pipe rupture or open SDS Valve) facilitated. Containment failure prior to VB is calculated to h a probability of below 1 x 10^{-7} per reactor year.

The probability of

yes

be negligible

Scenario 1: Containment Failure with SDS Valve discharge into IRWST

This scenario consists of an extended total loss of feedwater ev (TLOFW) where Feed and Bleed core heat removal is successful containment heat removal is unavailable due to failure containment spray heat exchangers. In this transient the SI pu will inject IRWST inventory into the RCS and the RCS dischar steam generated in the cooling process into the IRWST. The outc of the once-thru-core-cooling (OTCC) process is to maintain c temperatures at acceptable levels so long as makeup inventory available. Once the IRWST reaches saturation, steam produced the IRWST will be discharged into and pressurize the containme Without restoration of containment heat removal function, containment will fail and the IRWST liquid will flash, causing SI pumps to cavitate. Without restoration of primary side invent control, the core will slowly uncover and begin to melt.

Scenario 2: Containment Failure Following Primary Side P Ruptures

In this scenario a large RCS primary side pipe rupture occurs wh allows the discharge of superheated and saturated steam direc into the containment. Core heat removal, if available, w typically involve steaming of the corium debris and pressurizat of the containment. In this scenario however, the RCS discharge deposited into the containment directly. Thus, the IRWST is o heated via the collection of condensed steam. This scenario w result in a containment damaging condition in advance of reach saturation conditions in the IRWST. Thus, containm depressurization is not expected to result in flashing of the IR water and therefore core heat removal will continue until the IR is depleted.

19.11.4.2.1.1.1.2 Containment Failure Following Vessel Bre

System 80+ employs a unique cavity design to trap corium debris the reactor cavity (See Section 19.11.3.6) and a manually actua cavity flooding system to arrest corium-concrete attack and c

in the containment will be reduced from about 65 hours to between 40 and 48 hours following core uncovery.

19.11.4.2.1.2.4 Application to the PRA

The System 80+ PRA differentiates between containment overpressure failure due to primarily steam addition and that caused by a combination of steam and non-condensible sources. Scenarios of concern to containment failure involve severe accidents with both concrete attack and no containment heat removal with limited available water sources. These transients typically result in containment pressures under 120 psia. The probability of an overpressurization containment failure due to these sequences is ~~less than .02~~ small. Thus, failure represents a race between various modes of containment failure. Containment overpressure failure caused primarily by non-condensible gas evolution is not considered a serious containment threat.

For the condition that significant CCI occurs in the presence of a full cavity, but without containment heat removal two containment failure outcomes are possible. These are that CCI fails the basement (See Section 19.11.4.2.3) or that the containment fails by overpressurization. The later is believed to be more likely and of greater safety significance. The likelihood of a basemat containment failure in the presence of significant water is considered highly unlikely (probability less than .01). Containment failure due to overpressurization will occur and the time frame of the failure will be in the 40 to 60 hour time interval following core uncovery.

Basemat erosion can theoretically undermine the cavity wall foundation and cause a subsequent collapse. This situation was studied in the Grand Gulf PRA (see NUREG-1150, Reference 182). The potential for basemat erosion to cause a failure of System 80+ cavity wall has been structurally evaluated and is considered remote. This is a consequence of several System 80+ cavity design features. First, the sloping character of the debris trap confines the corium radial attack away from a major supporting wall. Second, structural analyses of the System 80+ reactor cavity shows that the reactor vessel and upper cavity load can be supported without any structural contribution of the lower cavity walls below the 73 foot elevation. Thus, even the remote possibility of cavity collapse, containment integrity will not be compromised.

19.11.4.2.2.5 Application to the PRA

In the preliminary version of the System 80+ PRA (Reference 146), it was explicitly assumed that as a consequence of the cavity design, the availability and actuation of the CFS was sufficient to prevent a basemat melt-through scenario. While there is general agreement that water will retard the corium progression into the concrete basemat, there is not yet conclusive proof that a deep accumulation of corium will be fully coolable by an overlying water pool. It is expected that the ongoing MACE (Melt/Debris and Coolability Experiment) program will correct the test shortcomings and shortly provide this information to confirm the existing PRA position. Until that time, future PRA assessments of System 80+ will allow for the potential for basemat failure in the presence of large quantities of water.

Based on a review of Sandia and EPRI debris coolability experiments, it was concluded that the median stable corium-water heat flux was about 0.5 Mw/m^2 (with an uncertainty of about .2 Mwt/m^2) provided that the corium crust and the molten material do not separate. As discussed above, the probability of the low heat fluxes observed in the MACE experiments are not considered prototypical. The likelihood that the corium-water heat transfer is below 0.10 Mw/m2 (preventing corium quench and causing ultimate basemat failure) is taken to be 0.01. It should be noted that while these low heat transfer sequences may progress to basemat melt-through, they will do so very slowly and in a well scrubbed environment. Detailed CCI modeling is discussed in Section 19.12.

Dry cavity melt-through scenarios can occur if the CFS is disabled or not actuated. Dry cavity sequences comprise 8.3% of the System 80+ PDSs. These sequences can result in:

1. basemat melt-through to the containment subsoil

2. corium penetration into the subsphere

3. corium erosion of cavity wall concrete, causing an induced containment failure

For purposes of the PRA radiological release calculations basemat melt-through scenarios into the containment subsoil, will be assigned a benign fission product release classification (See Section 19.11.4.3). Failures into the subsphere or reactor cavity wall failures will be considered as potential atmospheric releases. Detailed computer simulations of basemat erosion process indicate that radial penetration of corium into the SI room is highly unlikely. The probability of radial penetration into the SI room is conservatively defined as 0.05. Similarly, structural analyses indicate that complete cavity wall erosion will not cause a failure of RV to be supported. Consequently, no induced above ground containment failure is anticipated. For completeness this failure mode is retained for this analysis and is quantified with a conditional probability of 0.01.

Small

hydrogen combustion event at pressures just below the steam inerting limit. Because of the large amount of steam and carbon dioxide initially available, the combustion event is far more likely to be a deflagration than a detonation. According to the NRC Final SER on the URD (Reference 161), the late hydrogen burn issue can be addressed by considering combustion of the hydrogen equivalent of 100% oxidation of the RCS zirconium. Results of analyses presented in this section indicate that pressures generated during this event will be below the containment Service Level C and are well below the ultimate containment failure pressure.

19.11.4.2.4.2 Significance to System 80+

As discussed in Section 19.11.4.1, System 80+ is equipped with igniters to burn off steam at low concentrations. These igniters have been demonstrated effective in steam environments and therefore, when actuated early in the transient they should fully eliminate any significant hydrogen induced containment threat.

In the event that a significant accumulation of combustible gases develop without the occurrence of early smaller burns, a single large burn corresponding to the ignition of the hydrogen equivalent of 100% oxidation of the zircaloy active cladding, initiated at a system pressure just below the inerting containment steam concentration , will produce an AICC burn pressure of below 103 psia (See Section 19.11.4.1.3). Burns in this range pose a small, but finite threat to containment integrity.

19.11.4.2.4.3 Application to the PRA

A delayed hydrogen burn capable of threatening containment are considered credible only if no previous burns have been assumed. The presence of early burns via deflagration or diffusion flames is assumed to consume sufficient hydrogen to make a large containment threatening burn impossible. In the PRA this implies that early operator actuation of the hydrogen igniters will prevent a late containment threatening burn.

Since quenching of the corium debris will produce hydrogen, as will the concrete attack process, the potential for a high level of hydrogen is assumed.

For purposes of PRA quantification, situations where the igniters are actuated early during the uncovery sequence and operated continuously, the probability of a containment threatening hydrogen burn was considered to be 0.0.

For scenarios where igniters were not actuated and no prior burns occurred, the probability of a late containment burn was taken to be 1.0. The zircaloy oxidation level and pressure peak associated with the resultant burn was established for conditions with and

19.11.4.3.2 Advanced Source Term

The System 80+ fission product representation is based on features associated with the advanced source term (Reference 168). The phenomenological features of the advanced source term are highlighted below and discussed with reference to S80SOR and MAAP. Additional details on the application of the advanced source term methodology to the Level 3 (consequence) evaluation is presented in Chapter 19.12.

This section provides the phenomenological background supporting assumptions employed in defining the source term environment releases used in the System 80+ MACCS 1.5 consequence evaluation. In this presentation the fission product source term release has been divided into discussions on fission product release (including RCS transport and revaporization) and "in containment" deposition process. In establishing S80SOR source terms the general recommendations associated with the Reference 168 have been adopted, with a limited number of System 80+ specific additions and modifications. System 80+ MAAP analyses including advanced fission product release, transport and deposition models were used to provide confirmation of S80SOR release class predictions (see Section 19.12).

19.11.4.3.2.1 Fission Product Release

19.11.4.3.2.1.1 Fission product Release from the Core

19.11.4.3.2.1.1.1 Application to S80SOR Predictions

Fission product release from the core has been evaluated by Brookhaven based on data from fuel meltdown experiments and the NRC NUREG-1150 Source Term Code Package (STCP) predictions (Reference 198). This evaluation provided expected inventory release fractions for a molten core (FCOR) for use in an XSOR type code package.

In the BNL/NUREG-1150 assessment, the core fission product releases were subdivided into nine fission product release groups (See Table 19.11.4.3.2-1) and the releases were subdivided into two physical categories: releases with low core-wide zircaloy oxidation and with high core-wide zircaloy oxidation. Mean and median fractional releases are summarized in Table 19.11.4.3.2-2. The high and low oxidation categories were observed to have a marginal impact on fission product releases in the noble gas, iodine and cesium groups. A noticeable impact was noted for the elements Te, Sr, Ba, and Ru. These FCOR factors are considered applicable to System 80+ and were therefore used as input to the S80SOR FCOR input matrix.

19.11.4.3.3 Significance of DF Modeling to System 80+

System 80+ is designed to minimize fission product release to the containment atmosphere by passing all discharges from the pressurizer safety valves and RDS valves through piping submerged into a subcooled IRWST water pool. The effectiveness of fission product removal via overlying water pools can be significant. The Reactor Safety Study (WASH-1400) assumed the equivalent decontamination factor (DF) for a subcooled water pool to be 100, while saturated water pools were not credited for decontamination. More recent experimental evidence suggests that pool DFs can be larger for subcooled pools and that saturated pools (with lower DFs) can also significantly contribute to decontamination.

The cavity flooding system is also allowed to direct the IRWST liquid into the cavity to submerge, and cool the corium debris and scrub fission product releases should they occur.

The containment spray system is intended to both cool the containment atmosphere and scrub the atmosphere of fission products. This system has been designed to be highly reliable since it serves the combined heat removal function of the fan cooler/containment spray system of conventional PWRs. Sprays have been demonstrated to be highly effective in scrubbing particulate fission products and elemental iodine from the containment atmosphere.

In System 80+, pool scrubbing of fission products as assumed in the reactor cavity (Post VB) during CCI and for all IRWST discharges. Spray decontamination is also explicitly considered for System 80+.

19.11.4.3.4 Application to the PRA

The PRA estimates of the environmental releases from the containment based on a combination of MAAP calculations and S80SOR assessments. MAAP models approximately incorporate all the above fission product release, retention and atmospheric depletion processes (with the exception of releases during DCH, which are not currently modeled but will play little role in System 80+). This information is used to adjust S80SOR predictions. System 80+ S80SOR airborne concentrations are applied to MACCS 1.5 and population dose estimates are established (see Section 19.13).

19.11.4.3.5 Summary

In order to provide a realistic and comprehensive source term estimate for System 80+, the simplified XSOR approach adopted by NRC contractors for Reference Plant consequence analysis was modified and applied to System 80+ as S80SOR. Use of the S80SOR codes in establishing fission product releases provides a scrutable means of evaluating source terms and allows rapid source term evaluations for a large number of release classes. For the System 80+ PRA, approximately 40 release classes passed the final screening.

As was previously discussed, the role of MAAP in this arena was primarily to (1) provide information with regard to source term energetics and release timings, and (2) provide a deterministic basis for comparing S80SOR predictions. Additional discussion on the consequence analysis is presented in Section 19.13.

19.11.4.4.1.1.3 Reactivity Control

Since core recovery may occur with a nearly intact core geometry, it is important that the core be prevented from achieving criticality. A return to criticality under these circumstances will likely strain the meager plant inventory and heat removal capabilities and compromise the establishment of a safe stable state. Reactivity control is provided by insertion of control rods and assuring the delivery of sufficiently borated water into the RCS. Reactivity control is typically assured early in the transient via insertion of control rods.

19.11.4.4.1.1.4 Containment Integrity

Containment integrity is necessary to prevent significant radioactivity releases to the environment. Given that the highly reliable containment isolation systems function, containment integrity for the System 80+ containment requires that pressure and temperature challenges within the containment have a low probability of causing containment failure. If partial operation of one train of containment sprays can be guaranteed, most containment threats can be averted. If sprays are non-functional for an "in-vessel" recoverable sequence and the RCS continues to reject heat to the containment, containment failure cannot be averted unless the containment heat removal function is restored. For "in vessel" recoverable sequences with sprays available, the only containment threat is that associated with hydrogen combustion. Analyses show that even under these adverse circumstances the conditional containment failure threat associated with hydrogen combustion is ~~less than 0.01~~ very small.

19.11.4.4.1.2 Instrumentation / Equipment Requirements in Support of "In-Vessel" Recovery

To enable the operator to have the opportunity to maneuver the plant from a core damage state to a safe stable state where the core is indefinitely retained "in-vessel", the operating staff requires the use of a set of vital equipment and key instruments. The vital equipment is necessary to ensure that adequate inventory and heat removal can be provided to the RCS, reactivity control is maintained and that containment heat removal via sprays is

B. Vent to Containment Annulus

System 80+ has two 3-inch pipes from the hydrogen recombiner system which can be used to vent to the containment annulus from the control room. This vent size has the potential to maintain containment pressure in the vicinity of 100 psia. This is not a desired mode of pressure control since it is associated with considerable releases of fission products. However, should internal and external sprays be unavailable, a last means of prolonging containment integrity and controlling the fission product release will be to open these vents. Containment venting can also be used in conjunction with external spray to both extend containment integrity and mitigate the vent fission product release.

19.11.4.4.2.3 Summary

As is identified in the PRA, System 80+ has been designed so that the probability of the plant experiencing a severe accident is remote, (less than three in one million). The AMG for System 80+ is intended to aid the plant operating staff to cope with these beyond design basis events, should they occur. The functional approach inherent in the ABB-CE emergency procedures allows the basic EOG to be the foundation for the "in-vessel" aspects of the AMG. This guidance has been further supplemented by Severe Accident Management guidance associated with the EOG. Actions discussed in this section for responding to an "Ex-vessel" condition are directed at maintaining containment integrity and minimizing fission product releases.

19.11.5.4 Transient Analyses

The analyses selected for presentation in this section were chosen to provide a fundamental understanding of the System 80+ transient response under various severe accident scenarios. Sequences with relatively larger frequencies and which result in relatively larger contribution to the radiological releases were selected for illustration purposes. These include station blackout scenarios, large break LOCAs, small break LOCAs, total loss of feedwater scenarios, steam generator tube ruptures and the V sequence.

19.11.5.4.1 Station Blackout Sequences

The station blackout (SBO) sequences consist of a total loss of all AC power, including those from emergency diesel generators and the alternate combustion turbine/generator. The only power that may be available is the station battery power. Only one of the SBO sequences presented here assumes availability of battery power. The Cavity Flooding System may also be assumed to be either operational or not operational. Three cases are presented: Case 1 considers an SBO sequence with a flooded cavity (wet cavity) and no battery power; Case 2 deals with an SBO sequence with no cavity flooding (dry cavity) and no battery power; and Case 3 is an SBO with battery power available and cavity flooding (wet cavity).

The frequency for SBOs without batteries initially available are below the PRA cutoff frequency of 10^{-9}. The battery depletion SBO has an expected frequency of 3.20×10^{-8}.

19.11.5.4.1.1 Station Blackout Sequence with Battery Power Unavailable and Cavity Flood System Actuated

This station blackout sequence consists of a loss of all AC power. Station batteries are assumed unavailable during this accident scenario. It is also assumed that the operator floods the reactor cavity prior to vessel breach to ensure debris quenching and debris coolability following a potential failure of the RV lower head. The unavailability of containment heat removal results in an overpressure containment failure more than 60 hours after the initial Loss of Offsite Power (LOOP) condition. This transient is designated as LOOP-9E in the PRA ~~(Section 19.12)~~.

19.11.5.4.1.1.1 Dynamic Response

In this SBO scenario the loss of all AC power causes the control rods to drop into the core terminating the nuclear chain reaction. Since batteries are assumed unavailable, effective core cooling as well as RCS pressure and inventory control cannot be achieved.

It is expected that the operator will actuate the cavity flood system prior to vessel breach. The large floor area available for spreading the corium within the cavity results in a high confidence that the corium remaining within the cavity will be quenched. (For these analyses the corium heat removal rate at the upper corium surface is limited to about 35% of the Zuber pool boiling heat flux.) Thus, the primary containment threat under these conditions becomes the gradual overpressurization of the containment due to vaporization of the water covering the corium. In the absence of containment heat removal, the steam will continue to gradually heat up and pressurize the containment atmosphere to the point of containment failure. Based on MAAP analyses of the containment pressure response the time required for the containment atmosphere to reach ASME Service Level C Limits will be about 60 hrs from the onset of the SBO (See Figure 19.11.5.4.1.1-3). Containment temperature variation during this heatup process is illustrated in Figure 19.11.5.4.1.1-4. As can be seen containment temperatures are generally below the levels at which rapid degradation of the penetration sealant would be induced.

Figure 19.11.5.4.1.1-5 shows the basemat erosion for this sequence. Due to timely flooding of the cavity which quenches the corium, the basemat erosion is seen to be relatively small.

19.11.5.4.1.1.3 Fission Product Releases

A summary of fission product releases is provided in Table 19.11.5.4.1.1-3.

19.11.5.4.1.2 Station Blackout Sequence with Battery Power Unavailable and Cavity Flood System Unavailable

This station blackout sequence consists of a loss of all AC power with the station batteries assumed unavailable. It is also assumed that the operator fails to actuate the CFS and RV failure occurs in the presence of a dry cavity. Plant RCS responses for this transient are the same as those presented in Section 19.11.5.4.1.1.1. This transient is designated as LOOP-9F ~~(See Section 19.12)~~.

RV head failure occurs at about 3.5 hours. Initially, the RV lower head failure results in the deposition of a limited water mass into the reactor cavity. The sources of this inventory are the residual lower plenum liquid and the SIT inventory. The cavity remains wet and the debris is cool until the time of cavity dryout, about 10 hours (See Figure 19.11.5.4.1.2-1).

A summary of MAAP predicted sequence of key events and timing is provided in Table 19.11.5.4.1.2-1. A summary of key parameters and a summary of fission product group concentrations are

19.11.5.4.1.3 Station Blackout Sequence with Battery Power Available and Cavity Flood System Actuated

For this sequence, subsequent to a loss of all AC power, the station battery power is assumed to be available for up to 8 hours. During this time period battery power is primarily directed towards maintaining auxiliary feedwater flow to the steam generators. Prior to battery depletion, the operator is assumed to flood the reactor cavity to ensure debris quenching following a potential failure of the RV lower head. Subsequent to battery depletion, due to the assumed unavailability of containment heat removal, an overpressure containment failure is predicted to occur after 80 hours. This sequence is designated as SBOBD-E in the PRA (~~See Section 19.12~~).

19.11.5.4.1.3.1 Primary and Secondary System Response

This SBO scenario results in the unavailability of all engineered safety features systems with the exception of the auxiliary feedwater (AFW) system which is powered by a steam turbine and electrically controlled via inverters. As a result of core heat removal via the steam generators, the RCS pressure is maintained below 2250 psia during the time period of auxiliary feedwater availability (see Figure 19.11.5.4.1.3-1). Approximately ten hours into the event (almost two hours after all AFW is lost), the steam generators (SGs) dry out and heat removal from the RCS via the SGs is lost (see Figure 19.11.5.4.1.3-3). Loss of heat removal results in a repressurization of the RCS to the PSV setpoint pressure (see Figure 19.11.5.4.1.3-1). The PSVs cycle open and close to remove the decay heat from the RCS. The cycling of the PSVs without RCS makeup results in sustained loss of RCS inventory and incipient core uncovery at about 15 hours (see Figure 19.11.5.4.1.3-2). Without any engineered safeguards operational, the fuel rapidly heats up, melts, relocates to the lower plenum and fails the lower head of the reactor vessel (RV). As before, the RV failure mechanism is assumed to be a failure of a single lower head penetration initially, opening an initial 0.052 ft. radius hole in RV lower head.

A summary of the MAAP predicted sequence of key events and their timings is provided in Table 19.11.5.4.1.3-1. Additionally, a summary of key parameters and a summary of fission product group concentration are provided in Tables 19.11.5.4.1.3-2 and 19.11.5.4.1.3-3, respectively.

19.11.5.4.1.3.2 Containment Performance

The containment performance during this SBO sequence demonstrates the passive plant capabilities of System 80+ under best-estimate conditions. The lower compartment pressure and temperature variation for this event are presented in Figures 19.11.5.4.1.3-4

For this specific scenario, the secondary side of the steam generator remains full of liquid inventory (Figures 19.11.5.4.2.1-3 and -4). The broken SG then serves as a heat source and transfers small amounts of energy to the primary side steam. The unbroken SG serves as a heat sink where plated out fission products keep the SG at its safety relief setpoint.

19.11.5.4.2.1.2 Containment Response

Core concrete attack initiates at reactor vessel failure. In this analysis, the CFS is assumed to be actuated prior to vessel failure. The interaction of the molten corium and cavity water raises the containment pressure in a steady, linear manner until a peak of 156 psia at just under 60 hours after the break. Containment pressure and temperature responses are presented in Figures 19.11.5.4.2.1-5 and 19.11.5.4.2.1-6, respectively.

Core concrete interaction (CCI) initially occurs at RV failure and continues for several hours. The maximum concrete erosion depth is 0.25 ft.

19.11.5.4.2.1.3 Fission Product Releases

A summary of fission product releases is presented in Table 19.11.5.4.2.1-3.

19.11.5.4.2.2 Large Break LOCA with Dry Cavity

In this scenario, the operator fails to actuate the cavity flooding system and reactor vessel failure occurs in the presence of a dry cavity. A summary of event timings is shown in Table 19.11.5.4.2.2-1 and selected parameter values are provided in Table 19.11.5.4.2.2-2. The frequency of occurrence for this event is 1.36×10^{-11}/year (approximately 2 orders of magnitude below the PRA screening criteria).

19.11.5.4.2.2.1 Primary and Secondary System Response

The reactor vessel response is the same as that described for the large LOCA event in Section 19.11.5.4.2.1.1.

19.11.5.4.2.2.2 Containment Response

The interaction of the molten corium and cavity water raises the containment pressure in a monotonic manner. The containment pressure and temperature at 80 hours are 68 psia (Figure 19.11.5.4.2.2-1) and 380 °F (Figure 19.11.5.4.2.2-2), respectively. Spikes in the pressure trace correspond to burns precipitated by either hydrogen igniters or hydrogen combustion in the vicinity of the hot core debris.

19.11.5.4.2 Large Break LOCA

This sequence consists of a smaller large cold leg break (0.5 ft^2) coupled with a failure of the containment sprays, as well as unavailability of HPSI, LPSI, and charging pump flows. The cavity flooding system (CFS) is operational to flood the reactor cavity in the first transient analyzed but is unavailable in the second. Both large LOCA transients discussed in this section had occurrence frequencies below the PRA cutoff frequency of 10^{-9}. These sequences are designated as LL-3E and LL-3F ~~in Section 19.12~~, respectively.

19.11.5.4.2.1 Large Break LOCA with Wet Cavity

The initiating large LOCA involves a rapid depressurization of the primary system along with a rapid drop in reactor vessel water level. Water inventory is rapidly depleted from the RCS and as a result of the addition of accumulator water at 650 psia, a two phase level develops just above the top of the active core. In this scenario, the operator actuates the cavity flood system prior to vessel breach. Active engineered safeguards are unavailable with the exception of auxiliary feedwater. Coolant is quickly lost out the break and the core uncovers after 0.5 hour. Significant clad oxidation occurs following core uncovery followed by core melt and then reactor vessel failure occurring at 1.7 hours. A summary of event timings is shown in Table 19.11.5.4.2.1-1 and selected parameter values are provided in Table 19.11.5.4.2.1-2. ~~The frequency of occurrence for this event is 1.33×10^{-10}/year~~.

19.11.5.4.2.1.1 Primary and Secondary System Response

In this transient, a 0.5 ft^2 LOCA develops at time 0.0. The system rapidly depressurizes to under 50 psia (Figure 19.11.5.4.2.1-1). Accumulators discharge as the pressure falls below the accumulator setpoint of about 650 psia and are empty at 781 seconds.

The response of the RV level to this event is presented in Figure 19.11.5.4.2.1-2. MAAP predicts the two phase level to rapidly fall to near the top of the core. Discharge of the SITs temporarily replenishes vessel inventory. A sustained core uncovery ultimately occurs at about 0.5 hours into the event.

Core uncovery is followed by rapid zircaloy-water oxidation. The fuel is predicted to rapidly heat up and melt. Support plate failure is predicted to occur at 6100 seconds and RV lower head failure occurs shortly thereafter.

Concrete attack is predicted to be monotonically increasing throughout the event and reaches 100 inches of basemat at the analysis end time of 80 hours (Figure 19.11.5.4.2.2-3). Extrapolating the erosion predictions suggests a basemat melt-through into the extended foundation will occur in about 8 days.

19.11.5.4.2.2.3 Fission Product Releases

A summary of fission product releases is presented in Table 19.11.5.4.2.2-3.

19.11.5.4.3 Small Break LOCA

The accident initiator is a small LOCA (0.02 ft^2) coupled with the unavailability of safety injection. Containment sprays as well as auxiliary feedwater are assumed to be available. The cavity flooding system (CFS) is operational to reflood the core in the first transient analyzed but is unavailable in the second. The dry cavity small LOCA transient discussed in Section 19.11.5.4.3.2 had an occurrence frequency below the PRA cutoff frequency ~~of 10^{-9}~~. These sequences are designated as SL-11E and 11F ~~in Section 19.1~~2.

19.11.5.4.3.1 Small Break LOCA with Wet Cavity

This sequence is initiated by a small (0.02 ft^2) cold leg break. In this scenario, the operator actuates the cavity flood system prior to vessel breach. Loss of cooling water inventory drops the primary system pressure to the low pressurizer pressure reactor trip setpoint and scrams the reactor at 19.7 seconds. Main feedwater is automatically run back upon reactor trip to match the reactor power. Emergency core cooling water is unavailable, creating rapid boil-off of coolant inventory resulting in core uncovery at 1.06 hours. Zirconium oxidation begins shortly thereafter and rises dramatically at 1.5 hours resulting in 1718 pounds of hydrogen produced in the vessel prior to vessel breach. The fuel heats up and slumps into the lower head, with reactor vessel failure occurring at 3.2 hours. A summary of event timings is shown in Table 19.11.5.4.3.1-1 and selected parameter values are provided in Table 19.11.5.4.3.1-2. ~~The frequency of occurrence for this event is 1.49×10^{-7}/year.~~

19.11.5.4.3.1.1 Primary and Secondary System Response

After the initiation of the event, the system depressurizes to the SIT pressure setpoint. Here the introduction of SIT water helps the core to maintain pressure (Figure 19.11.5.4.3.1-1) at 500 psia and two phase level (Figure 19.11.5.4.3.1-2) at around 13.5 ft. Initial core uncovery is at 1.06 hours. The core is partially recovered by SIT injection.

Core uncovery is followed by rapid zircaloy-water oxidation. The fuel is predicted to rapidly heat up and melt. Support plate failure is predicted to occur at 3.2 hours and RV lower head failure occurs shortly thereafter.

The secondary side of the steam generators remain full of liquid inventory (Figures 19.11.5.4.3.1-3 and -4). The broken SG cycles between the secondary side valve setpoint of 1200 psia and 900 psia (Figure 19.11.5.4.3.1.5) while the unbroken SG cycles in a very tight band about the relief valve setpoint (Figure 19.11.5.4.3.1-6).

19.11.5.4.3.1.2 Containment Response

Containment sprays are actuated shortly after initiation of the transient when the containment pressure reaches the actuation setpoint. The IRWST initially is observed to drop in level as CFS is actuated and the IRWST water is sent to the holdup volume and reactor cavity. The IRWST level subsequently rises as RCS inventory is condensed and returned to the IRWST. A final surge in the IRWST level occurs at vessel breach when the SITs discharge the remainder of their inventory into the reactor cavity. The IRWST reaches an equilibrium level at after vessel failure (Figure 19.11.5.4.3.1-7).

Containment spray operation maintains a peak pressure of less than 20 psia in containment. Basemat erosion in the cavity is predicted to be negligible as is hydrogen production.

19.11.5.4.3.1.3 Fission Product Releases

A summary of fission product releases is presented in Table 19.11.5.4.3.1-3.

19.11.5.4.3.2 Small Break LOCA with Dry Cavity

In this scenario, the operator fails to actuate the cavity flooding system. A summary of event timings is shown in Table 19.11.5.4.3.2-1 and selected parameter values are provided in Table 19.11.5.4.3.2-2. ~~The frequency of occurrence for this event is 4.4×10^{-10}/year.~~

19.11.5.4.3.2.1 Primary and Secondary System Response

The reactor vessel response is the same as that for the wet cavity of 19.11.5.4.3.1.

19.11.5.4.5.2 Containment Performance

The PSV discharge is ducted via the pressurizer pressure relief piping into the IRWST. The discharge of steam into the IRWST heats up the IRWST water. Subsequent to vessel breach the containment atmosphere heats up and is pressurized due to the release of steam and corium from the reactor vessel (see Figure 19.11.5.4.5.1-4). The containment continues to be pressurized due to generation of steam within the cavity. This pressurization is terminated at about 3 hours when containment sprays are actuated on high containment pressure. Subsequently the containment pressure and temperature decrease to their initial value (see Figures 19.11.5.4.5.1-4 and 19.11.5.4.5.1-5). Figure 19.11.5.4.5.1-6 shows that the cavity basemat erosion is insignificant (less than 1 inch) during this transient. This is due to adequate quenching of the core debris in the reactor cavity.

19.11.5.4.5.3 Fission Product Releases

A summary of fission product group concentrations in the containment atmosphere at 24 hours after vessel breach is provided in Table 19.11.5.4.5.1-3.

19.11.5.4.6 V Sequence

The dominant System 80+ V Sequence consists of an intersystem LOCA (ISL) initiated from a full shear break in the 16 " diameter SCS line occurring within the containment building subsphere. ~~The cumulative release frequency for all V-sequence events is less than 5.1×10^{-10} per year~~. This event is identified in the PRA as PDS 17.

In this event all ECCS systems are operable. The failure of the SCS pipe outside of containment results in a gradual transfer of ECCS inventory from the containment to the subsphere. This ultimately results in failure of the ECCS function due to the unavailability of a water source. Details of this transient are discussed below.

19.11.5.4.6.1 RCS Response Characteristics

The ISL represents a large LOCA initiated outside of containment. Consequently the RCS response is similar to that of the large LOCA discussed in Section 19.11.5.4.2. In this case the SCS line break is equivalent to 1.4 square feet. The larger failure area results in a more rapid RCS response. In this event the core initially uncovers in 76 seconds (See for example Figure 19.11.5.4.6.1-1 and Table 19.11.5.4.6.1-1). SIT discharge rapidly temporarily recovers the core.

TABLE 19.11.5.4.1.1 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LOOP-9E Plant Damage State: 243	
Event Description: Station Blackout with Wet Cavity	
Time (seconds)	Event Timings
0.0	Accident Initiation
0.0	Reactor Trip
6919.3	Core Uncovery
12432.6	Core Support Plate Failure
12492.4	Reactor Vessel Failure
226800.0 (63 hrs)	Containment Reaches ASME Level "C" Pressure

~~See Section 19.12~~

TABLE 19.11.5.4.1.1 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: LOOP-9E* Plant Damage State: 241*	
Event Description: Station Blackout with Wet Cavity	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1405
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	970
Primary system pressure at Vessel Breach (psia)	2450
Maximum predicted concrete erosion at 24 hours (ft)	0.22
Maximum predicted concrete erosion at 48 hours (ft)	0.22
Containment pressure at Vessel Breach (psia)	17
Containment pressure at 24 hours (psia)	64
Containment temperature at 24 hours (°F)	286

* See Section 19.12

TABLE 19.11.5.4.1.1 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LOOP-9B* Plant Damage State: 24*			
Event Description: Station Blackout with Wet Cavity			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere following Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere at Containment Failure (fraction of initial inventory)
1	Nobles	0.96	0.98
2	CSI + RBI	0.099	3.1×10^{-3}
3	TEO2	0.00	0.00
4	SRO	0.008	2.5×10^{-8}
5	MOO2	0.0119	1.2×10^{-6}
6	CSOH + RBOH	0.127	4.4×10^{-3}
7	BAO	0.0086	2.7×10^{-7}
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	9.92×10^{-4}	8.5×10^{-9}
9	CEO2	0.0062	1.1×10^{-8}
10	SB	0.17	0.16
11	TE2	0.54	2.3×10^{-5}

* See Section 19.1?

[1] Fission Product Group

TABLE 19.11.5.4.1.2 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LOOP-9F* Plant Damage State: 241	
Event Description: Station Blackout with Dry Cavity	
Time (seconds)	Event Timings
0.0	Accident Initiation
0.0	Reactor Trip
6938.3	Core Uncovery
12581.5	Core Support Plate Failure
12661.3	Reactor Vessel Failure
≈ 8 days (approx.)	Containment Failure via Basemat Melt-through

* See Section 19.11.2

TABLE 19.11.5.4.1.2 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LOOP-9F* Plant Damage State: 241*			
Event Description: Station Blackout with Dry Cavity			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere following Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere at Containment Failure (fraction of initial inventory)
1	Nobles	0.98	N/A
2	CSI + RBI	0.096	N/A
3	TEO2	0.00	N/A
4	SRO	0.0018	N/A
5	MOO2	0.0108	N/A
6	CSOH + RBOH	0.127	N/A
7	BAO	0.0053	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	3.09×10^{-4}	N/A
9	CEO2	0.0011	N/A
10	SB	0.072	N/A
11	TE2	0.114	N/A

N/A: Not Applicable

~~* See Section 19.11.2~~

[1] Fission Product Group

TABLE 19.11.5.4.1.3 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: SBOBD-E Plant Damage State: 244	
Event Description: Station Blackout with Battery Depletion at 8 hrs (Reactor Cavity "Wet")	
Time (hrs)	Event Timings
0.0	Accident Initiation
0.0	Reactor Trip
8.0	AFW Stops due to Depleted Battery
12.0	Core Uncovery Begins
14.8	Lower Core Support Plate Fails
14.8	RV Lower Head Fails
14.82	SIT Water Depleted Containment Failure

~~* See Section 19.11~~

TABLE 19.11.5.4.1.3 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: SBOBD-E Plant Damage State: 244	
Event Description: Station Blackout with Battery Depletion at 8 hrs (Reactor Cavity "Wet")	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1380
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	1151
Primary system pressure at Vessel Breach (psia)	2450
Maximum predicted concrete erosion at 24 hours (ft)	< 0.1
Maximum predicted concrete erosion at 48 hours (ft)	< 0.1
Containment pressure at Vessel Breach (psia)	16
Containment pressure at 24 hours (psia)	36
Containment temperature at 24 hours (°F)	230

~~See Section 19.A.2~~

TABLE 19.11.5.4.1.3 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: SBOBD-E Plant Damage State: 244			
Event Description: Station Blackout with Battery Depletion at 8 hrs. (Reactor Cavity "Wet")			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere following Containment Failure (fraction of initial inventory)
1	Nobles	0.933	N/A
2	CSI + RBI	0.044	N/A
3	TEO2	0.00	N/A
4	SRO	0.0003	N/A
5	MOO2	0.0135	N/A
6	CSOH + RBOH	0.023	N/A
7	BAO	0.0031	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	1.77×10^{-5}	N/A
9	CEO2	5.95×10^{-5}	N/A
10	SB	0.125	N/A
11	TE2	0.005	N/A

N/A: Not Applicable

~~* See Section 19.11~~

[1] Fission Product Group

TABLE 19.11.5.4.2.1 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LL-3E Plant Damage State: 14	
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Cavity Flooded Prior to Vessel Breach	
Time (seconds)	Event Timings
0.0	Accident Initiation
1.2	Reactor scram
≈1.2	Accumulators begin to discharge
781.0	Accumulator discharge complete
1894.6	Core uncovery begins
6113.3	Support plate fails
6173.1	Reactor vessel failure
210267.3 (58.4 hrs)	Containment failure

~~See Section 19.12~~

TABLE 19.11.5.4.2.1 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: LL-3E Plant Damage State: 14	
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Cavity Flooded Prior to Vessel Breach	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	840
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	< 20
Primary system pressure at Vessel Breach (psia)	< 50
Maximum predicted concrete erosion at 24 hours (ft)	≈ 0.25
Maximum predicted concrete erosion at 48 hours (ft)	≈ 0.25
Containment pressure at Vessel Breach (psia)	32
Containment pressure at 24 hours (psia)	100
Containment temperature at 24 hours (°F)	320

* See section 19.12

TABLE 19.11.5.4.2.1 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LL-3R* Plant Damage State: 14*			
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Cavity Flooded Prior to Vessel Breach			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Fraction Leaked to Atmosphere at 24 Hrs After Vessel Breach (fraction of initial inventory)
1	Nobles	0.98	0.949
2	CSI + RBI	0.52	6.42×10^{-4}
3	TEO2	0.00	0.00
4	SRO	0.0043	1.597×10^{-6}
5	MOO2	6.5×10^{-4}	6.048×10^{-7}
6	CSOH + RBOH	0.52	1.09×10^{-3}
7	BAO	0.017	1.526×10^{-5}
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	5.78×10^{-4}	3.073×10^{-7}
9	CEO2	4.38×10^{-4}	3.136×10^{-7}
10	SB	0.207	3.07×10^{-3}
11	TE2	0.165	1.75×10^{-5}

~~* See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.2.2 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LL-3K* Plant Damage State: 11*	
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Reactor Cavity Dry	
Time (seconds)	Event Timings
0.0	Accident Initiation
1.1	Reactor scram
≈1.1	Accumulators begin to discharge
785.3	Accumulator discharge complete
1836.4	Core uncovery begins
6100.1	Support plate fails
6160.1	Reactor vessel failure
8.3 days (estimated)	Containment fails due to basemat melt through

* See Section 19.12

TABLE 19.11.5.4.2.2 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: LL-3F Plant Damage State: 11	
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Reactor Cavity Dry	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	840
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	< 20
Primary system pressure at Vessel Breach (psia)	< 50
Maximum predicted concrete erosion at 24 hours (ft)	4
Maximum predicted concrete erosion at 48 hours (ft)	≈ 6.7
Containment pressure at Vessel Breach (psia)	≈ 35
Containment pressure at 24 hours (psia)	≈ 48
Containment temperature at 24 hours (°F)	≈ 330

* ~~See Section 19.12~~

TABLE 19.11.5.4.2.2 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LL-3F Plant Damage State: 11			
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Reactor Cavity Dry			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere at Containment Failure (fraction of initial inventory)
1	Nobles	0.986	N/A
2	CSI + RBI	0.67	N/A
3	TEO2	0.00	N/A
4	SRO	0.0043	N/A
5	MOO2	3.38×10^{-4}	N/A
6	CSOH + RBOH	0.68	N/A
7	BAO	0.0195	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	6.17×10^{-4}	N/A
9	CEO2	1.7×10^{-3}	N/A
10	SB	0.227	N/A
11	TE2	0.181	N/A

N/A: Not Applicable

~~* See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.3.1 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: SL-11E* Plant Damage State: 201	
Event Description: Small Break LOCA Without SI, Cavity Flooded Prior to Vessel Breach	
Time (seconds)	Event Timings
0.0	Accident Initiation
19.7	Reactor scram
569.5	Containment sprays on
3816.7	Initial core uncovery begins
≈ 7200.0	Accumulators begin to discharge
11454.5	Support plate fails
11514.5	Reactor vessel failure
11559.4	Accumulator discharge complete
---	Containment failure prevented

* ~~See Section 19.12~~

TABLE 19.11.5.4.3.1 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: SL-11E* Plant Damage State: 201	
Event Description: Small Break LOCA Without SI, Cavity Flooded Prior to Vessel Breach	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1768
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	< 20
Primary system pressure at Vessel Breach (psia)	≈ 400
Maximum predicted concrete erosion at 24 hours (ft)	0
Maximum predicted concrete erosion at 48 hours, (ft)	0 (estimated)
Containment pressure at Vessel Breach (psia)	≈ 16
Containment pressure at 24 hours (psia)	≈ 15
Containment temperature at 24 hours (°F)	≈ 110

* See Section 19.12

TABLE 19.11.5.4.3.1 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: SL-11E* Plant Damage State: 20			
Event Description: Small Break LOCA Without SI, Cavity Flooded Prior to Vessel Breach			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere following Containment Failure (fraction of initial inventory)
1	Nobles	0.98	N/A
2	CSI + RBI	0.002	N/A
3	TEO2	0.99	N/A
4	SRO	0.003	N/A
5	MOO2	0.007	N/A
6	CSOH + RBOH	0.002	N/A
7	BAO	0.004	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	3.15×10^{-4}	N/A
9	CEO2	0.0027	N/A
10	SB	0.026	N/A
11	TE2	0.31	N/A

N/A: Not Applicable

* ~~See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.3.2 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: SL-11F Plant Damage State: 209	
Event Description: Small Break LOCA Without SI, Reactor Cavity Dry	
Time (seconds)	Event Timings
0.0	Accident Initiation
17.8	Reactor scram Auxiliary feedwater on MSIVs closed
597.4	Containment sprays on
3836.5	Sustained core uncovery begins
≈ 7200.0	Accumulator discharge complete
12316.0	Support plate fails
12382.3	Reactor vessel failure
12425.7	Accumulator discharge complete

~~* See Section 19.12~~

TABLE 19.11.5.4.3.2 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: SL-11F Plant Damage State: 209	
Event Description: Small Break LOCA Without SI, Reactor Cavity Dry	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1704
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	< 20
Primary system pressure at Vessel Breach (psia)	≈ 400
Maximum predicted concrete erosion at 24 hours (ft)	≈ 3.3
Maximum predicted concrete erosion at 48 hours (ft)	7.0 (estimate)
Containment pressure at Vessel Breach (psia)	≈ 16
Containment pressure at 24 hours (psia)	≈ 16
Containment temperature at 24 hours (°F)	≈ 120

~~See Section 19.13~~

TABLE 19.11.5.4.3.2 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: SL-11F Plant Damage State: 209			
Event Description: Small Break LOCA Without SI, Reactor Cavity Dry			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere at Containment Failure (fraction of initial inventory)
1	Nobles	0.98	N/A
2	CSI + RBI	9.7×10^{-4}	N/A
3	TEO2	0.00	N/A
4	SRO	1.02×10^{-2}	N/A
5	MOO2	1.287×10^{-3}	N/A
6	CSOH + RBOH	7.92×10^{-4}	N/A
7	BAO	0.005	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	1.13×10^{-3}	N/A
9	CEO2	1.01×10^{-2}	N/A
10	SB	0.035	N/A
11	TE2	0.728	N/A

N/A: Not Applicable

~~* See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.4.1 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LOFW-9E Plant Damage State: 243	
Event Description: Total Loss of Feedwater with Wet Cavity	
Time (seconds)	Event Timings
0.0	Accident Initiation
22.5	Reactor scram
2126.0	Steam generator dryout
4397.0	Initial core uncovery
8491.0	Support plate fails
9391.0	Reactor vessel failure

* See Section 19.12

TABLE 19.11.5.4.4.1 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: LOFW-9E Plant Damage State: 243	
Event Description: Total Loss of Feedwater with Wet Cavity	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1500
Primary system pressure at Vessel Breach (psia)	2500
Maximum predicted concrete erosion at 24 hours (ft)	< 0.25
Maximum predicted concrete erosion at 48 hours (ft)	< 0.25
Containment pressure at Vessel Breach (psia)	≈ 30
Containment pressure at 24 hours (psia)	≈ 70
Containment temperature at 24 hours (°F)	270

~~See Section 19.12~~

TABLE 19.11.5.4.4.1 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LOFW-9E Plant Damage State: 243			
Event Description: Total Loss of Feedwater with Wet Cavity			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Fission Products Leaked to Atmosphere following Containment Failure (fraction of initial inventory)
1	Nobles	0.98	0.99
2	CSI + RBI	0.125	3.1×10^{-3}
3	TEO2	0.00	0.00
4	SRO	0.0047	2.5×10^{-8}
5	MOO2	0.0032	1.2×10^{-6}
6	CSOH + RBOH	0.086	4.4×10^{-3}
7	BAO	0.0027	2.7×10^{-7}
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	5.58×10^{-4}	8.3×10^{-9}
9	CEO2	0.005	1.15×10^{-8}
10	SB	0.123	0.16
11	TE2	0.48	2.3×10^{-5}

~~* See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.4.2 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: LOFW-9F Plant Damage State: 241	
Event Description: Total Loss of Feedwater With Dry Cavity	
Time (seconds)	Event Timings
0.0	Accident Initiation
21.6	Reactor scram
2175.0	Steam generator dryout
4456.7	Initial core uncovery begins
8104.7	Support plate fails
9004.7	Reactor vessel failure

~~See Section 19.P2~~

TABLE 19.11.5.4.4.2 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: LOFW-9F Plant Damage State: 241	
Event Description: Total Loss of Feedwater With Dry Cavity	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1320
Primary system pressure at Vessel Breach (psia)	2500
Maximum predicted concrete erosion at 24 hours (ft)	≈ 1.5
Maximum predicted concrete erosion at 48 hours (ft)	≈ 4.5
Containment pressure at Vessel Breach (psia)	< 20
Containment pressure at 24 hours (psia)	44
Containment temperature at 24 hours (°F)	320

~~See Section 19.12~~

TABLE 19.11.5.4.4.2 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: LOFW-9F Plant Damage State: 241			
Event Description: Total Loss of Feedwater With Dry Cavity			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Concentration in Containment Atmosphere following Containment Failure (fraction of initial inventory)
1	Nobles	0.955	N/A
2	CSI + RBI	0.0939	N/A
3	TEO2	0.00	N/A
4	SRO	0.0039	N/A
5	MOO2	0.0016	N/A
6	CSOH + RBOH	0.052	N/A
7	BAO	0.002	N/A
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	2.99×10^{-4}	N/A
9	CEO2	0.004	N/A
10	SB	0.0788	N/A
11	TE2	0.4168	N/A

N/A: Not Applicable

~~See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.5.1-1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: SGTR-15A Plant Damage State: 194	
Event Description: SGTR with Isolation Failure (No SI)	
Time (seconds)	Event Timings
0.0	Accident Initiation
18.4	Reactor Trips
3927	Core Uncovery Begins
9072	Support Plate Fails
9132	RV Lower Head Fails
9202	Accumulator Water Depleted

~~See Section 19.12~~

TABLE 19.11.5.4.5.1 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: SGTR-15A Plant Damage State: 194	
Event Description: SGTR with Isolation Failure (No SI)	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	1913
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	150
Primary system pressure at Vessel Breach (psia)	2450
Maximum predicted concrete erosion at 24 hours (ft)	<0.1
Maximum predicted concrete erosion at 48 hours (ft)	<0.1
Containment pressure at Vessel Breach (psia)	15
Containment pressure at 24 hours (psia)	15
Containment temperature at 24 hours (°F)	105

~~* See Section 19.12~~

TABLE 19.11.5.4.5.1 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: SGTR-15A Plant Damage State: 194			
Event Description: SGTR With Stuck Open MSSV/No SI			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Fission Products Leaked to Atmosphere 24 hours after Vessel Breach
1	Nobles	N/A	0.938
2	CSI + RBI	N/A	0.453
3	TEO2	N/A	8.5×10^{-9}
4	SRO	N/A	2.2×10^{-3}
5	MOO2	N/A	6.4×10^{-2}
6	CSOH + RBOH	N/A	4.38×10^{-1}
7	BAO	N/A	2.2×10^{-1}
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	N/A	6×10^{-4}
9	CEO2	N/A	7.9×10^{-4}
10	SB	N/A	0.18
11	TE2	N/A	0.0054

N/A: Not applicable

~~* See Section 19.12~~

[1] Fission Product Group

TABLE 19.11.5.4.6 - 1

SUMMARY OF MAAP PREDICTED KEY EVENT TIMINGS FOR SYSTEM 80+

Plant Accident Sequence: VSEQ Oe Plant Damage State: 17 Oe	
Event Description: Large Break LOCA Without SI; Containment Sprays Unavailable and Reactor Cavity Dry	
Time (seconds)	Event Timings
0.0	Accident Initiation
1.4	Reactor scram
≈1.4	Accumulators begin to discharge
90	Accumulator discharge complete
7700	Sustained core uncovery begins
13881	Support plate fails
13940	Reactor vessel failure

~~See Section 19.12~~

TABLE 19.11.5.4.6 - 2

SUMMARY OF KEY PARAMETERS

Plant Accident Sequence: VSE[1] Plant Damage State: 1[1]	
Event Description: Large Break LOCA Without SI/Containment Sprays Unavailable and Reactor Cavity Dry	
Parameter	Value
Mass of hydrogen generated in vessel (lbm)	820
Mass of hydrogen remaining in vessel just prior to Vessel Breach (lbm)	< 20
Primary system pressure at Vessel Breach (psia)	< 50
Maximum predicted concrete erosion at 24 hours (ft)	3.4
Maximum predicted concrete erosion at 48 hours (ft)	≈ 4
Containment pressure at Vessel Breach (psia)	≈ 15
Containment pressure at 24 hours (psia)	≈ 15
Containment temperature at 24 hours (°F)	≈ 220

[1] ~~See Section 19.12~~

TABLE 19.11.5.4.6 - 3

SUMMARY OF FISSION PRODUCT GROUP (FPG) CONCENTRATIONS

Plant Accident Sequence: VSEQ Plant Damage State: 17			
Event Description: Large Break LOCA Without SI/Containment Sprays Unavailable and Reactor Cavity Dry			
FPG[1] #	FPG[1] component	Concentration in Containment Atmosphere at Vessel Breach (fraction of initial inventory)	Fission Products Leaked to Atmosphere 24 hours after Vessel Breach (fraction of initial inventory)
1	Nobles	N/A	0.999
2	CSI + RBI	N/A	0.9
3	TEO2	N/A	0.00
4	SRO	N/A	0.0144
5	MOO2	N/A	0.0035
6	CSOH + RBOH	N/A	0.909[2]
7	BAO	N/A	0.029
8	LA2O3 + PR2O3 + ND2O3 + SM2O3 + Y2O3	N/A	2.19×10^{-3}
9	CEO2	N/A	0.0124
10	SB	N/A	0.44
11	TE2	N/A	0.199

* ~~See Section 19.12~~

(1) Fission Product Group

(2) Plateout in SDC lines and pool scrubbing by water at pipe exit not included

N/A: Not Applicable

19.11.6 SUMMARY AND CONCLUSIONS

The severe accident mitigation features of the System 80+ have been described along with their impact on the phenomenological response of the plant to beyond design basis accidents. This report demonstrates that the System 80+ design is robust and is capable of mitigating the consequences of a wide spectrum of severe accident scenarios while maintaining containment integrity and minimizing radiation releases to the general public.

Bounding deterministic calculations indicate that early containment challenges associated with vessel breach phenomena and hydrogen combustion result in peak loadings below the ASME Service Level C containment limit and hence provide a high degree of confidence that containment integrity can be maintained. Steam explosion loadings have also been quantified deterministically. These assessments suggest that the System 80+ cavity design can withstand impulsive loadings associated with a steam explosion involving 5 to 10% of the ejected corium mass without serious damage to the reactor cavity. Further structural analyses confirm that the System 80+ design is sufficiently strong such that even in the event of a complete loss of load carrying capability of the reactor cavity, a consequential indirect breach of containment will not occur. The conditional failure probability of the containment due to this loading was ~~therefore~~ assessed to be ~~below 0.005~~ very low.

Additional early containment loadings associated with "in-vessel steam explosions", and RV rocket failure were assessed probabilistically. Based on this assessment, these containment failure modes were found to have a negligible contribution to the conditional containment failure probability.

Late containment failure was assessed deterministically using the MAAP 3.0B. Based on these studies it was concluded that for transients without containment heat removal, containment overpressure failure will not occur until after 50 hours following the initiation of the severe accident scenario. This slow pressurization response allows ample time for the operating staff to re-establish alternate containment cooling pathways and avert containment failure.

Deterministic basemat melt-through scenarios were performed using CORCON-MOD3. These analyses assumed that 100 % of the corium debris was cooled within the reactor cavity as a "layered impermeable media". Under these circumstances a local below ground penetration of the containment shell in the area of the basemat will be delayed for more than 24 hours after the onset of core melt. Furthermore, this penetration is not considered to be significant since the local melt-through of the shell does not compromise the containment strength and is expected to only marginally increase fission product leakage, if at all.

The term "fraction of core ejected" means the fraction of the core which is participating in the energy transfer to the containment atmosphere. The core could be ejected from the vessel, but its participation in further energy transfer could be inhibited by the cavity configuration, access to reactants, particle dynamics, etc. The three cases discussed in Section 19.11.4.1 of the main report were run for varying fractions of the core ejected to illustrate sensitivity to the performance of the reactor cavity.

4.0 DESCRIPTION OF ANALYSES

The LOTUS spreadsheet program was used to analyze three high pressure DCH scenarios:

- Case 1: Dry RCS and a dry reactor cavity
- Case 2: RCS with residual lower plenum inventory and a dry reactor cavity
- Case 3: RCS with residual lower plenum inventory and a fully flooded reactor cavity.

These cases are described in more detail below. Spreadsheet input and results are presented in Table 19.11B-1, and Figure 19.11B-1.

4.1 CASE 1: DCH PRESSURIZATION FOLLOWING A HIGH PRESSURE VB FROM A DRY RCS INTO A DRY REACTOR CAVITY

This case addresses a VB failure scenario where no liquid water is in the RCS or the reactor cavity (steam in the RCS was assumed to be present). All the heat from the cooldown of the core debris materials and from chemical reactions was assumed to be transferred to the containment atmosphere.

The initial composition of the containment atmosphere was determined by starting with the pressure and temperature obtained from the MAAP code for a representative System 80+ station blackout sequence, just prior to reactor vessel meltthrough. The initial amounts of oxygen and nitrogen were determined assuming a temperature of 80°F prior to the start of the accident sequence.

The heat sources were computed by summing the sensible heat of cooling from the initial temperature of the melt to the final temperature of the core materials, and adding the heat due to chemical reactions. The sources of the sensible, or stored, heat were the fuel, the zirconium oxide from the in vessel oxidation fraction, the unoxidized zirconium, and the steel. The heats of reaction of zirconium oxidation in steam to form hydrogen and of subsequent hydrogen burning in oxygen was also considered.

TABLE 19.11B-1

This table intentionally blank

Case 1. Containment Pressure vs. Core Fraction

CDPC10A3 as discussed, P vs FRACTION CORE, 10000 KG STEEL DI PRECORE/OK
CONTAINMENT PRESSURE CALCULATION, NO CAVITY WATER, RCS STEAM ONLY, VARY CORE FRACTION
2533K, 24.5MPa, IPWH

Baseline Cal Do not use						
Initial metal Th (K)	2533	2533	2533	2533	2533	2533	2533
Containment metal Ti (K)	350	350	350	350	350	350	350
Fraction of core reacted	1	1	0.8	0.6	0.4	0.2	0
Amount of steel (kg)	10000	10000	10000	10000	10000	10000	10000
Fraction of Zirc reacted in vessel	0.245	0.245	0.245	0.245	0.245	0.245	0.245
Ex vessel hydrogen, fraction of oxidn	1	1	1	1	1	1	1
Fraction of steel oxidizing	1	0	0	0	0	0	0
INITIAL AMOUNTS IN CONTAINMENT							
Moles of O2 = pi*eff_2/V/RT Kg-mol	719	719	719	719	719	719	719
Moles of N2 = pi*eff_8/V/RT Kg-mol	2877	2877	2877	2877	2877	2877	2877
Moles of H2O init as vapor	313	313	313	313	313	313	313
Water in cavity, Kg	217000	0	0	0	0	0	0
Fraction of cavity water participating	1	1	1	1	1	1	1
WATER IN RCS							
Volume = (4/3)pi*r3/2 (m3)	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982
Mass Liquid in Vol*1000Kg/m^3 (kg)	43319.82	0	0	0	0	0	0
u sat RCS water at 13.61 MPa (J/kg)	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.
T sat RCS water at 2000 psia (K)	608.8868	608.8868	608.8868	608.8868	608.8868	608.8868	608.8868
Mass RCS vapor (kg) =	29800	29800	29800	29800	29800	29800	29800
Cavity water boiling point K	435	467.7777	663.4917	457.3133	448.3032	435.9892	0
u sat RCS vapor at 2000 psia (J/kg)	2357000	2357000	2357000	2357000	2357000	2357000	2357000
HEAT SOURCES (Above does't match A1 spreadsheet from here on)							
Contribution of UO2 to heat water to T(inv)	7.8E+10	-5.0E+09	3.5E+09	9.1E+09	1.2E+10	9.3E+09	0
Cont ext reacted ZrO2 to hv wat to T f	1.5E+10	-9.5E+08	6.6E+08	1.8E+09	2.2E+09	1.7E+09	0
Cont ext unreacted ZrO2 to hv wat to Tf	4.5E+10	-2.9E+09	2.0E+09	5.4E+09	6.8E+09	5.3E+09	0
Cont steel	1.4E+10	-9.0E+08	6.3E+08	1.7E+09	2.1E+09	1.6E+09	0
Heat of reaction, initially unreacted Zr	1.5E+11	1.5E+11	1.2E+11	9.0E+10	6.0E+10	3.0E+10	0
Heat of reaction H burn	1.7E+11	1.7E+11	1.5E+11	1.2E+11	9.5E+10	6.9E+10	4.3E+10
Ht of reaction Fe to H to H2O	7.4E+10	0	0	0	0	0	0
Cont H2O from burnt/No, already in Q burnt	6.5E+10	-3.1E+09	2.3E+09	6.7E+09	9.8E+09	1.1E+10	1.0E+10
Sum of heat sources	6.1E+11	3.1E+11	2.8E+11	2.4E+11	1.9E+11	1.3E+11	5.3E+10
final temp (K) (input as new T?)	450	2668	2415	2114	1751	1306	747
u(hvj) at metal condenser BOF (J/Kg)	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8
u(hvap2) at final condenser X pass	6770137.9	8142278.4	7963312.7	7720464.0	7312738.4	6811779.6	5915402.2
u(sat vapor) at final pass (J/Kg)	2566166.	2583290.	2582617.	2578548.	2572905.	2565006.	2544497.
Sat vapor sp. vol. at final pass (m3/kg)	0.294100	0.142575	0.155437	0.178173	0.215537	0.287587	0.493994
Mass H2O initially in vapor + from burn	16658.8	16658.8	16692.05	14725.31	12758.56	10791.82	8825.076
Mass water evap from cavity	217000	0	0	0	0	0	0
Mass water evap from RCS (end init vapl	73119.82	29800	29800	29800	29800	29800	29800
Total water evaporated	290119.8	29800	29800	29800	29800	29800	29800
u final at T,p final, J/kg	2443125.	6147811.	5730430.	5232601.	4634116.	3901626.	2981354.
U gain all water vapor to Tfinal	5.4E+11	1.4E+11	1.2E+11	1.0E+11	8.2E+10	5.6E+10	2.3E+10
NO MORE CAVITY WATER, NO ENTRY							
T	450	2668	2415	2114	1751	1306	747
ADDITIONAL HEAT SINKS							
Heatup of O2	1.5E+09	3.5E+10	3.1E+10	2.7E+10	2.1E+10	1.5E+10	6.0E+09
Heatup of N2	6.0E+09	1.4E+11	1.2E+11	1.1E+11	8.5E+10	5.8E+10	2.4E+10
Sum of heat sinks (incl. U to H2O)	5.5E+11	3.1E+11	2.8E+11	2.4E+11	1.9E+11	1.3E+11	5.3E+10
Heat sources minus heat sinks	6.4E+10	94813858	-1.1E+08	-4.8E+07	61708452	53864909	21909863
Moles O2 left after combustion	222.9117	357.2	411.8318	466.4436	521.0554	575.7272	630.359
temp K	810	4802.4	4247	3805.2	3151.8	2350.8	1344.6
FINAL PRESSURE AT WATER B.P.							
P N2 English units psi	16.66861	98.82638	89.65492	78.30546	64.85944	48.37603	27.66990
P O2 left after combustion	1.291494	12.36999	12.80513	12.69608	11.74743	9.680758	6.062556
P H2O sum	99.38811	92.47688	80.31018	67.32659	53.30253	37.91896	20.63786
PRESSURE TOTAL PSI	117.3482	203.5732	182.5702	158.3281	129.9096	95.97570	54.37032
Other metal gases, carl rel to Row 179							
Gauge pressure		0	0	0	0	0	0
INPUT Gauss superheat Temp (K)	450	2668	2415	2114	1751	1306	747
Heat sources minus heat sinks	6.4E+10	94813858	-1.1E+08	-4.8E+07	61708452	53864909	21909863

TABLE 19.11B-1

Case 2. Containment Pressure vs. Case Fraction

COPCAA3 as dimensional, P vs FRACTION CORE, 10000 KG STEEL DI PRECORDIOR,
CONTAINMENT PRESSURE CALCULATION, NO CAVITY WATER, RCS WATER AND STEAM, VARY CORE FRACTION
2533K, 24.5%Zr, 95%H

Baseline Cal
Do not use

Hot metal Th (K)	2533	2533	2533	2533	2533	2533	2533
containment metal Ti (K)	350	350	350	350	350	350	350
Fraction of core ejected	1	1	0.8	0.6	0.4	0.2	0
Amount of steel (kg)	10000	10000	10000	10000	10000	10000	10000
Fraction of Zirc reacted in vessel	0.245	0.245	0.245	0.245	0.245	0.245	0.245
Ex vessel hydrogen, fraction of max	1	1	1	1	1	1	1
Fraction of steel oxidizing	1	1	1	1	1	1	1
INITIAL AMOUNTS IN CONTAINMENT							
Moles of O2 = pi*ref_ZIV/RT Kg-mol	719	719	719	719	719	719	719
Moles of N2 = pi*ref_RIV/RT Kg-mol	2877	2877	2877	2877	2877	2877	2877
Moles of H2O init as vapor	313	313	313	313	313	313	313
Water in cavity, Kg	217000	0	0	0	0	0	0
Fraction of cavity water participating	1	1	1	1	1	1	1
WATER IN RCS							
Volume = (4/3)pi*r3/2 (m3)	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982
Mass Liquid= Vol*1000Kg/m^3 (kg)	43319.82	43319.82	43319.82	43319.82	43319.82	43319.82	43319.82
u sat RCS water at 13.61 MPa (J/kg)	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.
T sat RCS water at 2000 psia (K)	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888
Mass RCS vapor (kg) =	29800	29800	29800	29800	29800	29800	29800
Cavity water boiling point K	435	467.7777	467.7777	462.8696	452.7848	437.9658	0
u sat RCS vapor at 2000 psia (J/kg)	2357000	2357000	2357000	2357000	2357000	2357000	2357000
HEAT SOURCES (Rows don't match A1 spreadsheet from here on)							
Oxidation of UO2 to heat water to T final	7.8E+10	9.5E+09	1.5E+10	1.8E+10	1.7E+10	1.2E+10	0
Cool ink reacted ZrO2 to be wet to T f	1.5E+10	1.8E+09	2.9E+09	3.4E+09	3.3E+09	2.2E+09	0
Cool ink unreacted ZrO2 to be wet to T f	4.5E+10	5.5E+09	8.9E+09	1.1E+10	1.0E+10	6.8E+09	0
Cool steel	1.4E+10	1.7E+09	2.7E+09	3.2E+09	3.1E+09	2.1E+09	0
Heat of reaction, initially unreacted Zr	1.5E+11	1.5E+11	1.2E+11	9.0E+10	6.0E+10	3.0E+10	0
Heat of reaction H burn	1.7E+11	1.7E+11	1.5E+11	1.2E+11	9.5E+10	6.9E+10	4.3E+10
Heat of reaction Fe to H to H2O	7.4E+10	7.4E+10	5.9E+10	4.4E+10	2.9E+10	1.5E+10	0
Cool H2O from burnt+to, already in O burn)	6.5E+10	8.0E+09	1.3E+10	1.7E+10	1.9E+10	1.7E+10	1.2E+10
Sum of heat sources	6.1E+11	4.2E+11	3.7E+11	3.1E+11	2.4E+11	1.5E+11	5.4E+10
T final temp (K) (input at row 77)	450	2279	2020	1720	1372	965	481
u(final) at initial conditions (J/Kg)	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8
u(final) at final condition X pass	677037.9	614278.4	614278.4	793727.9	751503.0	689456.0	579060.0
steam vapor at final pass (J/Kg)	2564164.	2583290.	2583290.	2582155.	2576020.	2566588.	2541284.
Sat vapor sp. vol. at final pass (m3/kg)	0.294100	0.142575	0.142575	0.157250	0.196300	0.274667	0.531519
Mass H2O initially in vapor + from burn	18658.8	18658.8	16692.05	14725.31	12758.56	10791.82	8825.076
Mass water evap from cavity	217000	0	0	0	0	0	0
Mass water evap from RCS (incl ini vapor)	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82
Total water evaporated	290119.8	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82
u final at T,p final, J/kg	2443125.	5496044.	5062090.	4566583.	3994562.	3328478.	2537605.
U gain all water vapor to T final	5.4E+11	2.8E+11	2.4E+11	2.0E+11	1.6E+11	1.1E+11	4.4E+10
NO MORE CAVITY WATER, NO ENTRY							
T	450	2279	2020	1720	1372	965	481
ADDITIONAL HEAT SINKS							
Heatup of O2	1.5E+09	2.9E+10	2.5E+10	2.1E+10	1.6E+10	9.3E+09	2.7E+09
Heatup of N2	6.0E+09	1.2E+11	1.0E+ 1	8.3E+10	6.2E+10	3.7E+10	7.9E+09
Sum of heat sinks (incl. U to H2O)	5.5E+11	4.2E+11	3.7E+11	3.1E+11	2.4E+11	1.5E+11	5.4E+10
Heat sources minus heat sinks	6.4E+10	1.3E-08	-1.9E-08	-5.8E-07	1.2E-08	13484289	19915827
Moles O2 left after combustion	222.9117	222.9117	304.4011	385.8906	467.3800	548.8695	630.359
temp K	810	4102.2	3636	3096	2469.6	1737	865.8
FINAL PRESSURE AT WATER B.P.							
P N2 English units psi	16.66861	84.41729	74.82357	63.71116	50.82076	35.74492	17.81690
P O2 left after combustion	1.291494	6.540703	7.916713	8.545548	8.256035	6.819361	3.903734
P H2O sum	99.38811	149.6099	129.7656	108.0739	84.27771	57.91942	28.19302
PRESSURE TOTAL PSI	117.3487	240.5479	212.5059	180.3306	143.3545	100.4837	49.91566
After ironical guesses, call ref to Row 179		0	0	0	0	0	0
Guess pressure	450	2279	2020	1720	1372	965	481
INPUT Guess superheat Temp (K)	6.4E+10	1.3E-08	-1.9E-08	-5.8E-07	1.2E-08	13484289	19915827
Heat sources minus heat sinks							

TABLE 19.11B-1

Case 1. Containment Pressure vs. Core Fraction

COPC10A3 as dimensioned, F = FRACTION CORE, 10000 KG STEEL IX PRECORDIOR,
CONTAINMENT PRESSURE CALCULATION, NO CAVITY WATER, PCS STEAM ONLY, VARY CORE FRACTION
2533K, 245FrZr, IPWH

Baseline Cal
Do not use

Initial heat content Th (K)	2533	2533	2533	2533	2533	2533	2533
Containment initial Ti (K)	350	350	350	350	350	350	350
Fm, Fraction of core reacted	1	1	0.8	0.6	0.4	0.2	0
Amount of steel (kg)	10000	10000	10000	10000	10000	10000	10000
Fraction of Zirc reacted in vessel	0.245	0.245	0.245	0.245	0.245	0.245	0.245
Ex vessel hydrogen, fraction of mass	1	1	1	1	1	1	1
Fraction of steel oxidizing	1	0	0	0	0	0	0
INITIAL AMOUNTS IN CONTAINMENT							
Moles of O2 = pi*eff(.2)V/RT Kg-mol	719	719	719	719	719	719	719
Moles of N2 = pi*eff(.8)V/RT Kg-mol	2877	2877	2877	2877	2877	2877	2877
Moles of H2O vol as vapor	313	313	313	313	313	313	313
Water in cavity, Kg	217000	0	0	0	0	0	0
Fraction of cavity water participating	1	1	1	1	1	1	1
WATER IN PCS							
Volume = (4/3)a^3/2 (m3)	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982
Mass Liquidw Vol*1000Kg/m^3 (kg)	43319.82	0	0	0	0	0	0
u sat PCS water at 13.61 MPa (J/kg)	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.
T sat PCS water at 2000 psia (K)	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888
Mass PCS vapor (kg) =	29800	29800	29800	29800	29800	29800	29800
Cavity water boiling point K	435	467.7777	483.4917	457.3133	448.3033	435.9892	0
u sat PCS vapor at 2000 psia (J/kg)	2357000	2357000	2357000	2357000	2357000	2357000	2357000
HEAT SOURCES (Ramm doesn't match A1 spreadsheet from here on)							
Combustion of UO2 to heat water to Tfinal	7.8E+10	-5.0E+09	3.5E+09	9.4E+09	1.2E+10	9.2E+09	0
Coal ox reacted ZrO2 to ht wat to T f	1.5E+10	-9.5E+08	6.6E+08	1.8E+09	2.2E+09	1.7E+09	0
Coal ox unreacted ZrO2 to ht wat to Tf	4.5E+10	-2.9E+09	2.0E+09	5.4E+09	6.8E+09	5.3E+09	0
Coal steel	1.4E+10	-9.0E+08	6.3E+08	1.7E+09	2.1E+09	1.6E+09	0
Heat of reaction, metallic unreacted Zr	1.5E+11	1.5E+11	1.2E+11	9.0E+10	6.0E+10	3.0E+10	0
Heat of reaction H burn	1.7E+11	1.7E+11	1.5E+11	1.2E+11	9.5E+10	6.9E+10	4.3E+10
Ht of reaction Fe to H to H2O	7.4E+10	0	0	0	0	0	0
Coal H2O from burn/Hts, already in O burni	6.5E+10	-3.1E+09	2.3E+09	6.7E+09	9.8E+09	1.1E+10	1.0E+10
Sum of heat sources	6.1E+11	3.1E+11	2.8E+11	2.4E+11	1.9E+11	1.3E+11	5.3E+10
final temp (K) (input as row 77)	450	2668	2415	2114	1751	1306	747
n							
vf(sat) at initial condensing BOF (J/Kg)	1113B5.8	1113B5.8	1113B5.8	1113B5.8	1113B5.8	1113B5.8	1113B5.8
ufinal(f) at final condensin T, psia	677037.9	814278.4	796332.7	770464.0	732738.4	681179.6	591540.2
vfinal vapor(f at final psia (J/Kg)	2566166.	2583290.	2582617.	2578548.	2572905.	2565006.	2544497.
Sat vapor sp. vol. at final psia (m3/kg)	0.294100	0.142575	0.155437	0.178173	0.215537	0.287587	0.493994
Mass H2O initially in vapor + hours burn	18658.8	18658.8	18692.05	14725.31	12758.56	10791.82	8825.074
Mass water evap from cavity	217000	0	0	0	0	0	0
Mass vapor evap from PCS (incl ini vap)	73119.82	29800	29800	29800	29800	29800	29800
Total water evaporated	290119.8	29800	29800	29800	29800	29800	29800
u final at T,p final, J/kg	2443125.	6147811.	5730450.	5232601.	6636116.	3901626.	2981354.
U gross all water vapor to Tfinal	5.4E+11	1.4E+11	1.2E+11	1.0E+11	8.2E+10	5.6E+10	2.3E+10
NO MORE CAVITY WATER, NO ENTRY							
T	450	2668	2415	2114	1751	1306	747
ADDITIONAL HEAT SINKS							
Heatup of O2	1.5E+09	3.5E+10	3.1E+10	2.7E+10	2.1E+10	1.5E+10	6.0E+09
Heatup of N2	6.0E+09	1.4E+11	1.2E+11	1.1E+11	8.5E+10	5.8E+10	2.4E+10
Sum of heat sinks (incl. U sat H2O)	5.5E+11	3.1E+11	2.8E+11	2.4E+11	1.9E+11	1.3E+11	5.3E+10
Heat sources minus heat sinks	6.4E+10	9.4813858	-1.1E-08	-4.8E-07	61708452	33864909	21909863
Moles O2 left after combustion	222.9117	357.2	411.8318	466.4436	521.0954	575.7272	630.359
temp F	810	4802.4	4347	3805.2	3151.8	2350.8	1344.6
FINAL PRESSURE AT WATER S.P.							
P N2 English units psi	16.66861	98.82638	89.45492	78.30546	64.85944	48.37603	27.66990
P O2 left after combustion	1.291e-94	12.26999	12.80513	12.69608	11.74743	9.680704	6.063556
P H2O sum	99.38811	92.47668	80.31018	67.32659	53.30253	37.91896	20.63786
PRESSURE TOTAL PSI	117.3482	203.5732	182.5702	158.3281	129.9096	95.97570	54.37032
After initial guess, call rel to Row 179							
Guess pressure		0	0	0	0	0	0
INPUT Guess superheat Temp (K)	450	2668	2415	2114	1751	1306	747
Heat sources minus heat sinks	6.4E+10	9.4813858	-1.1E-08	-4.8E-07	61708452	33864909	21909863

TABLE 19.11B-1

Case 2. Containment Pressure vs. Case Fraction

COPCBA3 as dispersed, P vs FRACTION CORE, 10000 KG STEEL IX PRECORECOR,
CONTAINMENT PRESSURE CALCULATION, NO CAVITY WATER, RCS WATER AND STEAM, VARY CORE FRACTION
2533K, 245MPa, 89MH

Boundary Cal
Do not use

Heat metal Th (K)	2533	2533	2533	2533	2533	2533	2533
Coolant metal T (K)	350	350	350	350	350	350	350
Fraction of core ejected	1	1	0.8	0.6	0.4	0.2	0
Amount of steel (kg)	10000	10000	10000	10000	10000	10000	10000
Fraction of Zirc reacted in vessel	0.245	0.245	0.245	0.245	0.245	0.245	0.245
Ex vessel hydrogen, fraction of mass	1	1	1	1	1	1	1
Fraction of steel oxidizing	1	1	1	1	1	1	1
INITIAL AMOUNTS IN CONTAINMENT							
Moles of O2 = pVol/.2IV/RT Kg-mol	719	719	719	719	719	719	719
Moles of N2 = pVol/.8IV/RT Kg-mol	2877	2877	2877	2877	2877	2877	2877
Moles of H2O vol as vapor	313	313	313	313	313	313	313
Water in cavity, Kg	217000	0	0	0	0	0	0
Fraction of cavity water participating	1	1	1	1	1	1	1
WATER IN RCS							
Volume = (4/3)pi*r3/2 (m3)	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982	43.31982
Mass Liquid= Vol*1000Kg/m^3 (kg)	43319.82	43319.82	43319.82	43319.82	43319.82	43319.82	43319.82
u sat RCS water at 13.61 MPa (J/kg)	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.	1672701.
T sat RCS water at 2000 psia (K)	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888	608.8888
Mass RCS vapor (kg) =	29800	29800	29800	29800	29800	29800	29800
Cavity water boiling psia K	435	467.7777	467.7777	462.8696	452.7848	437.9658	0
u sat RCS vapor at 2000 psia (J/kg)	2357000	2357000	2357000	2357000	2357000	2357000	2357000
HEAT SOURCES (Blows don't match A1 spreadsheet from here on)							
Cooldown of UO2 to heat water to Tfinal	7.8E+10	9.5E+09	1.5E+10	1.8E+10	1.7E+10	1.2E+10	0
Cool ex reacted ZrO2 to ht wat to T f	1.5E+10	1.8E+09	2.9E+09	3.4E+09	3.3E+09	2.2E+09	0
Cool ex unreacted ZrO2 to ht wat to Tf	4.5E+10	5.5E+09	8.9E+09	1.1E+10	1.0E+10	6.8E+09	0
Cool steel	1.4E+10	1.7E+09	2.7E+09	3.2E+09	3.1E+09	2.1E+09	0
Heat of reaction, inexactly unreacted Zr	1.5E+11	1.5E+11	1.2E+11	9.0E+10	6.0E+10	3.0E+10	0
Heat of reaction H burn	1.7E+11	1.7E+11	1.5E+11	1.2E+11	9.5E+10	6.9E+10	4.3E+10
Ht of reaction Fe to H to H2O	7.4E+10	7.4E+10	5.9E+10	4.4E+10	2.9E+10	1.5E+10	0
Cool H2O from burnt/ie, already in O burnt	6.5E+10	8.0E+09	1.3E+10	1.7E+10	1.9E+10	1.7E+10	1.2E+10
*sum of heat sources	6.1E+11	4.2E+11	3.7E+11	3.1E+11	2.4E+11	1.5E+11	5.4E+10
S final temp (K) (input at row 77)	450	2279	2020	1720	1372	965	481
u(Tin) at initial conditions (BOF (J/Kg)	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8	111385.8
u(liquid) at final condition X psia	477037.9	814278.4	814278.4	793727.9	751503.0	689456.0	579060.0
u(sat vapor) at final psia (J/Kg)	2564164.	2583290.	2583290.	2582155.	2576020.	2566588.	2541284.
Sat vapor sp. vol. at final psia (m3/kg)	0.294100	0.142575	0.142575	0.137250	0.196300	0.274667	0.331519
Mass H2O initially in vapor + from burn	18658.8	18658.8	16692.05	14725.31	12758.56	10791.82	8825.076
Mass water evap from cavity	217000	0	0	0	0	0	0
Mass water evap from RCS final init vapl	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82
Total water evaporated	290119.8	73119.82	73119.82	73119.82	73119.82	73119.82	73119.82
u final sat T,p final, J/kg	2443125.	5496344.	5082090.	4566583.	3994562.	3328478.	2537605.
U given all water vapour to Tfinal	5.4E+11	2.8E+11	2.4E+11	2.0E+11	1.6E+11	1.1E+11	4.4E+10
NO MORE CAVITY WATER, NO ENTRY							
T	450	2279	2020	1720	1372	965	481
ADDITIONAL HEAT SINKS							
Heatup of O2	1.5E+09	2.9E+10	2.5E+10	2.1E+10	1.6E+10	9.3E+09	2.0E+09
Heatup of N2	6.0E+09	1.2E+11	1.0E+11	8.3E+10	6.2E+10	3.7E+10	7.9E+09
Sum of heat sinks (incl. U sat H2O)	5.5E+11	4.2E+11	3.7E+11	3.1E+11	2.4E+11	1.5E+11	5.4E+10
Heat sources minus heat sinks	6.4E+10	1.3E+08	-1.9E+08	-5.8E+07	1.2E+08	13484289	19915827
Moles O2 left after combustion	222.9117	222.9117	304.4011	385.8906	467.3800	548.8695	630.359
temp K	810	4102.2	3636	3096	2469.6	1737	865.8
FINAL PRESSURE AT WATER S.P.							
P N2 English units psi	16.66861	84.41729	74.82357	63.71114	50.82076	35.74492	17.81690
P O2 left after combustion	1.791494	9.340703	7.916713	8.345548	8.256035	6.819361	3.903734
P H2O sum	99.38811	149.6099	129.7656	108.0739	84.27771	57.91942	28.19307
PRESSURE TOTAL PSI	117.3482	240.5679	212.5059	180.3306	143.3543	100.4837	49.91366
After metal guess, call rel to Row 179		0	0	0	0	0	0
Guess pressure	450	2279	2020	1720	1372	965	481
INPUT Guess superheat Temp (K)	6.4E+10	1.3E+08	-1.9E+08	-5.8E+07	1.2E+08	13484289	19915827
Heat sources minus heat sinks							

1.0 INTRODUCTION

The construction of the containment fragility curve used in the PRA is described in Section 19.11.3.1.2.4. The construction is based on general guidance used in the support of NUREG-1150. In estimating failure, it was assumed that once the material yield point is reached using an axisymmetric shell model described in Sections 19.11.3.1.2.3.1 and 19.11.3.1.2.3.2, the containment will fail.

The above procedure has been biased to provide a conservative estimate of the containment failure probability. This conservative bias arises from the following assumptions and procedures:

1. All properties are evaluated at high mean shell temperatures. It is expected that during most containment challenges to which the fragility curve is applied, the average containment shell temperature will be between 150°F and 250°F. This temperature range is based on the fact that the PRA containment challenges with sprays operational will maintain a cool containment atmosphere. For those transients where sprays are unavailable, the shell temperature prior to burn will be less than 250°F to ensure the containment atmosphere is not inerted. While burn temperatures can be high, their short duration (less than 30 seconds) and the large mass of the steel shell results in only minor increases in the mean shell temperature. This assumption conservatively biases the median containment strength calculation from 2% to 10%.

2. In the fragility curve construction, the median material yield stress was taken to be 1.10 times the minimum expected yield stress. Material data discussed in Reference 210 (see Section 19.16) indicates that the median shell stress is actually 1.167 times the minimum yield stress. The difference between these values was taken to approximately account for effects of material variations and modeling uncertainties.

3. The fragility curve used in the PRA assumed a linear fit between the points defined in the Table in Section 19.11.3.1.2.4. This procedure overestimated the failure probability of the shell in the tail region of the fragility curve below the 3% failure point (in the pressure region between 94 and 145 psia). The fragility curve challenges for System 80+ were mostly confined to containment pressure below 145 psia. The highest containment challenge noted for the very low probability high pressure direct containment heating (DCH) event resulted in a pressure of 151 psia (see Figure 19.11.4.1.1-4A).

2.0 COMPARISON OF C-E FRAGILITY CURVE WITH THE METHODOLOGY OF REFERENCE H1

An alternate method of defining a fragility curve may be established by defining a logarithmic standard deviation for material properties and for modeling uncertainty. Given a failure pressure calculated from mean material properties a mean failure pressure probability curve can be developed. The methodology is generally analogous to the seismic strength analysis employed in Section 19.7.5. For the ultimate pressure fragility curve, the true mean containment failure pressure (@ 290°F) based on the Reference 210 data would be 180.7 psia (166 psig). The beta factor based on the variation in the material yield point is 0.09. Material uncertainty in this range is typically consistent for

This Section Intentionally Blank

19.12 CONTAINMENT RESPONSE ANALYSIS

The objective of the containment response analysis is to ascertain the likelihood, magnitude, and timing of radiological releases to the environment following a severe accident. The analysis includes evaluation of the physical processes and phenomena involved in the release of radiological material from the fuel during a severe accident, assessment of the transport and deposition of this material inside containment, determination of the potential containment failure modes, and identification of the phenomena contributing to the various failure modes.

The containment response analysis for the System 80+ Standard Design consisted of five main tasks:

A. Evaluation of severe accident phenomenon for applicability to System 80+.

B. Definition and quantification of the Plant Damage States (PDSs).

C. Development of the Containment Event Tree (CET).

D. Quantification of the CET.

E. Definition of the Release Classes.

Task A, evaluation of severe accident phenomenon for applicability to System 80+ is discussed in detail in Section 19.11. The other tasks are discussed in detail in the following sections. (Section 19.12.1.1 provides a summary overview of severe accident phenomena that affect containment performance. This summary provides the basic groundwork used for establishing the Plant Damage State (PDS) definitions. See Section 19.11 for a detailed discussion of all of the severe accident phenomena.)

19.12.1 DEFINITION AND QUANTIFICATION OF THE PLANT DAMAGE STATES

19.12.1.1 Qualitative Evaluation of Containment Performance Phenomena

In order to determine the consequences of an accident, each of the accident sequences identified as leading to core damage in the level 1 analyses is further analyzed to determine if it will lead to containment failure or bypass, and, if so, the nature of its associated release. The mode and timing of the containment failure and the nature of the releases are affected by the physical phenomena occurring inside the reactor vessel and inside containment during the progression of the accident. These phenomena, called parameters, are based on analysis of radionuclide

REMAINDER OF SECTION 19.12 DELETED

This Section Intentionally Blank

19.13 CONSEQUENCE ANALYSIS

The objective of the consequence analysis is to determine the risk to the public resulting from the release of fission products to the environment during a severe accident. The risk measures calculated for System 80+ Standard Design include:

A. The whole-body dose at 300 meters from the reactor,

B. The whole-body dose at one half mile from the reactor, and

C. Whole-body dose vs distance.

The MACCS computer code[164,165,166,167] was used to calculate the Complementary Cumulative Distribution Function (CCDF) for whole-body dose at six selected distances for each of the release classes described in Section 19.12.3. In performing its dose calculations, MACCS uses four data files; the dose conversion file, the site reference file, the meteorological reference file and the input reference file. The standard dose conversion file as described in the MACCS users manual[167] was used in this analysis. The site reference file basically contains land use profiles and population distribution data for the specific plant site. The meteorological data file contains hourly weather conditions data for the plant site. The meteorological data and population data for a conservative ALWR reference site provided in the EPRI PRA Key Assumptions and Groundrules Document, Appendix A to Chapter 1, Volume 2 of the EPRI ALWR Utility Requirements Document[7], was used in this analysis.

The input data file contains a number of input parameters used to define the analysis conditions. This file includes some standard data such as dose conversion parameters, health effect parameters, some general economic data by state, and the definition of the spatial intervals. This data file also includes the analysis specific data such as core inventory of various radioisotopes, evacuation strategies and the definition of the specific releases in terms of release fractions, energy of release, time and duration of release, and location (height) of the release. The ORIGEN code[48] was used to calculate the core inventory of radioisotopes. The inventories are based on a core burnup of 28,000 MWD/MTU. The same inventories were used for the MAAP analyses to generate the release fractions.

To calculate the dose at various distances, one person was assumed in each of sixteen sectors around the reactor for each selected distance. It was assumed that no evacuation occurred.

The data used for definition of the releases for each of the release classes is based on the definition of the release classes presented in Section 19.12.3. The release data needed by MACCS

REMAINDER OF SECTION 19.13 DELETED

This section intentionally blank.

19.14 LEVEL II AND LEVEL III SENSITIVITY ANALYSES

In performing the containment response analysis and the consequence analysis, several assumptions were made regarding the progression of severe accident phenomena. Sensitivity analyses were performed to assess the potential impact on the System 80+ design due to certain assumptions regarding the physical processes and phenomena involved in the release of radioactive materials to the environment and the consequences of the release. The sensitivity analyses associated with containment response are presented in Section 19.14.1 and those associated with the release consequences are presented in Section 19.14.2.

19.14.1 CONTAINMENT RESPONSE SENSITIVITY ANALYSES

The results of the "present" or base case analysis of containment response show that the conditional probability for intact containment releases, RC1, is 0.887. Likewise, the conditional probabilities for (1) late containment failure releases, RC2, (2) early containment failure releases, RC3, (3) containment isolation failure releases, RC4, and (4) containment bypass releases, RC5, are 0.079, 0.011, 0.024 and 0.0, respectively. To assess the effects of certain assumptions used in the base case analysis, fourteen containment response sensitivity analyses were performed. These analyses assessed the impact of specified assumptions on the containment failure modes and the overall conditional containment failure probability. These analyses involved changing certain conditions or assumptions that are modeled in the containment event trees (CETs) and then requantifying the CETs to ascertain the impact. Table 19.14.1-1 summarizes the results of the sensitivity analyses for containment response. The base case results are also included in Table 19.14.1-1 for comparison purposes. The following subsections describe the individual sensitivity analysis and present their results.

19.14.1.1 Availability of Hydrogen Ignitors

The hydrogen ignitors are provided to prevent the build-up of hydrogen inside the containment following a severe accident. With the ignitors operating, hydrogen is burned at a low enough concentration to prevent a threat to containment integrity. Because multiple failures of the ignitors in each division must occur to prevent the burning of hydrogen at a low enough concentration, a low probability was assigned to the unavailability of the ignitors. A sensitivity analysis was performed to determine the effects of the hydrogen ignitors being unavailable. For this case the ignitors were assumed to always fail (i.e., a failure probability of 1 was assigned to "IGFAIL"). The CETs were then requantified for all PDSs.

REMAINDER OF SECTION 19.14 DELETED

REVISED PAGES OF SECTION 19.15

Risk significant SSCs for consideration in the D-RAP and other activities are identified in Section 19.15.6.

Section 19.15.1. Insights about the System 80+ design gained from the internal events risk profile and the external events risk profile are summarized in Sections 19.15.2 and 19.15.3, respectively. Shutdown and low-power operation are included as part of the System 80+ PRA, and the insights gained from the risk associated with these modes of operation are summarized in Section 19.15.4. The use of PRA in the design process is summarized in Section 19.15.5. The use of PRA results and insights to support certification and followup activities is summarized in Section 19.15.7. Significant PRA-based safety insights for the System 80+ design are provided in Table 19.15-1.

Summarized

During the detailed design phase for System 80+, site specific information and system design details will become available. [[The COL applicant should update the PRA using the final design information and site specific information. As deemed necessary, the update should include the shutdown risk evaluation and the internal fire and flood evaluation. Based on site specific information, the COL applicant should also re-evaluate the qualitative screening of external events. If any site specific vulnerabilities are found, the applicable external event(s) should be included in the updated PRA.[1] [COL Item 19-6]]].

[[In updating the internal fire evaluation, the COL applicant should verify the details and layout of critical components and the fire suppression systems. [COL Item 19-3] The applicant should also evaluate the potential effect of the fire suppression systems on the behavior of other systems. [COL Item 19-3]

In updating the internal flood evaluation, the COL should evaluate the interaction of the potential internal flood sources and the details of the layout of the critical components. [COL Item 19-3]]].

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 1 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
1. The COL applicant should perform a seismic walkdown to ensure that the as-built plant conforms to the assumptions in the System 80 + PRA -based seismic margins analysis and to assure that seismic spatial systems interactions do not exist. Details of the seismic walkdown will be developed by the COL applicant.	COL Item 19-4 Section 19.7.5.3
2. ABB-CE will maintain a list of the SSC HCLPF values used in the System 80+ Seismic Margins Assessment in the D-RAP. The COL Applicant should compare the as-built SSC HCLPFs to those assumed in the System 80+ seismic margins analysis (SMA). Deviations from the HCLPF values or assumptions in the SMA should be evaluated by the COL Applicant to determine if any vulnerabilities have been introduced.	COL Item 19-4 Section 19.7.5.3
3. ABB-CE will maintain a list of risk significant SSCs in the D-RAP	D-RAP
4 The COL will maintain an O-RAP based on the system reliability information derived from the PRA and other sources. The COL Applicant should incorporate the list of risk important systems, structures and components (SSCs) as presented in Table 19.15.6-1 in its D-RAP and O-RAP.	COL Item 17-3 Section 17.3.1 COL Item 19-7 Section 19.15.6
5. Integrity of divisional separation between redundant safety-related equipment is a key assumption in the System 80+ fire and flood risk analyses. This divisional separation, which is extended also in the service water and component cooling water structures, prevents fires and floods from propagating from one division to the other. There are no doors or passageways connecting the divisions of safety-related equipment up to elevation 70+0.	Addressed in all safety-related structures and systems. Certified Design Material
6. The control room has its own dedicated ventilation system. This eliminates the possibility of smoke, hot gases, and fire suppressants, originated in areas outside the main control room, to migrate via the ventilation system to the control room.	Certified Design Material

1. COL information item; See DCD introduction 1.5 2.

TABLE 19.15-1

(Sheet 3 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
12. [[During plant shutdown operation, the integrity of fire and flood barriers between areas in same division, such as quadrants, where systems comprising the alternate shutdown success paths are located, should be maintained. This will require configuration control of fire/flood barriers for shutdown operation by the COL applicant.]]!	[[COL Item 19-9 Section 19.8.1.2]]!
[[The COL applicant should incorporate in its configuration control program a requirement that, during modes 4, 5, and 6, the water tight flood doors and fire doors will be maintained closed on at least one quadrant within the subsphere (containing either an SCS or CSS pump) to help prevent common-mode failures from internal floods or fires. The SCS or CSS pump in this quadrant shall be operable. If the flood or fire doors to this quadrant must be opened for reasons other than to permit normal access, a fire watch will be established for the affected door.]]!	[[COL Item 19-9 Section 19.8.1.2]]!
13. The grid system for System 80+ will include at least two preferred power circuits, each having sufficient capacity. They will be continuously energized and available to provide power to safety related loads. The two designated offsite power transmission lines shall be designed and routed to minimize, to the extent practicable, the likelihood of their simultaneous failure. These circuits shall be routed to ensure no single event, such as a tower falling or a line breaking can simultaneously affect both circuits in a way such that neither can be returned to service. The two offsite power circuits shall terminate at two switchyards that are physically separate and electrically independent to the extent practicable.	Certified Design Material
14. [[During plant shutdown, risk can be minimized by appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration. This will be an important COL applicant activity.]]!	[[COL Item 19-9 Section 19.8.1.2]]!
15. Divisional separation exists also between redundant charging pumps and their power supplies and redundant trains of instrument air.	Figure 1.2-4 Sections 8.3.1.1.2.1 & 9.3.1.2.1

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 4 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
16. [[The COL applicant will develop procedures for manually aligning the alternate AC power supply (combustion turbine) when one of the two diesel generators is unavailable during a loss of offsite power event]].[1]	[[COL Item 19-8]].†
Breakers between the Permanent Non-Safety (PNS) and the class 1E buses will be interlocked so that a PNS bus cannot be aligned to a class 1E bus that is being powered by an EDG.	Certified Design Material
17. To provide sufficient diversity and defense in depth to mitigate all postulated accidents even assuming a common cause failure within the Plant Protection System, the System 80+ Instrumentation and Control System provides the Manual Hardwired ESFAS Actuation System for the controls and for display there are Hardwired Key Indications of Critical Function Status for post accident monitoring.	Certified Design Material

during

For display,

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 5 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
18. One function of the Rapid Depressurization System (RDS) (or bleed system) is to provide a safety-grade means of rapidly depressurizing the RCS manually from the control room so that the Safety Injection System (SIS) can be actuated, when the long-term decay heat removal fails. This is an important feature added to the System 80 + design that helps reduce the failure probability of long-term decay heat removal and plant risk with respect to operating reactor designs.	
The following are some important aspects of the RDS as represented in the PRA:	
The RDS valves are motor-operated and will not reclose on high containment pressure.	Certified Design Material
The RDS valves fail as-is and therefore they are not subject to automatic reclosing upon battery depletion.	Certified Design Material
The functions of the RDS are to provide a "feed and bleed" cooling capability in conjunction with the SIS, and to provide the capability to depressurize the RCS during a severe accident to minimize the potential for High Pressure Melt Ejection (HPME).	
ABB-CE will provide EPG guidance for use of the RDS for "feed and bleed" cooling.	Emergency Operations Guidelines (EOGs)
Procedures will be provided for use of the RDS for depressurization of the RCS during a severe accident.	EOGs
The RDS valves are qualified for design basis accident conditions.	Section 3.2
The reliability of the RDS is important. The COL will ensure the reliability of the RDS.	Section 16.3/3.4.18

TABLE 19.15-1

(Sheet 6 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
19. The following are some important aspects of the Shutdown Cooling System (SCS) as represented in the PRA:	
The SCS has two separate and redundant divisions, each with the heat removal capacity to cool the RCS to cold shutdown conditions.	Certified Design Material
The SCS and Containment Spray System (CSS) pumps are designed to be independent but identical and functionally interchangeable. Either pump in a division can provide flow to either the CSS header or the SCS heat exchanger.	Certified Design Material
With the SCS heat exchanger bypass throttle valves failed open, there is adequate flow (1000gpm) through the SCS heat exchanger to achieve cooldown over an extended time period.	Section 5.4.7.3
During plant shutdown operation, the SCS can be aligned to the IRWST to provide RCS inventory makeup or to perform a "feed and bleed" operation.	Certified Design Material
Instrumentation and controls are provided in the Remote Shutdown Panel to ensure that the SCS functions can be performed even when the main control room cannot be used due to a fire.	Certified Design Material
The SCS discharge valves are capable of opening with a delta p equal to the SCS pump shutoff head. This capability is needed for SCS injection from the IRWST to the RCS following an Aggressive Secondary Cooldown (ASC).	Certified Design Material
The SCS piping outside of containment has an ultimate strength in excess of the normal RCS pressure of 2250 psi.	Certified Design Material
The SCS pumps can be aligned to take suction from the In-Containment Refueling Water Storage Tank (IRWST). The SCS pumps can also be aligned to discharge to the IRWST via the SCS heat exchangers.	Certified Design Material
The SCS can be aligned to provide IRWST cooling. This backs up the CSS capability for providing IRWST cooling.	Certified Design Material

TABLE 19.15-1

(Sheet 7 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
19. (Continued)	
The valve isolating the SCS pump suction from the IRWST is capable of passing flow in either direction. This is required so that the SCS pump can draw suction from the IRWST to back up the appropriate CSS pump and the CSS pump can draw suction from the RCS to back up the SCS pump.	Certified Design Material
With the SCS pumps aligned to the IRWST, the pumps' NPSH is adequate to prevent pump cavitation and failure if the IRWST inventory is saturated.	Certified Design Material
The SCS pump motor in each division is not powered from the same Class 1E 4.16Kv bus as the CSS pump motor in the same division.	Certified Design Material
20. The following are some important aspects of the Safety Injection System (SIS) as represented in the PRA:	
Four redundant trains are arranged in two divisions so the two SIS divisions are completely physically separated from each other.	Certified Design Material
Each SIS pump train has an independent suction line connection to the IRWST.	Certified Design Material
The two SIS divisions are completely physically separated from each other outside containment.	Certified Design Material
Safety injection for "feed and bleed" is an important backup decay heat removal method during shutdown operation. A new technical specification was added requiring two of the four SIS trains to be available during most shutdown modes.	Section 16.3/3.5.3
Instrumentation and controls for trains 3 and 4 are provided in the Remote Shutdown Panel to ensure that the SIS functions can be performed even when the main control room cannot be used due to a fire.	Certified Design Material

TABLE 19.15-1

(Sheet 12 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
26. Aggressive Secondary Cooldown (ASC), which involves cooling of the RCS by opening the ADVs and ensuring that EFW is being delivered to both steam generators given failure of safety injection, has a significant impact on the core damage frequency contribution for small LOCAs and SGTR. Given a small LOCA or SGTR with failure of Safety Injection, the SCS can be aligned to provide the injection function if the RCS is depressurized to the SCS pump shut off head.	Certified Design Material
ABB-CE will provide EPG guidance for the use of the EFWS, and the TBS or ADVs for ASC and the alignment of the SCS for injection operation.	EOGs
27. The following are features of the System 80+ control room design which were assumed to minimize risk from fires in the control room:	
The materials in the control room panels do not independently support combusion.	Section 7.7.1.3.1
The energy sources coming into the control panels are limited to low power voltage to the maximum extent practical, thus practically eliminating potential ignition sources within the panels.	Section 7.7.1.3.1
A significant portion of the control and indication signals are interfaced to the main control panel via fiber optic cables.	Certified Design Material
28. Sufficient instrumentation and controls are provided at the Remote Shutdown Panel to bring the plant to safe shutdown in case the main control room must be evacuated. Indication and control are provided for EFW, SCS, ADVs, SIS, RDS, CCWS, and SSWS (ITAAC).	Certified Design Material
Equipment that do not have dedicated instrumentation and controls at the Remote Shutdown Panel can be controlled via the operator's module. This provides the ability to control most plant functions, albeit on a limited basis, from the Remote Shutdown Panel.	Section 7.4

TABLE 19.15-1

(Sheet 13 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
29. A control room fire will not impact the instrumentation and controls located at the Remote Shutdown Panel, or the equipment which is required to place the plant in cold shutdown, due to the following features of the System 80+ design:	
The main control room and the remote shutdown room are located at different elevations and in different fire areas.	Certified Design Material
The main control room ventilation system is different from the ventilation system for the remote shutdown room.	Certified Design Material
The stairwells connecting the main control room and the remote shutdown room are pressurized, thus not allowing smoke, hot gases and fire suppressants to migrate from one room to the other.	Section 9.4, Figures 1.2-5A through 1.2-9
The main control room is continuously pressurized to prevent the entry of smoke, hot gases, dirt and fire suppressants from other areas.	Certified Design Material
30. All fire barriers which provide separation between the two divisions are rated for at least 3 hours.	Certified Design Material
It was assumed that all fire doors and penetrations within the fire barriers are maintained with high reliability during power operation to prevent the propagation of fire from one area to the next.	D-RAP
31. The possible sources of internal flooding within the Nuclear Annex and Reactor Building are located below elevation 70+0.	Certified Design Material
32. [[Solid state switching devices and electro-mechanical relays resistant to relay chatter will be used in the Nuplex 80+ protection and control systems.]]1 Use of these devices and relays either eliminates or minimizes the mechanical discontinuities associates with similar devices at operating reactors.	Sections 7.1.1.7, 7.2.1.1 & 7.3.1.1 [[COL Item 19-10 (Relay Chatter Resistance)]]1
33. The Startup Feedwater System (SFWS), a non-safety related system, can be used to deliver feedwater to the SGs following a reactor trip. The SFWS pump is powered from the Permanent Non-Safety (PNS) bus and can be powered by the AAC. The SFWS pump can be aligned to the CST or the deaerator storage tank. With alignment to either storage facility, the NPSH for the pump is adequate to prevent pump cavitation and failure.	Sections 10.4.7.2.3 & 10.4.7.2.4 Figure 8.3.1-1

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 14 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
34. There will be a diverse RCP seal injection capability using a positive displacement pump that is diverse from the CVCS and can be powered from either the EDG or the AAC. The alternative positive displacement seal injection pump is located in such a manner as to minimize its vulnerability to internal floods and fires that could also affect the primary means of providing RCP seal cooling or RCP seal injection.	Certified Design Material Figure 1.2-5A
35. An emergency containment spray backup function provides a means of supplying water to the containment spray header from a station AC independent external source. The final design of the ECSBS is not completed. The design of the ECSBS is envisioned to include the following design features: (1) an 8-inch diameter "tee" connection to the containment spray recirculation line, (2) an extension of 8-inch diameter Class 2 piping from the "tee" connection from the containment spray recirculation line to the exterior of the Nuclear Annex, (3) external connections for temporary hookup of an external source of water that are located at or near grade, (4) a portable pumping source (e.g., fire truck) that is independent of site AC power buses. This pumping device will be capable of supplying sufficient flow to the containment spray header at 24 hours after a severe accident to provide sufficient heat removal capability via the spray droplets to prevent the containment pressure from exceeding the service level C pressure. Preliminary calculations indicate a flow rate of 750 gpm would be sufficient, and (5) all necessary hoses, fittings and spool pieces would be stored with the pumping device or at or near the "tee" connections. [[The detailed system design and location of all associated valves and connections should take into account expected radiation levels and shielding requirements for any required local operator actions]]' [[The specific flow rate for the pumping device will be determined as part of the detailed design]].' [[Detailed procedures for use of the system will be developed by the COL applicant]]'	Certified Design Material Sections 6.5.5 and 19.11.3.8 [[COL Item 19-5 Sections 19.11.3.8 and 6.5.5]].' [[COL Item 19-5 Section 19.11.3.8 and 6.5.5]].' [[COL Item 19-8 Section 19.15.6]].'

1. COL information Item, See DCD information Section 1.5.2

TABLE 19.15-1

(Sheet 15 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
36. There is a Hydrogen Mitigation System (HMS) utilizing ignitors to control hydrogen during a severe accident. [[The accident management procedures will address use of the HMS.]][1]	Certified Design Material [[COL Item 19-8 Section 19.15.6]][1]
37. The Hydrogen purge Vent to the annulus is not credited in the PRA. However, the use of this vent could decrease the late containment failure probability.	EOGs
38. Each half of the subsphere is compartmentalized to separate redundant safe shutdown components, to the extent practicable while maintaining accessibility requirements. The subsphere, which houses the front line safety systems is compartmentalized into quadrants, with two quadrants on either side of the divisional structural wall. Flood barriers provide separation between quadrants, while maintaining equipment removal capability. Emergency feedwater pumps are located in separate compartments within the quadrants with each compartment protected by flood barriers. Flood barriers also provide separation between electrical equipment and fluid mechanical systems at the lowest elevation within the Nuclear Annex.	Certified Design Material
Elevated equipment pads prevent equipment from being inundated in the event of flooding.	Section 3.4.4.1
There are three-hour fire barriers as well as flood barriers between quadrants in the subsphere.	Certified Design Material
Within each division, there are two Class 1E 4160 KV switchgears. These are separated by three-hour fire barriers and are arranged to be associated with one of the subsphere quadrants. Power cables from the diesel generator room in a given division to their associated switchgear are fully separated, and the cables from the switchgear to their associated pumps are fully separated.	Section 9.5.1.14

4.16 KV

1. COL information item; See DCD. Introduction Section 1.5.2.

TABLE 19.15-1

(Sheet 16 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
39. Flood protection is integrated into the floor drainage systems. The floor drainage systems are separated by division and Safety Class 3, Seismic Category 1 valves which prevent backflow of water to areas containing safety related equipment. Each subsphere quadrant contains its own separate sump equipped with redundant Safety Class 3, Seismic Category 1 sump pumps and associated instrumentation. These pumps are also powered from the diesel generators in the event of loss of offsite power. The Nuclear Annex also has its own divisionally separated floor drainage system, having no common drain lines between divisions. Floors are gently sloped to allow good drainage to the divisional sumps. Floor drains are routed to the lowest elevation to prevent flooding of the upper elevations. The lowest elevation in each division has adequate volume to collect water from a break in any system without flooding the other division. In addition, potential discharge of fixed fire suppression systems and fire hoses is considered in the sizing of floor drains to preclude flooding of areas should the fire protection systems be initiated.	Certified Design Material Section 9.3.3
40 [[The COL should maintain a well trained and prepared fire brigade]]. 1	Section 19.15.3.2
41. The System 80+ low pressure systems which interface with the RCS are protected against ISLOCA by a combination of increases in the piping pressure limits and autoisolation capability based on pressure sensors.	Certified Design Material
42 [[The COL applicant should consider the information on risk important operator actions from the PRA as presented in Table 19.15.6-2 in developing and implementing procedures, training and other human reliability related programs]]. 1	[[COL Item 19-8 Section 19.15.6]]. 1
43 [[During detailed design phase, the COL applicant should update the PRA using the final design information and site specific information. As deemed necessary, the COL applicant should update the PRA, including the shutdown risk evaluation, and the internal fire and flood evaluation. Based on site specific information, the COL applicant should also re-evaluate the qualitative screening of external events. If any site specific susceptibilities are found, the applicable external event should be included in the updated PRA]]. 1	[[COL Item 19-6 Section 19.15]]. 1

1. COL information item;
See DCD Introduction Section 1.5.2.

TABLE 19.15-1

(Sheet 17 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
44. The structure that houses the combustion gas turbine must have a HCLPF of at least that of the gas turbine itself, or must be designed in such a manner so that failure of this structure following a seismic event up to HCLPF of the gas turbine will not affect the operability of the gas turbine.	Section 19.7.5.3
45. During the HFE V&V, the risk significance of tasks impacted by findings will be considered in the finding resolution process. The resolution process will qualitatively confirm that the findings, as dispositioned, will not lead to a risk-significant increase in error potential from that represented in the HRA, or additional risk-significant errors not modeled in the HRA. ("Human Factors Engineering Verification and Validation Plan for NUPLEX 80+", NPX80-IC-VP790-03, Section 8.1)	Supports Certified Design Material
46. No water lines are routed above or through the control room and the computer room. HVAC water lines contained in rooms around the control room are located in rooms with raised curbs to prevent leakage from entering the control room.	Section 3.4
47. A reactor cavity flood system is provided to enhance the coolability of ex-vessel core debris. [[Procedures for use of the cavity flood system during a severe accident will be developed by the COL applicant as part of their plant-specific severe accident management procedures. The reliability of the cavity flood system and associated valves is important. The COL applicant will ensure the reliability of the cavity flood system.]][1].	Certified Design Material [[COL Item 19-8, Section 19.15.6]][1]. D-RAP, Table 19.15.6-1

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15-1

(Sheet 18 of 18)

SIGNIFICANT PRA-BASED SAFETY INSIGHTS FOR SYSTEM 80+

INSIGHT	DISPOSITION
48. Containment integrity is important to reduce the risk to the public. The major containment penetrations (equipment hatch, personnel airlocks and fuel transfer tube) will be designed to assure that they will not fail up to ASME service level "C" for the containment shell. Penetrations will be designed and sealant materials will be selected to ensure that the seal and mounting will provide a minimum of 1 day containment integrity.	D-RAP, Table 19.15.6-1
Containment integrity is important to reduce the risk to the public. The major containment penetrations (equipment hatch, personnel airlocks and fuel transfer tube) will be designed to assure that they will not fail up to ASME service level "C" for the containment shell. Penetrations will be designed and sealant materials will be selected to ensure that the seal and mounting will provide a minimum of 1 day containment integrity.	D-RAP, Table 19.15.6-1
49. The reliability of the MSSVs, ADVs, and MSIVs is important. The COL applicant will ensure the reliability of these components.	D-RAP, Table 19.15.6-1
50. Flood barriers separating the flood zones in the nuclear annex, the CCWS Heat Exchanger buildings and the SSWS pump structure are designed to withstand water pressure generated by internal flooding .	Certified Design Material
Flood barriers, including water tight doors and penertations, will be addressed in the O-RAP.	D-RAP, Table 19.15.6-1

Operation reliability assurance process.

Reactor Cavity Design for Debris Coolability

Another feature of the reactor cavity that is important to severe accident progression is the ability to quench and cool core debris in the cavity. The flow area in the System 80+ design meets the EPRI debris spreading criterion to enhance the potential for debris cooling. In addition, the reactor Cavity Flooding System (CFS) is designed to flood the reactor cavity in the event of a severe accident for the purpose of covering the core debris with water and maintaining a long-term debris coolability. The CFS also serves to scrub fission products. The CFS is designed to flood the reactor cavity in the event of a severe accident using water from the HVT portion of the containment water storage system.

Hydrogen Mitigation System

The System 80+ design incorporates a deliberate ignition system to maintain containment hydrogen concentrations below a detonable limit. The system uses igniters ~~of the glow plug design~~ and is manually remote controlled. Because of the proven design of the glow plug igniters and the reliability of the electrical distribution system used in the System 80+ design, the Hydrogen Mitigation System (HMS) is a significant risk reduction contributor to containment failure.

19.15.2 INTERNAL EVENTS RISK PROFILE INSIGHTS

19.15.2.1 Core Damage Frequency of the Level I PRA

The Level I portion of the System 80+ PRA addresses the internal (and the external) initiators of accident sequences which lead to core damage. Core damage is assumed to occur if the collapsed level in the reactor has decreased such that the active fuel in the core is uncovered and a temperature of 2200°F or higher is reached in any node of the core as defined in best-estimate thermo-hydraulic calculations. The methodology for the Level I portion of the PRA for internal events complies with the recommendations of the PRA Key Assumptions and Groundrules of EPRI ALWR Requirements Document[7]. The small event tree/large fault tree (fault tree linking) approach was used to evaluate core damage frequency. Generic industry data, as presented in the EPRI ALWR Requirements Document[7], was used to perform the PRA. The methods used for the external events evaluation are summarized in Section 19.15.3.

The core damage frequency for internally initiated events is summarized in Section 19.15.2.1.1. The dominant accident sequences and their major contributors to core damage frequency for internal events are summarized in Section 19.15.2.1.2. In Section 19.15.2.1.3, the impact of several System 80+ design features, as they relate to the reduction of core damage frequency for internal events, are presented. Finally, the insights drawn from the uncertainty, sensitivity, and importance analyses are presented in Section 19.15.2.1.4.

19.15.2.1.1 Core Damage Frequency by Initiating Events

~~The estimated core damage frequency attributable to internal events for the System 80+ plant is 1.7E-06. Table 19.15.2-1 presents the core damage frequency contributions by initiating events (for comparison, the core damage frequency for the Standard System 80 design is also presented). The core damage frequency of the System 80+ design is a factor of 128 less than the core damage frequency of the System 80 design. This factor was derived using the same groundrules of the System 80 PRA. The relative contributions (percent of total) of the various internal events to the total core damage frequency are tabulated in Table 19.15.2-1 and shown graphically in Figure 19.15.2-1.~~

For the System 80 design, loss of offsite power and station blackout dominates (47%) the core damage frequency profile. This is followed by the LOCAs ~~(32%)~~ and then transients ~~(15%)~~. The contribution by ATWS is relatively small ~~(6%)~~. For the System 80+ design, the LOCA categories of initiating events dominate ~~(37%)~~ the core damage frequency profile. This is followed by the transient category ~~(34%)~~ of events and SGTR category ~~(10%)~~ of events. The contribution from loss of offsite power (including

station blackout) is relatively small because of the following features that were incorporated into the design:

A. Multiple independent connections to the grid.

B. Turbine-generator runback capability to maintain hotel loads.

C. Alternate standby AC source (combustion turbine).

D. Six vital 125 VDC batteries.

The contribution from ATWS is also relatively small.

19.15.2.1.2 Dominant Accident Sequences for Internal Events

The general assumptions that were made in developing the accident sequences are outlined below. Assumptions that are applicable to specific accident sequences are outlined under the appropriate initiating event. ~~System oriented assumptions, which include success criteria, are provided in the various subsections of Section 19.6. Because of the large number of system assumptions, they are not repeated in this section.~~

A. Except for a large or medium Loss of Coolant Accident (LOCA), a reactor trip is the primary means of reactivity control for all initiating events.

B. For accident sequences that include failure of containment heat removal or failure to cool the IRWST, it was assumed that the CVCS can provide an alternative source of borated water to replenish the IRWST inventory. Some IRWST inventory (in the form of steam - flashing) will be lost after the containment fails.

C. The list of initiating events analyzed during power operation was assumed to be complete and comprehensive. This list was generated based on initiating events addressed in previous PRAs, guidance from the PSA Procedures Guide, and features which are unique to the System 80+ design.

D. For those accident sequences which include inoperable systems/components due to loss of power to the system/components, it was assumed that certain operator recovery actions could be performed to restore power to the affected systems/components, and consequently prevent core damage.

E. It was assumed that, in general, mechanical failures of components cannot be repaired within the 24 hour mission time. As a result, mechanical failures are assumed to be

non-recoverable and are therefore not credited as a means of preventing core damage.

F. For all initiating events, except large and medium LOCAs, it was assumed that the preferred means of removing decay heat from the reactor is via the steam generator(s). If decay heat cannot be removed via this means,then "feed and bleed" is an alternate means of accomplishing this function.

G. Steam removal from the secondary side is the preferred means of removing decay heat from the reactor core during the short-term phase of decay heat removal. Because of the diverse and redundant paths available for steam removal, failure to accomplish this function is assumed to be an extremely low probability event (when compared to failure of other functions on the event trees). Hence, failure of this function is not explicitly modeled in the event trees.

H. For transient and small LOCA sequences where long-term decay heat removal is accomplished via long-term emergency feedwater delivery, it was conservatively assumed that the Emergency Feedwater Storage Tank (EFWST) inventory would need to be replenished within the 24 hour mission time. ~~Calculations have indicated that the EFWST inventory would last much longer than 24 hours.~~

The dominant accident sequences due to internal initiated events and their contributions to the core damage frequency for the System 80+ design are presented in Table 19.15.2-2. The dominant accident sequences are described below.

LOSS OF FEED FLOW EVENTS

The following assumptions were made for the loss of feed flow accident sequences.

A. Following a reactor trip, it was assumed that the RCS pressure will not increase to the lift pressure of the Primary Safety Valves. Hence, consequential PSV induced LOCA was not modeled.

B. The Startup Feedwater System can be used to deliver feedwater to the steam generators following a reactor trip. Because this system is connected to the main feedwater system it was assumed to be also unavailable following a loss of main feedwater event.

Four dominant accident sequences were identified for loss of main feedwater flow events, LOFW-9, LOFW-4, LOFW-8, and LOFW-5. ~~The calculate frequencies for these accident sequences are 4.4E-07, 3.6E-08, 2.1E-08, and 5.1E-09 per year respectively.~~

STEAM GENERATOR TUBE RUPTURE (SGTR) EVENTS

The following assumptions were made for Steam Generator Tube Rupture (SGTR) accident sequences.

A. The representative SGTR event was assumed to be a complete severance of a single tube. Multiple tube ruptures are less likely than a single tube rupture. In addition, the success criteria of the systems called upon to respond are substantially the same as those for a single tube rupture. Therefore, multiple tube ruptures are not addressed separately.

B. Following a turbine and reactor trip, the secondary side pressure may increase to the lift pressure of the first bank of Main Steam Safety Valves (MSSVs).

Five dominant accident sequences were identified, SGTR-17, SGTR-9, SGTR-16, SGTR-12, and SGTR-8. ~~The calculated frequencies for those dominant sequences are 2.7E-07, 3.1E-08, 1.5E-08, 6.9E-09, and 3.1E-09 per year respectively.~~

A. SGTR-17 is an accident sequence which involves a steam generator tube rupture event followed by failure of the Safety Injection System (SIS) and the inability to aggressively cooldown the secondary side of the plant to initiate shutdown cooling injection. Failure of SIS results in loss of the preferred way of making-up and controlling the lost RCS inventory. By aggressively cooling down and depressurizing the RCS, the SCS can be used to provide the necessary makeup to the reactor core. Therefore, a failure of SIS and failure to establish aggressive cooldown results in core damage. The dominant contributors to this sequence are: (1) common cause failure of the safety injection line check valves, (2) common cause failure of safety injection line motor operated valves, (3) common cause failure of safety injection pumps to start or run, and (4) operator fails to perform aggressive cooldown.

Aggressive Secondary Cooldown (ASC) has a significant impact on the core damage frequency contribution for SGTR. Therefore, the emergency operating procedures for responding to as SGTR should specifically address ASC. This should include procedural steps for early identification of the failure of safety injection and specific steps for instituting the cooldown by opening the ADVs and ensuring that EFW is being delivered to both generators. The procedure should also specify that even if ASC is in progress, the ruptured steam generator should be isolated when the RCS temperature and pressure have decreased to the point at which there is reasonable assurance that the MSSVs on the ruptured generator will not lift. The procedures

the EFW pump discharge check valves, (3) operator fails to initiate "feed and bleed", and (4) common cause failure of the "feed and bleed" valves.

E. SGTR-8 is an accident sequence which involves a Steam Generator Tube Rupture event followed by an unisolable leak in the ruptured steam generator and failure to maintain secondary heat removal. Unisolable leak results in the increase in the level and, subsequently, pressure in the ruptured steam generator rises. Therefore, failure to maintain secondary heat removal results in loss of decay heat removal from the reactor core. This scenario leads to core damage. The dominant contributors to this sequence are: (1) common cause failure of the Atmospheric Dump Valves (ADVs) and (2) failure of the Condensate Storage Tank (CST) discharge manual and check valves to open.

SMALL LOCA EVENTS

The following assumptions were made for the small Loss of Coolant Accident (LOCA) sequences.

A. The break size is not large enough to remove decay heat from the core. Therefore, the removal of decay heat via the secondary side is required.

B. If the Safety Injection System (SIS) fails to control and maintain RCS inventory, it was assumed that the Shutdown Cooling System (SCS) can be used to provide RCS inventory control provided an aggressive depressurization of the RCS is performed.

Three dominant accident sequences were identified for small Loss of Coolant Accident (LOCA) events, SL-11, SL-10, and SL-4. ~~The calculated frequencies for these dominant accident sequences are 1.6E-07, 9.0E-09, and 8.9E-09 per year, respectively.~~

A. SL-11 is an accident sequence which involves a small break loss of coolant followed by failure of SIS and failure to aggressive cooldown the secondary side. To mitigate a small LOCA, makeup of the lost reactor coolant must be provided. Normally the SIS provides this function, but for this sequence it fails. The other line of defence would be to aggressively cooldown the secondary side and use the SCS pumps to provide the needed makeup. Aggressive cooldown also fails and the lost coolant is not restored. Consequently, core damage occurs. The dominant contributors to this sequence are: (1) common cause failure of the safety injection line check valves, (2) common cause failure of the safety injection line motor valves, (3) common cause failure of the safety injection pumps to start or run, and (4)

A. A reactor trip is not required to mitigate a medium LOCA event.

B. The break size is large to remove decay heat from the reactor core. Therefore, the removal of decay heat via the secondary side is not required.

C. SIT injection is not required for RCS inventory control and prevention of significant core damage for a medium LOCA.

Two dominant accident sequences were identified for medium LOCA events, ML2-3 and ML1-3. ~~The calculated frequencies for these accident sequences are 1.6E-07 and 1.4E-07, respectively.~~ (To facilitate the definition and evaluation of the Plant Damage States (PDS) for the containment response analysis, the medium LOCA category of events were split into two separate events bases on the estimated in-vessel pressure at the time of the onset of core damage.)

A. ML2-3 is an accident sequence which involves a medium LOCA event followed by failure of the SIS. Failure of the SIS during the early phase of the medium LOCA (i.e., during direct vessel injection) results in failure to provide makeup to the reactor core and also to remove heat from the core. Failure of the SIS during the latter phase of the medium LOCA (i.e., simultaneous hot-leg and direct vessel injection) results in boron crystallization which blocks flow through the core and consequently core damage occurs. The dominant contributors to this sequence are: (1) common cause failure of the hot-leg isolation valves, (2) common cause failure of the safety injection line check valves, (3) common cause failure of hot-leg check valves, (4) operator fails to initiate hot-leg injection, and (5) common cause failure of the safety injection line motor valves.

B. ML1-3 is an accident sequence which is similar to ML2-3, except that the in-vessel pressure at the onset of core damage is less than the in-vessel pressure associated with ML2-3 sequence.

LARGE LOCA EVENTS

The assumptions for the large LOCA sequences are similar to assumptions A and B for the medium LOCA sequences and are therefore not repeated.

Two dominant accident sequences were identified for large LOCA events, LL-3 and LL-4. ~~The calculated frequencies for these accident sequences are 1.1E-07 and 4.7E-09, respectively.~~

A. LL-3 is an accident sequence which involves a large loss of coolant followed by failure of the SIS. The inventory of

the Safety Injection Tanks (SITs) discharges into the RCS to provide the instantaneous makeup required following the rapid depressurization of the RCS caused by the large LOCA. The SIS then failed to provide its function. Failure of the SIS during the early phase of the medium LOCA (i.e., during direct vessel injection) results in failure to provide makeup to the reactor core and also to remove heat from the core. Failure of the SIS during the latter phase of the medium LOCA (i.e., simultaneous hot-leg and direct vessel injection) results in boron crystallization which blocks flow through the core and consequently core damage occurs. The dominant contributors to this sequence are: (1) common cause failure of the safety injection line check valves, (2) common cause failure of the safety injection line motor valves, (3) common cause failure of the hot-leg check valves, (4) common cause failure of hot-leg isolation valve, and (5) operator fails to initiate hot-leg injection.

B. LL-4 is an accident sequence which involves a large loss of coolant followed by failure of the SITs. The required instantaneous makeup of reactor coolant is not provided and consequently core damage occurs. The dominant contributors to this sequence are: (1) common cause failure of safety injection line check valves, and (2) common cause failure of SIT discharge check valves.

VESSEL RUPTURE EVENT

This event is defined as any breach of the primary pressure boundary that causes loss of reactor coolant in excess of the capacity of the SIS. If this event were to occur, it is assumed that it would lead directly to core damage and there are no sequences with mitigating system failures associated with it. ~~The estimate frequency for this event is 1.0E-07 per year.~~

OTHER TRANSIENT EVENTS

The following assumptions were made for transient accident sequences other than loss of main feedwater flow.

A. The Startup Feedwater System or the Emergency Feedwater System can be used to deliver feedwater to the steam generators following a reactor trip.

B. Following a reactor trip for a loss of condenser vacuum initiating event, the RCS pressure may approach the lift pressure of the Primary Safety Valves (PSVs). Hence, consequential PSV induced LOCA for loss of condenser vacuum was modeled.

Other Transients are those non-LOCA events other than loss of main feedwater in which a process parameter perturbation leads to a reactor trip. Four dominant accident sequences were identified for Other Transient events, TOTH-4, TOTH-12, TOTH-5, and TOTH-9. ~~The calculated frequencies for these accident sequences are 6.9E-08, 2.7E-08, 6.9E-09, and 2.3E-09 per year, respectively.~~

A. TOTH-4 is an accident sequence which involves a transient other than loss of main feedwater followed by failure of long-term decay heat removal and failure of the SIS. The EFWS is used during the early phase of plant cooldown to remove decay heat from the RCS. Once SCS entry conditions are met, long-term decay heat removal is normally initiated to continue the cooldown process. This function is not accomplished for this sequence because of failure of the SCS during initiation or during operation and makeup to the emergency feedwater storage tanks is not provided. Without the added makeup the EFWS cannot continue the decay heat removal process. Failure of long-term decay heat removal using the SCS and the EFWS would then cause operator to initiate "feed and bleed". However for this sequence, the SIS also fails and "feed" cannot be accomplish. As a result, the decay heat removal process is terminated and core damage eventually occurs. The dominant contributors to this sequence are: (1) common cause failure of safety injection line check valves, (2) independent failure of CST make-up valve (check or manual), and (3) operator fails to align CST to EFW Storage Tanks.

B. TOTH-12 is an accident sequence which involves a transient, failure of the primary safety valves (PSVs) to re-seat, and failure of the safety injection system (SIS). Because of the pressure transient associated with this event, the primary safety valves open to relieve primary pressure. However, the valves do not re-seat as required and a PSV induced LOCA occurs. The SIS would provide make-up for the lost RCS inventory under these conditions, but the SIS fails and consequently core damage eventually occurs. The dominant contributors to this sequence are: (1) failure of the PSVs to re-seat, (2) common cause failure of the safety injection line check valves, (3) common cause failure of the safety injection line motor operated valves, and (4) common cause of the safety injection pumps to start or to run.

C. TOTH-5 is an accident sequence which involves a transient other than loss of main feedwater followed by failure of long-term decay heat removal and failure of the SDS. This sequence is similar to TOTH-4, except that "bleed" fails instead of "feed". The dominant contributors to this sequence are: (1) common cause failure of the SCS suction valves, (2) failure of the CST make-up valve (check or manual), (3) operator fails to initiate "feed and bleed",

(4) common cause failure of the "feed and bleed" valves, and
(5) operator fails to align CST to EFW Storage Tanks.

D. TOTH-9 is an accident sequence which involves a transient other than loss of main feedwater followed by failure of the EFWS, the Startup Feedwater System (SFWS), and the SDS. The inability to deliver feedwater to the steam generators terminates the preferred means of removing decay heat. "Feed and bleed" operation then becomes the next alternative for removing heat from the core. Both the "feed" portion and the "bleed" portion must function for this operation to be successful. For this sequence, the SDS also fails to provide "bleed" and therefore all mean of removing decay heat from the core is lost. Consequently, core damage eventually occurs. The dominant contributors to this sequence are: (1) common cause failure of the EFW distribution line check valves, (2) common cause failure of the EFW pump discharge check valves, (3) failure of the startup feedwater pump to start, and (4) operator fails to initiate "feed and bleed".

ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS) EVENTS

The following assumptions were made for Anticipated Transient without Scram (ATWS) accident sequences.

A. It was assumed that if the peak RCS pressure resulting from an ATWS event exceeds the ASME level C stress limits, the RCS pressure boundary will be breached and the SIS isolation check valves will be deformed so that they will not open.

B. Sufficient negative Moderator Temperature Coefficient (MTC) will preclude the RCS peak pressure from exceeding the level C stress limits.

C. It was assumed that at least three of the four primary safety valves must open to prevent the RCS pressure from exceeding the level C stress limits.

D. Once the RCS pressure is relieved, the PSVs should re-close. It was assumed that if any PSV fails to re-close, reactor coolant will be lost through the stuck open PSV and the leak is equivalent to a medium LOCA.

E. Because of the high differential pressure between the primary and secondary sides, a consequential steam generator tube rupture may occur following an ATWS event.

Two dominant accident sequences were identified for ATWS events, ATWS-29 and ATWS-9. ~~The calculated frequencies for these accident sequences are 4.7E-08 and 2.9E-09 per year, respectively.~~

A. ATWS-29 is an accident sequence which involves a transient without scramming the reactor in conjunction with an adverse Moderator Temperature Coefficient (MTC). For this sequence, the MTC is not negative enough to reverse by reactivity feedback the increasing temperature and pressure of the RCS. As a result the reactor vessel eventually fails.

B. ATWS-9 is an accident sequence which involves ATWS followed by successful delivery of emergency feedwater to the steam generators, failure to deliver borated water to the RCS, and failure of "bleed" operation. Failure to borate the RCS prohibits the ability to decrease the reactivity, and therefore reactivity control cannot be accomplished. The failure of "bleed" prevents the depressurization of the RCS to allow the injection of borated water by the safety injection pumps. The dominant contributors to this sequence are: (1) operator fails to initiate boron delivery via the CVCS, (2) operator fails to initiate "feed and bleed", and (3) common cause failure of the "bleed" valves.

LOSS OF OFFSITE POWER (LOOP)/STATION BLACKOUT (SBO) EVENTS

The following assumptions were made for Loss of Offsite Power (LOOP) and Station Blackout (SBO) accident sequences.

A. A loss of offsite power event includes loss of the two offsite power sources (switchyards), and the turbine/generator does not run back and maintain hotel loads such that actuation of the emergency power source is required.

B. Best estimates analyses show that the increase in RCS pressure following a LOOP event is well below the lift pressure of the PSVs. Therefore, a LOCA due to failure of the PSVs to reseat is not modeled.

C. If AC power (alternate AC source or offsite power) cannot be restored within 10 hours, station blackout with complete depletion of the batteries will occur and core damage will also occur.

Three dominant accident sequences were identified for LOOP/SBO events, LOOP-9, LOOP-8, and SBO. ~~The calculated frequencies for these sequences are 3.9E-09, 3.4E-09, and 2.1E-08 per year, respectively.~~

A. LOOP-9 is an accident sequence which involves a loss offsite power followed by failure of the EFWS, and failure of the SDS. For this sequence, the primary safety valves open and re-seat as required following the plant trip. Because the EFWS has failed, the removal of decay heat from the reactor core via the steam generators cannot be accomplished. "Feed

and bleed" would be the next means of removing decay heat, but the SDS also fails. "Bleed" is not accomplish because of SDS failure. As a result, all means of removing decay heat from the core is now lost and core damage eventually occurs. The dominant contributors to this sequence are: (1) common cause failure of the EFW distribution line check valves, (2) common cause failure of the EFW pump discharge check valves, (3) operator fails to initiate "feed and bleed", and (4) common cause failure of the "bleed" valves.

B. LOOP-8 is an accident sequence which is similar to LOOP-9, except that the "feed" portion of "feed and bleed" fails instead of "bleed". The dominant contributors to sequence LOOP-8 are: (1) common cause failure of the EFW turbine-driven pumps, (2) common cause failure of the emergency diesel generators to operate, (3) common cause failure of the emergency diesel generators on demand, and (4) common cause failure of the EFW distribution line check valves.

C. SBO is treated as a special LOOP event. For this event, the offsite power sources, the onsite emergency diesel generators, and the alternate AC source are unavailable. Therefore, the only mitigating system available is the EFWS, using the turbine-driven pumps. After eight hours the batteries would be depleted if an AC power source is not restored. Once the batteries are depleted, long-term decay heat removal would be terminated and core damage eventually occurs. The dominant contributors to this sequence are: (1) common cause failure of the emergency diesel generators on demand, (2) failure to start and load standby AC source, (3) common cause failure of DG sequencers, and (4) failure of the emergency diesels to start and load.

LOSS OF HVAC EVENTS

The following assumptions were made for Heating, Ventilation and Air-Conditioning (HVAC).

A. The loss of one division of HVAC was assumed to be any failure in one of the two divisions of HVAC that is not restored before a critical temperature is exceeded in a room containing temperature sensitive electrical and electronic equipment. The temperature sensitive equipment is assumed to fail and cause the loss of control for the associated division of safety related systems. Consequently, one division of safety related systems would be unavailable to perform their functions.

One dominant accident sequence was identified for loss of HVAC events, LHV-5. ~~The calculated frequency for this accident sequence is 4.0E-09 per year.~~

A. LHV-5 is an accident sequence which involves loss of one division of HVAC followed by failure of long-term decay heat removal and failure of SDS. The Emergency and Startup Feedwater systems are used to remove decay heat from the RCS until shutdown cooling entry conditions are met. Once shutdown cooling conditions are met, the SCS would then be used to remove decay heat. However for this sequence, the SCS fails either during initiation or during operation and the EFWS cannot continue to remove decay heat because makeup to the Emergency Feedwater Storage Tanks is not provided. Failure of the feedwater and shutdown cooling systems causes the preferred means of removing decay heat to be lost. "Feed and bleed" would then be the alternate means of removing decay heat from the core. The SDS is used to provide the "bleed" function in the "feed and bleed" operation, but this system also fails. Failure of both the preferred and the alternate means of removing decay heat eventually causes core damage to occur. The dominant contributors to this sequence are: (1) common cause failure of the "bleed" valves, (2) operator fails to initiate "feed and bleed", (3) failure of the SCS suction valve, (4) failure of the CST makeup valve (check or manual), and (5) operator fails to align CST to EFW Storage Tanks.

LARGE SECONDARY SIDE BREAK (LSSB) EVENTS

The following assumptions were made for Large Secondary Side Break (LSSB) accident sequences.

A. The location of an LSSB event (inside containment or outside containment) is not modeled because plant and operator responses with respect to core damage prevention will be similar.

B. It was assumed that there is a potential for return to power if the rod with the most negative reactvity worth is stuck outside the core and the RCS is not borated.

One dominant accident sequence was identified for LSSB events, LSSB-9. ~~The calculated frequency for this sequence is 2.1E-09 per year.~~

A. LSSB-9 is an accident sequence which involves a Large Secondary Side Break event followed by failure of the EFWS and failure of the SDS. For this sequence, the EFWS fails to deliver feedwater to the intact steam generator. If decay heat cannot be removed via the steam generator, the "feed and bleed" would be the next alternative. Both the "feed" portion and the "bleed" portion must operate successfully to remove decay heat. The SDS which performs the "bleed" operation also fails in this sequence. The removal of decay heat from the core is therefore terminated

and core damage eventually occurs. The dominant contributors to this sequence are: (1) common cause failure of the EFW distribution line check valves, (2) common cause failure of the EFW pump discharge check valves, (3) operator fails to initiate "feed and bleed", and (4) common cause failure of the "bleed" valves.

19.15.2.1.3 Risk-Reduction Design Features

The System 80+ possesses several features, as described in Section 19.15.1.1, that are beneficial to reducing the frequency of core damage. The major reductions in core damage frequency (CDF), when compared with System 80, are associated with:

A. LOOP/SBO events, ~~(CDF reduced from 3.8E-05 to 2.8E-08)~~

B. Transient (Loss of Main Feedwater and Other Transient) events, ~~(CDF reduced from 1.2E-05 to 5.7E-07)~~

C. Steam Generator Tube Rupture events, ~~(CDF reduced from 1.1E-05 to 3.0E-07)~~

D. Small LOCA events, and ~~(CDF reduced from 9.4E-06 to 2.1E-07)~~

E. ATWS events, ~~(CDF reduced from 4.8E-06 to 4.9E-08)~~

The following features of the System 80+ design are the major contributors to the reduction of the core damage frequency (with respect to the System 80 design) for the above categories of internally imitated events.

A. LOOP/SBO - multiple offsite power sources, alternate standby AC power source, dedicated batteries for each emergency diesel generator, four trains of emergency feedwater (two with turbine-driven pumps), turbine-generator capable of running back to hotel loads.

B. Transients - four trains of emergency feedwater (two with turbine-driven pumps), redundant sources of emergency feedwater, high reliable normally running Component Cooling Water/Station Service Water systems, separate Startup Feedwater System (actuated before EFWS), turbine generator capable of running back to hotel loads, two redundant and diverse Emergency Feedwater Actuation Systems, once through cooling capability ("feed and bleed").

C. Steam Generator Tube Rupture - four trains of Emergency Feedwater System (two with turbine-driven pumps), four trains of safety injection, once through cooling capability ("feed and bleed").

D. Small LOCA - In-containment Refueling Water Storage Tank (eliminated the need for switch-over of pump suction), four trains of Emergency Feedwater System (with two turbine-driven pumps), four trains of Safety Injection System, once through cooling capability ("feed and bleed").

E. ATWS - larger pressurizer, larger steam generators, Safety Depressurization System, diverse protection system.

19.15.2.1.4 Insights from the Uncertainty, Sensitivity, and Importance Analyses

19.15.2.1.4.1 Insights from the Uncertainty Analysis

~~The System 80+ PRA results for internal events, as presented Table 19.15.2-3 of this report,~~ are summarized in terms of mean value and associated error factor, which is a measure of the uncertainty. (~~The~~ error factor is the average ratio between the 95th percentile to the 50th percentile and the 50th percentile to the 5th percentile.) The first 14 accident sequences listed in Table 19.15.2-2 contribute more than 90% of the overall total core damage frequency for internal events of the System 80+ design. The magnitude of uncertainties that characterize the first 14 dominant accident sequences is shown in Table 19.15.2-3. This table lists the dominant core damage sequences, the mean core damage frequency and associated error factor for each of the dominant core damage sequences, the major contributors to each ~~dominant sequence, and the error factor associated with each of the major contributors.~~ The major insights from the uncertainty analysis are listed below:

A. The majority of the major contributors to the dominant accident sequences have relatively small uncertainties (i.e., error factor less than 10) associated with them.

B. A few of the major contributors to the dominant accident sequences have relatively large uncertainties (i.e., error factor of 10 or greater). The contributors with large uncertainties included hardware failures such as common cause failure of the safety injection pumps ~~(EF = 16.1)~~, common cause failure of the emergency DG sequencers ~~(EF = 11.2)~~, independent failure of the CST manual makeup valve ~~(EF = 15)~~, and vessel rupture ~~(EF = 10.0)~~. The human errors with large uncertainties include operator fails to initiate "feed and bleed" ~~(EF = 11.7)~~, operator fails to perform aggressive secondary side cooldown following SGTR ~~(EF = 15.0)~~, operator fails to perform aggressive cooldown following a small LOCA ~~(EF = 16.6)~~, and operator fails to align CVCS to fill IRWST following SGTR ~~(EF = 25.3)~~.

C. The hardware failures and human errors with large uncertainties associated with them are the major contrib-

utors to the uncertainty associated with the calculated core damage frequency for internal events.

19.15.2.1.4.2 Insights from Level I Sensitivity Analyses

Several cases of sensitivity analyses were preformed for the System 80+ design to determine what impact, if any, the following issues would have on the core damage frequency. The sensitivity insights are summarized ~~in Table 19.15.2-4.~~ below.

OVERALL OPERATOR ERROR RATE

The probability that the operator fails to perform a specified task was determined using the SHARP[39] methodology. It has been shown in previous PRAs that the core damage frequency can be sensitive to human error probabilities. As a result, a sensitivity was performed to determine the impact on the core damage frequency for internal events. All operator error probabilities and non-recovery probabilities were increase by a factor of 10 and the total core damage frequency for internal events was then requantified. The results for this case ~~are presented in Table 19.15.2-4 as case No. 1. For this case, the results show that the "present" core damage frequency would increase by a factor of approximately 6. This implies~~ show that the core damage frequency for the System 80+ design is somewhat sensitive to operator error probabilities.

CONTROL ROOM RESPONSE

Several types of operator actions are performed during the progression of an accident sequence. Actions are performed inside the control room as well as outside the control room. An issue has arisen regarding the capability of the operator to perform mitigating actions outside the control room once an accident or transient has occurred. To address this issue, a sensitivity analysis was performed which credited only the operator actions that took place from the control room. The results, ~~case No. 2 of Table 19.15.2-4, show that the "present" core damage frequency would increase by approximately two orders of magnitude. Consequently,~~ the System 80+ design is extremely sensitive to operator actions which are performed outside the control room during the progression of an accident, ~~sequence.~~

MOTOR-OPERATED VALVE FAILURE RATE

A large number of motor-operated valves are used in safety related systems of the System 80+ design. In general, these valves are required to change position in order for the systems to perform their safety related functions. There has been a concern that the failure rates of motor-operated valves have been under-estimated. Consequently, a sensitivity analysis was

performed to address this issue. The results for this case ~~are presented in Table 19.15.2-4 as case No. 3. The results show that the "present" core damage frequency would increase by a factor of approximately 5 and~~ show that the core damage frequency for internal events is not highly sensitive to the failure rates of motor-operated valves.

SITs FOR MEDIUM LOCA

For the System 80+ PRA, a best-estimate thermo-dynamic analysis was performed to confirm the belief that the Safety Injection Tanks (SITs) were not needed to prevent core damage following a medium LOCA event. In previous PRAs, it was assumed that three of the four SITs must inject to prevent core damage from occurring following a large or medium LOCA event. This assumption is included only in the large LOCA model and not in the medium LOCA models, and a sensitivity analysis was therefore performed to address this issue. ~~The results for this case are presented in Table 19.15.2-4 as case No. 4.~~ There were no measurable changes in the ~~"present"~~ core damage frequency when the SITs were credited for preventing core damage following a medium LOCA event. The System 80+ design is not sensitive to core damage frequency for internal events this issue.

FEASIBILITY OF AGGRESSIVE SECONDARY SIDE COOLDOWN

For small LOCAs and Steam Generator Tube Ruptures (SGTRs), it was assumed that if safety injection was not available for inventory control, the RCS could be depressurized via a rapid cooldown of the secondary side then aligning the SCS pumps to provide injection for RCS inventory control. This assumption was based on analyses for the System 80 plants documented in CEN-239[9,10,11]. A confirmatory analysis was performed to demonstrate that these analyses are applicable to the System 80+ design. However, the impact on core damage if aggressive cooldown is not feasible still remained an issue and was therefore addressed via sensitivity analysis. ~~The results for this case are presented in Table 19.15.2-4 as case No. 5.~~ The results indicate that the ~~"present" core damage frequency would increase by a factor of approximately 4, and the System 80+ PRA results for internal events are~~ not highly sensitively to the ability to perform aggressive cooldown of the secondary side following a small LOCA or SGTR event.

RCP SEAL FAILURE FOLLOWING STATION BLACKOUT EVENT

With a loss of station AC power (Station Blackout), cooling water to the seals of the Reactor Coolant Pump (RCP) will be lost. The NRC has postulated in their evaluation of Station Blackout[57] that under these conditions, the seals will begin to degrade and gross seal leakage on the order of several hundred gallons per minute

may occur. The CEOG contends that this in not credible for pumps used in C-E plants[58]. A sensitivity analysis was performed to assess the impact on core damage frequency if there is a finite probability that the System 80+ RCP seals will fail following a Station Blackout (SBO) or loss of cooling water event.

In the System 80+ PRA, SBO is defined as a Loss of Offsite Power (LOOP) with demand failure of both emergency diesel generators and failure of the standby AC power source. If following an SBO, RCP failures occur, core damage can be prevented if offsite power is restored and the injection pumps are started before the core is uncovered. The available time to recover offsite power is a function of the RCP seal leak rate. For this sensitivity analysis, it was assumed that the RCP seal leak rate was such that the time available to recover offsite power before the core would become uncovered was one hour.

Loss of component cooling water, as an initiating event, will also result in the loss of cooling water flow to the seals of two of the four RCPs. ~~The results for this case are presented in Table 19.15.2-4 as case No. 6.~~

The modeling and quantification of the effects of RCP seal failure on core damage frequency show that the ~~"present"~~ core damage frequency for internal events ~~would increase by less than 1%. Thus, the System 80+ core damage frequency for internal events~~ is not sensitive to RCP seal failure following a SBO or loss of cooling water event.

COMPONENTS UNAVAILABLE DUE TO MAINTENANCE

Components in safety related systems are periodically tested per technical specification requirements. In some cases, the components may be unable to perform their safety related function during the test. In addition, if the component is found to be failed during the test, it is taken out of service for maintenance. While the component is out of service for maintenance, it is unable to perform its safety related function. Component unavailability due to test and maintenance was included in the System 80+ PRA models. A sensitivity analysis was performed to evaluate the impact on core damage frequency if it was assumed that all components were able to perform their safety related function while in test and that no maintenance was performed on safety related equipment while the plant was at power.

~~The results for this case are presented in Table 19.15.2-4 as case No. 7.~~ The results show that the core damage frequency for internal events did not change, ~~from its "present" value~~.

ADVERSE MTC

An ATWS is an event in which an anticipated transient occurs but the reactor is not shutdown by automatic insertion of the control rods. One factor that influences the progression of an ATWS event is the Moderator Temperature Coefficient (MTC). If the MTC is more positive than a calculated critical value, the peak RCS pressure will exceed the level C stress limit pressure and a non-mitigatable LOCA is assumed to occur. For System 80+, the critical MTC was calculated to be -0.30E-4 $\Delta\rho/°F$. For MTC values more positive than -0.30E-4 $\Delta\rho/°F$, the peak RCS pressure will exceed the level C stress limit pressure if less than tree PSVs open. For System 80+, it has been determined that the MTC value should be less than -0.30E-4 $\Delta\rho/°F$ for 99% of the core life. The dominant ATWS core damage sequence is (ATWS occurs) AND (MTC is adverse). A sensitivity analysis was performed to assess the impact on core damage frequency if the MTC was found to be adverse over a larger fraction of the core life.

~~The results for this case are presented in Table 19.15.3-4 as case No. 8.~~ The results ~~show that the "present" core damage frequency for internal events would increase by a factor of 1.3. This~~ indicate that the System 80+ core damage frequency for internal events is not very sensitive to the adverse MTC probability.

LOSS OF OFFSITE POWER FREQUENCY

~~For the System 80+ PRA, the core damage frequency contribution attributable to events initiated by LOOP was calculated to be 2.8E-08 per year. This represents approximately 2% of the total core damage frequency for internal events.~~ In past PRAs, the core damage frequency attributable to LOOP has been greater in both absolute value and relative contribution to the total. There are a number of reasons for the reduction in the core damage frequency contribution for LOOP for System 80+. These include: (1) the capability of the main turbine/generator to runback and pickup hotel load on loss of offsite power, (2) two separate switchyards for incoming power, (3) a four train EFW system with two 100% capacity turbine driven pumps, (4) 6 vital batteries ~~which provide an 8 hour coping capability,~~ and (5) a standby combustion turbine which can backup the emergency diesel generators.

125 V DC

Based on the first three features, a LOOP initiating event was defined as a loss of site power which required the startup and loading of the emergency diesel generators. ~~The LOOP frequency calculated for System 80+ is 5.0E-3 per year. This is almost an order of magnitude lower than a LOOP frequency based purely on the failure of the grid. This value, as presented in the KAG[7], is 3.5E-2/year.~~ A sensitivity analysis was performed to

determine the impact on the ~~"present"~~ core damage frequency if the LOOP frequency was increased by an order of magnitude. ~~The results for this case are presented in Table 19.15.2-4 as case No. 9.~~ The results ~~show that the core damage frequency would increase by approximately 20%. This~~ indicates that the System 80+ overall core damage frequency is somewhat sensitive to the frequency of LOOP.

An additional LOOP sensitivity analysis was performed to evaluate the effect of changing the base Loss of Grid frequency ~~from 0.035 per year to 0.15 per year. The effective System 80+ LOOP frequency for this case was 3.32E-2 per year as opposed to the base case frequency of 5.0E-3 per year.~~ For this case, the ~~"present"~~ core damage frequency ~~shown as case No. 9A in Table 19.15.2-4, would increase by approximately 9% which~~ is not significant.

VESSEL RUPTURE

Vessel rupture was originally evaluated in WASH-1400[14]. It is typically defined as a rupture of the vessel or a large LOCA in excess of the ECCS capabilities. Vessel rupture is assumed to directly lead to core damage. This event and its initiating frequency have essentially been accepted as is since WASH-1400 because it has little impact on the overall core damage frequency for existing plants. ~~However, it contributes approximately 6% of the core damage frequency for internal events.~~ With current materials and current manufacturing methods, it has been questioned as to whether or not vessel rupture is a credible event for an ALWR. A sensitivity analysis was therefore performed to evaluate the impact on plant core damage frequency if vessel rupture was assumed not to be credible. As expected, the ~~"present"~~ core damage frequency for internal events would decrease ~~by approximately 6%. The results for this case are presented in Table 19.15.2-4 as case No. 10A.~~

COMMON CAUSE FAILURES

~~As shown in Section 19.15.2.1.4.3,~~ The System 80+ plant core damage frequency for internal events is dominated by common cause failures. It has been contended that with: (1) complete divisional separation, (2) improved staff training, and (3) improved maintenance techniques and proper selection of components; the potential for common mode failure can be essentially eliminated. A sensitivity analysis was performed to evaluate the impact on plant core damage frequency of the assumption that all common mode failures except for diesels and batteries were eliminated. ~~The results for this case are presented as case No. 10B of Table 19.15.2-4.~~ The results of this analysis show ~~that~~ the ~~"present"~~ core damage frequency ~~would decrease by a factor of approximately 7. This is somewhat of a~~ modest decrease. Combining the assumptions that vessel rupture

is not credible and that common mode failure of equipment other than the diesel generators and batteries are not credible would decrease the "present" core damage frequency by a factor of 12. The combined impact of these two assumptions on core damage frequency would be significant.

SGTR OPERATOR ERROR FAILURE RATES

Several operator actions are required to mitigate a Steam Generator Tube Rupture (SGTR) event. These actions are performed to minimize the leakage of reactor coolant to the secondary side, to isolate the ruptured generator, and to control the level and pressure of the ruptured steam generator. By performing the operator actions when required, plant cooldown will occur in a timely manner and the integrity of the secondary side will be maintained (i.e., prevent a steam generator bypass condition from occurring).

Seven sensitivity analysis cases were performed to evaluate the impact of operator error rates on SGTR core damage frequency. The first case involved increasing the error rates of operator actions associated with steam generator tube rupture (SGTR) by a factor of 10, collectively. The second through the seventh case also involved increasing the operator error rates by a factor of 10, but on an individual basis. The impact of operator error rates on the overall core damage frequency for internal events was also evaluated for each of the seven sensitivity cases.

The results of the sensitivity cases are presented in Table 19.15.2-4a. The results for Case 1 indicate that the SGTR core damage frequency would be affected significantly by the cumulative effects of the increased operator error rates. The SGTR core damage frequency would increase by a factor of 12.5. For Case 2, the SGTR core damage frequency would increase by a factor of 9.3. The result for each of the other sensitivity cases shows that the SGTR core damage frequency would increase by less than a factor 2. It is thus concluded that the SGTR core damage frequency is highly sensitive to the cumulative effect of increasing the operator error rates by an order of magnitude. The SGTR core damage frequency is also highly sensitive to an increase in the operator error rate for failing to perform aggressive secondary cooldown by an order of magnitude. It is also concluded that except for failure to perform aggressive secondary cooldown, the SGTR core damage frequency is insensitive to an increase of a factor of 10 to the individual operator error rate.

The results presented in Table 19.15.2-4a for Case 1 also indicate that the overall core damage frequency for internal events would increase by factor of 2.6 and the increase is due to the cumulative effect of increasing the operator error rates associated with SGTR by an order of magnitude. For Case 2, the

operator error rate for failing to perform aggressive secondary cooldown was increased by an order of magnitude. Due to this change, the overall core damage frequency increased ~~by a factor of 2.3~~ slightly. The results for the other sensitivity cases show that the core damage frequency for internal events would increase ~~by 14% or less~~. It is, therefore, concluded that the overall core damage frequency for internal events is sensitive to the cumulative effect of increasing the operator error rates associated with SGTR by an order of magnitude. It is also concluded that the overall core damage frequency is sensitive to an increase of an order of magnitude to the operator error rate for failure to perform aggressive secondary cooldown.

19.15.2.1.4.3 Insights from the Importance Analyses

Importance analyses were performed at the system level and the component level for the System 80+ design. At the system level, the risk achievement and risk reduction measures of importance were calculated for the mitigating systems of the System 80+ design. The risk achievement worth is expressed as the ratio giving the factor by which risk increases due to the system of concern not being available. Likewise, the risk reduction worth is a measure of the risk that would be reduced by decreasing the unavailability of the system to zero (i.e., the system is always operating or is operable when demanded). ~~The system level measure of importance are provided in Table 19.15.2-5. The results are sorted on the risk achievement measure, with the most important system (highest risk achievement worth listed first followed by the next and the least important (lowest risk achievement worth) listed last~~. Some insights gained from the system level importance analyses are listed below:

A. The systems that would adversely impact (increase) the overall core damage frequency for internal events the most include the Electrical Distribution System, the Emergency Feedwater System, the Safety Injection System, and the Component Cooling Water/Station Service Water Systems.

B. The system that would be the most beneficial (i.e., system with a high reliability) in reducing the overall core damage frequency for internal events is the Emergency Feedwater System followed by the Safety Injection System and then the Safety Depressurization System.

Several importance measures were also calculated for the events of the System 80+ PRA. The calculated component importance measures are:

A. FUSSELL-VESELY - The Fussell-Vesely importance gives the risk associated with a given component or event. This importance measure determines how much the component is contributing to the overall core damage frequency.

B. BIRNBAUM - The Birnbaum importance measures the difference in core damage frequency with and without the occurrence of an event. The Birnbaum gives the increase in risk associated with the failure of a component.

C. CRITICALITY - The Criticality importance measure gives the core damage frequency that the system failure is a result of the failure of a critical component.

D. RISK ACHIEVEMENT WORTH - The Risk Achievement Worth is expressed as a ratio giving the factor by which risk increases due to a component not being available.

E. RISK REDUCTION WORTH - The Risk Reduction Worth is a measure of the risk that would be reduced by reducing the unavailability of the component of interest to zero.

F. UNCERTAINTY IMPORTANCE - The Uncertainty Importance is the measure of the standard deviation about the mean frequency. By reducing the uncertainty of a given event, the uncertainty of the overall core damage frequency will also decrease. This importance measure identifies those events whose uncertainty contributes the most to the overall core damage frequency.

The importance measures are calculated to analyze how each basic event influences the overall core damage frequency and to analyze how the events ranks against one another.

~~A list of component importance measures is presented in Table 19.15.2-6. The components are sorted according to their risk achievement worth. The most important (highest risk achievement worth) component is listed first followed by the next important component. Finally, the least important (lowest risk achievement worth) component is listed last~~. The following general insights are provided for the component importance measures:

A. Of the top fifty components listed, with respect to risk achievement worth, common cause failures are the most important category ~~(34 failures),~~ followed by initiating events ~~(8 events),~~ then independent faults ~~(4 faults),~~ and then human errors ~~(4 events)~~.

B. Because of the redundancy and diversity of the mitigating systems, independent faults are not the most important (high risk achievement worth) events that would adversely impact the core damage frequency for internal events.

C. Common cause failures of Electrical Distribution System components are important (high risk achievement worth) events. These events include: (1) common cause failure of the 125 VDC class 1E buses, (2) common cause failure of the 480 VAC load center transformers, (3) common cause failure of the 4.16 KV class 1E buses, (4) common cause failure of 480 VAC class 1E load centers, and (5) common cause failure of 480 VAC motor control centers.

D. Common cause failures of the distribution line check valves and the pump discharge check valves in the Emergency Feedwater System are also important (high risk achievement worth) events.

E. Several operator errors also have high risk achievement worth. Such events include: (1) operator fails to initiate hot-leg injection, (2) operator fails to align the CST to the Emergency Feedwater Storage Tanks, (3) operator fails to reclose ADVs on ruptured SG-2, and (4) operator fails to initiate "feed and bleed".

F. The most important (high risk achievement worth) independent faults are associated with failure of the CST valves. These valves are used primarily to provide makeup to the emergency feedwater storage tanks in order to continue and maintain the decay heat removal from the reactor core.

G. Loss of main feedwater is the most important (highest risk reduction worth) event in terms of reducing the ~~"present"~~ core damage frequency for internal events.

H. Common cause failure of the safety injection line check valves (which are used during safety injection, SCS injection, and shutdown cooling operations) is the next important event in terms of risk reduction. ~~The "present" core damage frequency of internal events would decrease by approximately 30%, if common cause failure of the safety injection line check valves never occurred.~~

I. Operator errors also play a big part in reducing the ~~"present"~~ core damage frequency for internal events. The most important operator errors in terms of risk reduction worth are: (1) operator fails to initiate "feed and bleed" ~~= 20% reduction~~, (2) operator fails to provide aggressive secondary cooldown following a Steam Generator Tube Rupture event ~~= 19% reduction~~, and (3) operator fails to provide aggressive secondary cooldown following a small LOCA event ~~13% reduction~~.

19.15.2.2 Analysis of Containment Performance and Source Terms - Level II PRA

The objective of the containment response analysis is to ascertain the likelihood, magnitude, and timing of radiological releases to the environment following a severe accident. In order to determine the consequences of an accident, each of the accident sequences identified as leading to core damage in the Level I PRA is further analyzed to determine if it will lead loss of containment integrity, and if so, the nature of its associated release. The mode and timing of the containment failure and the nature of the releases are affected by the physical phenomena of the accident. The combinations of these physical phenomena define specific event sequence with unique consequences. These

combinations of consequences are the potential Plant Damage States (PDSs) resulting from the accident. The parameters used to define the PDSs are based on factors that have the greatest effect on the public and include the following:

A. Source term magnitude and isotopic content.

B. Energy of the release.

C. Duration of the release.

D. Warning time for evacuation.

Based on the qualitative evaluation of the containment response phenomena for System 80+ design, a set of ~~eight~~ PDS parameters and their associated values were defined. Several ~~(6480)~~ possible combinations of parameter values for the ~~eight~~ PDS parameters were noted, all of which were not physically possible. Therefore, a set of rules were developed and applied to delete the combinations that were physically impossible. ~~After applying the deletion rules, 345 logical PDSs survived the screening~~. In order to ascertain the information for mapping the core damage sequences into the appropriate PDS, six containment safeguard states were developed. These containment safeguard states were linked with the dominant core damage sequences to form plant accident states which contained enough information to be mapped directly into the PDSs. ~~Twenty six of the 89 accident sequences for internal events and 3 of the 9 accident sequences due to tornado strikes were linked with the containment safeguard states to form plant accident states. Approximately 67% of the plant accident states had frequencies below a certain screening value and were therefore eliminated from further evaluation. The eliminated plant accident states represent 1% of the overall core damage frequency.~~

To provide some initial insight into the potential severe accident progression, the relative split of the PDSs between parameter values for major parameters was evaluated and summarized below (the percentages presented are based on the core damage frequency contribution and not sequence count):

RCS PRESSURE AT CORE DAMAGE

Approximately 18% of the PDSs are low pressure sequences, 47% are medium pressure sequences, and 35% are high pressure sequences. Of the high pressure sequences, 26% have a cycling relief valve release rate and 9% have a small LOCA release rate.

CORE MELT TIMING

Approximately 77% of the sequences resulted in core damage within 8 hours (early). Sequences resulting in core damage between 8

and 24 hours account for 21%. Only one PDS with two sequences had core damage after 24 hours. This PDS accounts for approximately 2%.

CAVITY CONDITION

The cavity was not flooded in only 8% of the sequences. For the remaining 92% of the sequences, the cavity was flooded.

CONTAINMENT SPRAY STATUS

For 81% of the sequence, the Containment Spray System was available. The Containment Spray System was not available for the remaining 19% of the sequences.

RELEASE POINT

Approximately 37% of the sequences resulted in initial releases directly to the containment. Initial releases were to the IRWST for 46% of the sequences. Approximately 17% of the sequences resulted in initial releases through the steam generators. The containment bypass sequence has a negligible contribution to the core damage frequency.

19.15.2.2.1 Containment Failure Frequency

The results from the containment response analysis show that the System 80+ containment is robust and quite capable of accommodating severe accident challenges. ~~The conditional probability for intact containment releases, RC1, is 0.887. Likewise, the conditional probabilities for the various types of containment failures are: (1) 0.079 for late containment failure releases, RC2, (2) 0.011 for early containment failure releases, RC3, (3) 0.024 for releases due to containment isolation failure, RC4, and (4) 0.0 for containment bypass failure releases, RC5.~~ The Conditional Containment Failure Probability (CCFP) is shown to be small. ~~The above results are shown in Table 19.15.2-7 and Figure 19.15.2-2.~~ Combining the CCFP with the core damage frequency calculated from the Level I portion of the PRA ~~(2.0E-06 per year)~~ results in a very low frequency ~~(2.2E-07 per year, seismic events excluded)~~ of containment failure from severe accidents.

~~A further breakdown of the contributors to the conditional containment failure probability due to the timing of core damage is shown in Tables 19.15.2-8 and 19.15.2-9. The relative contributions to CCFP for early (i.e., less than 8 hours after the initiating event occurs) core damage sequences are provided in Table 19.15.2-8. Similarly, the relative contributions to CCFP for mid (8 - 24 hours after the initiating event occurs) core damage sequences are provided in Table 19.15.2-9.~~

The insights and leading contributors to containment failure are summarized in Section 19.15.2.2.2.

19.15.2.2.2 Dominant Contributors to Containment Failure

Table 19.15.2-7 shows the fractional contributions by containment failure modes to the core damage frequency for internal and external events, excluding seismic events. The containment remained intact for about 88.7% of the core damage sequences. Of the 11.3% of core damage sequences in which the containment does fail, the late containment failure mode is the most dominant contributor followed by containment isolation failures, early containment failures, and then containment bypass failures.

The breakdown of contributors to containment failure is also shown as a pie chart in Figure 19.15.2-2. The majority of containment failures (69%) involve late containment failures. An additional 20.7% of the containment failures is due to the containment isolation failure mode followed by early containment failures and containment bypass failures with 9.6% and 0.2%, respectively.

is the next dominant failure

LATE CONTAINMENT FAILURES

The leading contributor to containment failure following a severe accident is "Late Containment Failure". This failure mode represents approximately 69% of the overall containment failure frequency. The frequency for this containment failure mode is 1.5E-7 per year. The major contributor to this failure mode includes base mat melt-through. All dry cavity cases result in containment failure and a very small percentage of the wet cavity cases are assume to result in containment melt-through.

CONTAINMENT ISOLATION FAILURES

Containment isolation failures are the second largest contributor to the frequency of containment failure. The frequency of this failure mode is 4.6E-08 per year and it accounts for approximately 21% of the overall containment failure frequency.

EARLY CONTAINMENT FAILURES

Early containment failures are the third largest contributor to the frequency of containment failure. The frequency of this failure mode is 3.1E-08 per year and it accounts for approximately 10% of the overall containment failure frequency. The major contributors to this failure mode includes rapid steam generation and steam explosions, missile or rocket impingement, hydrogen burns, and direct containment heating.

CONTAINMENT BYPASS

The containment bypass sequences are virtual non-contributors to the overall frequency of containment failure. ~~The frequency for this failure mode is 5.2E-10 per year, the majority of~~ which is cause by the Interfacing System LOCA sequence.

19.15.2.2.3 Fission Product Release Characteristics

The insights regarding the relative significance of the various fission product release classes are provided below.

RELEASE CLASSES

~~A total of 63~~ The release classes with ~~non-zero frequencies were identified. This includes 41 early core melt frequency release classes, 20 mid core melt sequence release classes and 2 late core melt sequence release class. Of these release classes, only those that had~~ frequencies above a certain screening value ~~(i.e., 1.0E-09 per year)~~ were considered for further evaluation. A noted exception to the screening is the containment bypass release class. This release class is caused by an Interfacing System LOCA. Although the frequency of this release class is less than the screening value, it is retained for further evaluation. The release classes that were eliminated from further evaluation represent ~~less than 1%~~ a small fraction of the total core damage frequency.

RELEASE CHARACTERISTICS

Each of the end-points of the Containment Event Tree (CET) uniquely specifies the status of the containment following a severe accident, whether it is intact or breached and if breached the mode of containment failure. The status of the various phenomena which have the potential to affect the source term characteristics is also uniquely specified for each end-point of the CET. As a result, each end-point of the CET represents a distinct release class which can be fully characterized by the following parameters:

A. Frequency of occurrence.

B. Isotopic content and magnitude of the release.

C. Energy of the release.

D. Time of the release.

E. Duration of the release.

F. Location of the release.

~~Values for the above parameters are summarized in Tables 19.15.2-10, except for the isotopic content and magnitude of the release which is summarized in Table 19.15.2-11. As shown in Table 19.15.2-11,~~ release class RC4.36L has the highest release fractions for the radionuclide groups. This release class represents a SGTR and containment isolation failure followed by a dry cavity and the containment sprays being unavailable. Other release classes with high release fractions include RC4.30E (similar to RC4.36L, except that the containment sprays are available) and RC4.22E (similar to RC4.36L, except that the containment sprays are available and the cavity is flooded).

19.15.2.2.4 Insights from Level II Sensitivity Analyses

The results from the containment response analysis show that the System 80+ containment is robust and quite capable of accommodating severe accident challenges. To assess the impact of certain assumptions that were made in performing the containment response analysis, the Level II portion of the PRA, several sensitivity analyses were performed. These analyses determined what effect certain assumptions may have on the containment failure modes and associated conditional failure probabilities. ~~The results from the sensitivity analyses are summarized in Table 19.15.2-12.~~

The major insights from the Level II sensitivity analyses are presented below:

A. Hydrogen ignitors are provided to prevent the build-up of hydrogen inside the containment following a severe accident. However, the conditional probabilities for the various containment failure modes are insensitive to the availability of the hydrogen ignitors following a severe accident.

B. The System 80+ containment characteristics do not favor deflagration to detonation transition and the release classes are not sensitive to deflagration to detonation transition.

C. Late containment failure releases are somewhat sensitive to low heat transfer rate from the corium to the cavity water. This release class is also very sensitive to the amount of water that is discharged to the cavity by the Cavity Flooding System following a severe accident.

D. Late containment failure releases are sensitive to the recovery of containment heat removal following a severe accident.

E. The conditional probabilities for System 80+ release classes are not sensitive to temperature induced creep failure of the RCS piping and the depressurization of the RCS, using the Safety Depressurization System.

F. The frequency of containment isolation failure releases is mildly coupled to the reliability of the Containment Isolation System (CIS). A very reliable CIS would result in a very low frequency for containment isolation failure releases.

19.15.2.3 Release Consequences Assessment - Level III PRA

The characteristics of the release classes determined by the containment response analysis are the primary input to the consequence analysis which calculates the risk measures, including:

A. The whole-body dose at 300 meters from the reactor,

B. The whole-body dose at one half mile from the reactor, and

C. Whole-body dose vs. distance.

The Complementary Cumulative Distribution Functions (CCDFs) for the above risk measures were generated. ~~These distributions are presented in Figures 19.15.2-3 through 19.15.2-5. Figure 19.15.2-3 presents~~ The total CCDF for the whole-body dose at 300 meters ~~meters. This CCDF~~ represents the total frequency of exceeding a given whole-body dose at a radius of 300 meters from the reactor. ~~Figure 19.15.2-4 presents~~ The total CCDF for the whole-body dose at one-half mile ~~This CCDF~~ represents the total frequency of exceeding a given whole-body dose at a radius of one half mile from the reactor. In addition to 300 meters and on-half mile, whole-body doses were calculated for distances at four miles, 11 miles, 25 miles, and 60 miles from the reactor. ~~The whole-body doses with exceedance probabilities of 1.00E-06 and 1.00E-07 for the various distances from the reactor are presented in Figure 19.15.2-5.~~

The large offsite-release goal adopted by Combustion Engineering for the System 80+ Standard Design is:

> "In the event of a severe accident, the dose beyond a one-half mile radius from the reactor shall not exceed 25 rem. The mean frequency of occurrence for higher offsite doses shall be less than once per million reactor-years, considering both internal and external events."

This goal is consistent with the ALWR large offsite release goal established by EPRI in the ALWR Utility Requirements Document[7].

~~As can be seen from Figure 19.15.2-4,~~ The frequencies with which a whole-body dose of 25 rem is exceeded at one-half mile ~~is approximately 5.2E-8 per year. Also, as can be seen from Figure 19.15.2-3, the frequency with which a whole body dose of 25 Rem is exceeded at 300 meters is approximately 6.2E-8 per year. In both cases, the frequency of exceeding 25 Rem is~~ and 300 M are less than the goal of 1.0E-6 per year. ~~Therefore,~~ The System 80+ Standard Design meets the large offsite release goal with substantial margin. ~~Figure 19.15.2-4 also shows that the probability of exceeding a whole-body dose of one Rem at one-half mile from the reactor is 3.0E-07 per year.~~

19.15.2.3.1 Dominant Contributors to Risk

As mentioned in the previous section, risk measures at various distances from the reactor were calculated for the System 80+ design. The dominant contributors to the whole-body dose at 300 meters and one-half mile measures are identified by release class. The dominant contributors are described below.

DOSE AT 300 METERS

The dominant release classes for a whole-body dose of 25 Rem at a distance of 300 meters from the reactor include RC4.36L, RC4.30E, RC4.22E, RC3.4E, RC3.1E, and RC2.5M. ~~The probabilities of exceeding 25 Rem at 300 meters for these release classes are 3.1E-08, 6.5E-09, 6.0E-09, 4.3E-09, 3.3E-09, and 2.9E-09 respectively.~~ A description for each of these release classes is provided below.

A. RC4.36L covers the releases associated with a containment isolation failure with vaporization releases and re-vaporization releases for sequences in which the core damage occurs after 24 hours. Scrubbing of in-vessel fission products is not successful and scrubbing of vaporization and re-vaporization releases is not accomplished.

   The dominant PDS for this release class ~~is PDS194. This PDS~~ is characterized by a Steam Generator Tube Rupture with successful safety injection and successful operation of the Emergency Feedwater Water System. However, the ruptured steam generator is not isolated and RCS pressure control is also not established, and the leakage from the primary side to the secondary side remains high. The inventory of the IRWST is not replenished and is therefore depleted in approximately 25 hours. Core damage is assume to occur once the IRWST is depleted followed by vessel failure approximately one hour later. For this PDS, the cavity is dry and the Containment Spray System is unavailable due to depletion of the IRWST inventory. Releases occur via the unisolated ruptured steam generator.

are bounded by the releases for PDS3. Therefore, this release class is dominated by PDS235 and PDS3. PDS235 is characterized by a loss of main feedwater and failure of the Emergency Feedwater System. The "bleed" portion of "feed and bleed" also fails for this PDS. Core damage is assumed to occur within 4 hours after the initiating event followed by vessel failure within the next hour. The Containment Spray System is available and the cavity is flooded for this PDS.

PDS3 is characterized by a large LOCA with failure of safety injection. Core damage is assumed to occur within 4 hours after the initiating event, followed by vessel rupture an hour later. For PDS3, the Containment Spray System is also available and the cavity is also flooded.

The releases for this release class are assumed to start at the time of containment failure which occurs immediately after vessel failure and last for ~~approximately 200 seconds.~~ a very short period. The release to the environment is assumed to occur at an elevation of 16.6 meters above grade.

E. Release class RC3.1E covers the releases associated with an early containment failure with successful in-vessel fission product scrubbing and no vaporization or re-vaporization releases for sequences in which core damage occurs within the first eight hour following the initiating event.

The dominant PDSs for this release class include PDS235, PDS3, and PDS85. The releases for PDS85 are bounded by the releases for PDS3. Therefore, this release class is dominated by PDS235 and PDS3. PDS235 is characterized by a loss of main feedwater and failure of the Emergency Feedwater System. The "bleed" portion of "feed and bleed" also fails for this PDS. Core damage is assumed to occur within 4 hours after the initiating event followed by vessel failure within the next hour. The Containment Spray System is available and the cavity is flooded for this PDS.

PDS3 is characterized by a large LOCA with failure of safety injection. Core damage is assumed to occur within 4 hours after the initiating event, followed by vessel rupture an hour later. For PDS3, the Containment Spray System is also available and the cavity is also flooded.

The releases for this release class were assumed to start at the time of containment failure, and the releases to the environment were assumed to occur at an elevation of 16.6 meters above grade level.

F. Release class RC2.5M covers the releases associated with a late containment failure with vaporization releases but no re-vaporization releases for sequences in which core damage occurs within 8 hours to 24 hours time frame. In-vessel fission product scrubbing was successful but scrubbing of the vaporization releases is not successful.

The sole contributor to this release class is PDS242. PDS242 is characterized as a station blackout transient with successful operation of emergency feedwater until the batteries are depleted at 8 hours. Core damage is assumed to occur at 10 hours with vessel failure at 11 hours. Containment spray is not available and the cavity is not flooded. The containment will fail due to basemat melt through. There is a 5% chance that the melt through will be into the subsphere. Remail

The releases for this release class were assumed to start at the time of containment failure at 65 hours and continue for 24 hours. The release to environment was assumed to occur at grade.

DOSE AT ONE-HALF MILE

Three dominant release classes were identified for the whole-body dose of 25 Rem at a distance of one-half mile from the reactor. These release classes include RC4.36L, RC4.30E, and RC4.22E. ~~The probabilities of exceeding 25 Rem at one-half mile for these release classes are 3.1E-08, 6.5E-09, and 6.0E-09, respectively.~~ A description for each of the dominant release classes is provided above in the sub-section on "DOSE AT 300 METERS".

19.15.2.3.2 Insights from Level III Sensitivity Analyses

The results of the consequence analysis were compared with the NRC's health objectives and risk goals. The comparison shows that the System 80+ design meets the NRC's large release guidelines and by implication the health objectives are also met. For the base case consequence analysis, releases due to containment isolation failure were the dominant contributors to

whole-body dose at distances (i.e., 300 meter and one-half mile) from the reactor. To assess the impact of certain assumptions that were made in performing the consequence analysis, which is the level III portion of the PRA, several sensitivity analyses were performed. ~~The results of the sensitivity analyses are summarized in Table 19.15.2-13.~~

The major insights from the Level III sensitivity analyses are presented below:

A. The risk measures for whole-body doses at 300 meters and one-half mile from the reactor are relatively insensitive to the location of the release point (i.e., whether the release occurs at the top of the containment building or at grade level).

B. The overall risk of the System 80+ design, as characterized by the risk measures described in this report, is relatively insensitive to containment bypass releases that are not scrubbed prior to their release into the environment.

C. The reliability of the containment isolation function can have a significant impact on the overall risk of the System 80+ design.

D. The risk measures at 300 meters and one-half mile are somewhat sensitive to basemat melt-through that occurs more frequently than currently anticipated.

E. Because of enhanced features and improvements are incorporated into the System 80+ design, the frequency of Interfacing System LOCA is several orders of magnitude lower than existing PWRs. Because of this low frequency, containment bypass releases are not major contributors to the risk of the System 80+ design. However, the overall risk of the System 80+ design is sensitive to the frequency of Interfacing System LOCA if it were to increase by several orders of magnitude.

F. The risk of the System 80+ design is sensitive to the isotopic content that is used to characterize the various release classes.

G. The risk of the System 80+ design is slightly sensitive to the concrete ablation rate.

19.15.3 EXTERNAL EVENTS RISK PROFILE INSIGHTS

The external events analyses for the System 80+ design included both qualitative and quantitative analyses. Bounding site characteristics were used for the quantitative analyses to minimize potential future restrictions on plant siting. The qualitative external events evaluation involved the following: (1) identification of the external events to be considered, (2) grouping of events with similar plant effects and consequences, (3) establishment of screening criteria to eliminate events that are insignificant contributors to risk, and (4) identification of events that require further quantitative evaluation. Based on the qualitative evaluation, most of the external events were eliminated from further quantitative evaluation. Four external events (tornado, fire, flood, and seismic) were identified as having the potential to induce system failures and therefore required further quantitative evaluation.

The major findings and insights obtained for tornados, fires, floods, and seismic events are provided in Sections 19.15.3.1, 19.15.3.2, 19.15.3.3, and 19.15.3.4, respectively.

19.15.3.1 Insights from the Tornado Strike Analysis

The core damage frequency due to tornado strike events is calculated to be 2.5E-07 per year. The dominant contributors to the core damage frequency of tornado strike events are provided in Table 19.15.3-1. For the System 80+ PRA, the following assumptions were made for the tornado strike accident sequences.

A. It was assumed that offsite power will be lost for more than 24 hours and the plant will rely on the emergency diesel generators during this period.

B. The turbine/generator will be unable to run back and pickup hotel loads following a tornado strike.

C. The alternate AC power source was conservatively assumed to be unavailable following a tornado strike.

D. The Station Service Water System (SSWS) intake structure was assumed to be vulnerable to accumulation of debris due a tornado strike event and was included in the models. The protection of the SSWS intake structure against the accumulation of debris due to a tornado strike could prevent or minimize the loss of suction to the SSWS pumps. [The COL applicant should re-evaluate the vulnerability of the SSWP intake to tornado-generated debris. [COL Item 19-1]]!

E. Safety related structures outside the nuclear island will not be destroyed by a tornado strike.

1. COL information item; see DCD introduction section 1.5.2.

F. The air intake for the emergency diesel generator rooms was assumed to be protected from tornado and tornado generated missiles.

G. The Condensate Storage Tank is unavailable to provide makeup to the Emergency Feedwater Storage Tanks.

Three dominant accident sequences were identified for tornado strike events: TRND-4, TRND-SBO, and TRND-5. ~~The calculated frequencies for these accident sequences are 2.5E-07, 1.7E-8, and 4.1E-9 per year respectively.~~

A. TRND-4 is an accident sequence which involves a tornado strike event followed by successful opening and reseating of the primary safety valves, failure of decay heat removal, and failure of the SIS. For this sequence, the EFWS is used to remove decay heat from the RCS until shutdown cooling entry conditions are met. Once shutdown cooling entry conditions are met, the SCS would be aligned for decay heat removal. However, the SCS fails to perform its function and consequently the only other means of removing decay heat from the core is via "feed and bleed" operation. In order for "feed and bleed" to be successful both the "bleed" portion and the "feed" portion must operate. In addition to SCS failure, "feed" also fails for this sequence. This results in the termination of decay heat removal and consequently core damage occurs. The dominant contributors to this sequence are: (1) common cause operating failure of the emergency diesel generators, (2) operating independent failure of the emergency diesel generators. The diesel generators will be included in D-RAP.

B. TRND-SBO is an accident sequence which involves a tornado strike event followed by station blackout with battery depletion. For this accident sequence, the emergency diesel generators also fail and the only mitigating system available is the EFWS, using the turbine-driven pumps. After eight hours of operation, the batteries would be depleted and long term decay heat removal would be terminated. Consequently, core damage occurs. The dominant contributors to this sequence are: (1) blockage of the station service water intake structure due to tornado generated debris, (2) common cause failure of the emergency diesel generators, and (3) independent demand failures of the emergency diesel generators.

C. TRND-5 is an accident sequence which involves a tornado strike event followed by failure of long-term decay heat removal and failure of the SDS. This accident sequence is similar to TRND-4, except that "bleed" fails instead of "feed". The dominant contributors to this accident sequence are: (1) blockage of the station service water intake structure, (2) failure of the operator to initiate "feed and

bleed", (3) common cause operating failure of the emergency diesel generators.

The major insight gained from the tornado strike evaluation is that the single most dominant contributor to core damage is caused by blockage of the intake structure. Blockage of the intake structure for the station service water pumps is caused tornado generated debris. Blockage would result in loss of cooling water to the emergency diesel generators and all safety-related motor-driven pumps. The EFWS, using the turbine-driven pumps, would be the only means of removing decay heat from the core until the batteries are depleted.

19.15.3.2 Insights from the Fire Risk Assessment

A qualitative fire risk assessment was performed for the System 80+ design. The evaluation addressed each of the fire areas defined, except the containment area and the control room area. Each fire area was analyzed to assure that in the event that all the active equipment in the area affected by a fire were rendered inoperable, redundant systems, trains, or channels would be available in another fire area. This would enable safe shutdown to be achieved and maintained.

The following assumptions were made in performing the fire scoping assessment.

A. Because of the enhanced features of the System 80+ control room design, a fire in the control room is assumed to be an insignificant contributor to core damage due to internal fires.

B. It was assumed that the materials used in the control room panels do not independently support combustion.

C. The energy sources coming into the control room panels was assumed to be limited to low power voltage, to the maximum extent practicable. Such limited energy sources practically eliminates potential ignition sources within the panels. A significant portion of the control and indication signals are interfaced to the main control panel via fiber optic cables.

D. If a fire occurs inside the main control room and the operator determines that the control room should be evacuated, it is assumed that the operator will trip the reactor and transfer control to the Remote Shutdown Room prior to evacuation.

N. The reliabilities of the fire detection and suppression systems are assumed to be at least 80% and 96%, respectively.

O. Although fire brigade action to suppress fires was not modeled in the scoping fire risk evaluation, the capabilities of the plant fire brigade are important to maintaining a low fire risk. The COL applicant should maintian a well trained and prepared fire brigade.

A quantitative assessment of the risk due to internal fires can not be made at this time because detailed design information for cable routing and the fire detection and fire suppression system is not presently available. However, a scoping evaluation is performed to assess the risk due to internal fires, ~~in areas of the Nuclear Annex other than the containment or the control room.~~ Two types of fires were considered in the scoping evaluation: (1) a fire in an area which could disable safety-related equipment in that area and which has the potential for initiating a transient, and (2) a fire in an area which by itself could disable safety-related equipment but would require the penetration of a fire barrier in order to initiate a transient. ~~The first type of fire is designated as type "a" and the second type as type "b". The fire ignition sources and frequencies by applicable areas are presented in Table 19.15.3-2.~~

Although a detailed quantitative analysis of internal fires was not performed at this stage of the System 80+ design, a scoping estimate of the risk due to fire was calculated by using a conservative scoping value ~~(4.6E-02 per year)~~ for fire event frequency and by assuming that the effects on plant systems would be the same as a loss of one division of component cooling water/station service water. Using this approach, ~~the estimated scoping value core damage frequency due to internal fires is 6.1E-08 per year and~~ the sequence of importance involves an internal fire followed by failure of long-term decay heat removal and failure of SDS.

Based on the robust seal design for the RCPs used in the System 80+ design and on the results of tests and operating experience, ABB-CE asserts that the RCP seals will not fail on loss of seal injection and seal cooling. However, in the interests of completeness, an assessment of a postulated fire induced RCP seal LOCA was included as part of the quantitative fire scoping evaluation. The scoping value for core damage frequency associated with the postulated fire induced seal LOCA was calculated, ~~to be 5.2E-10 per year~~. The potential risk due to a postulated fire inside containment was also assessed. ~~The estimated scoping value of core damage frequency due to fire inside containment is 1.3E-09 per year. Thus, the total estimated scoping value of core damage frequency for internal fires is 6.3E-08 per year.~~

The following insights were drawn from the internal fire scoping assessment:

A. The consequences of internal fires at the plant are bounded by a fire that would disable all the safety related equipment in the division where the fire originated.

B. The propagation of a fire from one division to the next is prevented by the divisional separation of redundant safety related equipment with a 3 hour fire barrier which is maintained during power operation. The fire barriers will be included in D-RAP.

C. In order to minimize or eliminate control room fires, the control room panel specifications must be met. These specifications prohibit the use of neoprene, limit the use of PVC, and prohibit the use of materials that would independently support combustion. The energy sources coming into the control room panels must be limited to low voltage.

D. A control room fire is not a dominant contributor to the overall core damage frequency due to internal fires.

E. Instrumentation and controls are provided at the Remote Shutdown Panel to ensure that the plant can handle a transient from the Remote Shutdown Room.

F. Because the main control room is continuously pressurized, the entry of smoke, hot gases, dirt, and fire suppressants originating from outside the main control room will be prevented.

G. The main control room utilizes a ventilation system which is separate from the rest of the control building. Therefore, the migration of smoke, hot gases, and fire suppressants that originate in areas outside the main control room such as the electrical equipment areas to the control room will not occur via the ventilation system or any other means.

H. Separate ventilation systems are provided for each of the divisional separated building. Therefore, a fire in one division cannot migrate to the next division via the ventilation system.

I. Although ABB-CE asserts that the RCP seals will not fail on loss of seal injection and seal cooling due to the robust seal design, an assessment of a postulated fire induced RCP seal LOCA was included as part of the quantitative fire scoping evaluation. This evaluation indicates that a fire induced RCP seal LOCA is not a dominant contributor to the estimated scoping core damage frequency estimate for internal fires.

J. Deterministic evaluations indicate that there is no credible fire inside containment that could damage redundant trains

K. It is assumed that the frequency of an internal flood during power operation is no worse than one in a hundred plant years.

L. It was assumed that a failure of the Circulating Water System or the main condenser large enough to cause flooding in the Turbine Building can be detected and the flooding source isolated. Administrative procedures are in place to isolate the flooding source.

M. The major piping penetrations between the Nuclear Annex and the Turbine Building are assumed to be sealed and located above the maximum flood level associated with flooding of the Turbine Building.

N. There are no safety related components located in the Turbine Building. Therefore, it was assumed that flooding of the Turbine Building will be limited to non-safety related equipment.

O. All entrances from the Turbine Building to the Nuclear Annex were assumed to be located above the maximum flood level for the Turbine Building.

Although a detailed quantitative analysis of internal floods was not performed at this stage of the System 80+ design, a scoping estimate of the risk due to flood was calculated by using a conservative scoping value ~~(1.0E-02 per year)~~ for flooding event frequency and by assuming that the effects on plant systems would be the same as a loss of one division of component cooling water/station service water. Using this approach, ~~the scoping estimate of core damage frequency due to internal floods is 1.3E-08 per year.~~ The sequence of importance involves an internal flood followed by failure of long-term decay heat removal and failure of SDS.

Based on the robust seal design for the RCPs used in the System 80+ design and on the results of tests and operating experience, ABB-CE asserts that the RCP seals will not fail on loss of seal injection and seal cooling. However, in the interests of completeness, an assessment of a postulated flood induced RCP seal LOCA was included as part of the quantitative flood scoping evaluation. ~~The scoping value for core damage frequency associated with the postulated flood induced seal LOCA was calculated to be 1.2E-10 per year. Thus, the total estimated scoping value of core damage frequency for internal floods is 1.3E-08 per year.~~

Based on the above assumptions made for the flooding evaluation, the following flood insights were derived for the System 80+ design:

A. The divisional flood barrier between redundant divisions of safety related equipment is an important design feature which ensures that flooding of both divisions of safety related equipment will not occur.

B. Maintaining the flood barrier is also important in ensuring that the core damage frequency due to internal floods will remain as low as the current value. The flood barriers will be included in D-RAP.

C. The divisional separation of redundant safety related equipment in the Component Cooling Water Heat Exchanger structure and the Station Service Water Pump structure is also an important design feature. This ensures that flooding of both divisions of Component Cooling Water Heat Exchangers and station service water pumps will not occur.

D. By maintaining the flood barriers for the various flood zones, flooding will not propagate from one flood zone to the next within the Nuclear Annex.

E. All the major flood sources within the Nuclear Annex are located below the 70+0 elevation. Flooding of equipment located above this elevation will not occur.

F. All safety related structures are designed to withstand the static and dynamic forces of flooding. Therefore, the structural wall between the Nuclear Annex and the Turbine Building will not fail.

G. Based on the assumption regarding the location of penetrations between the Nuclear Annex and the Turbine Building, a flood in the Turbine Building will not propagate to the Nuclear Annex and affect the operability of safety related equipment.

H. Provided the interface requirements are met by the applicant, flooding in the Turbine Building will have no impact on plant safety.

I. It is important to locate all entrances from the Nuclear Annex to the Turbine Building above the maximum flood level of the Turbine Building. This will ensure that the propagation of flood water from the Turbine Building to the Nuclear Annex will not occur.

J. Since the plant grade is sloped away from safety relate structures, flooding of these structures from Turbine Building sources will not occur.

K. Although ABB-CE asserts that the RCP seals will not fail on loss of seal injection and seal cooling due to the robust seal design, an assessment of a postulated flood inducted RCP seal LOCA was included as part of the quantitative flood scoping evaluation. This evaluation indicates that a flood induced RCP seal LOCA is not a dominant contributor to the estimated scoping core damage frequency estimate for internal floods.

19.15.3.4 Insights from the Seismic Margin Analysis

In the seismic margin analysis, the following assumptions were made:

A. A seismic initiator hierarchy tree was developed to represent the order of impact for the various seismic initiators. It was assumed that the order of impact in terms of severity is as follows:

1. Seismically induced Gross Structural Collapse
2. LOCA in Excess of ECCS Capability
3. Seismically induced Medium LOCA
4. Seismically induced Small LOCA
5. Seismically induced ATWS
6. Seismically induced Loss of Site Power
7. Seismically induced Transient

B. It was assumed that if one component fails to operate due to a seismic event, all similar component(s) in that system would also fail (one-fail-all-fail).

C. All random (independent) component failures and human errors with low probability ~~of less than 10^{-3} and all human errors with a probability of less than 10^{-2}, except selected human errors with a probability of less than 10^{-2},~~ were deleted from the initial seismic fault trees in accordance with the guidelines provided by the NRC.

D. The High Confidence Low Probability of Failure (HCLPF) acceleration values for the component and structural failures in the seismic event trees and fault trees were calculated using design specific response spectra and the Conservative Deterministic Failure Margin (CDFM) approach presented in EPRI NP-6041-SL[176].

E. It was assumed that a seismic event would not significantly alter the stress level nor the time available in which the operator actions required to mitigate the consequences of such an event need to be performed. Thus, the seismic margin analysis used the same human error rates as those used in the internal events analysis.

O. It was assumed that the occurrence of a seismic event did not automatically result in loss of offsite power or failure of the standby combustion turbine regardless of the "g" level.

P. The System 80+ Class 1E electrical distribution system is provided with protection schemes which conform to the requirements of IEEE STD-741-1986. The protective schemes are designed to isolate faulted equipment from the rest of the system to minimize the effect of the fault and to maximize the availability of the remaining equipment. The basic schemes consist of ground fault protection, instantaneous overcurrent and timed overcurrent protection. In developing the SMA models, it was assumed that the seismic failure of equipment in the Electrical Distribution System were "open circuit" failures. Implicit within this assumption is the assumption that if a "hot short" failure were to occur, the appropriate circuit interrupter(s) would open on overcurrent to prevent "backward" propagation of the fault.

Q. Seismically induced sliding of the nuclear island structure is assumed to result in severing of all piping or cabling into the nuclear island. This was conservatively assumed to lead directly to core damage.

R. Seismically induced sliding of the CCW Heat Exchanger Building was assumed to result in severing of CCW piping to the nuclear island for both divisions of CCW. This results in loss of all CCW.

~~The HCLPF for System 80+ standard design plant is 0.6g (more detailed information is provided in Section 19.7.5). The dominant contributors to the plant HCLPF are provided in Table 19.7.5.3-1.~~

The following dominant sequences were identified for the seismic event.

A. The dominant contributor to the plant HCLPF is seismically induced gross structural failure of the containment vessel which was assumed to lead directly to core damage and containment failure. Because this sequence leads directly to containment failure, the operability of the containment safeguard systems is of no importance.

B. The second dominant contributor to the plant HCLPF is a seismically induced LOCA in Excess of ECCS Capacity caused by a seismically induced failure of the RCP supports.

depressurization in preparation for feed and bleed cooling.

D. ~~Four sequences have a HCLPF value of 0.89g. These are SEIS-SBO, EQT-7, EQLP-8 and EQA-10.~~ EQT-7 is a seismically induced Transient with failure of the EFW system to deliver emergency feedwater flow, successful feed and bleed cooling and failure of containment heat removal (failure to coo. IRWST). EQLP-8 is a seismically induced Loss of Site Power with failure of the EFW system to deliver emergency feedwater flow, successful depressurization of the RCS but failure of the SIS to provide feed. EQA-10 is a seismically induced ATWS with failure of the EFW system to deliver emergency feedwater flow. ~~The HCLPF value of 0.74g is associated with a structural failure of the walls between the Emergency Feedwater Storage Tanks (EFWSTs) and diesel generator rooms.~~ Seismically induced failure of ~~this~~ the common wall would result in the EFWST inventory being drained into the diesel generator room and flooding out the diesel generator. This would result in loss of the EFW and the diesel generator.

between the Emergency Feedwater Storage Tanks (EFWSTs) and diesel generator rooms

19.15.4 SHUTDOWN AND LOW-POWER OPERATION RISK INSIGHTS

A study of the risk associated with the low power and shutdown modes of operation was performed ~~(see Section 19.8)~~. The scope of this assessment included the evaluation of both internal events and external events occurring during low-power and shutdown modes of operation.

Event trees were developed and quantified for loss of Decay Heat Removal (DHR) and loss of coolant inventory as initiating events during Modes 4 through 6. The core damage frequencies associated with loss of offsite power, fire, and floods were also quantified. In quantifying the core damage frequency (CDF), emphasis was placed on the human errors because they have been shown, in earlier studies, to be dominant contributors to shutdown risk. The system failure probabilities were evaluated using modifications to the fault trees, ~~presented in Section 19.6.~~

The results obtained from the shutdown and low-power risk evaluation are summarized in Section 19.15.4.1. Similar to the PRA that was performed during power operation, insights were gained for the shutdown risk evaluation. Such insights are summarized in Section 19.15.4.2. The general assumptions that was made in developing the accident sequences for the shutdown risk assessment are outlined below.

A. Modes 2 and 3 were not considered in the shutdown study because the plant configuration is very similar to Mode 1 and therefore the effects are enveloped in the Mode 1 analysis.

B. The end point of the event trees is the establishment of Decay Heat Removal (DHR) path or a "feed and bleed" path.

C. Containment heat removal has been neglected because of the lower decay heat load than at full power and heat removal can be accomplished with the containment coolers or containment venting before containment over-pressurization.

D. No credit was given for the use of the steam generators as a DHR path (it was assumed that they were always unavailable).

E. No credit was given for the use of the SITs as a source of coolant even though they are available during certain stages of the shutdown.

F. During Modes 6 with the head detensioned but not removed and during Modes 5 with reduced inventory, it is assumed that a "bleed" path is required for "feed and bleed".

G. No credit is given for recovery from operator errors by additional personal in the control room.

19.15.4.1 Results

~~The estimate core damage frequency attributable to internal and external events during shutdown and low-power modes of operation is 8.4E-07 per year.~~ ~~Table 19.15.4-1 identifies the contributors to core damage frequency~~ (CDF) ~~by shutdown and low power modes of operation and by initiating event.~~ Reduced inventory operation during mode 5 (Mode 5R) ~~accounts for 48% of~~ the internal risk is the leading contributor to Loss of DHR is the dominant initiator for accident sequence in this mode of operation. (This mode of operation and sequence were also identified in earlier PRAs as being the dominant contributors to CDF.) Internal events occurring during modes 6E and 6I are the second leading contributors ~~(29%)~~ to CDF. During mode 6E or 6I, the IRWST is empty and therefore not available as a source of coolant for any makeup or feed and bleed operation. LOCA is the dominant initiator for accident sequence in this mode of operation because the capability to provide makeup to the core is limited. The third leading contributors to CDF occur during Modes 4, 5, and 6F (IRWST full). Loss of offsite power is the dominant initiator for accident sequence during this mode of operation because of the long time interval spent in this configuration and the need to restore AC in about two hours.

~~The importance of the various internal initiating event types in terms of CDF contribution is also shown in Table 19.15.4-1.~~ Loss of Offsite Power (LOOP) is the leading contributor ~~(39%)~~ to CDF for internally initiated events during low-power and shutdown modes of operations. Even with requirements for two switch-yards and two standby generators to be available during shutdown, the risk was not negligible. Loss of DHR was the second largest initiating event type in terms of contribution to CDF ~~(36% of internal CDF)~~.

Fires ~~(3.0E-07 per year) account for 36% of~~ dominate the total internal and external CDF during shutdown and low-power operations. The CDF due to flooding ~~was calculated to be 8.2E-8 per year and~~ was modeled as part of the LOCA risk.

~~Table 19.15.4-2 compares~~ was compared The CDF for low-power and shutdown events with those for power operation. The CDF for low-power and shutdown modes is ~~20% of the~~ a significant contributor to the System 80+ total CDF. The CDF for shutdown and low-power events is significantly less than the EPRI goal of 1.0E-05 per year. The total System 80+ CDF is also less than the EPRI goal.

~~Table 19.15.4-3 lists~~ The dominant sequences leading to core damage (1) Loss of DHR in reduced inventory ~~accounts for 24% of the internal event CDF~~. (2) LOOP in Modes 4, 5, and 6F is the second largest sequence, (3) LOCAs in Modes 6E, and 6I when the IRWST and SIS is not necessarily available ~~are the third largest sequence.~~

~~Table 19.15.4-4 compares~~ The results of this study with other shutdown PRAs. In all these studies, loss of DHR during reduced during low-power and shutdown modes are; were compared

Loss of DHR Insights

The major insights from the loss of decay heat removal during low-power and shutdown modes of operation are listed below:

A. Reduced inventory is the most critical operation. The operator should be aware of this and plant activities should be scheduled accordingly. Use of nozzle dams is encouraged as a method of limiting the time spent in this mode.

B. The operator must have procedures and training to align the SCS train to the IRWST and use it to makeup inventory or do a feed and bleed operation.

C. Failure of the standby SCS train for either DHR or feed operation is dominated by failure of control valves and MOVs. An aggressive valve testing and maintenance program on the SCS and CSS would reduce shutdown risk.

D. The use of the CVCS to makeup inventory is an important recovery action in reduced inventory operation. It also acts as a temporary ~~(about 12 hours)~~ cooling technique. The operator should have procedures and training on its use.

E. Safety injection in conjunction with bleed is an important means of removing decay heat during shutdown modes. Having two of the four SIS trains available during most shutdown modes is an important new technical specification.

F. The CSS pumps are used as backup to the SCS pumps. The operator must therefore be properly trained in performing the procedure(s) to alignment the CSS pumps for operation if the SCS pumps should fail. Again, valve maintenance and testing is important for shutdown risk reduction.

LOCA Insights

The major insights for LOCAs during low-power and shutdown modes of operation are listed below:

A. SCS injection is an important means of makeup following a LOCA. Therefore, the development of appropriate procedures and the training of the operator to perform these procedures are necessary and important in mitigating LOCA events during low-power and shutdown modes of operation.

B. The dominant failure mode for SCS injection is failure of control valves and MOVs. A valve maintenance program is important.

C. The use of the SIS to provide injection during a LOCA important. Since manual actuation is required, training and procedures are required to properly accomplish this task.

19.15.5 USE OF PRA IN THE DESIGN PROCESS

Probabilistic Risk Assessment (PRA) was used extensively in the System 80+ design process. PRA was used to confirm that the System 80+ design complied with the applicable risk goals, and to select among the alternate design options.

The insights gained from past PRAs, especially the System 80, were used to identify vulnerabilities in operating plants. This information was then used to incorporate features in the System 80+ design that reduced or eliminated these vulnerabilities. PRA was then used to confirm the risk reduction associated with these improvements. Examples are the risk reduction ~~presented in Section 19.15.2.1.1~~ for LOOP/SBO, SGTR, transients, small LOCA, and ATWS accident sequences, ~~in Section 19.15.2.1.1.~~

Another use of the PRA in the System 80+ design process, which was also of a confirmatory nature, was to demonstrate compliance with applicable risk goals.

The System 80+ PRA was also used to evaluate design alternatives. The major design options are cited below.

COMPONENT COOLING WATER SYSTEM CONFIGURATION

Early in the program, System 80+ had a standby, safety related Essential Component Cooling Water System and Essential Service Water System for cooling safety related loads. Demand failure of the pump and valves in these systems were found to be significant risk contributors. As a result, the System 80+ design was changed to a normally operating Component Cooling Water System (CCWS) and a Station Service Water System (SSWS) where the non-safety loads can be shed when required. The selected CCWS and SSWS have two divisions with two pumps in each division. One pump in each division is normally operating and the second pump is in standby and will start if the operating pump in the same division trips. A subsequent evaluation was also made to determine if the standby pumps had to be automatically loaded on the emergency diesel generators and started following a LOOP event. The evaluation indicated that there would be no significant risk impact if the standby pumps were aligned to the emergency diesel generators following a LOOP event but were not started unless the previously operating pump fails to restart. Thus larger and consequently less reliable emergency diesel generators were not required.

16. An alternative design that consists of a third diverse Plant Protection System.

17. A perfect containment spray system that prevents high pressure containment failures caused by slow steam pressurization.

18. A filtered vent design that prevents all slow high pressure containment failures.

19. An ideal concrete composition that prevents basemat melt-through.

20. A reactor vessel exterior cooling system that prevents vessel melt-through and direct containment heating.

21. An ideal hydrogen (H_2) ignitor that would prevent releases associated with containment failures from hydrogen burns or explosions.

22. Passive autocatalytic recombiners that would combine molecules of hydrogen and oxygen gases into water.

23. An alternative design that scrubs the discharge of the main steam safety valves and the atmospheric dump valves to remove most of the fission products following a steam generator tube rupture event.

24. An alternative design that monitors containment isolation. Addition of redundant and diverse limit switch to each containment isolation valve is included.

25. A cavity cooling design alternative that uses the existing SCS heat exchangers in the IRWST to cool the reactor vessel cavity under natural circulation.

26. A floodable rubble bed in the bottom of the vessel cavity as an alternate design to cool the debris bed and remove heat. The rubble bed would remain dry until the corium enters the bed. This would minimize the potential for the steam explosion.

27. An alternative design that consists of a ceramic lined crucible with cooling located in the vessel cavity.

Table 19.15.5-1 summarizes the results of the design alternative evaluation. The first column of this table identifies the type of design alternative, followed by the annual risk reduction to the general population using $1000 per person-rem/year reduction for each design alternative. The next column, labeled capital benefit, is an equivalent present worth of the annual dose reduction. It is also the maximum amount that could be spent in

capital in order to be cost beneficial. The fourth column is a capital cost estimate for the design alternatives. The net benefit (capital benefit less capital cost) is given in the last column.

This table intentionally blank.

TABLE 19.15.5-1
(Sheet 1 of 2)

SUMMARY OF THE RISK REDUCTIONS OF THE DESIGN ALTERNATIVES

DESIGN ALTERNATIVE	ANNUAL RISK REDUCTION $/Y	CAPITAL BENEFIT*	CAPITAL COST	NET CAPITAL BENEFIT
100% SG INSPECTION	~~$100.38~~ 156.15	~~$605~~ 941	$1,500,000	~~($1,499,395)~~ 1,499,059
SECONDARY SIDE GUARD PIPES	$0.73	$4	$1,100,000	($1,099,996)
ALT. DC BATTERY AND EFWS	$1.87	$11	$2,000,000	($1,999,989)
12-HOUR BATTERIES	$0.71	$4	$300,000	($299,996)
ALT. PRESSURIZER AUX SPRAY	~~$90.44~~ 133.96	~~$545~~ 807	$5,000,000	~~($4,999,455)~~ 4,999,193
ALT. HPSI	~~$83.38~~ 82.94	~~$502~~ 500	$2,200,000	~~($2,299,498)~~ 2,299,500
ALT. RCS DEPRESSURIZATION	~~$15.14~~ 14.18	~~$91~~ 85	$500,000	~~($499,909)~~ 499,915
DIESEL SI PUMPS (2)	~~$83.79~~ 83.35	~~$505~~ 502	$2,000,000	~~($1,999,532)~~ 1,999,535
EXTENDED RWST SOURCE	~~$32.80~~ 88.40	~~$198~~ 533	$1,000,000	~~($999,802)~~ 999,467
THIRD DIESEL GENERATOR	$0.45	$3	$25,000,000	($9,999,997)
TORNADO-PROTECTION FOR COMBUSTION TURBINE	$1.60	$10	$3,000,000	($2,999,991)
FUEL CELLS	$1.87	$11	$2,000,000	($1,999,989)
HOOKUP FOR PORTABLE GENERATOR	$1.87	$11	$10,000	($9,989)
ALT. ATWS RELIEF VALVES	~~$1.02~~ 0.97	$6	$1,000,000	($999,994)

* THE CAPITAL BENEFIT IS THE PRICE OF A PIECE OF EQUIPMENT THAT HAS A LEVELIZED (ANNUAL) COST EQUAL TO THE ANNUAL BENEFIT IN RISK REDUCTION AND ASSUMES NO MAINTENANCE OR TESTING OF ADDITIONAL EQUIPMENT.

This table intentionally blank.

TABLE 19.15.5-1
(Sheet 2 of 2)

SUMMARY OF THE RISK REDUCTIONS OF THE DESIGN ALTERNATIVES

DESIGN ALTERNATIVE	ANNUAL RISK REDUCTION $/Y	CAPITAL BENEFIT*	CAPITAL COST	NET CAPITAL BENEFIT
ATWS INJECTION SYSTEM	$1.02	$6	$300,000	($299,994)
DIVERSE PPS SYSTEM	$1.02	$6	$3,000,000	($2,999,994)
ALT. CONTAINMENT SPRAY	~~$7.27~~ 7.35	$44	$1,500,000	($1,499,956)
FILTERED VENT (CONTAINMENT)	$0.53	$3	$10,000,000	($9,999,997)
ALT. CONCRETE COMPOSITION	~~$4.87~~ 4.86	$29	$5,000,000	($4,999,971)
RV EXTERIOR COOLING	~~$32.64~~ 30.69	~~$197~~ 185	$2,500,000	~~($2,499,803)~~ 2,499,815
ALT. H2 IGNITORS	~~$0.75~~ 0.92	~~$5~~ 6	$1,000,000	~~($999,995)~~ 999,994
PASSIVE AUTOCATALYTIC RECOMBINERS (PARS)	$0.75	$5	$760,000	($759,995)
MSSV AND ADV SCRUBBING	~~$97.30~~ 152.99	~~$586~~ 922	$9,500,000	($9,499,414) 9,499,078
ALT. CONTAINMENT MONITORING SYSTEM	~~$1.67~~ 1.66	$10	$1,000,000	($999,991)
CAVITY COOLING	~~$32.64~~ 32.60	$197	$50,000	($49,818)
WATER COOLED RUBBLE BED	$4.87	$29	$18,800,000	($18,799,971)
REFRACTORY LINED CRUCIBLE	$4.87	$29	$108,000,000	($107,999,971)

* THE CAPITAL BENEFIT IS THE PRICE OF A PIECE OF EQUIPMENT THAT HAS A LEVELIZED (ANNUAL) COST EQUAL TO THE ANNUAL BENEFIT IN RISK REDUCTION AND ASSUMES NO MAINTENANCE OR TESTING OF ADDITIONAL EQUIPMENT.

19.15.6 RISK SIGNIFICANT SSCs FOR CONSIDERATION IN THE RAP AND OTHER ACTIVITIES

Table 19.15.6-1 presents a list of risk significant Systems Structures and Components (SSCs) that should be included in the D-RAP as described in Section 17.3. [The COL applicant should consider inclusion of these SSCs in their D-RAP and operations reliability assurance process [COL Item 19-7].][1] These SSCs were selected based on their risk importance as determined in the Level 1 analyses, the Level 2 analyses, the Level 3 analyses, the shutdown risk evaluation, the internal fire and flood evaluation, and the seismic margins evaluation. For the Level 1 analyses and the shutdown risk analyses, systems and components were included as risk significant if their Risk Achievement Worth (RAW) was greater than or equal to 5.0 or their Risk Reduction Worth (RRW) was 1.10 or greater. SSCs with a RAW between 2.0 and 5.0 were selected if their RRW was greater than 1.05. For the Seismic Margins Assessment, a SSC was included if it was a dominant contributor to the Plant HCLPF. For the Level 2, Level 3, and internal fire and flood analyses, items were included based on engineering judgement. SSCs were also included in the list if specific engineering commitments were made by the system designers. Table 19.15.6-1 contains three columns. The first column identifies the system, structure or component. The second column presents the rationale (basis) for including the SSC in the D-RAP (i.e., RAW > 5.0, Level 2 considerations, engineering judgement, engineering commitment, etc.). The third column briefly describes the item and any associated insights. The third column also identifies any test interval or maintenance assumptions that were used in the PRA. This table does not include any failure rate or unavailability information. All component failure rates are documented in Section 19.5 and its associated appendices. The random failure rates for the individual components for the specific failure modes of concern are summarized in Table 19.5-2. The common cause failure rates are summarized in Table 19.5-3. The maintenance unavailabilities are summarized in Table 19.5-4. The component and structure HCLPF values are summarized in Tables 19.7.5.1-1 and 19.7.5.1-2. Table 3.9-15 summarizes the In-Service Testing program for all safety related pumps and valves and presents the applicable test intervals.

Table 19.15.6-2 presents a list of Important Operator Actions selected from the PRA. These operator actions were selected based on their risk importance as determined in the Level 1 analyses, the Level 2 analyses, the Level 3 analyses, the shutdown risk evaluation, the internal fire and flood evaluation, and the seismic margins evaluation. For the Level 1 analyses and the shutdown risk analyses, operator actions were included as important if their Risk Achievement Worth (RAW) was greater than or equal to 5.0 or their Risk Reduction Worth (RRW) was 1.10 or greater. Operator actions with a RAW between 2.0 and 5.0 were selected if their RRW was greater than 1.05. For the Seismic Margins Assessment, an operator action was included if failure to

1. COL information item; see DCD introduction section 1.5.2.

perform that action could result in a lower overall plant HCLPF value. For Level 2, Level 3, and internal fire and flood analyses, items were included based on engineering judgement.

The COL applicant is responsible for developing all plant procedures. These procedures include, but are not limited to, the normal operating procedures, system operating procedures, maintenance procedures, emergency operating procedures and severe accident procedures. The Emergency Operating Guidelines (EOGs) provide guidance to the COL applicant for developing the detailed Emergency Operating Procedures. Appendices to the EOGs provide guidance on severe accident procedures and emergency operating considerations during shutdown operations. [[In developing and implementing procedures, training and other human reliability related programs, the COL applicant should consider the information on risk important operator actions presented in Table 19.15.6-2. [COL Item 19-8]]!.

[[In the severe accident management procedures, the COL applicant should include procedures for the use of the Cavity Flood System, the Hydrogen Mitigation System, and the Emergency Containment Spray Backup function of the CSS. [COL Item 19-8]]!.

[[The COL should develop procedures for manually aligning the Alternate AC power supply when one of the two emergency diesel generators is unavailable during a loss of offsite power. [COL Item 19-8]]!.

1. COL information item; see DCD introduction section 1.5.2.

TABLE 19.15.6-1

(Sheet 1 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
SYSTEM: Emergency Feedwater System (EFWS)	RAW* > 5.0	The EFWS is used for secondary side heat removal following a transient or small LOCA. The EFWS consists of two trains, one per steam generator (SG). Each train has two 100% capacity redundant and diverse pumps, one motor driven and one turbine driven. Each train has its own EFW storage tank which can be refilled from the condensate storage tank or the demineralized water makeup system. There is a cross-connect between the two trains on the discharge side of the pumps. The cross-connect line is isolated by two NC manual isolation valves. In the PRA, only unscheduled maintenance was assumed. Maintenance unavailability was assigned at the subtrain level ~~based on generic data provided in the EPRI PRA Key Assumptions and Groundrules (KAG) document[7].~~
Component: EFW Motor driven pumps	RAW > 5.0 (CCF)	The EFW pumps deliver EFW to the SGs for secondary side decay heat removal. Each train has one 100% capacity motor-driven pump powered from the appropriate vital 4.16 KV bus. Consistent with current practices, the EFW pumps are tested on a quarterly basis with unscheduled maintenance performed on failure. Maintenance unavailability is covered by the subtrain level maintenance unavailability (see above).
Component: EFW Turbine driven pumps	RAW > 5.0 (CCF)	The EFW pumps deliver EFW to the SGs for secondary side decay heat removal. Each train has one 100% capacity turbine-driven pump powered by steam derived from its associated SG. Consistent with current practices, the EFW pumps are tested on a quarterly basis with unscheduled maintenance performed on failure. Maintenance unavailability is covered by the subtrain level maintenance unavailability (see above).
Component: EFW pump discharge check valves	RAW > 5.0 (CCF)	Consistent with current practices, these check valves are assumed to be tested on a cold shutdown basis with maintenance performed on failure.
Component: EFW distribution line check valves	RAW > 5.0 (CCF)	These check valves are assumed to be tested on a cold shutdown basis with maintenance performed on failure.

TABLE 19.15.6-1

(Sheet 2 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

assumed to be

SSC	Rationale	Insights and Assumptions
Component: EFW distribution line AC motor operated valves	RAW > 5.0 (RAW)	These valves must open to deliver EFW to the respective SG in the event of a transient. These valves are also used to control EFW flow to the SGs during long term EFW usage. Consistent with current practices, these valves are tested on a quarterly basis with unscheduled maintenance performed on failure. The maintenance unavailability is covered by the subtrain maintenance unavailability.
Component: EFW Storage Tank (EFWST)	SMA, Flood	The EFWSTs provide the inventory for the EFW system. Seismic failure of the wall between the EFWST and the adjacent DG room would result in flooding of the DG room with failure of the DG and the loss of EFW inventory. Each EFWST also represents a potential flood source for the subsphere for its associated division.
Component: Condensate Storage Tank (CST)	SMA	If the EFW system is used for extended time periods, the CST provides a source to replenish the EFWST inventory. Seismic failure of this tank would preclude extended EFW usage following a seismic event. ~~The seismic fragility (CDFM HCLPF) used for this tank was 0.56g.~~
Component: EFW storage tank inlet valves	RAW > 5.0 (CCF)	~~Generic demand failure rate used~~. No specific assumptions on test or maintenance intervals
Component: EFW motor driven pump breakers	RAW > 5.0 (CCF)	The motor-driven EFW pump circuit breakers must close to provide power to the motor-driven EFW pumps. The breakers are tested at the same time the motor-driven pumps are tested.
Component: EFWST fill line manual isolation valve between CST and EFWSTs	RAW > 5.0	~~Generic demand failure rate used~~. No specific assumptions on test or maintenance intervals.
Component: EFWST fill line check valve between CST and EFWSTs	RAW > 5.0	~~Generic demand failure rate used~~. No specific assumptions on test or maintenance intervals.

TABLE 19.15.6-1

(Sheet 4 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: 480 VAC class 1E Motor Control Centers	RAW > 5.0 (CCF)	The 480 VAC class 1E MCCs provide power to the various 480 vac safety loads. The 480 VAC MCCs are normally energized with the breaker(s) or contactors to the safety load(s) open to remove power from the load. The load would be energized by closing the breaker(s) or contactors. Faults in the MCCs are detected on occurrence and unscheduled maintenance is performed on failure.
Component: 4.16KV class 1E Buses	RAW > 5.0 (CCF)	The 4.16KV buses provide the AC power to AC-powered safety related loads. 4.16KV power for the pump motors is provided directly from the 4.16 KV buses. 480 VAC power is provided to the load centers via load center transformers. The 4.16 KV buses also indirectly provide power to the vital DC buses via the battery chargers which are powered from 480 VAC vital MCCs. The 4.16 KV buses are continuously energized and faults are detected on occurrence. Unscheduled maintenance is performed on failure.
Component: 4.16KV Permanent Non-Safety buses	RAW > 5.0 (CCF)	The 4.16 KV Permanent Non-Safety (PNS) bus provides 4..KV power and 480 VAC power via stepdown transformers to the permanent non-safety loads. The 4.16 KV PNS bus is continuously energized and faults are detected on occurrence. Unscheduled maintenance is performed on failure.
Component: 125 VDC class 1E vital batteries	RAW > 5.0 (CCF)	The 125 VDC batteries provide 125 VDC power to the 125 VDC vital buses in the event that AC power is unavailable. During normal operation, the battery chargers maintain a floating charge on the batteries. Consistent with current standard practices, the battery terminal voltage is assumed to be verified ~~every 7 days.~~ OK
Component: Emergency Diesel Generators (EDGs)	RAW > 5.0 (CCF) assumed to be	The EDGs supply 4.16 KV power to the Class 1E loads in the event that offsite power is not available following a transient or accident. The EDGs are tested on a ~~monthly~~ basis. OK Unscheduled maintenance is performed on failure. ~~Maintenance unavailability was calculated based on the EDG failure rate, a monthly test interval, and an allowed outage time of 72 hours.~~

TABLE 19.15.6-1

(Sheet 5 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: Emergency Diesel Generator Load Sequencers	RAW > 5.0 (CCF)	The Engineered Safety Features Component Control System has the load sequencers for the vital 4.16 KV buses. They protect the DG from overload and also prevent vital buses from all loading at once if offsite power is lost and regained. The load sequencers are implemented in the Programmable Logic Controllers (PLCs). The PLCs have internal diagnostic tests on a continuous basis and failures are annunciated. Maintenance is performed on failure.
Component: Emergency Diesel Generator Supply Breakers to 4.16KV class 1E buses	RAW > 5.0 (CCF)	These breakers connect the EDGs to the 4.16 KV vital buses. These breakers are tested in conjunction with the monthly EDG tests. ↑ assumed to be
Component: Alternate AC source (Combustion Turbine)	Engineering Judgement	The Alternate AC (AAC) source will supply 4.16 KV power to the permanent non-safety bus in the event that offsite power is unavailable. In addition, the AAC source can also supply power to one division of Class 1E loads if the EDGs are unavailable. ~~The PRA used a generic unavailability for the AAC source as provided in the EPRI PRA Key Assumptions and Groundrules[7].~~ No specific assumptions were made as to testing and maintenance intervals for the AAC.
Component: DG room ventilation fans	RAW > 5.0 (CCF)	The DG room ventilation system is temperature actuated. Based on operating experience information, it is anticipated that the DG room ventilation system will be actuated when the DGs are started for their monthly testing. Thus, the DG room ventilation fans are assumed to be effectively tested on a monthly basis in conjunction with the DG test.
Component: DG room ventilation dampers	RAW > 5.0	The DG room ventilation system is temperature actuated. Based on operating experience information, it is anticipated that the DG room ventilation system will be actuated when the DGs are started for their monthly testing. Thus, the DG room ventilation dampers are assumed to be effectively tested on a monthly basis in conjunction with the DG test.

TABLE 19.15.6-1

(Sheet 6 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: EDG air starting system	Engineering Judgement	Each EDG is assumed to have two independent air starting systems. The starting capability of these systems ~~and~~ tested in conjunction with the monthly EDG test. The replenishment capability of the starting air system is constantly verifiable because the starting air compressors must function to supply air to the starting air tanks due to leakoff and EDG panel usage.
Component: EDG fuel oil storage systems	Engineering Judgement	Each EDG has a complete and separate fuel oil system. These fuel oil systems were assumed to be inspected, tested and maintained consistent with current practices.
Component: Turbine generator	Engineering Judgement	The turbine generator system is designed to be capable of running back to and maintaining "hotel" load following a loss of load.
SYSTEM: Component Cooling Water (CCWS) /Station Service Water (SSWS) Systems	RAW > 5.0	The CCWS is a closed loop system that provides cooling water flow to remove heat released from plant systems and components. The CCWS also provides cooling water flow for decay heat removal from the SCS during shutdown cooling and from the CSS flow during containment spray operation. The CCWs rejects the heat to the SSWS via the ~~SSWS~~ heat exchangers. The SSWS is an open loop system, which takes suction from the ultimate heat sink, passes the flow through ~~SSWS~~ heat exchanger to remove the heat from the CCWS, and then discharges the heated water to the ultimate heat sink. The CCWS and SSWS each consist of two divisions. Each division of SSWS and CCWS have two 100% capacity pumps. One pump in each division is normally operating and the other pump is in standby. If the operating pump trips, the standby pump would be started. Each division also has two 100% capacity SSWS/CCWS heat exchangers with one in service and the other in standby. Manual valve alignment is required to valve in the standby heat exchanger. Pump and heat exchanger maintenance is performed on the pump or heat exchanger that is in standby. The SSWS and CCWS are in operation duri normal power operation and faults in operating equipment are detected on occurrence.

TABLE 19.15.6-1

(Sheet 7 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: CCWS inlet flow control valves to SCS heat exchangers	RAW > 5.0 (CCF)	These valves open to provide CCWS flow through the shutdown cooling heat exchanger during shutdown cooling operation. It was assumed that, consistent with current practices, these valves were tested on a quarterly basis and unscheduled maintenance performed on failure.
Component: Service Water Intake Structure	Tornado Strike Evaluation	The SSWS uses a common intake structure for both divisions. The intake structure is that structure in which the SSWS draws suction from the ultimate heat sink. The SSWS intake structures are required to meet Reg Guide 1.27 requirements. In the event of a tornado strike on site, the tornado might deposit sufficient debris in the intake structure to cause blockage of the intake structure. If complete blockage occurs, all SSW ~~and CCW~~ flow will be lost. Provisions should be incorporated to protect the intake structure against the accumulation of sufficient debris to block the structure.
Component: CCWS surge tanks	SMA	The CCWS surge tanks are located in the upper levels of the nuclear annex at elevation 170+0. Seismic failure of these tanks could lead to loss of all CCW inventory with subsequent failure of CCW.
Component: CCWS heat exchanger building	SMA	The CCWS heat exchanger buildings are separate from the nuclear annex building. Seismically induced differential sliding of these buildings could result in failure of the CCWS piping from the heat exchanger buildings to the nuclear annex with consequential failure of the CCWS.
Component: SSWS pump building	SMA, Fire, Flood	The SSWS pump building is a Seismic Category 1 structure which houses the SSWS pumps for both divisions. This structure is outside the CESSAR-DC scope. It was assumed that this structure would have divisional separation equivalent to that in the nuclear annex such that the propagation of internal floods or fires from one division to the other is prevented. It was also assumed that this Seismic Category 1 structure has a seismic strength equivalent to the nuclear annex structure.
SYSTEM: Safety Injection (SI) System	RAW > 5.0	The function SI system is to inject borated water into the RCS to provide RCS inventory control in response to a LOCA or and SGTR. The SI system also provides inventory injection for feed and bleed cooling in conjunction with the RDS.

TABLE 19.15.6-1

(Sheet 8 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: SI pumps	RAW > 5.0 (CCF)	The SI pumps are required to provide RCS inventory control in response to LOCAs, SGTRs, and situations requiring RCS feed and bleed cooling. The SI pumps also provide long term reactivity control via the injection of borated water. Consistent with current practices, the SI pumps were assumed to be tested quarterly. Unscheduled maintenance is performed on failure.
Component: SI pump motor breakers	RAW > 5.0 (CCF)	The SI pump motor circuit breakers are normally open and must close to provide power to the SI pump motors. The breakers are tested at the same frequency as the SI pumps.
Component: SI pump discharge check valves	RAW > 5.0 (CCF)	Consistent with current practices, these check valves are assumed to be tested on a fuel cycle basis with maintenance performed on failure.
Component: Safety Injection Direct Vessel Injection (DVI) line motor operated valves	RAW > 5.0 (CCF)	The SI DVI MOVs must open to provide injection flow to the DVI lines to provide RCS inventory makeup. Consistent with current practices, these valves are assumed to be tested on a quarterly basis with maintenance performed on failure.
Component: DVI line check valves	RAW > 5.0 (CCF)	This includes all the SI check valves in the DVI line inside containment. These valves must open for injection flow to reach the reactor vessel. The test interval was assumed to be one fuel cycle. Maintenance is performed on failure and only when the plant is shutdown.
Component: Hot Leg Injection line check valves	RAW > 5.0 (CCF)	These check valves are in the hot leg injection lines. These valves must open to provide hot leg injection to prevent boron crystallization after initial response to large and medium LOCAs. The test interval for these check valves was assumed to be one fuel cycle. Maintenance on these valves is performed on failure and only when the plant is shutdown.
Component: Hot Leg injection line motor-operated isolation valves	RAW > 5.0 (CCF)	The hot leg injection MOVs must open to provide hot leg injection to prevent boron crystallization after initial response to large and medium LOCAs. Consistent with current practices, these valves are assumed to be tested on a quarterly basis with maintenance performed on failure.
Component: SIT discharge check valves	RAW > 5.0 (CCF)	In the event of a LOCA, these valves must open for the SIT inventory to inject into the RCS. These valves are tested once a fuel cycle during plant refueling. No scheduled maintenance is performed on these valves while the plant is at power.

assumed to be

TABLE 19.15.6-1

(Sheet 9 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: Safety Injection Tanks (SITs)	RAW > 5.0 (CCF)	The SITs provide a source of inventory for passive injection into the RCS in response to large and medium LOCAs and during aggressive secondary cooldown for SCS injection for small LOCAs. SIT pressure and level are monitored ~~every 12 hours~~, but the tanks are inspected and tested only on a fuel cycle basis and all maintenance is performed while the plant is shutdown.
SYSTEM: Engineered Safety Features Actuation System (ESFAS)	RAW > 5.0	The ESFAS provides the signals to actuate equipment in the front line safety systems following a transient or accident. The System 80+ ESFAS was assumed to be as reliable as the System 80 ESFAS. The analysis of the System 80 ESFAS assumed the system was tested on a monthly basis with maintenance performed on failure. For System 80+, most of the ESFAS logic is automatically tested continuously with alarms if problems detected. In addition, a full channel functional test is performed ~~every 92 days~~ periodically to verify that the ESFAS is operable, and to confirm that the automatic testing is functioning properly.
Component: ESFAS relays	SMA	Solid state switching devices and electromechanical relays will be used in the NUPLEX 80+ protection and control systems. Solid state switching devices are immune to mechanical switching discontinuities. Robust electromechanical relays are selected for NUPLEX 80+ applications such that inherent mechanical contact chatter is within the requisite system performance criteria.
SYSTEM: Reactor Protection System (RPS)	Engineering Judgement	The RPS provides the signals to trip the reactor following a transient or accident. Failure to trip the reactor results in an ATWS. The System 80+ RPS was assumed to be as reliable as the System 80 RPS. The analysis of the System 80 RPS assumed the system was tested on a monthly basis with maintenance performed on failure. For System 80+, most of the RPS logic is automatically tested continuously with alarms if problems detected. In addition, a full channel functional test is performed ~~every 92 days~~ periodically to verify that the RPS is operable, and to confirm that the automatic testing is functioning properly.

TABLE 19.15.6-1

(Sheet 11 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: SCS suction MOVs	RAW > 5.0 (CCF)	The SCS suction MOVs must open in order to start shutdown cooling. These valves are located inside containment, are interlocked on RCS pressure and are part of the RCS pressure boundary. Therefore, these valves can not be tested at power. Consistent with current practices, these valves are tested on a cold shutdown basis and maintenance is performed only when the plant is shutdown.
Component: SCS suction isolation MOVs	RAW > 5.0 (CCF)	The SCS suction isolation MOVs must open in order to establish shutdown cooling. These valves are interlocked on RCS pressure, like the suction MOVs , but they are outside containment and are not part of the RCS pressure boundary. It was assumed that these valves could be tested on a quarterly basis. ~~However, the IST in Table 3.9-15 (Amendment T) specifies that these valves are tested on a cold shutdown basis. This difference is addressed in Table 19.6A-1.~~
Component: SCS discharge check valves	RAW > 5.0 (CCF)	These check valves must open to establish shutdown cooling flow. These check valves are assumed to be tested on a cold shutdown basis consistent with current practices. Maintenance is performed on failure.
Component: SCS heat exchanger flow control valves.	RAW > 5.0 (CCF)	The SCS heat exchanger flow control valves must open in order for SCS flow to pass through the heat exchangers to reject the core heat to the CCW and SSW systems. These valves were assumed to be tested on a quarterly basis and maintenance performed on an as needed basis.
Component: SCS pumps	Shutdown Risk Analysis	The SCS pumps recirculate the RCS fluid through the SCS heat exchangers to cool the RCS from shutdown cooling entry conditions to cold shutdown conditions and to maintain cold shutdown conditions. The SCS pumps can be backed up by the CSS pumps during shutdown cooling. The SCS pumps can be used to back up the CSS pumps. The SCS pumps can also be aligned to inject to the RCS if the RCS is depressurized to the SCS pump shutoff head. The SCS pumps were assumed to be tested on a quarterly basis consistent with current practices.

TABLE 19.15.6-1

(Sheet 12 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: SCS/CSS Crossover Valves	Engineering Judgement, Shutdown Risk Assessment	In order to use the SCS pumps to backup the CSS pumps or to use the CSS pumps to backup the SCS pumps, the SCS/CSS suction and discharge crossover valves must be opened. These valves were assumed to be tested on a quarterly ~~based~~ basis with maintenance performed on an as needed basis.
SYSTEM: Rapid Depressurization System (RDS)	RAW > 5.0	The RDS consists of two trains, each containing two MOVs in series, that provides a discharge path from the top of the pressurizer to the IRWST. The primary function of the RDS is to provide a means of depressurizing the RCS in the event of a severe accident with the RCS at high pressure to prevent a High Pressure Melt Ejection. The RDS also provides the "bleed" capability for feed and bleed (or once through) cooling of the RCS.
Component: Rapid Depressurization Valves (RDVs)	RAW > 5.0 (CCF)	The RDVs must open for feed and bleed cooling, or for depressurization of the RCS during a severe accident. These valves are inside containment and are part of the RCS pressure boundary so they can not be tested at power. These valves are tested on a fuel cycle basis and maintenance is performed on these valves only when the plant is shut down and depressurized.
Component: RDV inverters	RAW > 5.0 (CCF)	The RDV valves are 480 VAC motor operated valves which are powered from the 125 VDC class 1E vital buses via dedicated inverters. Failure of the inverters would result in failure of the RDVs to open. These inverters are continuously energized and failures are indicated. Maintenance is performed on failure.
SYSTEM: Containment Spray System (CSS)	RAW > 5.0, Level 2	The CSS provides containment temperature and pressure control following accidents such as LOCAs and steam line breaks inside containment. The CSS also provides containment temperature and pressure control following a severe accident.
Component: Containment Spray pumps	Level 2	The CSS pumps deliver spray flow from the IRWST to the spray headers. The CSS pumps are assumed to be tested on a quarterly basis with unscheduled maintenance performed on failure. The SCS pumps can be used to backup the CSS pumps, and the CSS pumps can be used to backup the SCS pumps.

pump recirculation

TABLE 19.15.6-1

(Sheet 13 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: Low Temperature Overpressure (LTOP) valves	Shutdown Risk Evaluation, RAW > 5.0	The LTOP valves are to provide RCS overpressure protection during low temperature operations. These valve also provide a "bleed" path for feed and bleed cooling during low temperature low pressure conditions with the shutdown cooling system valves open. It was assumed that these valves are tested and maintained consistent with current practices.
SYSTEM: Emergency Containment Spray Backup System (ECSBS)	Level 2	The function of the ECSBS is to provide an independent self contained means of supplying water to the containment spray header for containment heat removal during emergency conditions where the CSS and SCS pumps are not available.
Component: CS header "T"	Level 2	~~An 8 inch~~ "T" connector is provided in each CS ~~header~~ line outside containment so that the CS headers can accept spray flow from an external source.
Component: ECSBS pumping device	Level 2	The ECSBS will have an independent pumping device that is capable of delivering sufficient flow to the containment spray headers at 24 hours after the onset of a severe accident to prevent the pressure in containment from exceeding level C pressure limits. No specific assumptions were made about the testing or maintenance of this pumping device.
SYSTEM: StartUp Feedwater System	Engineering Judgement	The function of the startup feedwater system is to provide feedwater flow during low power/startup/shutdown conditions. The startup feedwater system can backup the EFWS.
Component: Startup feedwater pump	Engineering Judgement	The startup feedwater pump is used to provide feedwater flow during low power/startup/shutdown conditions. The startup feedwater pump can act as a backup to the EFW pumps. ~~Generic failure rates were used for this component~~. No specific assumptions were made as to the test interval or the maintenance frequency for this pump.
SYSTEM: Main Steam System	RAW > 5.0	The Steam Removal System consists of the main steam line and associated valves up to the turbine control valves. The valves in this system include those which provide for containment isolation following a steam line break or an SGTR and those which provide steam removal during a cooldown of the plant.

TABLE 19.15.6-1

(Sheet 14 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: Atmospheric Dump Valves (ADVs)	RAW > 5.0 (CCF)	These valves provide a controllable means of releasing steam from an SG to the atmosphere to prevent challenging the MSSVs. These valves were assumed to be tested on a quarterly basis.
Component: Main Steam Isolation Valves (MSIVs)	Engineering Judgement (CCF)	The MSIVs provide containment isolation following a steam line break. The MSIVs are also used to isolate the ruptured Steam Generator (SG) following an SGTR once the RCS pressure has been reduced to the point at which the MSSVs will not lift. The MSIVs have a partial stroke test on a quarterly basis with a full stroke test on a cold shutdown basis. Maintenance is performed only when the plant is shutdown.
Component: Main Steam Safety Valves (MSSVs)	Engineering Judgement	The MSSVs are the code safety valves for the SGs. Failure of the MSSVs to open could result in overpressurization of the SGs. If the MSSVs are challenged following an SGTR and fail to reseat, they provide a direct release path to atmosphere. The MSSVs are not tested at power. They were assumed to be tested consistent with current practices.
Component: Turbine Bypass Valves (TBVs)	Engineering Judgement	Following a turbine trip, the turbine bypass valves open to discharge steam directly to the condenser, bypassing the turbine, to avoid unnecessary reactor trips and to prevent opening of the Primary Safety Valves and the Main Steam Safety Valves. The turbine bypass valves are air operated valves that fail closed on loss of air. These valves are interlocked so that they do not open on turbine trip if the condenser is not available. ~~A generic failure rate was used for these valves~~. No specific assumption was made as to the test and maintenance intervals for these valves.
SYSTEM: Reactor Coolant System (RCS)		
Component: Primary Safety Valves (PSVs)	RAW > 5.0 (CCF)	The PSVs are the code safety valves for the RCS. Failure of one of these valves to reseat following a challenge such as an ATWS would result in LOCA. The PSVs cannot be tested at power. It was assumed that the PSVs are tested consistent with current practices. All PSV maintenance is performed while the plant is shutdown and depressurized.

TABLE 19.15.6-1

(Sheet 17 of 18)

RISK SIGNIFICANT SSCs FOR INCLUSION IN THE D-RAP

SSC	Rationale	Insights and Assumptions
Component: Flood Doors	Flood Risk Evaluation	Flood doors are provided for each flood zone in the Nuclear Annex subsphere area to prevent the propagation of an internal flood from one flood zone to another. These flood doors are normally closed and their positions are indicated in the control room. If a flood door must be held open for maintenance access or other reason, a watch is maintained at the affected flood door. No specific assumptions were made in the PRA as to maintenance for the flood doors.
Component: Floor Drain Sump Discharge Check Valves	Engineering Judgement, Flood	Flooding from the Radwaste Building and Turbine Building through the floor drain sump pump discharge lines to the Nuclear Annex is prevented by the reverse flow check valves located at each of the sump pump discharges. The check valves on the Reactor Building Subsphere floor drain sump pumps and Diesel Generator Building floor drain sump pumps are Safety Class 3. These valves are reverse flow tested quarterly as specified in the IST plan ~~in Table 3.9-15.~~ The check valves on the discharge of the Nuclear Annex radioactive floor drain sumps, CVCS area floor drain sumps, and non-radioactice floor drain sumps are non-safety related. These valves should also be reverse flow tested on a quarterly basis ~~as part of the Q-RAP.~~
SYSTEM: Containment		
Component: Containment shell	Level 2, SMA	The containment shell is the primary barrier preventing release of radioactive material following a core damage accident. Also, seismically induced overturning/sliding of the containment shell was found to be the dominant contributor to the plant level HCLPF value in the SMA.
Component: IRWST/ HUT screens	Engineering commitment	The HUT/IRWST screens prevent trash and debris from entering the HUT and the IRWST and potentially blocking the suction lines for the safety pumps or the cavity flood valves. These screens are assumed to be inspected and cleaned on a fuel cycle basis. They are indirectly tested during the quarterly safety injection pump tests.

TABLE 19.15.6-2

(Sheet 1 of 2)

IMPORTANT OPERATOR ACTIONS FROM THE PRA

Important Operator Action	Source	RAW[1]	RRW[2]
Operator fails to initiate Hot Leg Injection	Level 1	~~1.62E+02~~ >5.0	~~1.02E+00~~ <1.1
Operator fails to align EFWSTs to CST	Level 1	~~1.29E+02~~ >5.0	~~1.01E+00~~ <1.1
Operator fails to initiate RCS heat removal via Feed and Bleed Cooling	Level 1	~~1.93E+01~~ >5.0	~~1.20E+00~~ >1.1
Operator fails to initiate SCS for long-term decay heat removal	Level 1	~~6.81E+00~~ >5.0	~~1.00E+00~~ ≤1.1
Operator fails to align SCS pumps for RCS injection following aggressive secondary cooldown	Level 1	~~5.49E+00~~ >5.0	~~1.02E+00~~ <1.1
Operator fails to perform aggressive secondary cooldown (permitting injection via SCS) after SGTR	Level 1	~~3.49E+00~~ <5.0	~~1.19E+00~~ >1.05
Operator fails to perform aggressive secondary cooldown (permitting injection via SCS) after small LOCA	Level 1	~~2.85E+00~~ <5.0	~~1.12E+00~~ >1.05
Operator fails to reclose ADVs on ruptured SG	Level 1	~~1.98E+01~~ >5.0	~~1.00E+00~~ <1.1
Operator fails to align CVCS to refill IRWST following an SGTR	Level 1	~~4.07E+00~~ <5.0	~~1.01E+00~~ >1.01
Operators fail to align AAC to Vital AC buses following loss of offsite power and failure of EDGs	Level 1	Medium (Engineering Judgement	Medium (Engineering Judgement)
Operator fails to initiate cavity flooding	Level 2	High[3]	High[3]
Operator Fails to Depressurize RCS prior to Vessel breach using RDVs	Level 2	High [3]	High [3]
Operator fails to initiate Hydrogen Mitigation System	Level 2	Medium[3]	Medium[3]
Operator fails to align emergency backup containment spray system for use.	Level 2	Medium[3]	Medium[3]
Operator fails to Isolate an isolatable LOCA and isolate containment during shutdown operations	Shutdown Risk Evaluation	~~1.87E+02~~[4] >5.0[4]	~~1.01E+00~~[4] <1.1[4]
Operator fails to initiate feed using SCS during shutdown operations	Shutdown Risk Evaluation	~~2.21E+01~~[4] >5.0[4]	~~1.42E+00~~[4] >1.1[4]

TABLE 19.15.6-2

(Sheet 2 of 2)

IMPORTANT OPERATOR ACTIONS FROM THE PRA

Important Operator Action	Source	RAW[1]	RRW[2]
Operator fails to start and load standby AC source during shutdown operations	Shutdown Risk Evaluation	~~1.20E+01~~[4] $>5.0^{-4}$	~~1.40E+00~~[4] $>1.1^{-4}$
Operator fails to isolate an Isolatable leak/LOCA during shutdown operations.	Shutdown Risk Evaluation	~~1.08E+01~~[4] $>5.0^{-4}$	~~1.16E+00~~[4] $>1.1^{-4}$
Operator fails to start standby SCS train during shutdown operation	Shutdown Risk Evaluation	~~8.56E+00~~[4] $>5.0^{-4}$	~~1.32E+00~~[4] $>1.1^{-4}$
Operator fails to initiate feed using the SIS during mode 5 operations	Shutdown Risk Evaluation	~~7.06E+00~~[4] $>5.0^{-4}$	~~1.24E+00~~[4] $>1.1^{-4}$
Operator fails to restore SCS train given that leak/LOCA is isolated	Shutdown Risk Evaluation	~~6.19E+00~~[4] $>5.0^{-4}$	~~1.00E+00~~[4] $<1.05^{-4}$
Operator fails to restore DHR in 73 hours given loss of DHR in mode 6 with refueling pool full and IRWST empty.	Shutdown Risk Evaluation	~~5.40E+00~~[4] $>5.0^{-4}$	~~1.05E+00~~[4] $<1.1^{-4}$
Operator fails to recover DHR within 12 hours following loss of DHR with successful boiloff makeup using the CVCS	Shutdown Risk Evaluation	~~4.15E+00~~[4] $<5.0^{-4}$	~~1.54E+00~~[4] $>1.05^{-4}$
Operator fails to use the CVCS to makeup inventory in mode 5	Shutdown Risk Evaluation	~~3.52E+00~~[4] $<5.0^{-4}$	~~1.21E+00~~[4] $>1.05^{-4}$
Operator fails to suppress fire during shutdown operations	Shutdown Risk Evaluation	~~2.76E+00~~[4] $<5.0^{-4}$	~~1.24E+00~~[4] $>1.05^{-4}$

NOTES

1. RAW = Risk Achievement Worth
2. RRW = Risk Reduction Worth
3. The RAW and RRS values were not calculated for Operator actions in the level 2 analyses. Qualitative importances were assigned based on engineering judgement.
4. The RAW and RRW values presented for the Shutdown Risk Evaluation are event tree branch point RAW and RRW values and include contributions from both operator errors and equipment failures.

19.16 REFERENCES

1. 10 CFR Part 52; Early Site Permits; Standard Design Certification; and Combined Licenses for Nuclear Power Reactors; 54FR 15372; April 18, 1989.
2. Not used. This Reference intentionally Blank
3. Base Line Level 1 Probabilistic Risk Assessment for the System 80 NSSS Design; Enclosure (1)-p to LD-88-008; Combustion Engineering, Inc.; January, 1988.
4. System 80™ CESSAR FSAR; Combustion Engineering, Inc.; August, 1985.
5. NUREG/CR-2815; "Probabilistic Safety Analysis Procedures Guide"; Papazoglou, I. A., Buri, R. A.; Brookhaven National Lab.; January 1984.
6. NUREG/CR-2300; "PRA Procedures Guide"; April 1982.
7. NP-6780-L, Advanced Light Water Reactor (ALWR) Utility Requirements Document, Rev. 3, EPRI, November, 1991.
8. NUREG-1150; "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants"; Second Draft for Peer Review; U.S. Nuclear Regulatory Commission; June, 1989.
9. Depressurization and Decay Heat Removal - Response to NRC Questions; CEN-239; June 1983.
10. Probabilistic Risk Assessment of the Effect of PORVs on Depressurization and Decay Heat Removal - Palo Verde Nuclear Generating Station Units 1, 2 and 3; CEN-239, Supplement 3; July 1983.
11. Probabilistic Risk Assessment of the Effect of PORVs on Depressurization and Decay Heat Removal - Washington Nuclear Project Unit 3; CEN-239, Supplement 4 (Draft); October 1983.
12. C-E Emergency Procedure Guidelines; CEN-152, Revision 1; November 1982.
13. "Standard Technical Specifications for Combustion Engineering Pressurized Water Reactors"; NUREG-0212, Rev. 03, Draft; July 1982.
14. Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants; WASH 1400/ NUREG-75/014; October 1975.
15. Zion Probabilistic Safety Study; Commonwealth Edison.

This Reference intentionally blank

16. Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3; NSAC/60; June 1984.

17. Interim Reliability Evaluation Program: Calvert Cliffs Unit 1, SAI-001-82-BE; January 15, 1982.

18. Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant; SAND82-0978, NUREG/CR-2787; June 1982.

19. "Probabilistic Safety Study - Westinghouse Advanced Pressurized Water Reactor"; RESAR-SP190; Westinghouse Electric Corporation; June 1985.

20. Seabrook Station Probabilistic Safety Assessment; PLG-0368; Prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company; Pickard, Lowe and Garrick, Inc.; June, 1984.

21. Individual Plant Evaluation Methodology for Pressurized Water Reactors"; Technical Report 86.3A1; Westinghouse Electric Corporation; April 1987.

22. NUREG-1335; "Individual Plant Examination: Submittal Guidance"; U. S. Nuclear Regulatory Commission; August, 1989.

23. CENPD-278-P; "CENTS - COMBUSTION ENGINEERING NUCLEAR TRANSIENT SIMULATION CODE"; Nuclear Power Systems, Combustion Engineering; December, 1987.

24. Fauske & Associates, Inc.; Modular Accident Analysis Program (MAAP); Atomic Industrial Forum; IDCOR Program Technical Report 16.2-3; February, 1987.

25. DOE/ID-10216; Modifications for the Development of the MAAP-DOE Code; Volumes 1-7; December, 1988.

26. Haasl, D. F., Roberts, N. H., "Fault Tree Handbook"; NUREG-0492; U. S. Nuclear Regulatory Commission; November, 1978.

27. EPRI NP-2230; "ATWS: A Reappraisal, Part 3, Frequency of Anticipated Transients"; January 1982.

28. Oswald, A. J., Gentillon, C. D., Matthews, S. D., Meachum, T. R.; "Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP) Guide"; EGG-EA-5887; June 1982.

This reference intentionally blank

29. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability for Nuclear Power Generating Stations; IEEE-STD500-1984.

30. Nuclear Plant Reliability Data System (NPRDS) Reportable System and Component Scope Manual for Combustion Engineering Pressurized Water Reactors; INPO 83-020C, Rev. 2; Institute of Nuclear Power Operations; September 1985.

31. EPRI NP 3967; "Classification and Analysis of Reactor Operating Experience Involving Dependent Events"; June 1985.

32. EPRI NP 5777; "Data-based Defensive Strategies for Reducing Susceptibility to Common Cause Failures"; Vol. 1 Defensive Strategies; Vol. 2 Data Analysis; June 1988.

33. NUREG/CR-2770; "Common Cause Fault Rates for Valves"; February 1983.

34. NUREG/CR-2771; "Common Cause Fault Rates for Instrumentation and Control Assemblies"; February 1983.

35. NUREG/CR-2098; "Common Cause Fault Rates for Pumps"; February 1983.

36. NUREG/CR-2099; "Common Cause Fault Rates for Diesel Generators"; June 1982.

37. Swain, A. D. and Guttman, H. E.; Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations; NUREG-CR-1278; 1983.

38. Bell, B.J. and Swain, A.D.; "A Procedure for Conducting a Human Reliability analysis for Nuclear Power Plants"; NUREG/CR-2254.

39. Hannaman, G.W. and Spurgin, A.J.; "Systematic Human Action Reliability Procedure (SHARP)"; EPRI NP-3583.

40. NUREG/CR-4639; "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)"; Volume 5, Parts 1 and 2, Revision 3; December 1990.

41. "Computer-Aided Fault Tree Analyser" computer Program, Version 2.2, By Science Applications International Corporation and EPRI; May, 1992.

42. Indian Point 2 and 3 Probabilistic Safety Study; prepared for Consolidated Edison Company of New York, Inc., and Power Authority of the State of New York; Pickard, Lowe, and Garrick, Inc.; March, 1982.

This reference intentionally blank.

43. Fullwood, R.R.; Probabilistic Risk Assessment: Fundamentals; prepared by Brookhaven National Laboratory, prepared for the U.S. Nuclear Regulatory Commission; March, 1987.

44. NUREG-0800; Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition; U.S. Regulatory Commission; July, 1981.

45. "Fire Induced Vulnerability Evaluation Methodology (FIVE), CoarsePlant Screening Guide"; Prepared for the Electric Power Research Institute by Professional Loss Control, Inc.; Contract RP 3000-41; 1992.

46. NUREG/CR-2552(SAND82-0342); "CRAC2 Model Description"; Richie, L. T., Alpert, D. J., Burke, R. P., Johnson, J. D., Ostmeyer, R. M., Aldrich, D. C., Blond, R. M.; prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratory; March, 1984.

47. NUREG/CR-2326(SAND81-1994); "Calculation of Reactor Accident Consequences - Version 2, CRAC2 Computer Code Users Guide"; Richie, L. T., Alpert, D. J., Burke, R. P., Johnson, J. D., Ostmeyer, R. M., Aldrich, D. C., Blond, R. M.; prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratory; 1981.

48. "ORIGEN 2 Isotope Generation and Depletion Code - Matrix Exponential Method"; CCC-371; Oak Ridge National Laboratory; Oak Ridge, Tennessee; September, 1983.

49. "System 80+ Shutdown Risk Evaluation Report"; ALWR-DCTR-10; ABB-Combustion Engineering Nuclear Power Systems; Windsor, Connecticut; July, 1992.

50. CE-CES-49; "Users Manual for CESAM - Combustion Engineering's Monte Carlo Sampling Code"; April, 1985.

51. 10 CFR Part 50.34F "Additional TMI - Related Requirements"

52. NUREG-0020; "Licensed Operating Reactors, Status Summary Report"; U. S. Nuclear Regulatory Commission; January, 1992

53. Reactor Protection System Test Interval Evaluation; CE-NPSD-277; December, 1984.

54. RPS/ESFAS Extended Test Interval Evaluation; CEN-327; Combustion Engineering, Inc.; May, 1986.

55. RPS/ESFAS Extended Test Interval Evaluation; CEN-327, Supplement 1; Combustion Engineering, Inc.; January, 1989.

This reference intentionally blank.

56. "Reliability Evaluation of the C-E Proposed Alternate Reactor Trip System"; 00000-NSR-ART1; Combustion Engineering, Inc.; June 1984.

57. NUREG-1032; "Evaluation of Station Blackout Accidents at Nuclear Power Plants"; U.S. Nuclear Regulatory Commission' May 1985.

58. "A Combustion Engineering Review of NUREG-1032; Evaluation of Station Blackout Accidents at Nuclear Power Plants"; C-E NPSD-340; performed by Combustion Engineering for the C-E Owners Group; March 1986.

59. 10 CFR Part 50.62; "Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"; U. S. Nuclear Regulatory Commission.

60. "Anticipated Transients without Scram for Light Water Reactors"; NUREG-0460; U. S. Nuclear Regulatory Commission; April, 1978.

61. "Rules and Regulations, Title 10, Chapter 1, Code of Federal Regulations-Energy, Part 100, Reactor Site Criteria"; U.S. Nuclear Regulatory Commission; as amended through April 30, 1975.

62. CEN-134-P; "C-E NSSS Owner's Response to NUREG-0460, Volume 4:March 1980" Combustion Engineering, Inc.; October, 1980.

63. SECY-83-293; "Amendments to 10CFR50 Related to Anticipated Transients without Scram (ATWS) Events"; USNRC; July 19, 1983.

64. CENPD-263-P, "ATWS Early Verification: Response to NRC Letter of February 15, 1979, for Combustion Engineering NSSS's"; November, 1979.

65. "BNFL New Reactor Study, System 80+™ Standard Design, Key Issue Paper on Reactor Shutdown (ATWT and Return to Power)"; ABB-Combustion Engineering Nuclear Power; Windsor, Connecticut; August, 1992.

66. NUREG/CR-5102(BNL-NUREG-52135); "Interfacing Systems LOCA: Pressurized Water Reactors"; Bozoli, G., Kohut, P., Fitzpatrick, R.; prepared for the U. S. Nuclear Regulatory Commission by Brookhaven National Laboratory; February, 1989.

This reference intentionally blank.

67. NUREG/CR-4550(SAND86-2084); "Analysis of Core Damage Frequency From Internal Events: Methodology Guidelines - Volume 1"; Drouin, M. T., Harper, F. T., Camp, A. L.; prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratory; September, 1987.

68. NUREG/CR-4780(EPRI NP-5613); "Procedures for Treating Common Cause Failures in Safety and Reliability Studies"; Mosleh, A. et. al.; Prepared for the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute by Pickard, Lowe and Garrick, Inc.; January, 1988.

69. Finnicum, D. J., Rzasa, P. W., Serafin, S. A.; Design and Application of Combustion Engineering's Reliability Data Systems for Nuclear Steam Supply Systems; presented at the Eighth Annual Reliability Engineering Conference for the Electric Power Industry; April 21 - 23, 1981; Portland, Oregon.

70. Nuclear Power Experience; Vol. PWR-2.

71. NUREG/CR-2728; "Interim Reliability Evaluation Program Procedure Guide"; Carlson, D. D.; Prepared for the U. S. Nuclear Regulatory Commission by Sandia National Laboratory; January, 1983.

72. NUREG/CR-4834; "Recovery Action in PRA for the Risk Methods Integration and Evaluation Program (RMIEP)"; Whitehead, D.W.: Prepared for the U. S. Nuclear Regulatory Commission by Sandia National Laboratory; June, 1987.

73. "Generic Issue-23, Evaluation of the Reactor Coolant Pump Seal Integrity Issue", ABB-CE, CEN-408, September, 1991.

74. "Generic Issue-23, Evaluation of the Reactor Coolant Pump Seal Integrity Issue", ABB-CE, CEN-408, September, 1991.

75. Seight, L., Meyers, R., "RCP Seal and Lower Bearing", A.P.S., 86-RC-089, 4/1/86.

76. Calderone, J.W., Herzig, N.S., "Millstone Unit 2 Reactor Coolant Pump Seals", NU, GRE-84-688, December 11, 1984.

77. Johnson, R.W., "RCP Seal Failure from Loss of Component Cooling Water", CE, SER 85-79, April 26.1985.

78. Paggen, V.A., "Inadvertent "a" ESF Actuation", CE, SER 85-169, August 20, 1985.

79. Uhrig, R.E., FP&L, "Adequacy of RCP Seal Design during Postulated Station Blackout Conditions", Letter to Eisenhut, D.G., NRC, L-81-107, March 10, 1981.

This reference intentionally blank.

80. Mroczka, E.J., NU, Letter to Chief, Regulatory Publication Branch, NRC, 56 FR 16130, October 1, 1991.

81. Hill, R.C., et.al., "Reactor Coolant Pump Shaft Seal Stability During Station Blackout (Draft)", NUREG/CR-4821 (EGG-2492), December 1986.

82. Marr, A.H., et.al., Loss of Component Cooling Water Capability of a PWR Reactor Coolant Pump", paper 80-C2/PVP-23, ASME Century 2 Pressure Vessel and Piping Conference, San Francisco, Ca., August 12, 1980.

83. Marsi, J.A., Gopalakrishnan, S., "Full Scale Station Blackout Test Conducted on Advanced RCP Mechanical Seals", Nuclear Plant Journal, September-October 1988, Page 86.

84. INPO Notepad, August 26, 1985.

85. Short, T.E.,OPPD, "Loss of Cooling Water to RCP Seals", Letter to Lear, G., NRC, FC-413-75A, June 26, 1975.

86. INPO Notepad, April 7, 1986.

87. INPO Notepad, August 9, 1985.

88. Nuclear Power Experience, Vol. PWR-2, V. Reactor Coolant System, A. Pump.

89. Waters, J. E., Personal Communication with E. R. Siegmann, 3/6/85.

90. Generic Letter 83-28; "Required Actions Based on Generic Implications of Salem ATWS Events"; U. S. Nuclear Regulatory Commission; July 8, 1983.

91. Harrison, D. G.; "Advanced Reactor Severe Accident Program - Combustion Engineering Interim External Events Integration - WBS 10.4.4"; prepared by Tenera, L. P. for EG&G Idaho, Inc., and the U.S. Department of Energy; February, 1989.

92. Summitt, R. L.; "Tornado Risk Analysis in Support of the Combustion Engineering System 80+ Probabilistic Risk Assessment of External Events"; performed by Safety and Reliability Optimization Services, Inc., for Combustion Engineering, Inc.; January, 1990.

93. Brooks, R. D.; "Advanced Reactor Severe Accident Program - Interim Estimation of Core-Damage Frequency to C-E System 80+ due to Seismic Initiating Events - WBS-10"; RDC-69-89; Tenera L.P.; Knoxville, Tennessee; October, 1989.

This reference intentionally blank.

94. "Tornado Missile Simulation and Design Methodology"; Volumes 1 and 2; EPRI NP-2005; August, 1981.

95. American Nuclear Society; Guidelines for Combining Natural and External Man-Made Hazards at Power Reactor Sites; ANSI/ANS-2.12-1978.

96. Consumers Power Company; Big Rock Point Plant PRA; March, 1981.

97. Reg Guide 1.115

98. Lobner, P., Goldman, L., Horton, W., Finn, S.; "Ranking of Light Water Reactor Systems for Sabotage Protection"; SAND82-7053; Sandia National Laboratory; July, 1982.

99. NUREG/CR-2643; "A Review of Selected Methods for Protecting Against Sabotage by an Insider"; August, 1982.

100. LD-88-091; "CESSAR-DC, Program for Addressing Sabotage Protection"; letter from A. E. Scherer (C-E) to G. S. Vissing (NRC); September 14, 1988.

101. Fire Hazards Assessment, ABB Combustion Engineering/U.S. Department of Energy Advanced Light Water Reactor Certification Program; Volumes 1 - 5, March 13, 1992; Duke Engineering Services, Inc.

102. EPRI NP-4144; "Turbine Generator Fire Protection by Sprinkler System"; July, 1985.

103. Berry, D.G., Minor, E.E.; "Nuclear Power Plant Fire Protection Fire Hazard Analysis"; NUREG/CR-0654; September, 1979.

104. NUREG/CR-4840; Procedure for the External Event Core Damage Frequency Analyses for NUREG-1150"; SAND88-3102; November, 1990.

105. Summitt, R. L.: "Probabilistic Assessment of the EPRI Requirements for Evolutionary Pressurized Water Reactors Supplement 1 - Containment Analysis Task 4.3.4"; DOE/ID-10268.

106. Chu, T. L., et.al.,"PWR Low Power and Shutdown Accident Frequencies Program, Phase 1A - Coarse Screening Analysis," Brookhaven National Laboratory, Letter Report FIN L-1344, November 13, 1991.

107. NUREG-1150, Vol. 2; "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants: Appendices A, B, and C: Final Report"; October, 1990.

This reference intentionally blank.

108. Ayres, D., et. al.; "Effects of a Hypothetical Core Melt on a PWR Vessel with Top Entry Instruments"; IDCOR Technical Report Task 15.2a; June, 1983.

109. NUREG/CR-3916; "Pressurized Melt Ejection into Water Pools"; Tarbell, W. W., et. al.; Sandia National Laboratory; March, 1991.

110. Alsmeyer, H.; "Melt Attack and Penetration of Radial Concrete Structures Cooled by Outside Water"; 20th Water Reactor Safety Meeting; October, 1992.

111. NUREG/CR-2442, "Reliability Analysis of Steel Containment Strength", Griemann, L. G., et. al.; Ames Laboratory, Iowa State University, June, 1982.

112. Moody, F., Muralidaran, R., Dua, S.S.; "Assessment of Ex-vessel Steam Pressure Spikes in BWR Mark II Containments"; 19th Water Reactor Safety Meeting; October, 1991.

113. Cole, R.H.; Underwater Explosions; Princeton University Press; Princeton, New Jersey; 1948.

114. SECY-90-016. "Evolutionary Light Water Reactor (LWR) Certification Issues and their Relationship to Current Regulatory Requirements", January 12, 1990.

115. DOE/ID-10271 "Prevention of Early Containment Failure due to High Pressure Melt Ejection and Direct Containment Heating for Advanced Light Water Reactors," Carter, J. C., et.al., March, 1990.

116. SECY-93-087, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor Designs," April 2, 1993.

117. NUREG/CR-5567, "PWR Dry Containment Characterization," Wang, 1990.

118. NUREG/CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 1, "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters: Expert Opinion Elicitation on In-Vessel Issues," Sandia National Laboratory, November, 1990.

119. NUMARC Technical Basis Report (DRAFT), June 1992.

120. "Low Pressure Cutoff for Melt Dispersal from Reactor Cavities," Tutu, N. K., Ginsberg, T., Fin Frock, C., Fourth Proceedings of Nuclear Thermal Hydraulics, Washington, D.C., 1988.

This reference intentionally blank.

121. "Progression Understanding Direct Containment Heating in Pressurized Water Reactors," Ginsberg, T., Tutu, N., Proceedings of the Third International Topical Meeting in Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, Korea, November, 1988.

122. "Adiabatic Equilibrium Models for Direct Containment Heating," M. Pilch, 19th Annual WRSM, October, 1991.

123. "Direct Containment Heating (DCH), Integral Effects Tests in the COREXIT Facility at ANL," Spencer, B. W., et.al., Presentation at CSARP Review Meeting, May 4-8, 1992.

This reference intentionally blank.

124. "Experimental Results of Integral Effects Tests With 1/20th Scale Zion Subcompartment Structures in the Surtsey Test Facility," M. D. Allen, M. M. Pilch, Presentation at Severe Accident Research Partner's Meeting, Bothesda, MD, May, 1992.

125. NUREG/CR-4914, (SAND87-940) "The Influence of Selected Containment Structures on Debris Dispersal and Transport Following HPME From a Reactor Vessel", Sandia, September, 1987.

126. NUREG-1116, "A Review of the Current Understanding of the Potential for Containment Failure from In-Vessel Steam Explosions," USNRC, June, 1985.

127. NUREG-1150, "Reactor Risk Reference Document: Appendices J-O: Draft for Comment)," USNRC, February, 1987.

128. Squarer, D., Leverett, M. C., "Steam Explosion in Perspective", Proceedings on the International Meeting on Light Water Reactor Severe Accident Evaluation", Cambridge, MA, August, 1983.

129. Theofanous, T. G., " Assessment of Steam Explosion Induced Containment Failure: Part 1: Probabilistic Aspects", Nuclear Science and Engineering, Vol 97, 1987.

130. GRS-74, "German Risk Study: Nuclear Power Plants Phase B: A Summary," June, 1989.

131. NUREG-1150, Vol. 2, "Severe Accident Risks: An Assessment for Five Nuclear Power Plants: Appendices", (Final Report) USNRC, May, 1990.

132. Coradini, M. L., " Vapor Explosions: A Review of Experiments and Accident Analysis", Nuclear Safety, Vol. 32, No. 3, July-September, 1991.

133. EPRI NP-2955,"Intermediate-Scale Combustion Studies of Hydrogen-Air-Steam Mixtures", R.K. Kumar, H. Tamm, W.C. Harrison, Palo Alto, Ca., June 1984.

134. NP-3878,"Large Scale Hydrogen Combustion Experiments", EPRI, October, 1988.

135. NUREG/CP-0076, "On Two Aspects of Hydrogen Risk," Forestier, A., Goldstein, S., Proceedings of the Third Workshop on Containment Integrity, 1986.

136. NUREG/CR-5662,(BNL-NUREG-52271), "Hydrogen Combustion Control and Value-Impact Analysis for PWR Dry Containments", Yang, J.W., et. al., May, 1991.

137. HEDL-TME-82-8,"Hydrogen Control Systems for Severe Accident Conditions: A State of Technology Report", Hanford Engineering Development Laboratory, 1982.

138. NUREG/CR-5275: "FLAME Facility: Effect of Obstacles and Transverse Venting on Flame Acceleration and Transition to Detonation for Hydrogen - Air Mixtures at Large Scale," Sandia, April 1989.

139. "The Possibility of Local Detonations During Degraded Core Accidents in the Belleonte Nuclear Power Plant," Sherman, M., Berman, M., Nuclear Technology, Vol. 81, April 1988.

This reference intentionally blank.

140. ~~"Deflagration~~ Detonation Transition in Hydrogen-Air-~~Steam~~ Mixtures: ~~Relevance of Experimental Results for~~ Real Accident ~~Situations," Behrens,~~ O., et.al., Nuclear ~~Engineering~~ and Design, Vol. 130, 1991.

141. CENPD-141, "Reactor Plant Subcompartment Analysis", Combustion Engineering, Inc., March, 1978.

142. NUREG/CR-4551, Vol. 3, Rev. 1, Part 1, "Evaluation of Severe Accident Risks: Surry Unit 1," Sandia National Laboratory, October, 1990.

143. EPRI NP-2953,"Hydrogen Combustion and Control Studies in Intermediate Scale", Torok, R., et. al., June 1983.

144. NUREG/CR-5728, "Experiments to Investigate the Effect of Flight Path on Direct Containment Heating in the Surtsey Test Facility", Allen, M.D., Pilch, M., October, 1991.

145. CE-NPSD-74-P, "Evaluation of Design Features which Minimize the Probability of Interfacing System LOCAs for System 80+ Standard Design," Combustion Engineering, Inc., May, 1992.

146. DCTR-RS-02,Rev 0, Probabilistic Risk Assessment for the System 80+ Standard Design", Combustion Engineering, Inc., January, 1991.

This reference intentionally blank.

147. Benz, R., et. al., " Melt Water Interaction in Tank Geometry: Experimental and Theoretical Results", Proc. of 4-th CSNI Specialist Meeting on Fuel Coolant Interaction, Bournemouth, England, April 1979.

148. EPRI-NP-5127, Spencer, B. W., "Hydrodynamics and Heat Transfer Aspects of Corium Water Interactions, March, 1987.

149. DOE/ID 10290," Technical support for the Hydrogen Control Requirement for the EPRI Advanced Light Water Reactor Requirements Document", January, 1990.

150. DOE/ID-10278, "Technical Support for the Debris Coolability Requirements for Advanced Light Water Reactors in the Utility/EPRI Light Water Reactor Requirements Document" June, 1990.

151. Bjornsson, H., et. al., "Penetration of Water into Hot Rock Boundary of Magna at Grimsvoth", Nature, Vol. 295, February 18, 1982.

152. "Core Concrete Interactions with Overlying Water Pools," E. Copus, 19th Annual WRSM, October, 1991.

This reference intentionally blank.

153. Letter, S. Additon, (Tenera) to S. Sorrell (DOE), "Subject: Initial Report of MACE Ib", April 14, 1992.

154. DOE/ID 10298,"Licensing Design Basis Source Term Update for the Evolutionary Advanced Light Water Reactor," September, 1990.

155. FAI/91-13, "MAAP 3.0B PWR Revision 17: Transmittal Documentation", Fauske and Associates, Inc., January, 1991.

156. NUREG/CR-4551 (SAND86-1309), Vol 3, Rev 1, Part 1,"Evaluation of Severe Accident Risks: Surry Unit 1: Main Report", Sandia National Laboratory, October, 1990.

157. Greene, G.A., et. al., "Experimental Studies on Melt Spreading, Bubbling Heat Transfer and Coolant Layer Boiling", 16-th Water Reactor Safety Meeting, Gaithersburg, Md, October 24-27, 1988.

158. NUREG/CR-3916,"Pressurized Melt Ejection Into Water Pools", Tarbell, W.W., et. al., Sandia National Labcratory, March, 1991.

159. Alsmeyer, H., et. al.,"Beta Experimental Results on Melt/Concrete Interaction: Silicate Concrete Behavior," Proceeding of the Committee on the Safety of Nuclear Installations (CSNI) Specialists' Meeting on Core-Debris-Concrete Interactions, September 3-5, 1986.

160. Alsymeyer, H., et. al.,"Beta Experimental Results on Melt/Concrete Interaction: Limestone Concrete Behavior," Proceeding of the Committee on the Safety of Nuclear Installations (CSNI) Specialist's Meeting on Core Debris-Concrete Interactions," September 3-5, 1986.

161. "Final Safety Evaluation Report for Utility Requirements Document", USNRC, May, 1992 (Draft).

162. NUREG/CR-3468 (SAND84-0383), "Hydrogen: Air: Steam Flammability Limits Combustion Characteristics in the FITS Vessel", Marshall, B. W., 1986.

163. NUREG/CR-4551, Vol 5,Rev 1, Part 1, "Evaluation of Severe Accident Risks and the Potential for Risk Reduction: Sequoyah Power Station, Unit 1: Main Report", Sandia National Laboratory, December, 1990.

164. NUREG/CR-4691, Vol. 1; "MELCOR Accident Consequence Code System (MACCS) - User's Guide"; Sandia National Laboratories; February, 1990.

165. NUREG/CR-4691, Vol. 2; "MELCOR Accident Consequence Code System (MACCS) - Model Description"; Sandia National Laboratories; February, 1990.

166. NUREG/CR-4691, Vol. 3; "MELCOR Accident Consequence Code System (MACCS) - Programmer's Reference Manual"; Sandia National Laboratories; February, 1990.

167. NUREG/CR-4551, Vol. 2, Rev. 1, Part 7; "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters - MACCS Input", Sandia National Laboratories; December, 1990.

168. NUREG-1465; "Accident Source Terms for Light-Water Nuclear Power Plants"; Draft Report for Comment; U.S. Nuclear Regulatory Commission.

169. WCAP-13389 (Non Proprietary Version),"AP600 Phenomenological Evaluation Summaries", June 1992.

170. Cole, R. H., Underwater Explosions, Princeton University Press, Princeton, New Jersey, 1948.

This reference intentionally blank.

171. Moody, F., Muralidaran, R., Dua, S.S., "Assessment of Ex-Vessel Steam Pressure Spikes in BWR MARK II Containments", 19 th Water Reactor Safety Meeting, October, 1991.

172. NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States", Draft Report dated February, 1992.

173. PLG-0602, Analysis of Fire Frequency During Shutdown, March 1988, prepared as part of the Seabrook Probabilistic Safety Study Shutdown, May 1988.

174. EPRI Proprietary Report TR-100370, Fire-Induced Vulnerability Evaluation Methodology, October, 1992.

175. NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management."

176. EPRI NP-6041-SL, Revision 1; A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1); August, 1991.

177. EPRI NP-5223; Generic Seismic Ruggedness of Power Plant Equipment; ANCO Engineers, Inc.; for the Electric Power Research Institute, May, 1987.

178. Campbell, A. S., "Thermodynamic Analysis of Combustion Engines", John Wiley & Sons, Inc., 1979.

179. NUREG/CR-5809, "An Integrated Structure and Scaling Methodology for Severe Accident Technical Issue Resolution (DRAFT for Comment), Technical Program Group, USNRC, Nov. 1991.

180. NUREG-1150, "Severe Accident Risks: An Assessment for Five US Nuclear Power Plants", December, 1990.

181. NUREG/CP-0125, "The Probability of Containment Failure by Direct Containment Heating", M. Pilch et. al., October, 1992.

182. NUREG-1150, Vol 2., "Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Appendices A, B and C", USNRC, December 1990.

183. NUREG-4551, Volume 2:, Evaluation of Severe Accident Risks:, Quantification of Major Input Parameters: Expert Elicitation on In-Vessel Issues",

184. Rempe, J, et. al., "Light Water Reactor Lower Head Failure Analysis (DRAFT)", NUREG/CR-5642, EGG-2618, December, 1991.

This reference intentionally blank.

197. NUREG/CR-5901, "A Simplified Model of Aerosol Scrubbing by a Water Pool Overlying Core Debris Interacting With Concrete", Powers, D.A., Sprung, J.L., October, 1992.

198. NUREG/CR-5747, "Estimate of Radionuclide Release Characteristics Into Containment Under Severe Accident Conditions", Nourbakhsh, H.P., January, 1992.

199. "Natural Removal of Containment Fission Product Aerosols", Li, J., Leaver, D., Sher, R., paper presented at PSA'93, Tampa, Fla., January, 1993.

200. NUREG/CR-4551, Vol. 6, Rev.1, Part 2, "Evaluation of Severe Accident Risks; Grand Gulf Unit 1: Appendices", Brown, T. D., et. al., December, 1990.

201. NUREG/CR-5843, SAND92-0167, "CORCON MOD3: An Integrated Computer Model for Analysis of Molten Core-Concrete Interactions (Draft)", Bradley, D.R., Gardner, D.R., October, 1992.

202. DOE/ID-13177-2, "Low Volatile Fission Product Release During Reactor Accidents", Osetek, D. J., October, 1992.

203. MAAP 3.0B User's Manual, FAI, March, 1990.

204. C.C. Chu and J.J. Sienicki, "MELTSPREAD-1 Calculations of the Transient Spreading of Core Materials in the Ap600 and SBWR Containments," ANL/RE/LWR 91-3, Argonne National Laboratory, Reactor Engineering Division (November 1991).

205. "Extreme Loading of Inner Structures of the Next Generation PWR-Containments," Kreig, R., et.al., 5th International Workshop on Containment Integrity, June 1992.

206. "A Generic Approach for Containment Success Criteria Under Severe Accident Loads," Sammataro, R., et.al. 5th International Workshop on Containment Integrity, June, 1992.

207. ANSYS Engineering Analysis System User's Manual, G. J. DeSalvo, and J. A. Swanson, Swanson Analysis Systems, Inc.

208. Regulatory Guide 1.92, "Combining Modal Responses and Spatial Components in Seismic Response Analysis".

209. Regulatory Guide 1.61, "Damping Values for Seismic Design of Nuclear Plants".

This reference intentionally blank.

210. "AP600 Containment Design for Severe Accidents," Orr, et al., paper presented at Fourth Symposium of Current Issues Related to Nuclear Power Plant Structures, Equipment and Piping, Raleigh, North Carolina, December, 1992.

211. "Performance of Containment Penetrations Under Severe Accident Loadings", M. B. Parks and D. B. Clauss, Sandia National Laboratories.

212. "Initial Report of MACE Test M1B", Memo, S. Additon (TENERA) to S. Sorrell (DOE-Idaho), April 14, 1992.

213. NUREG/CR-2462, "Capacity of Nuclear Power Plant Structures to Resist Blast Loadings", R.G. Kennedy, et. al, September, 1983.

214. FSP-93-005, "Parameter List for System 80+ at 103% Power", January 15, 1993 ABB-Combustion Engineering (Proprietary).

215. "Recommended Sensitivity Analyses for an Individual Plant Examination Using MAAP3.0B", Gabor, Kenton & Associates, March 1991 (Draft).

216. S. Sorrell (DOE) to C. Buchholz (GE), Subject: FAI Trip Report for the NRC DCH Test Program Peer Review Meeting", RTD-344-92.

217. NSAC/60, "Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3", NSAC, June, 1984.

218. NUREG/CR-0098; "Development of Criteria for Seismic Review of Selected Nuclear Power Plants"; Newmark, N. M., Hall, W. J.; May, 1978.

219. Summitt, R. L.; "Combustion Turbine Generator Seismic Evaluation Guidance WBS 4.1"; Prepared for USDOE under Contract No. DE-AC07-921D13175 by SAROS, Inc.; September, 1992.

220. NUREG/CR-3862, "Development of Transient Initiating Event Frequencies For use in Probabilistic Risk Assessments"; Mackowiak, D.P., Gentillon, C.D.; EG&G Idaho, May, 1985.

221. NUREG/CR-5691, "Instrumentation Availability for a Pressurized Water Reactor with a Larger Dry Containment During Severe Accidents," Arcieri, W.C., et. al., March, 1991.

222. HGN-112-ND, Generic Safety Evaluation Report Relating to Mark III Containment Hydrogen Control, USNRC, September 1990, Transmitters via Letter from A. Thadani (USNRC) to Langley, J.R., (HCOG), July 27, 1990.

This reference intentionally blank.

223. HGN-098-NP, "Evaluation of Scoping Test Results," Langley, J.R. (HCOG) to USNRC, November, 1990.

224. NUREG-1417. "Safety Evaluation Report: related to Hydrogen Control Owner's Group Assessment of Mark III Containments," USNRC, October, 1990.

225. NUREG-0022, "Safety Evaluation Report: McGuire Nuclear Power Plant; Supplement 7," May, 1983.

226. "Resolution of Equipment Survivability Issues for the Seqouyah Nuclear Power Plant," dated May, 19, 1981.

227. NUREG/CR-5982, BNL-NUREG-2354, "Effectiveness of Containments Sprays in Containment Management," Nourbakhsh, H.P., et.al., May, 1993.

228. NUREG/CR-5096, "Evaluation of Seals for Mechanical Penetrations of Containment Buildings", Graves, G. H., et al., 1988.

229. NUREG/CR-5334, "Severe Accident Testing of Electrical Penetration Assemblies", Clauss, D. B., November, 1989.

230. "Performance of Containment Penetrations Under Severe Accident Loadings", Parks, M. B., Clauss, D. B., Water Reactor Safety Meeting, October, 1990.

231. EPRI-NP-4354, "Large-Scale Hydrogen Burn Equipment Experiment," Achenbach, J.A., December 1985.

232. NUREG/CR-4763, "Safety Related Equipment Survival in Hydrogen Burns in Large, Dry PWR Containment Building," Sandia National Laboratories, 1988.

233. NUREG-1267, "Technical Resolution of Generic Safety Issue A-29 Nuclear Power Plant Design for Reduction of Vulnerability to Industrial Sabotage," U. S. Nuclear Regulatory Commission, September 1989.

234. NSAC-84, "Zion Nuclear Plant Residual Heat Removal PRA," Nuclear Safety Analysis Center, EPRI/NSAC, July 1985.

235. NUREG/CR-5015, "Improved Reliability of Residual Heat Removal Capability in PWR as Related to Resolution of Generic Issue 99," prepared for U. S. Nuclear Regulatory Commission by Brookhaven National Laboratory, May 1988.

236. Generic Letter 88-17, "Loss of Decay Heat Removal," U. S. Nuclear Regulatory Commission, October 17, 1988.

This reference intentionally blank.

237. NUREG/CR-5820, "Consequences of Loss of the RHR System in Pressurized Water Reactors," prepared for U. S. Nuclear Regulatory Commission by Idaho National Engineering Laboratory, May 1992.

238. ORACLE Relational Database Management System, Version 6.0.36, Oracle Corporation, 1992.

239. Berman, M., Sherman, M., "The Possibility of Local Detonations During Degraded Core Accidents in Bellefonte Nuclear Power Plant," Nuclear Technology, Vol. 81, p. 63, April 1990.

240. NUREG/CR-5360, "XSOR Codes Users Manual," prepared for U. S. Nuclear Regulatory Commission by Hong-Nian Jow, Murfin, W. B., Johnson, J. D., November 1993.

This reference intentionally blank.