

GE-Hitachi Nuclear Energy Americas LLC

James C. Kinsey
Project Manager, ESBWR Licensing

PO Box 780 M/C A-55
Wilmington, NC 28402-0780
USA

T 910 675 5057
F 910 362 5057
jim.kinsey@ge.com

MFN 07-463

Docket No. 52-010

August 30, 2007

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: **Response to Portion of NRC Request for Additional Information
Letter No. 77 Related to ESBWR Design Certification Application
– Safety Analyses – RAI Number 15.0-18**

Enclosure 1 contains GE-Hitachi Nuclear Energy Americas (GEH) response to the subject NRC RAI transmitted via Reference 1. Enclosure 2 contains the DCD Markups associated with this response.

If you have any questions or require additional information regarding the information provided here, please contact me.

Sincerely,



James C. Kinsey
Project Manager, ESBWR Licensing



Reference:

1. MFN 06-391 – Letter from US Nuclear Regulatory Commission (NRC) to David H. Hinds, *Request for Additional Information Letter No. 77 Related to ESBWR Design Certification Application*, dated October 11, 2006

Enclosures:

1. Response to NRC Request for Additional Information Letter No. 77 Related to ESBWR Design Certification Application – Safety Analyses, RAI Number 15.0-18
2. DCD Markups

cc: AE Cabbage USNRC (with enclosures)
GB Stramback GEH /San Jose (with enclosures)
RE Brown GEH /Wilmington (with enclosures)
eDRF 0072-1523

MFN 07-463

Enclosure 1

**Response to NRC Request for
Additional Information Letter No. 77
Related to ESBWR Design Certification Application**

Safety Analyses

RAI Number 15.0-18

NRC RAI 15.0-18:

Verification of key assumptions, such as the reliability of I&C systems.

Full Text: DCD Tier 2 Appendix 15A provides an analysis to determine the frequency of occurrence of events classified as infrequent events. Section 15A.4 lists four "analysis assumptions" that are to be confirmed by the COL applicant:

(1) The feedwater control system (FWCS) is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the Feedwater System Controller be higher than 1000 years. Compliance to this requirement should be established through a reliability analysis by the vendor for the controller.

(2) The steam bypass and pressure control (SB&PC) system is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller be higher than 1000 years. Compliance to this requirement should be established through a reliability analysis by the vendor for the controller.

(3) The reactor water cleanup (RWCU)/shutdown cooling (SDC) system shall be designed with an interlock that prevents accidental engagement of the system in shutdown cooling mode when the reactor is in operation. The interlock feature shall be designed to be single-failure proof.

(4) No single failure in the nitrogen system can lead to an Inadvertent Opening of a Safety/Relief Valve.

(A) It is anticipated that the COL applicant would not be able to submit a reliability analysis of this equipment since it would not yet be procured. Explain the rationale for requiring that the COL applicant confirm the reliability of equipment rather than performing bounding assessments of the event frequencies, based on high level design features and principles.

(B) Since the event frequencies provided in Appendix 15A form the basis for the categorization of events as "infrequent events" rather than anticipated operational occurrences, these key design features and principles should be included in Tier 1 design descriptions and ITAAC should be provided to verify them.

(C) Add a COL information item to include the FWCS and the SB&PC in the design reliability assurance program (D-RAP) to ensure that the COL holder will evaluate the reliability of these components and determine if the equipment is acceptable or if it must be redesigned to achieve a lower failure rate.

GEH Response:

GEH has removed the four referenced analysis assumptions to be confirmed by the COL Applicant from DCD Tier 2 Appendix 15A. These analysis assumptions have been relocated in other DCD Subsections and will be confirmed during the design certification process:

- (1) The feedwater control system (FWCS) is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the Feedwater System Controller be higher than 1000 years. Compliance to this requirement is established through a reliability analysis by the vendor for the controller.

These requirements are transferred to Subsection 7.7.3.

- (2) The steam bypass and pressure control (SB&PC) system is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the SB & PC Controller be higher than 1000 years. Compliance to this requirement is established through a reliability analysis by the vendor for the controller.

These requirements are transferred to Subsection 7.7.5.

- (3) The reactor water cleanup (RWCU)/shutdown cooling (SDC) system is designed with an interlock that prevents accidental engagement of the system in shutdown cooling mode when the reactor is in operation. The interlock feature is designed to be single-failure proof.

These requirements are transferred to Subsection 5.4.8 and 7.4.3

- (4) No single failure in the nitrogen system can lead to an Inadvertent Opening of a Safety/Relief Valve.

These requirements are transferred to Subsection 9.3.8.

The actual reliability of the SB&PC controller is expected to be much better than the specified minimum MTTF requirement of 1,000 years. Assuming either failure mode is equally possible, the frequency of controller failing in a manner to cause minimum demand is once in 2,000 years. The failure mode and frequency are discussed in Sections 15A.3.2 and 15A.3.5. Therefore the design requirement is bounding.

It is not necessary to include these design features and principles in the Tier 1 Design Description and ITAAC since the requirement does not meet any of the Tier 1 inclusion criteria defined in DCD Subsection 14.3.7.

It is not necessary to require the COL Holder to evaluate the reliability of the FWCS and SB & PC Controllers since the requirement for the MTTF is now a design requirement.

DCD Impact:

- DCD Tier 2, Subsections 5.4.8, 7.4.3, 7.7.3, 7.7.5, 9.3.8, 15A.4 and affected subsections are revised as noted on the attached markups and will be provided in Revision 5.

Enclosure 2

MFN 07-463

DCD Markups

- Purify the reactor coolant during normal operation and shutdown;
- Supplement reactor cooling when the reactor is at high pressure in the hot standby mode;
- Assist in the control of reactor water level during startup, shutdown, and in the hot standby mode;
- Induce reactor coolant flow from the reactor vessel bottom head to reduce thermal stratification during startup;
- Provide shutdown cooling and cooldown to cold shutdown conditions; and
- Provide heated primary coolant for RPV hydrostatic testing and reactor startup.

The RWCU/SDC system is discussed in further detail in Subsections 5.4.8.1 and 5.4.8.2.

5.4.8.1 Reactor Water Cleanup Function

The reactor water cleanup function is performed by the RWCU/SDC system during startup, normal power generation, cooldown and shutdown.

5.4.8.1.1 Design Bases

Safety Design Bases

The RWCU/SDC system does not perform any safety-related functions. Therefore, the RWCU/SDC system has no safety design bases other than for safety-related containment penetrations and isolation valves, as described in Subsection 6.2.4, and provide instrumentation to detect system pipe break outside the containment as described in Subsection 7.4.3

Power Generation Design Bases

The RWCU/SDC system is designed to:

- Remove solid and dissolved impurities from the reactor coolant and measure the reactor water conductivity during all modes of reactor operation. This is done in accordance with Regulatory Guide 1.56, "Maintenance of Water Purity in Boiling Water Reactors";
- Discharge excess reactor water during startup, shutdown, and hot standby conditions and during refueling to the main condenser or to the radwaste system;
- Minimize Reactor Pressure Vessel (RPV) temperature gradients by enhancing circulation through the bottom head region of the RPV and to reduce core thermal stratification at low power;
- Provide heated primary coolant for RPV hydrostatic tests and reactor startup; and

- Have redundant cleanup capacity with respect to major system components.

The RWCU/SDC Shutdown Cooling function modes are interlocked with Reactor Power operation to prevent increases in reactivity. During reactor Power operation, the operator cannot start or select the RWCU/SDC Shutdown Cooling function modes. This interlock feature is designed to be single failure proof. Interlocks are also provided to prevent inadvertent operation of pumps at higher speed and higher flow during Reactor Power operation. An alarm is initiated if flow is higher than normal and the reactor is at power.

function and providing instrumentation for detection of system breaks outside the containment (IEEE Std. 603, Sections 4.1 and 4.2). The containment is isolated by signals from the LD&IS as described in Subsection 7.3.3 and the water purification equipment of the RWCU/SDC system is also isolated by signals from LD&IS received from the Standby Liquid Control (SLC) system.

7.4.3.1.3 Power Generation Design Bases

The RWCU/SDC system instrumentation shall be designed to provide suitable process indication, alarms, and manual and automatic devices for controlling the system as it:

- Removes impurities;
- Limits excess reactor water level during reactor heatup, startup, shutdown cooling and hot standby modes of plant operation;
- Minimizes reactor temperature gradients;
- Heats the reactor pressure vessel (RPV) for hydrostatic tests; and
- Removes reactor core decay heat during normal plant shutdowns.

The RWCU/SDC shutdown cooling function modes are interlocked with reactor power operation to prevent increases in reactivity. During reactor power operation, the operator cannot start or select the RWCU/SDC shutdown cooling function modes. This interlock feature is designed to be single failure proof. Interlocks are also provided to prevent inadvertent operation of pumps at higher speed and higher flow, and opening of regenerative heat exchanger (RHX) bypass valves during reactor power operation. An alarm is initiated if flow is higher than normal and the Reactor is at power.

7.4.3.2 System Description

7.4.3.2.1 Summary Description

The RWCU/SDC system performs essentially three basic plant functions. It provides a continuous purifying treatment of the reactor water during startup, normal operation, cooldown, hot standby, and shutdown modes of plant operation. It also removes core decay heat in conjunction with the main condenser or the isolation condensers during plant shutdown modes. Thirdly, the system (with the feedwater system) provides reactor vessel heat-up during cold start-up. There are two redundant RWCU/SDC trains. The overall functional description of the RWCU/SDC system is contained in Subsection 5.4.8. The instrumentation maintains the RWCU/SDC system process conditions within the limits necessary to control the system and satisfy the design bases. Protective features include isolating the RWCU/SDC system from the RPV with a LD&IS signal present. The above isolation features protect the reactor core by

7.7.3.1.2 Power Generation (Non-safety) Design Bases

The FWCS is designed so that the functional capabilities of safety-related systems are not inhibited (IEEE Std. 603, Section 5.6.3). The FWCS regulates the flow of feedwater into the RPV to maintain predetermined water level limits during transients and normal plant operating modes. The desired range of water level during normal power operation is based on steam separator performance. The requirements include limiting carryover, which can affect turbine performance, and limiting carryunder, which can affect overall plant efficiency.

If the RPV water rises to Level 8, then equipment protective action will trip the main turbine and reduce feedwater demand to zero. The feedwater pumps will trip if the water continues to rise to Level 9. If the water falls to Level 3, then the RPS will shut down the reactor. The RPS is a fully independent safety-related system (Subsection 7.2.1). If the water continues to drop and reaches Level 2, the high-pressure make-up function of the CRD system will initiate. The CRD system is fully independent of other plant delivery or injection systems.

7.7.3.2 System Description

7.7.3.2.1 General Description

The FWCS is a power generation (control) system that maintains proper RPV water level in the operating range from high (Level 9) to low (Level 2). During normal operation, feedwater flow is delivered to the RPV through three Reactor Feed Pumps (RFPs) which operate in parallel. Each RFP is driven by an adjustable-speed induction motor that is controlled by an ASD. In normal operation, the fourth RFP is in standby mode and will start automatically if any operating feedwater pump trips while at power. In abnormal operation, the fourth RFP can be set in manual mode or can be removed from service for maintenance.

The FWCS is implemented on the triple redundant, Fault-Tolerant Digital Controller (FTDC) **including power supplies and input/output signals. The controller is designed for a Mean Time to Failure (MTTF) of no less than 1000 years.** The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. Each FTDC channel executes the control software for the control modes. At the operator's discretion, the system operation mode can be selected from the main control console. The FWCS functional diagram is provided as Figure 7.7-3.

During normal operation the FWCS sends three speed-demand signals, each of which reflects a voted FWCS processor output, to each feed pump ASD. The ASD will perform a mid value vote and use it to control the speed/frequency of the feed pump motor. The mid value vote is also returned to the FWCS as an analog input and compared with the speed demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, a "lock-up" signal is sent to a "lock-up" voter and an alarm is activated in the MCR.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 System Design Bases

7.7.5.1.1 Safety Design Basis

The SB&PC system does not perform or ensure any safety-related function, is classified as a nonsafety-related system, and has no safety-related design basis. In Mode 1, only one of the three triple redundant controllers can be removed from service.

7.7.5.1.2 Power Generation (Non-safety) Design Bases

The SB&PC system is designed so that the functional capabilities of safety-related systems are not inhibited (IEEE Std. 603, Section 5.6.3). The SB&PC system is essential to the power generation cycle because it controls reactor pressure during plant startup, power generation, and shutdown modes of operation.

The design objective is to enable a fast and stable response to pressure and system disturbances, and to pressure setpoint changes over the operating range. This is done using Turbine Control Valves (TCVs) through the TGCS and Turbine Bypass Valves (TBVs) for controlling reactor pressure. In addition, the design objective of the SB&PC is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot use all of the steam generated by the reactor.

7.7.5.2 System Description

7.7.5.2.1 General Description

The purpose of the SB&PC system is to control reactor pressure during plant startup, power generation, and shutdown modes of operation. **The SB&PC System is implemented on the triplicate (FTDC). Power supplies and input/output signals are redundant. The controller is designed for a MTTF of no less than 1000 years.** This **Control of reactor pressure** -is accomplished through control of the TCVs through the TGCS and TBVs, so that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety/relief valve opening is minimized. Triplicated ~~FTDCs~~ using feedback signals from RPV dome pressure sensors, generate command signals for the TBVs and pressure regulation demand signals used by the TGCS to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC system sends the excess steam flow directly to the main condenser through the TBVs.

The ability of the plant to load follow the grid-system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the SB&PC system adjusts the demand signals sent to the TGCS so that the TGCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure.

Controls and valves are designed so that steam flow is shut off when of control system electrical power or hydraulic system pressure is lost.

9.3.7-6 ASME B31.3, Process Piping (see Table 1.9-22)

9.3.8 High Pressure Nitrogen Supply System

9.3.8.1 Design Bases

Safety (10 CFR 50.2) Design Bases

The High Pressure Nitrogen Supply System (HPNSS) does not perform any safety-related function. Therefore, the HPNSS has no safety design basis other than provision for safety-related containment penetrations and isolation valves, as described in Subsection 6.2.4.

Power Generation Design Bases

The HPNSS distributes clean, dry, oil free nitrogen gas to containment nitrogen users from the Containment Inerting System (CIS). Nitrogen loads include the Automatic Depressurization Subsystem (ADS) Safety Relief Valve (SRV) accumulators, the Isolation Condenser (IC) steam and condensate line isolation valve accumulators, the Main Steamline Isolation Valve (MSIV) accumulators, and other pneumatically operated valves.

The HPNSS provides a means for switchover from CIS to nitrogen bottle backup during low CIS supply pressure.

The HPNSS provides a means for manual switchover from the HPNSS supply to the IAS supply to provide an operating gas for HPNSS loads during refueling outages.

No single control or instrumentation failure will prevent the ADS SRV's or IC Isolation Valves (ICIV) from performing their required safety-related function as required. No failure in one branch of the HPNSS prevents the other branch of the HPNSS from performing its function.

No single failure in the High Pressure Nitrogen Supply System nitrogen system can lead to an inadvertent opening of an SRV.

9.3.8.2 System Description

Summary Description

The HPNSS consists of the distribution piping between the CIS and the containment nitrogen users. The HPNSS also provides bottled high-pressure nitrogen gas that is clean, dry and oil free to the NBS ADS SRV accumulators, IC line isolation valves' accumulators, MSIVs, and other nitrogen loads if the CIS fails to maintain the required nitrogen supply pressure.

All containment nitrogen loads are normally supplied by the CIS. The CIS nitrogen supply line branches into two HPNSS distribution lines. One branch line supplies the low-pressure nitrogen loads (i.e., MSIVs, instruments, and pneumatic-operated valves)

15A. EVENT FREQUENCY DETERMINATION

15A.1 SCOPE

This Appendix provides the analysis to determine the frequency of occurrence of events classified as infrequent events in Table 15.0-7. The overall objective of this analysis is to determine the frequency of occurrence for these events, to allow them to be categorized as Anticipated Operational Occurrences or Infrequent Events. Events less frequent than 1 event in 100 years are classified as infrequent events.

15A.2 METHODOLOGY

The methodology used in this evaluation is based on industry established methods given in Probabilistic Risk Assessment (PRA) guidelines described in Reference 15A-1. The following types of analysis were applied in determining the event frequency:

- Where an initiating event is explicitly modeled in the ESBWR PRA, the frequency for this event is taken directly from the PRA. However, for some cases where more detail is required, additional analyses not given in the PRA were conducted. The frequencies of events that were not modeled in the PRA are addressed in this analysis.
- The event frequency is determined from actual BWR operating experience, modified to reflect the ESBWR improved design features. Where the analysis depends on specific assumed design features or testing, these features and tests are identified as ESBWR design requirements. ~~Any cases involving Combined Operating License (COL) Applicant confirmation are identified.~~
- Several events involve multiple independent hardware failures or human errors. For these events, the event frequency is based on conservative estimates of the hardware failures (including common cause failures) and human errors.

To account for any data or modeling uncertainties, the final event frequencies have been reviewed to ensure a factor of 3 times above the criterion for an infrequent event. This factor increase is consistent with current PRA practices dealing with uncertainties.

15A.3 RESULTS

The analysis for each event includes a description of the event, a discussion of the analysis used to determine the event frequency, and a summary of the results. ~~Any case where a COL Applicant confirmation is required is identified in the summary.~~ The following subsections present the analysis results for each event.

15A.3.1 Pressure Regulator Failure – Opening of All Turbine Control and Bypass Valves

15A.3.1.1 Introduction

The Steam Bypass and Pressure Control (SB&PC) System controls the reactor pressure during plant operation. The SB&PC system controllers, which take input from the reactor dome pressure and other operating parameters, regulate the reactor pressure during normal operation by sending control signals to the Turbine Control Valves (TCVs). However, whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC controllers send a signal to the Turbine Bypass Valves (TBVs) to open. While the SB&PC system is designed to a high degree of reliability, multiple failures in the system could lead to a failure of the controller in the upscale position, which would send a demand signal to all the TCVs and TBVs to open. Such an event is identified as the “Pressure Regulator Failure – Opening of All Turbine Control & Bypass Valves” event. The occurrence frequency of this event is evaluated in this subsection.

15A.3.2.2 Analysis

The description of the SB&PC system is provided in Subsection 7.7.5.

The SB&PC system is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. The FTDC is designed to a high degree of reliability. **Based on Subsection 7.7.5, It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller is at least be higher than 1,000 years. This requirement has been identified as a COL Applicant confirmation item in Section 15A.4.**

The actual reliability of the SB&PC controller is expected to be much better than the specified minimum MTTF requirement of 1,000 years. The controller can either fail high causing maximum demand or fail low causing minimum demand. Assuming that either failure mode is equally possible, the frequency of controller failing in a manner to cause maximum demand is estimated to be once in 2,000 years.

15A.3.2.3 Result

The frequency of pressure regulator failure – opening of all turbine control and bypass valves, is once in 2,000 years and therefore, the event frequency meets the criterion of being less than once in 100 years.

15A.3.2 Pressure Regulator Failure – Closure of All Turbine Control and Bypass Valves

15A.3.2.1 Introduction

The Steam Bypass and Pressure Control (SB&PC) System controls the reactor pressure during plant operation. The SB&PC system controllers, which take input from the reactor dome pressure and other operating parameters, regulate the reactor pressure during normal operation by sending control signals to the Turbine Control Valves (TCVs). However, whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC controllers send a signal to the Turbine Bypass Valves (TBVs) to open. While the SB&PC system is designed to a high degree of reliability, multiple failures in the system could lead to a failure of the controller in the downscale position, which would send a demand signal to all the TCVs and TBVs to close. Should this occur, it would cause full closure of all TCVs as well as closure of any bypass valves that are open. Such an event is identified as the “Pressure Regulator Failure – Closure of All Turbine Control and Bypass Valves” event. The occurrence frequency of this event is evaluated in this subsection.

15A.3.2.2 Analysis

The description of the SB&PC system is provided in Subsection 7.7.5.

The SB&PC system is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. The FTDC is designed to a high degree of reliability. **Based on Subsection 7.7.5, It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller is at least be higher than 1,000 years. This requirement has been identified as a COL Applicant confirmation item in Section 15A.4.**

The actual reliability of the SB&PC controller is expected to be much better than the specified minimum MTTF requirement of 1,000 years. The controller can either fail high causing maximum demand, or fail low causing minimum demand. Assuming either failure mode is equally possible, the frequency of controller failing in a manner to cause minimum demand is once in 2,000 years.

15A.3.2.3 Result

The frequency of pressure regulator downscale failure – closing of all turbine control and bypass valves is once in 2,000 years, and therefore, the pressure regulator failure (maximum demand) event frequency meets the criterion of being less than once in 100 years.

15A.3.5 Feedwater Controller Failure - Maximum Demand

15A.3.5.1 Introduction

The Feedwater Control System (FWCS) is a power generation system, which is designed to maintain proper water level in the reactor during operation. The event of concern is one that results from one or more failures in the FWCS that causes multiple FW pumps to go to maximum output. This results in the feedwater pumps delivering a large amount of water, which increases the reactor water level to Level 8, at which time the feedwater pumps are tripped by an independent system, the main turbine is tripped and a reactor scram is initiated. Such an event is called the “Feedwater Controller Failure – Maximum Demand” event. The frequency of this event is evaluated in this subsection.

15A.3.5.2 Analysis

The description of the FWCS is provided in Subsection 7.7.3.

The FWCS is designed to maintain proper reactor pressure vessel water level in the operating range from high water level (Level 9) to low water level (Level 2). During normal operation, feedwater flow is delivered to the reactor vessel through three Reactor Feedpumps (RFPs), which operate in parallel. Each RFP is driven by an induction motor that is controlled by an adjustable speed drive (ASD). The fourth RFP is in standby mode and auto-starts if any operating feedpump trips while at power.

The FWCS is equipped with a triple-redundant, fault-tolerant digital controller (FTDC) including power supplies, and input/output signals. The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. The FTDC is designed to a high degree of reliability. **Based on Subsection 7.7.3, It is required that the Mean Time to Failure (MTTF) of the Feedwater System Controller is at least be higher than 1,000 years. This requirement has been identified as a COL Applicant confirmation item in Section 15A.4.**

The actual reliability of the Feedwater controller is expected to be much higher than the specified minimum MTTF requirement of 1,000 years. It is assumed that the feedwater controller can fail high or fail low with equal probability. If any one of the three controllers fails either high causing maximum demand (or fails low causing minimum demand), the other two controllers would continue to function and the frequency of two or three controllers failing in a manner to cause maximum demand is once in 2,000 years.

15A.3.5.3 Result

The frequency of the feedwater controller failing in a manner to cause maximum demand of feedwater is less than once in 2,000 years and therefore, the event frequency meets the criterion of being less than once in 100 years.

15A.3.7 Inadvertent Shutdown Cooling Function Operation

15A.3.7.1 Introduction

The ESBWR is equipped with the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system, which is designed to perform Shutdown Cooling in one of its operating mode. The operator initiates shutdown-cooling mode of operation after the plant is shutdown, either normally, or after a reactor scram. It should not be possible for the operator to initiate shutdown-cooling mode of operation when the reactor is at power. However, combination of undetected failures and operator errors could lead to inadvertent shutdown. The frequency inadvertent shutdown cooling operation is estimated in this subsection. The RWCU/SDC system is described in Subsection 7.4.3.

15A.3.7.2 Analysis

The RWCU/SDC system design information are not available in sufficient detail to describe the interlock feature in the design that prevents the operator from inadvertently engaging the system in the SDC mode of operation. **Based on Subsection 7.4.3, This ~~this~~ interlock feature is designed to be single-failure proof. This requirement is identified as a COL Applicant confirmation item in Section 15A.4.** The operator is not likely to engage the RWCU/SDC system in the SDC mode when the plant is in operation. However, if the interlock does not work for some reason, and the operator commits this error, then there is a potential for the RWCU system to be placed in the inadvertent SDC mode.

The frequency that the single-failure-proof interlock is in a failed state is very low. For this analysis, it is estimated to be 1.0E-3 per year. The probability that the operator would make a mistake and try to initiate RWCU system in the SDC mode is estimated to be 1.0E-3. The combined frequency of successful inadvertent SDC mode of operation is estimated to be 1.0E-3 times 1.0E-3 = 1.0E-6 per year.

15A.3.7.3 Result

The frequency of the inadvertent SDC function operation is estimated to be 1.0E-6 per year. The event frequency is one in a million years, and therefore, the event frequency meets the criterion of being less than once in 100 years.

The inadvertent opening of the SRVs is termed an “Inadvertent opening of a Relief Valve” or IORV event. The IORV event frequency is estimated in this subsection.

15A.3.8.2 Analysis

There are five ways in which an SRV can open inadvertently:

- (1) Incorrect setpoint or spring adjustments
- (2) Excess nitrogen pressure
- (3) Spring relaxation
- (4) Spurious opening signal
- (5) Operator error

Each of these modes is discussed in more detail below:

Incorrect Setting: Incorrect (low) setpoint setting or improperly locked setpoint spring, allowing the spring adjustments to back off with vibration can potentially lead to an inadvertent opening. This calibration action, as well as the maintenance action, are very important actions that are performed with a lot of care and are checked and verified before the valve is put in service. The failure of undetected operator actions leading to an incorrect setting or spring adjustments is estimated to be negligible.

Excess Nitrogen Pressure: Excess nitrogen pressure could result in inadvertent valve opening. ~~Based on subsection 9.3.8, The design requirement specified as a COL Applicant confirmation item in Section 15A.4 is that no single failure in the nitrogen~~ system can lead to an IORV event.

Failure of control valves that can lead to this condition is estimated based on the failure rate of 1.0E-6 per hour for the air-operated valve to spuriously transfer to de-energized position, from Table A2-1 of Reference 15A-1. The failure frequency of one valve during one year of operation is estimated by multiplying the failure rate by 8760 hours, which yields a frequency of 0.086 per year. The failure of the second valve when the first one is being repaired can lead to nitrogen overpressure. Assuming a repair time of one week, 168 hours, for the first valve, the frequency of two valve failure = $(0.086)(1.0E-6)(168) = 1.448E-6$ per year, rounded to 1.5E-6 per year.

15A.3.16.2 Analysis

To date there has not been a direct release of the contents of a waste gas decay tank or other direct release to the environment. The total U.S. reactor experience (1969–1997) is 1,392 PWR calendar years and 710 BWR calendar years as reported in NUREG/CR-5750 (Reference 15A-6). Given that there have been no events of this type in 2,102 calendar years reported in NUREG/CR-5750, the frequency of occurrence based on 0 failures and 2,102 calendar years is 1 event in 3,033 years at the 50% confidence level.

15A.3.16.3 Results

The probability of occurrence of an uncontrolled direct release of liquid waste to the environment is calculated to be 1 event in 3,033 years. Thus the event frequency meets the criterion of being less than once in 100 years.

15A.4 SUMMARY

The frequency of occurrence for each the events classified as infrequent events in Table 15.0-7 has been analyzed. Each event has been shown to have frequency of occurrence less than once in 100 years and therefore is classified as an infrequent event. A summary of the event frequency estimates is shown in Table 15A-3.

~~The following analysis assumptions are to be confirmed by the COL Applicant:~~

- ~~□ The FWCS is equipped with a triple redundant, fault tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the Feedwater System Controller be higher than 1000 years. Compliance to this requirement should be established through a reliability analysis by the vendor for the controller.~~
- ~~□ The SB&PC system is equipped with a triple redundant, fault tolerant digital controller (FTDC) including power supplies, and input/output signals. It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller be higher than 1000 years. Compliance to this requirement should be established through a reliability analysis by the vendor for the controller.~~
- ~~□ The RWCU/SDC system shall be designed with an interlock that prevents accidental engagement of the system in shutdown cooling mode when the reactor is in operation. The interlock feature shall be designed to be single failure proof.~~
- ~~□ No single failure in the nitrogen system can lead to an Inadvertent Opening of a Safety Relief Valve.~~

15.A.4.1 COL Information

None