



GE Energy

James C. Kinsey  
Project Manager, ESBWR Licensing

PO Box 780 M/C J-70  
Wilmington, NC 28402-0780  
USA

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

MFN 07-221

Docket No. 52-010

May 5, 2007

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

**Subject: Response to Portion of NRC Request for Additional Information Letters, Nos. 77 and 90 – Safety Analysis – RAI Numbers 15.0-20 through 15.0-23, 15.0-25 and 15.4-21**

Enclosure 1 contains GE's response to the subject NRC RAIs transmitted via the Reference 1 and 2 letters.

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

Sincerely,

*Kathy Sedney for*

James C. Kinsey  
Project Manager, ESBWR Licensing

*DD68*

Reference:

1. MFN 06-377, Letter from U.S. Nuclear Regulatory Commission to David Hinds, *Request for Additional Information Letter No. 77 Related to the ESBWR Design Certification Application*, October 11, 2006
2. MFN 07-084, Letter from U.S. Nuclear Regulatory Commission to David Hinds, *Request for Additional Information Letter No. 90 Related to the ESBWR Design Certification Application*, January 28, 2007

Enclosures:

1. MFN 07-221– Response to Portion of NRC Request for Additional Information Letters, Nos. 77 and 90 – Safety Analysis – RAI Numbers 15.0-20 through 15.0-23, 15.0-25 and 15.4-21
2. MFN 07-221– Response to Portion of NRC Request for Additional Information Letters, Nos. 77 and 90 – Safety Analysis – RAI Numbers 15.0-20 through 15.0-23, 15.0-25 and 15.4-21 – DCD Markups

cc: AE Cabbage USNRC (with enclosures)  
GB Stramback GE/San Jose (with enclosures)  
RE Brown GE/Wilmington (with enclosures)  
eDRF 0064-5127 for RAI 15.0-20  
0064-5128 for RAI 15.0-21  
0064-5129 for RAI 15.0-22  
0064-5131 for RAI 15.0-23  
0064-5132 for RAI 15.0-25  
0067-7071 for RAI 15.4-21

**Enclosure 1**

**MFN 07-221**

**Response to Portion of NRC Request for  
Additional Information Letter No. 90  
Related to ESBWR Design Certification Application**

**Safety Analysis**

**NRC RAIs 15.0-20 through 15.0-23, 15.0-25 and 15.4-21**

**NRC RAI 15.0-20:**

*Please provide additional information to justify and/or clarify assumptions and statements made in DCD Tier 2, Revision 1, Sections 15A.3.3 and 15A3.4:*

*(A) A simplified process flow diagram of the Turbine Bypass System and associated fault tree that models the failure of seven or more of the 12 available Turbine Bypass Valves (TBVs) on demand. This information should be readily available since it is part of the information needed to respond to RAI 19.1.0-55 of the PRA (basic event N21-SYS-FF-BYPASS). Please include discussion of assumptions made about the failure of TBVs and support systems (e.g., AC power, I&C, compressed air, and individual valve accumulators).*

*(B) It is stated (DCD Tier 2, Revision1, page 15A-4) that "In the absence of specific data, the failure rates for the TBVs are estimated to be 6.0E-3 per demand, based on the failure for the safety/relief valves..." The staff believes that the probability that a TBV fails when demanded to open depends on its failure mode and testing frequency. For example, if a TBV is considered to be an air-operated valve (AOV) that can fail to operate to other than the deenergized position, the failure rate of 3E-6/hour should be used in conjunction with an exposure time of 24 months. This would result in a failure probability on demand of 2.63E-2, which is significantly higher than the assumed probability of 6E-3. Please discuss.*

*(C) It is stated (DCD Tier 2, Revision1, page 15A-4) that "The common cause failure probability of seven valves is estimated by multiplying the individual TBV failure by a beta factor of 0.02. The value of 0.02 is judged to be a conservative value, especially since each valve is equipped with its own accumulator." However, the data used to estimate common cause failure (CCF) multipliers do not include support system failures, such as compressed air. Therefore, the assumed beta factor may not be conservative. Actually, the value of the CCF multiplier for four or more AOVs reported in the ALWR Utility Requirement Document (Reference 15A-1 of the DCD) is close to 10 percent. Please discuss.*

*(D) It is stated (DCD Tier 2, Revision1, page 15A-4) that "The only relevant support system is the AC power and loss of AC power results in a different category of initiating event. Therefore, the failure of AC power is not considered...." The staff believes that all failures that cause turbine bypass failure should be included in the assessed frequency (with the exception of loss of condenser, which is an analyzed event which includes and bounds the event considered in this analysis). Please discuss.*

*(E) Please clarify the statement regarding the existence of groups of 3 or 6 TBVs that are actuated by hydraulic fluid from the main hydraulic lines separated by check valves. How is this design feature modeled for the purpose of assessing the probability of turbine bypass failure? Also, please clarify the statement that "...the accumulator in each of the TBVs is designed with sufficient capacity to open at least six times."*

*(F) Please clarify whether the design of the TBVs is finalized and list any requirements for ensuring the availability of individual accumulators for the TBVs with the capabilities assumed in this analysis.*

*(G) The frequency of Loss of Preferred Power (DCD Tier 2, Revision1, Section 15A.3.4) was assumed to be 4.6E-2 per year (PRA value). However, since the frequency of Loss of Preferred Power is site-specific, the assumed value may not be a bounding value which envelopes all potential sites. Please discuss.*

**GE Response:**

**Summary of Items 15.0-20 (A) through (G)**

The justification for the frequency of two events is provided:

**Turbine Trip with Total Bypass Failure (Section 15A.3.3)**

This frequency is composed of two contributors:

Turbine Trip Frequency = 1.3/yr (conservative estimate)

Total Bypass Failure = 4.4E-04 (see Item (A))

The calculated TBV failure probability (4.4E-04/demand) is higher than that assumed in the DCD (1.2E-04/demand) to account for support systems and combinations of other failures.

The DCD will be updated to reflect this latest evaluation of the TBV failure probability. Frequency = 1.3/yr \* 4.4E-04 = 5.7E-04/yr

This calculated frequency is higher than the original frequency estimate of 1.56E-04/yr; however, this revised frequency is below 1E-2/yr and therefore, the event is still classified as an infrequent event.

**Generator Load Rejection with Total Turbine Bypass Failure (Section 15A.3.4)**

This frequency is composed of two contributors:

Generator Load Rejection Frequency = 0.45/yr(1)  
[NUREG/CR-3862 Table 9](1)

Total Turbine Bypass Failure = 4.4E-04 (see Item (A))

The DCD will be updated to reflect this latest evaluation of the TBV failure probability.

Frequency = 0.45/yr \* 4.4E-04 = 2.0E-04/yr.

This calculated frequency is higher than the original frequency estimate of 5.52E-6/yr, however, this revised frequency is below 1E-2/yr and therefore, the event is still classified as an infrequent event.

**Conclusion**

These two events remain classified as infrequent events.

---

<sup>(1)</sup> It is noted that the 0.45/yr frequency is based on the data from pre-1985. It is recognized that these initiator frequencies have decreased by more than a factor of 4 since that time. (See discussion in RAI 15.0-21.)

**Item (A):**

*A simplified process flow diagram of the Turbine Bypass System and associated fault tree that models the failure of seven or more of the 12 available Turbine Bypass Valves (TBVs) on demand. This information should be readily available since it is part of the information needed to respond to RAI 19.1.0-55 of the PRA (basic event N21-SYS-FF-BYPASS). Please include discussion of assumptions made about the failure of TBVs and support systems (e.g., AC power, I&C, compressed air, and individual valve accumulators).*

**GE Response:**

Figure 15.0-20(A)-1 is a simplified schematic of the process flow diagram for the Turbine Bypass System (TBS).

Figure 15.0-20(A)-2 is a simplified fault tree to estimate the failure probability of the TBS.

The hydraulic system for the TBVs consists of the subsystems and components identified on Figure 15.0-20(A)-1. The critical items to note are the following:

1. The design specification requires that no single failure results in the failure of more than half of the TBVs.
2. The redundant hydraulic pumps are backed up by the accumulators (one per TBV for a total of 12).
3. A check valve is installed on each of two banks of TBVs (6 TBVs per bank) to allow accumulator pressure to be maintained if the hydraulic pumps fail.
4. A check valve is also installed on the discharge of each pump.
5. There is a triple redundant fault tolerant digital controller for the load driver and coil servo valves.
6. There are three redundant power supplies to the load driver and coil servo valves, one of which is battery backed.

The applicable dominant failure modes include the following:

1. Failure of multiple TBVs. This is treated as a common cause failure of 7 of 12 TBVs leading to failure. (Basic Event EHC-TBV-MECH-CCF)
2. Failure of power supplies to the triple redundant fault tolerant digital control logic (Gate EHC-TBV-PWR) which may result from:
  - a. Common cause failure of power supplies (Basic Event: EHC-TBV-PWR-CCF).
  - b. Loss of power due to independent causes (Gate: EHC-TBV-PWR-ALL).
3. Complete failure of one of the two TBV banks and a failure of at least one TBV in the second bank (Gates: EHC-TBV-MODE1 and EHC-TBV-MODE2).
4. Failure of 7 or more TBVs regardless of bank (Gate: EHC-TBV-MODE3).

5. Common cause failure of the triple redundant fault tolerant digital controller (Basic Event: EHC-SIGNAL-CCF) (Includes failure of both hydraulic pumps and check valves to hold hydraulic pressure).

The simplified fault tree for these failure modes is included on Figure 15.0-20(A)-2.

Assumptions:

The TBV failure probability is discussed in 15.0-20(B)

The common cause failure probability for BETA of 0.02 for the TBVs is shown to be conservative relative to the latest NRC Multiple Greek Letter (MGL) common cause data (NUREG/CR-5497).

Data Source	AOV CCF Data			
	$\beta$	$\gamma$	$\delta$	$\beta \gamma \delta$
NUREG/CR-5497				
FTO	0.35	0.287	0.215	2.1E-03
FTC	0.044	0.112	0.343	1.69E-03

This shows that the latest NRC sponsored data for multiple Air Operated Valve (AOV) failures result in a common cause conditional probability for multiple valves of 2.1E-03 compared with that used in section 15A.3.4.2 of the DCD of 0.02. The conservative common cause failure probability of 0.02 is retained.

The sum of the independent failures of any of 6 TBVs is assessed as  $6 * (6E-3) = 3.6E-2$ . (See basic events EHC-TBV-BNK1-1OF6 and EHC-TBV-BNK2-1OF6.)

Independent failures of any of 6 accumulators coupled with failure of the hydraulic supply to the bank of TBVs are assumed sufficient to fail at least 1 TBV of a bank. The sum of the independent accumulator failure probabilities for one of two banks is assessed as  $6 * (1E-3) = 6E-3$ . (See basic events EHC-ACC-BNK1-ONE and EHC-ACC-BNK2-ONE.)

For transient induced challenges, the conditional probability of the Loss of Preferred Power (Offsite AC Power) is used to replace %LOPP. The value used is 2.0E-02, which is derived from NRC evaluations in Ref [2]. This value is conservative because it assumes a coincident LOCA signal present.

The assumed mission time for the TBVs is 6 sec.

Each accumulator is adequate for the assumed mission time of 6 seconds for the TBS.

Results:

The results of the fault tree evaluation for the failure of the TBS is provided for two cases:

Case	TBS Failure Probability
Loss of Preferred Power (%LOPP set to 1.0)	1.43E-03
Transient (%LOPP set to conditional probability of 2E-2)	4.4E-04

# ESBWR Turbine Bypass Valves EHC

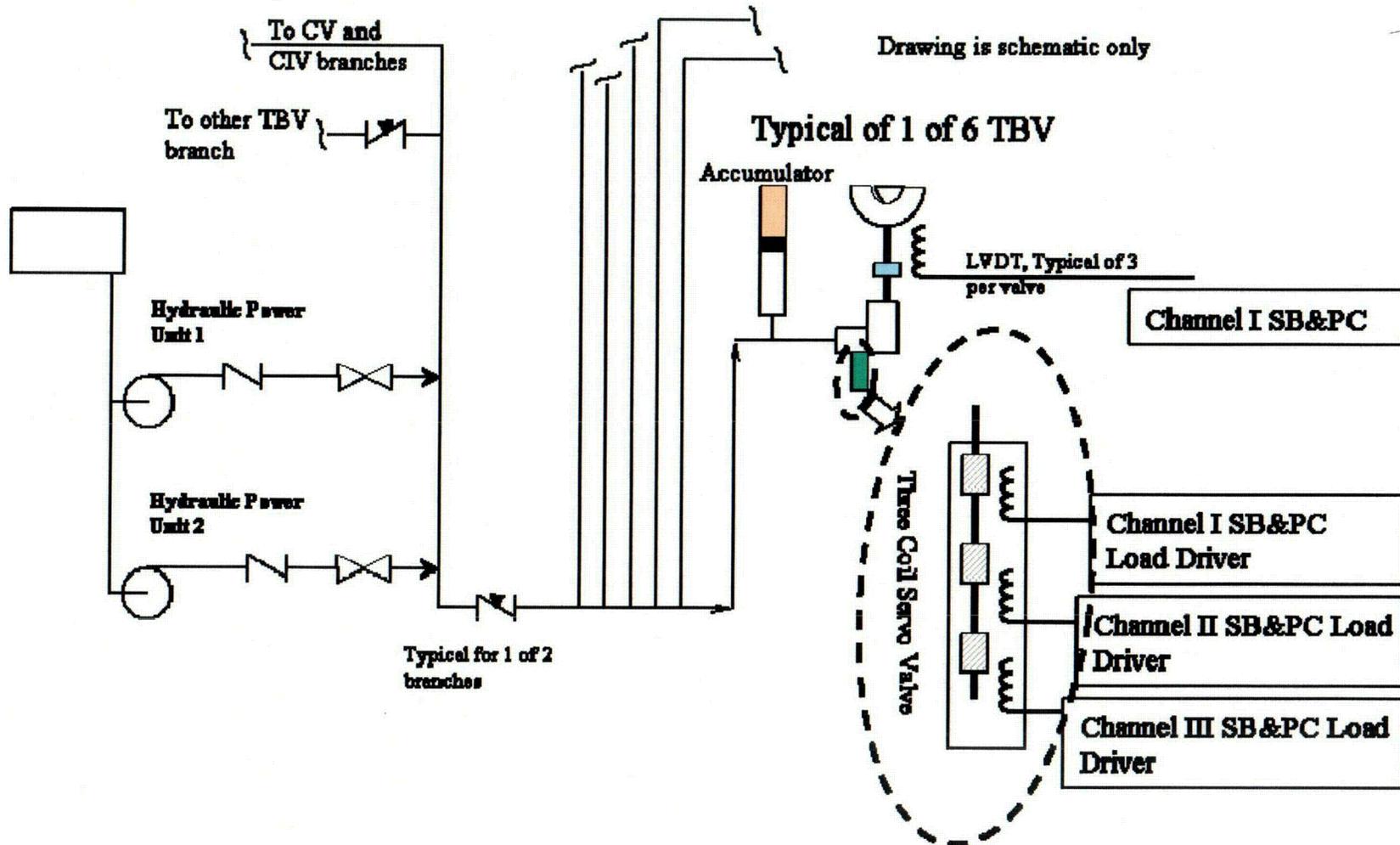
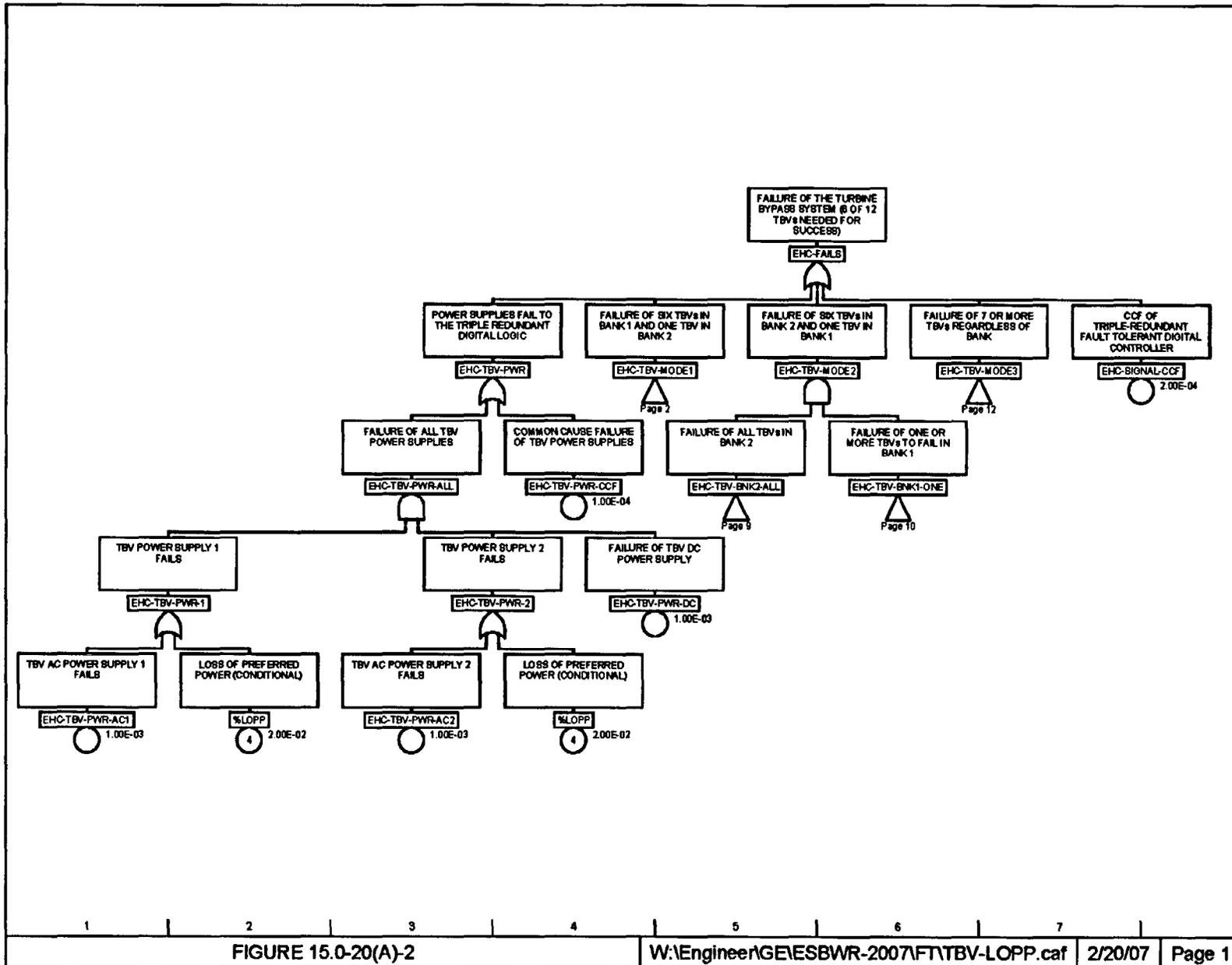
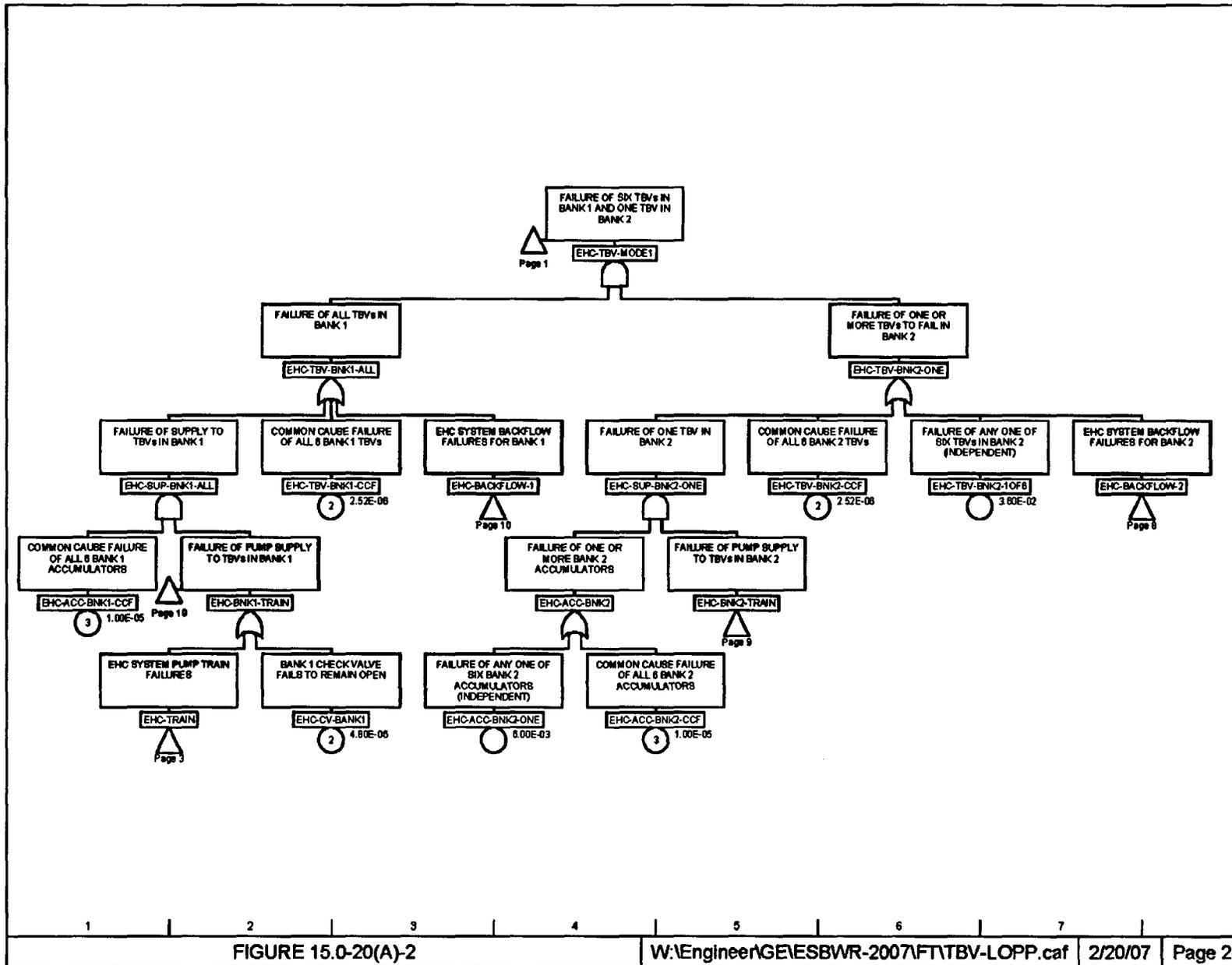


Figure 15.0-20(A)-1 TBV Related Systems

**Figure 15.0-20(A)-2**

**Turbine Bypass System Fault Tree Given Transient Challenge  
(13 Pages)**





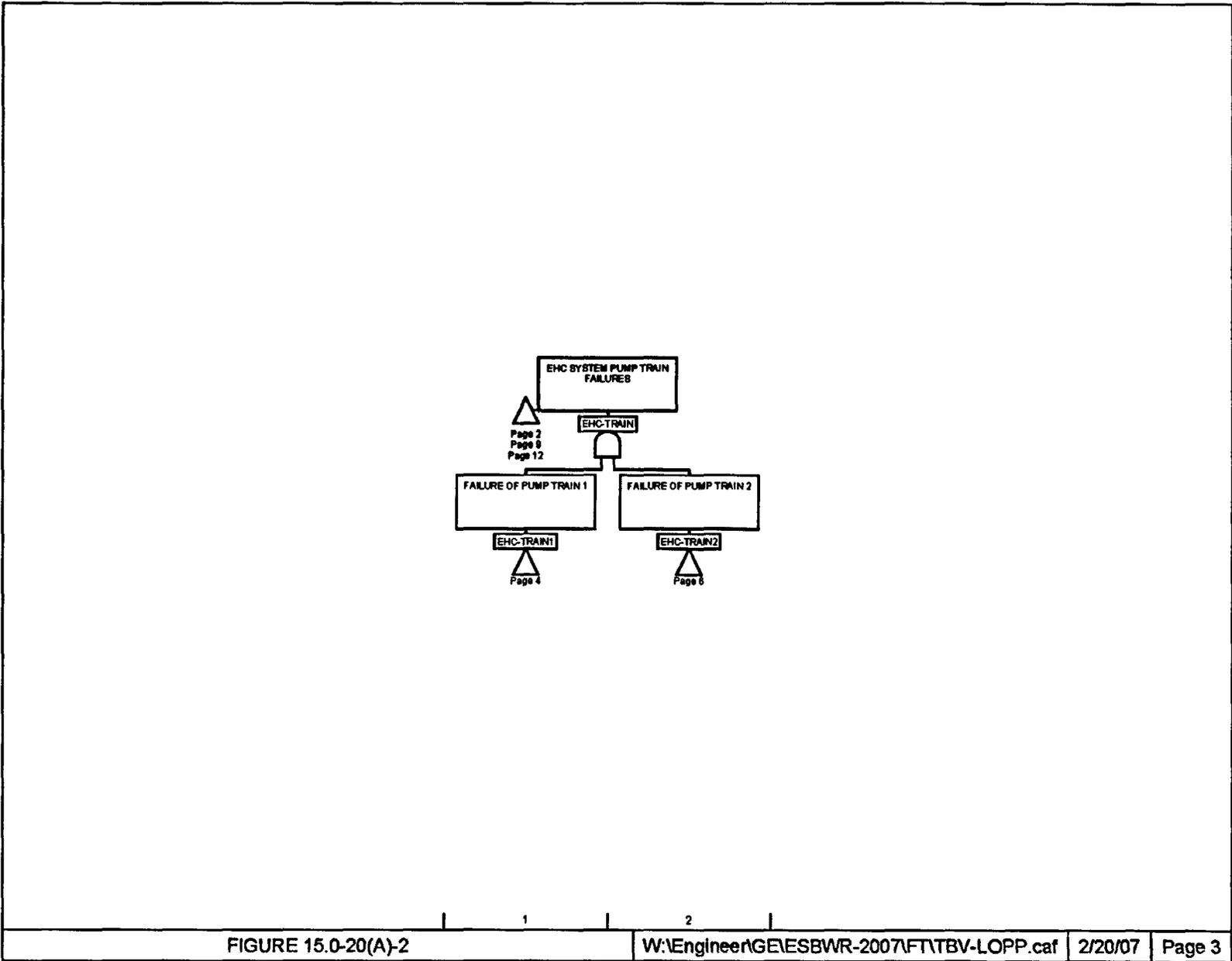


FIGURE 15.0-20(A)-2

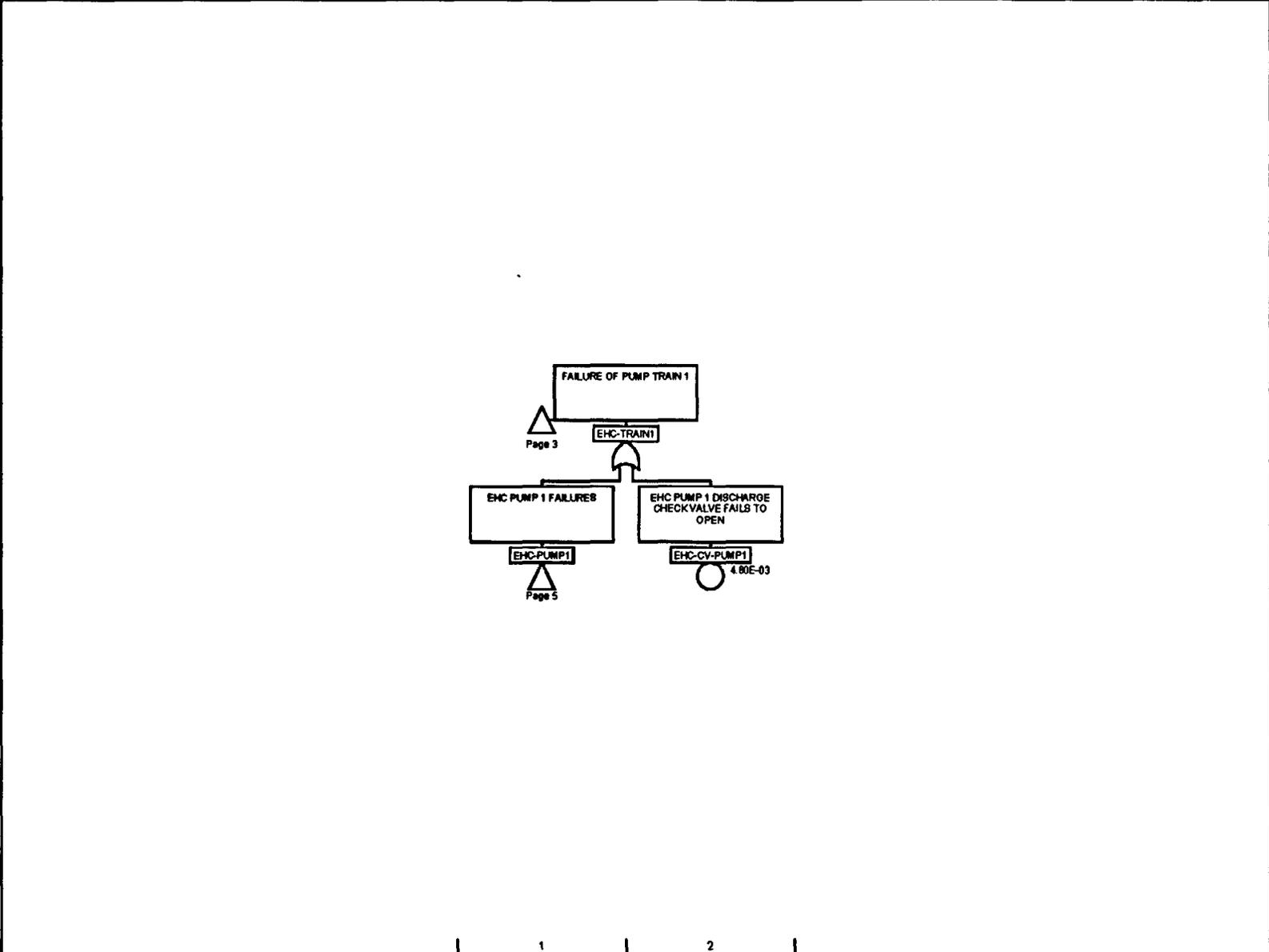


FIGURE 15.0-20(A)-2

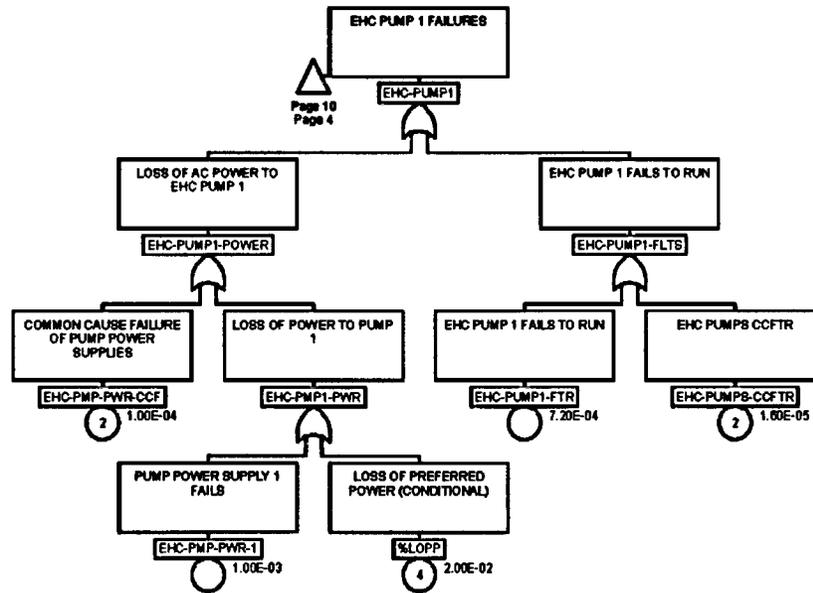


FIGURE 15.0-20(A)-2

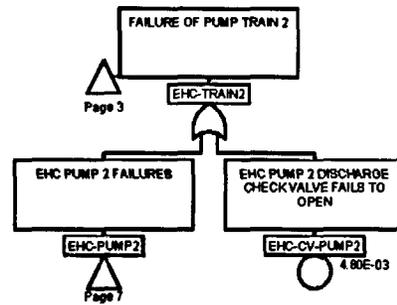
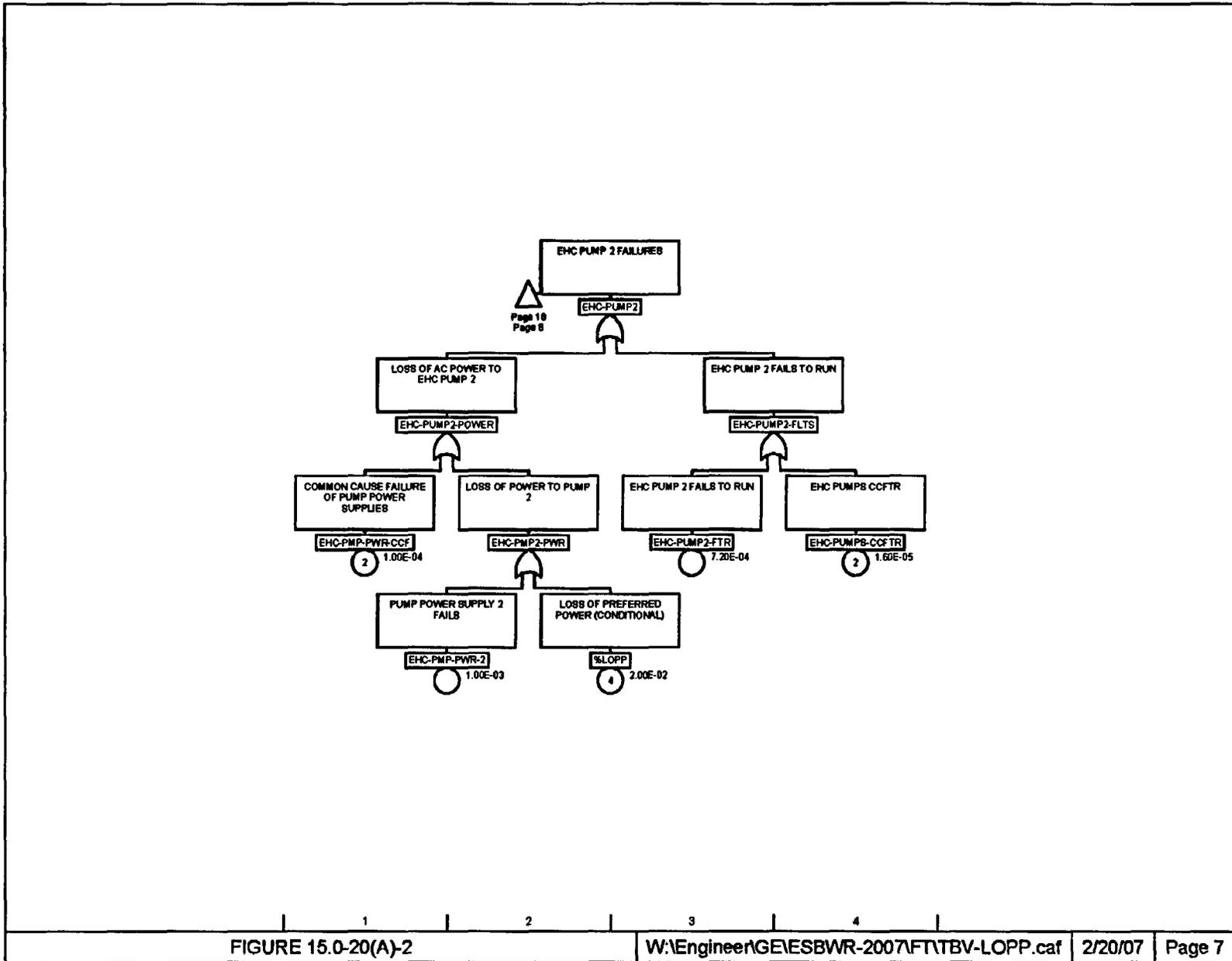


FIGURE 15.0-20(A)-2



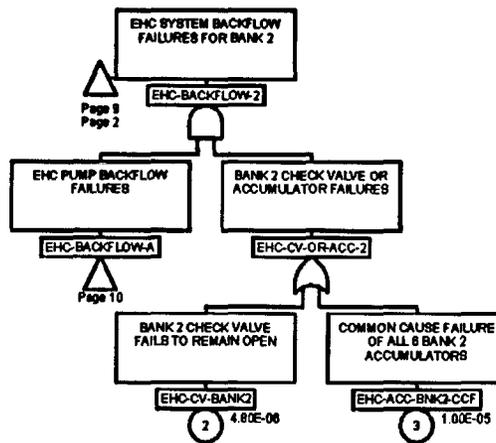


FIGURE 15.0-20(A)-2

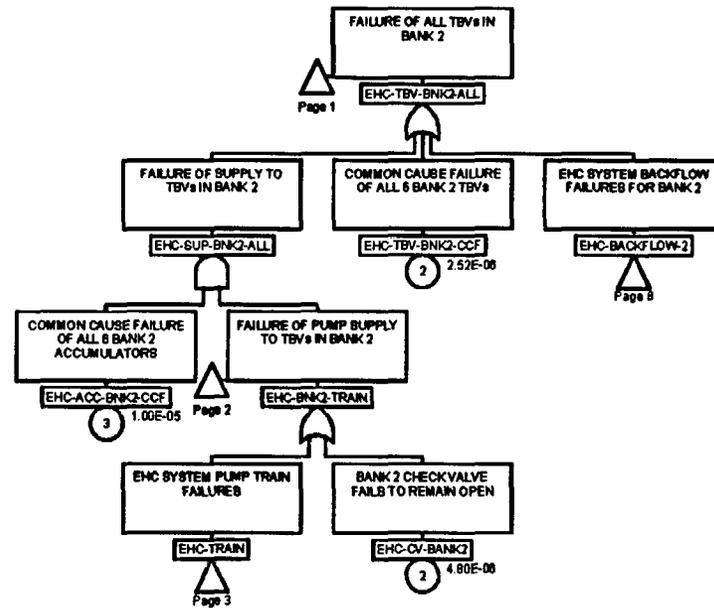


FIGURE 15.0-20(A)-2

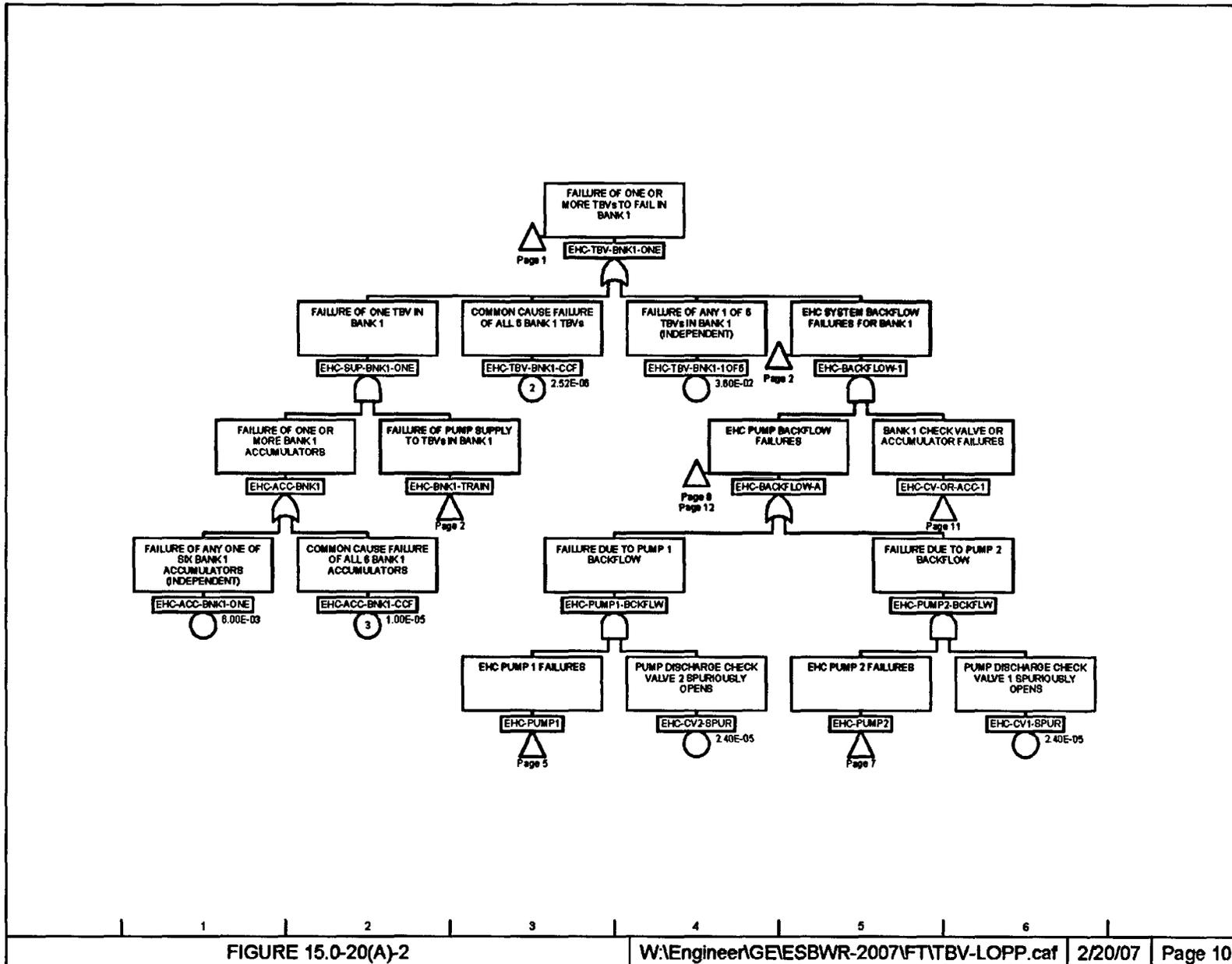


FIGURE 15.0-20(A)-2

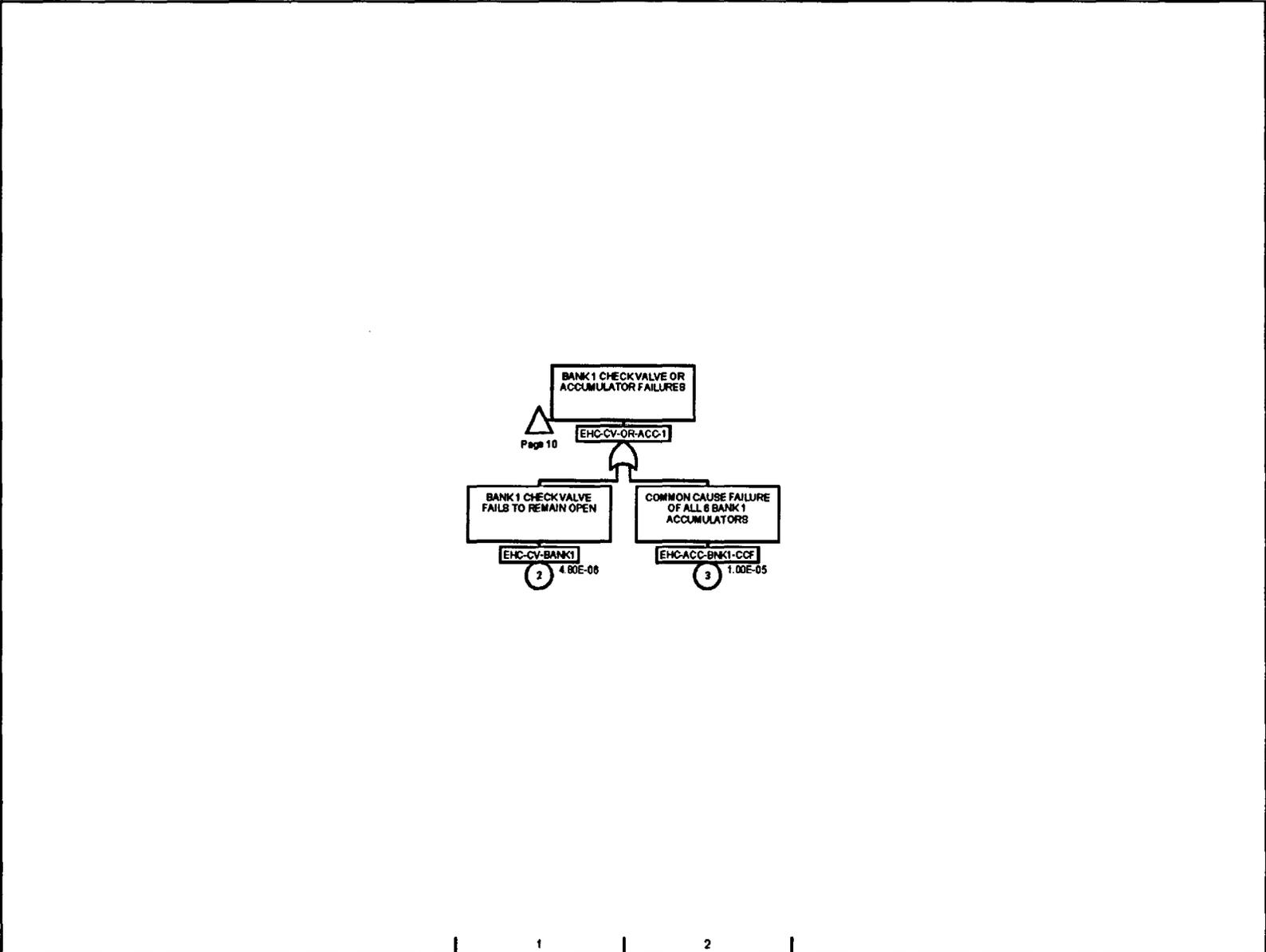


FIGURE 15.0-20(A)-2

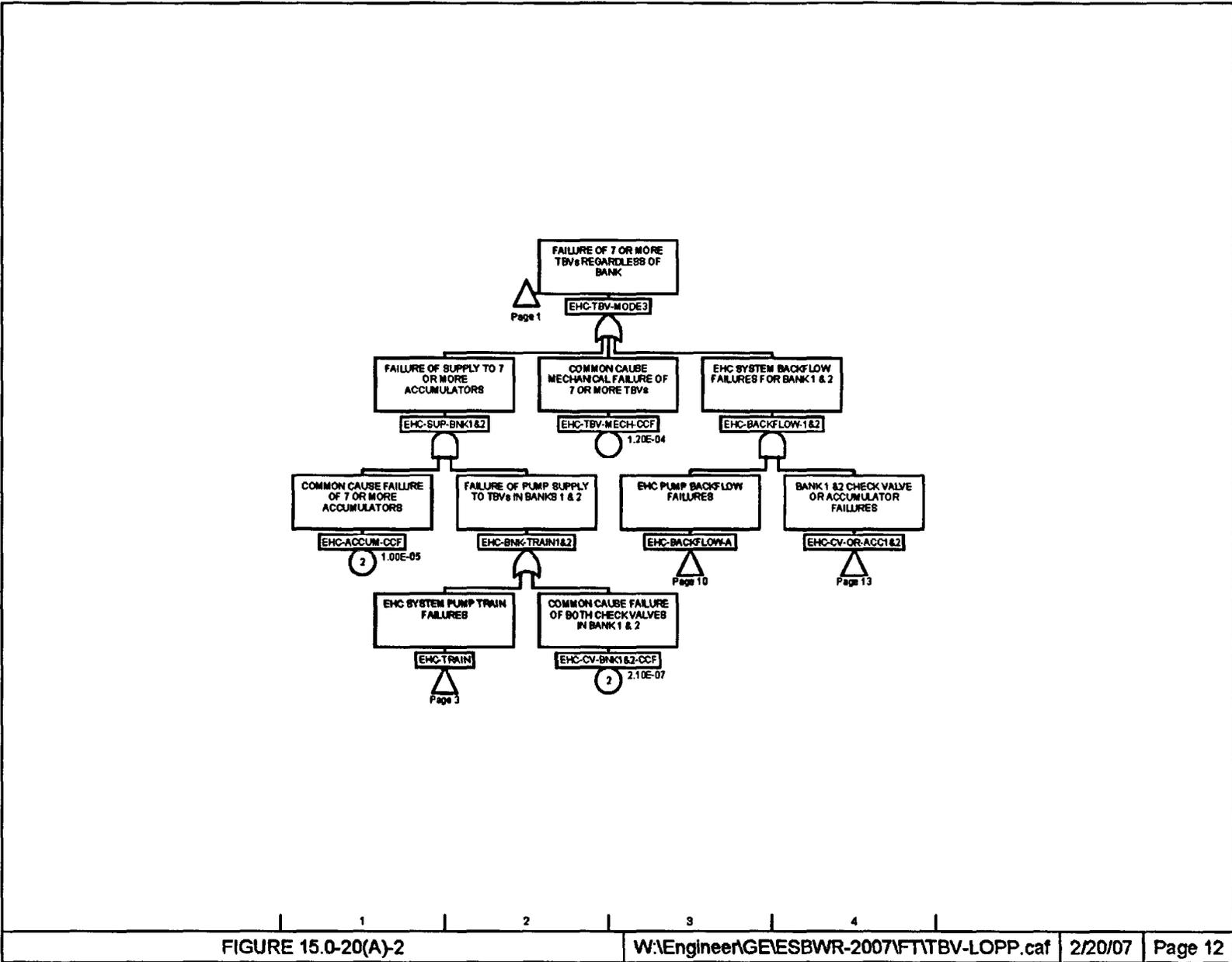


FIGURE 15.0-20(A)-2

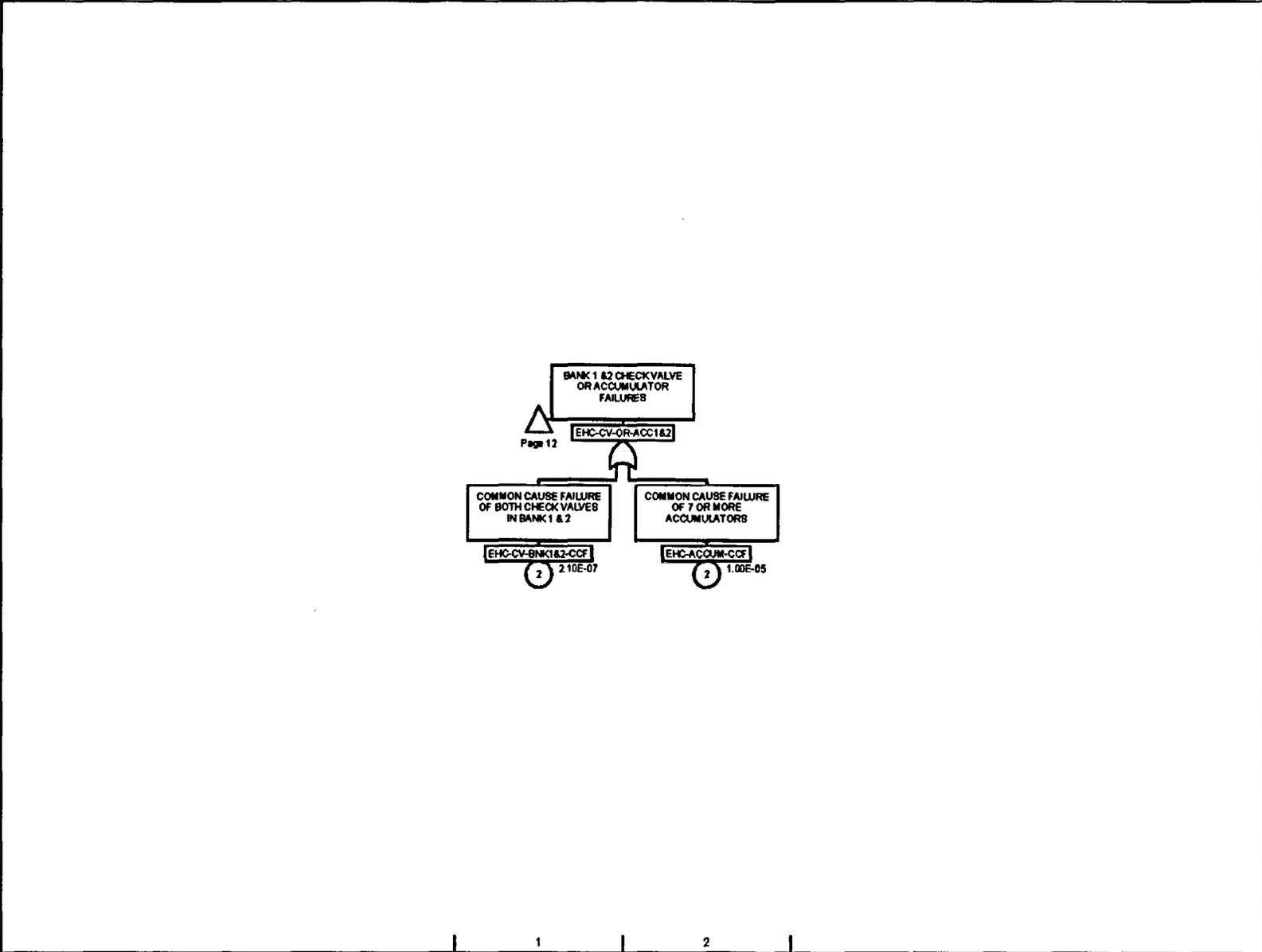


FIGURE 15.0-20(A)-2

**Item (B):**

*It is stated (DCD Tier 2, Revision1, page 15A-4) that: "In the absence of specific data, the failure rates for the TBVs are estimated to be 6.0E-3 per demand, based on the failure for the safety/relief valves...". The staff believes that the probability that a TBV fails when demanded to open depends on its failure mode and testing frequency. For example, if a TBV is considered to be an airoperated valve (AOV) that can fail to operate to other than the deenergized position, the failure rate of 3E-6/hour should be used in conjunction with an exposure time of 24 months. This would result in a failure probability on demand of 2.63E-2, which is significantly higher than the assumed probability of 6E-3. Please discuss.*

**GE Response:**

Data evaluation is always a difficult problem for characterizing new equipment with no specific operating experience. It is recognized that the failure probability of the TBVs are best described with their own data, if available. The ESBWR TBVs may be of sufficiently different design that current operating experience data would not account for the design differences. Nevertheless, the environment, the maintenance processes, and the management oversight at nuclear plants are judged to have a significant impact on failure rates therefore, the use of similar component failure rates from nuclear plants is considered appropriate and desirable.

In an attempt to respond to the possible variation in data that could be selected, a brief table of available failure rates is provided below with the data source cited.

NRC Research has sponsored an extensive evaluation of data in reactor plants. This data is also trended to demonstrate the effects of improved plant operations as a function of calendar year.

Possible options for the data include the following:

Type	Failure Rate (Fail To Open)	Reference Source
Safety Relief Valves	6.0E-03/d	ALWR <sup>1</sup>
AOV	2.0E-03/d	ALWR
AOV	2E-03/d	NUREG/CR-4550
AOV BWR	7.9E-07/hr	NUREG-1715, Vol. 3, July 2001
AOV	5.53E-04/d	NUREG-1715 update, 1987-2004, NRC Web site
AOV	2.28E-04/d	NUREG-1715 update, 2004, NRC Web site <sup>(*)</sup>

(\*) NRC Evaluation of AOV "Fail to Open" Trend

<sup>1</sup> Advanced Light Water Reactor Utility Requirement Document

The selection of how to model the failure rate is a key question. The selection can be to model the failure rate as a demand failure rate or an hourly standby failure rate with the appropriate surveillance interval. In reality, it is recognized that, in general, the true failure rate is a combination of the “shock” failure rate (demand failure rate) and the hourly failure rate

$$\lambda_T = \alpha\lambda_d + \beta\lambda(t) + \frac{T}{2}$$

where  $\alpha$  and  $\beta$  are selected to represent the degree of belief in the respective failure rate models

$$\alpha + \beta = 1.0$$

Because the coefficients  $\alpha$  and  $\beta$  for this equation have not been developed, the following table summarizes the comparison of TBV failure probabilities for “Fail to Open” that can be selected using either the demand model or the standby hourly model.

Fail to Open Failure Rate	Component	Reference	Failure Probability (2 year Refuel Cycle)
6E-03/demand	SRV	EPRI ALWR Data	6E-03
2.28E-04/demand	AOV	NUREG-1715 Update, 1987-2004 (for 2004 year) NRC Web site	2.28E-04
7.9E-07/hr	AOV	NUREG-1715, Volume 3, July 2001	6.9E-03
4.58E-07/hr	AOV	Extrapolation of NUREG-1715, Vol. 3, July 2001 hourly failure rate	4.01E-03

The calculation of the failure probability using the hourly failure rate from NUREG-1715 has three potential conservatisms:

- It does not account for shutdowns during the refuel cycle that would act as a test of the TBVs.
- It does not account for the trend calculated by the NRC of decreasing AOV failure rate from 1987 to 2004 reflected in the per demand failure rates.

Year	Mean Failure Rate (/d)
1987	1.07E-03
1998	3.93E-04
2004	2.28E-04

- It assumes TBV tests are only conducted at refuel outages. However, the TBVs are tested weekly. [Ref [3]] Therefore, the use of the above formula results in a TBV failure probability of:

$$\lambda \frac{T}{2} = 4.58E - 07 / \text{hr} * 168 \text{ hours} / 2 = 3.84E - 05$$

If we examine the effect of this second conservatism by assuming that the hourly failure rate in 1998 is decreased by the same ratio as the per demand failure rate, the AOV hourly failure rate decreases from the 1998 assessment of 7.9E-07/hr to 4.58E-07/hr.

As can be seen from the third potential conservatism, the TBV failure probability assumption used in the DCD sections 15A.3.3.2 and 15A.3.4.2 of 6.0E-03 per demand is very conservative when the hourly TBV failure rate is used with a realistic evaluation of the test frequency (i.e., weekly).

#### Summary

As can be seen, the NRC evaluation of the data provides a per demand failure rate for the AOVs which has shown the trend in AOV failure rate to be decreasing with the implementation of the Maintenance Rule and the increase in plant availability and capacity factors.

#### Demand Failure Rate

Therefore, it is judged that a failure rate of 2.28E-4/demand is supported by the NRC evaluated operating experience up through 2004.

#### Hourly Failure Rate

In the case of the hourly failure rate, the NRC has not provided a similar 2004 update to the hourly failure rate to reflect the observed trend of lower AOV failure rates. If the hourly failure rate model is used along with the NRC AOV data evaluation from 1998 of the hourly failure rate, the failure probability is the following:

$$\lambda \frac{T}{2} = 7.9E - 07 / \text{hr} * 8760 \text{ hours} = 6.9E - 03$$

This does not account for the noted decreasing trend of AOV failure rates calculated by the NRC<sup>(1)</sup>. If the decreasing trend is accounted for, this results in the following:

---

<sup>(1)</sup> The failure probability is 4.0E-03 if the trend in decreasing AOV failure rate is accounted for.

$$\lambda \frac{T}{2} = 4.58E - 07 / \text{hr} * 8760 \text{ hours} = 4.0E - 03$$

**Conclusion**

This approach results in an AOV failure probability over a 2 year cycle that is essentially the same as that used in the ESBWR submittal of 6.0E-03<sup>(1)</sup>. This is recognized to be conservative given the weekly tests of the TBVs.

**Item (C):**

*It is stated (DCD Tier 2, Revision1, page 15A-4) that: "The common cause failure probability of seven valves is estimated by multiplying the individual TBV failure by a beta factor of 0.02. The value of 0.02 is judged to be a conservative value, especially since each valve is equipped with its own accumulator." However, the data used to estimate common cause failure (CCF) multipliers do not include support system failures, such as compressed air. Therefore, the assumed beta factor may not be conservative. Actually, the value of the CCF multiplier for four or more AOVs reported in the ALWR Utility Requirement Document (Reference 15A-1 of the DCD) is close to 10 percent. Please discuss.*

**GE Response:**

The common cause failure probabilities are justified in Item (A).

The support system dependencies are explicitly included in the fault tree developed in Item (A).

The individual TBV failure probability is discussed in Item (B).

All of this information is consolidated into the fault tree requested in Item (A) with the result shown in Item (A). The conclusion with regard to the Turbine Bypass System is discussed under Item (A).

**Item (D):**

*It is stated (DCD Tier 2, Revision1, page 15A-4) that: "The only relevant support system is the AC power and loss of AC power results in a different category of initiating event. Therefore, the failure of AC power is not considered....". The staff believes that all failures that cause turbine bypass failure should be included in the assessed frequency (with the exception of loss of condenser, which is an analyzed event which includes and bounds the event considered in this analysis). Please discuss.*

**GE Response:**

A revised analysis of the Turbine Bypass System (TBS) is developed and provided in Item (A). All support system failures including the loss of AC power (local failures) are included in the Item (A) fault tree. Loss of Preferred Power (LOPP) is a separate initiating event.

This RAI response under Item (A) presents the requested fault tree to identify possible contributors to turbine bypass failure. This fault tree is evaluated for the two principal transient categories: LOPP and other.

The Turbine Bypass System (TBS) failure probability calculated for the "other" category is applicable to the two transients of interest in this RAI:

- Turbine Trip with Total Bypass Failure
- Generator Load Rejection with Total Turbine Bypass Failure

**Item (E):**

*Please clarify the statement regarding the existence of groups of 3 or 6 TBVs that are actuated by hydraulic fluid from the main hydraulic lines separated by check valves. How is this design feature modeled for the purpose of assessing the probability of turbine bypass failure? Also, please clarify the statement that ""....the accumulator in each of the TBVs is designed with sufficient capacity to open at least six times.""*

**GE Response:**

**TBV Group Size**

There are no longer groups of three TBVs in the ESBWR design.

The design specification for the turbine bypass system dictates that the TBVs are to be divided into at least two groups of six.

**TBVs**

Each TBV is independently controlled and has its own accumulator. (See Item (A) and RAI Figure 15.20(A)-1).

**Accumulators**

The accumulator is an adequate replacement for the hydraulic pumps to support the required 6 seconds of TBV operation to meet the Chapter 15 assumptions.

**Item (F):**

*Please clarify whether the design of the TBVs is finalized and list any requirements for ensuring the availability of individual accumulators for the TBVs with the capabilities assumed in this analysis.*

**GE Response:**

The TBV design is not finalized. The ESBWR DCD documents the accumulator requirements.

Each TBV has its own accumulator. The accumulators are required to provide TBV operation for 6 seconds. Currently, 6 cycles are used to specify the accumulator capacity to ensure that at least 6 seconds of operation is available to meet the assumptions of the Chapter 15 analysis.

**Item (G):**

*The frequency of Loss of Preferred Power (DCD Tier 2, Revision1, Section 15A.3.4) was assumed to be 4.6E-2 per year (PRA value). However, since the frequency of Loss of Preferred Power is site-specific, the assumed value may not be a bounding value which envelopes all potential sites. Please discuss."*

**GE Response:**

The Generator Load Rejection frequency cited in Subsection 15A.3.3 is based on using a surrogate event, the loss of offsite AC power (LOOP). This approach was taken because there is no recent data collection of transient frequencies that breaks out this event, i.e., NUREG/CR-5750 [4] does not identify this as a separate transient category.

The NRC sponsored research in NUREG/CR-3862 does list this as a separate transient category (for data from the 1970s – 1980s). However, it is well known that the initiating event frequencies have decreased dramatically (approximately by a factor of 3) since that time. The NUREG/CR-3862 [5] frequency estimate for load rejection is 0.45/yr.

The following discussion is focused on establishing the basis for the loss of offsite AC power frequency.

The NRC has sponsored a study of the loss of offsite AC power (LOOP) for current generation nuclear plants. See NUREG/CR-6890. [1]. This can be equated to the ESBWR loss of preferred power (LOPP) frequency. This analysis represents the most recent comprehensive evaluation of the loss of offsite AC power and includes the data from the August 14, 2003 Northeast blackout event.

NUREG/CR-6890 [1] is used to develop a generic prior distribution for the ESBWR LOOP initiator frequency. NUREG/CR-6890 separates LOOP events into the following four causal categories:

- Plant centered
- Switchyard centered
- Grid related
- Weather related

Section 3 of NUREG/CR-6890 defines the baseline period for determining industry LOOP frequencies based on data for 1997 – 2004. The baseline period is derived recognizing the improved performance indicating a reduction in the frequency of plant centered and switchyard centered LOOPS, and the deregulation of the electrical industry and resultant changes to electrical grid operation, which may signal degradation in grid related loop frequencies. The grid related and weather related categories use the same data period as the plant centered and switchyard centered LOOP events (1997 – 2004) to capture the most recent data. It is noted that the two latter categories (grid and weather related LOOP events) show an increasing trend during this data period.

Section 3 of NUREG/CR-6890 provides three methods to determine LOOP frequency:

- (1) **Industry Frequency:** Utilizes the industry data in the four LOOP causal categories to obtain the total industry LOOP frequency.
- (2) **Regional Frequency:** Utilizes industry data for the plant centered, switchyard centered, and weather LOOP categories; however, uses region specific grid related LOOP data.
- (3) **Plant Specific Frequency:** Utilizes the industry specific LOOP category frequencies and Bayesian updates each category with plant specific data to obtain a total plant specific LOOP frequency.

Table 15.0-20-1 is taken from NUREG/CR-6890 and summarizes the generic prior distributions for loss of offsite AC power based upon operating experience for plants at-power. This sample of experience is considered representative of the decreasing trend in LOOP frequencies due to improved plant and grid performance.

As can be seen from the table, the total loss of offsite AC power (plant at-power) is 3.59E-02/Rx Cr Yr. This can be converted to per Rx Yr by multiplying by the availability factor (assume 0.95 for ESBWR):

$$F_{LOPP} = \frac{3.59E-02}{Rx \text{ Critical Yr}} * \frac{.95 Rx \text{ Critical Yr}}{Rx \text{ Yr}}$$

$$F_{LOPP} = 3.41E-02 / Rx \text{ Yr}$$

This result is below the loss of offsite AC power frequency used in the ESBWR analysis, and is considered an appropriate estimate of the loss of offsite AC power based on GE accumulated experience.

The level of conservatism in the estimate of the loss of offsite AC power frequency is confirmed by the observation that the trend in the frequency is decreasing with time. For example, from NUREG/CR-6890, Table 3-5, the following comparison is found:

Time Period	Loss of Offsite AC Power (Per Rx Critical Yr)
1986-1996	4.56E-02
1997-2004	3.59E-02

The quoted ESBWR LOPP assumed in Section 15A is approximately that found from the earlier operating experience evidence. More recent data continues to support the fact that the frequency trend is decreasing.

Regional Effects

The ability to divide the US average Loss of Offsite AC Power for plants operating at-power among regions was also investigated in NUREG/CR-6890. The results indicated the following for plants at-power:

LOOP Category	Region-Wide Variation
Plant Centered	None
Switchyard Centered	None
Weather	None
Grid	Possible, but data is marginal

NUREG/CR-6890 indicates that, because of the paucity of data, it may not be appropriate to attempt dividing the at-power LOOP frequency among regions of the U.S. However, if the regional grid data is evaluated (note that the NERC regions have changed since the time that this data was even collected), the regions with the highest grid LOOP frequency are the Western Regional Grid and the NPCC. From Table 3-6 of NUREG/CR-6890, the NERC region with the highest frequency of grid failures is NPCC at 6.42E-02/Rx Critical Yr. given data over the period 1986-2004. If we add the ensuing two calendar years of experience (2005 and 2006) to NPCC using the NUREG/CR-6890 formalism of a constrained non-informative prior ( $\alpha = 0.5$ ,  $\beta = 26.83$ ), we find:

$$\text{LOOP}_{\text{GRID}}^{(1)} = \frac{\alpha + \text{events}}{\beta + \text{Critical Years}}$$

$$\text{LOOP}_{\text{GRID}}^{(1)} = \frac{0.5 + 6}{26.83 + 93} = 5.42\text{E} - 02$$

Using the Regional Calculation for NPCC, we find:

LOOP Category	NPCC Loss of Offsite AC Power Frequency (Per Critical Yr)
Plant Centered	2.07E-03
Switchyard Centered	1.04E-02
Grid	5.42E-02

<sup>(1)</sup> NPCC region from NUREG/CR-6890:

$$\text{LOOP}_{\text{GRID}} = \frac{6.5}{101.23 \text{ RxCrYr}}$$

This estimate is updated with the two years of NPCC data from 2005 and 2006 when no grid failure LOOP events were recorded in the NRC LER database.

Weather	4.83E-03
TOTAL	7.15E-02

This is converted to per reactor year by multiplying by the criticality factor, i.e., 0.95:

$$\text{LOOP}_{\text{NPCC}} = 6.79\text{E} - 02 / \text{RxYr}$$

If one assumes that the grid reliability varies by region and that the limited data over 10 years is adequate to represent the regional grid data, then the loss of offsite AC power would need to increase by a factor of 1.48.

#### Summary

There are three alternatives for resolution of the Generator Load Reject with Turbine Bypass failure:

- (1) Use old data for load reject frequency
- (2) Use trends in initiating event frequencies to adjust the projected future load reject frequency
- (3) Use surrogate value of LOOP frequency to represent the load reject frequency

#### Alternate 1: Use of Old Generator Load Reject Frequency Data

Even if the old initiating event frequency data from pre 1985 (NUREG/CR-3862 [5]) for the load rejection frequency is used, the frequency of the event Generator Load Rejection with failure of the TBVs is calculated to be as follows:

$$0.45/\text{yr} * 4.4\text{E}-4 = 2.0\text{E}-4/\text{yr}$$

This still would be in the "infrequent" event category.

The DCD Section 15A.3.4 will be updated to include this frequency estimate for this event as noted in the attached markup since it provides the most conservative of three alternatives.

#### Alternate 2: Use Initiating Event Frequency Trend Data to Update

The BWR initiating event frequencies have shown a continuously decreasing trend from the data collected in the early 1980s [5] to those data from more recent data evaluations [4]. RAI 15.0-21 summarizes the trends in the initiating event data and it is found that there is a general decrease of a factor of 4 in the initiating event frequencies. Applying this factor of 4 to the generator load rejection frequency from NUREG/CR-3862 [5] yields a frequency of 0.11/yr.

Therefore, the frequency of generator load rejection with failure of the TBVs is calculated to be as follows:

$$0.11/\text{yr} * 4.4\text{E}-4 = 4.8\text{E}-5/\text{yr}$$

Again, this would be classified in the "infrequent" event category.

**Alternate 3: Use Surrogate Value of LOOP Frequency**

The third alternative may be the least desirable; i.e., the use of a surrogate initiating event, LOOP, to represent the generator load reject frequency. If selected, the following summarizes this alternative.

PRA's are to represent the realistic evaluation of the risk profile. This suggests the use of the best estimate accumulated experience applicable to the future operation of the ESBWR design. This results in using the average U.S. LOOP frequency of  $3.41E-02/RxYr$ .

If conservatism is imposed on the calculation to ensure that all sites are enveloped, and if the 10 years of data from 1997 through 2006 is judged representative of LOOP experience in the future, then the LOOP frequency should be increased to  $6.79E-02/RxYr$ .

Consistent with the use of mean estimates for the component and initiating event frequencies, it is judged appropriate to use the U.S. average loss of offsite AC power frequency of  $3.41E-02/RxYr$ . This would reduce the calculated risk estimates in the ESBWR PRA.

**References:**

- [1] Eide, S.A., Gentillon, C.D., Wierman, T.E., Rasmuson, D.M., Reevaluation of Station Blackout Risk at Nuclear Power Plants: Analysis of Loss of Offsite Power Events: 1986-2004, NUREG/CR-6890, Vol. 1, December 2005.
- [2] USNRC Memorandum to Samuel J. Collins, Director Office of Nuclear Reactor Regulation, from Ashok C. Thadani, Director of Nuclear Regulatory Research, "Transmittal of Technical Work to Support Possible Rulemaking on a Risk-Informed Alternative to 10 CFR 50.46 / GDC 35", July 31, 2002.
- [3] Telecon 1/30/07, E.T. Burns (ERIN), Rick Wachowiak, Bret Nelson (GE).
- [4] Poloski, J.P., et al., for the U.S. Nuclear Regulatory Commission, "Rates of Initiating Events at U.S. Commercial Nuclear Plants; 1987 through 1995", NUREG/CR-5750, February 1999.
- [5] Mackowiak, D.P., et al., for the U. S. Nuclear Regulatory Commission, "Development of Transient Initiating Event Frequencies For Use in Probabilistic Risk Assessments", NUREG/CR-3862, May 1985.

**Affected Documents:**

DCD Tier (2), Subsections 15A.3.3, 15A.3.4 and Table 15A-3 will be revised as noted on the attached markup.

**Table 15.0-20-1 Plant Level LOOP frequency distributions**

Plant-Level LOOP Frequency Distribution <sup>a</sup>									
Mode	LOOP Category	5%	Median (50%)	Mean	95%	Error Factor	Gamma Shape Parameter ( $\alpha$ )	Gamma Scale Parameter ( $\beta$ , years)	Source <sup>b</sup>
Critical operation (1997-2004)	Plant centered <sup>c</sup>	8.14E-06	9.42E-04	2.07E-03	7.96E-03	8.44	0.50	241.43	CNID
	Switchyard centered <sup>c</sup>	4.07E-05	4.71E-03	1.04E-02	3.98E-02	8.44	0.50	48.29	CNID
	Grid related	7.33E-05	8.48E-03	1.86E-02	7.16E-02	8.44	0.50	26.83	CNID
	Weather related	1.90E-05	2.20E-03	4.83E-03	1.86E-02	8.44	0.50	103.47	CNID
	All	4.57E-03	2.87E-02	3.59E-02	9.19E-02	3.21	1.58	44.02	Simulation

- a. The frequency units for 5%, median, mean, and 95% are per reactor critical year (/rcry) or per reactor shutdown year (/rsy).
- b. CNID – constrained noninformative distribution, simulation – sum of 4 categories simulated and fit to gamma.
- c. For risk studies that combine the plant-centered and switchyard-centered LOOPS, the gamma distribution has  $\alpha = 0.50$  and  $\beta = 40.10$ . The mean of this distribution is  $1.25E-2/rcry$ .

**NRC RAI 15.0-21:**

*Justify assumptions in frequency estimate for "Loss of Feedwater Heating with Failure of Selected Control Rod Run-In" (Section 15A.3.6).*

*The staff notices that only I&C failures are discussed (see RAI 15.0-19) and that the loss of a division of non-Class 1E AC power is not considered in the frequency estimation (see RAI 15.0-21). These issues should be addressed. Also, additional information is needed on the assumed frequency of failure of feedwater heater and the modeling of I&C system in the analysis.*

*(A) The frequency of the failure of feedwater heater is assumed to be 0.02 events per year. This value is taken from an old report of initiating events used in PRAs (NUREG/CR-3862, 1985) and may include significant uncertainty. Such uncertainty may not be as important in the PRA as in the assessment of the frequency of FSAR Chapter 15 events. Please provide additional information to justify the robustness of the assumed frequency value.*

*(B) Additional information is needed for the staff to understand how the I&C systems were modeled in assessing the frequency of the "Loss of Feedwater Heating with Failure of Selected Control Rod Run-In" event. A simplified I&C block diagram, showing the processing of signals, important elements and design features (e.g., redundancy and diversity) and assumptions (e.g., independence and separation) for both automatic and manual actuation of components, would be very helpful. Such a simplified I&C block diagram could help answer staff questions, such as the following:*

*(1) It is stated that the failure probability of the FWCS controller to send the redundant signals to the Rod Control & Information System (RC&IS) equipment, following a loss of feedwater heater event, is judged to be negligible because the FWCS is required for continued plant operation. This assumes that the failure of the FWCS is immediately detected and there are no significant hardware or software common cause failures. Please explain the basis of such assumptions.*

*(2) It appears from the discussion that the RC&IS hardwired signals are back up to the RC&IS dual-redundant signals send to individual control rod logic equipment. However, in calculating the event frequency, the failure probabilities of these two events are added, instead of multiplied. Please clarify. In addition, please confirm that no operator action is required for the hardwired signals.*

**GE Response to Item A:**

**Introduction**

The NRC (NUREG/CR-5750 [1]) recognized a significant decrease in initiating event frequencies as a function of time. To demonstrate the approximate magnitude of this reduction in initiating event frequencies, a comparison is performed between the two principal initiating event studies:

NUREG/CR-3862 (1970-1983) [2]

NUREG/CR-5750 (1987-1995) [1]

### Problem Statement

Certain initiating event categories that were identified in NUREG/CR-3862 for quantification have subsequently been subsumed in NUREG/CR-5750 more general categories. For ESBWR, it is useful to point to the more refined categories in the previous report, NUREG/CR-3862. However, the previous data is known to have inflated frequencies relative to current plant performance.

### Purpose

The purpose of this assessment is to justify the initiating event frequencies for certain categories assessed in NUREG/CR-3862 using reasonable assumptions regarding trends of data to allow estimation of future initiating event frequencies.

### Analysis

This evaluation addresses the decreasing trend in industry initiating event frequencies. A factor of change is determined in this analysis by comparing two industry initiating event analyses that utilize data from two separate time periods. The analyses are NUREG/CR-3862 that evaluates data over approximately the 1970-1983 time period, and NUREG/CR-5750 that evaluates data over the 1987-1995 time period.

Table 15.0-21-1 compares the two analyses and their initiating event frequencies (per reactor year)<sup>(2)</sup> and calculates a factor of change. The NUREG/CR-3862 events are grouped and matched according to the corresponding NUREG/CR-5750 event category. For example, the Loss of Offsite Power (LOOP) category from NUREG/CR-5750 is matched with a similar LOOP category from NUREG/CR-3862, while the General Transient event category from NUREG/CR-5750 is matched with a combination of transient events from NUREG/CR-3862 (the sum of these event frequencies are compared to the single event frequency of the General Transient category from NUREG/CR-5750). The factor of change is determined by dividing the initiating event frequencies calculated from the earlier data period (NUREG/CR-3862) by the frequencies from the new data (NUREG/CR-5750). These change factors (reductions in initiating event frequencies) are listed in the last column of Table 15.0-21-1.

### Conclusion

Based upon the calculations of Table 15.0-21-1, the initiating event frequencies from NUREG/CR-5750 have significantly decreased from those found in NUREG/CR-3862. Each transient category shows a factor decrease of greater than approximately 4 for each event (except for a Total Loss of Feedwater Flow). The factor decrease for the sum of the initiating events is a factor of 5.68.

Therefore, it can be concluded that there is a significant downward trend in industry initiating event frequencies of a factor of greater than four (4).

---

<sup>(2)</sup> The NUREG/CR-5750 transient events are listed along with their associated frequencies per critical year. The calculated historical criticality factor of 0.75 from NUREG/CR-5750 is applied to each frequency to determine the frequencies on a per reactor year basis.

This comparative analysis supports the use of the NUREG/CR-3862 data for individual initiating event categories that are not segregated in NUREG/CR-5750. It further supports applying the conservative reduction factor of four (4) to estimate a projected future initiating event frequency.

Summary of Response to Item (A) Based on Above Analysis

The frequency for the transient "loss of feedwater heating" is not estimated in the latest NRC sponsored work in NUREG/CR-5750 "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995" [1] (the latest recognized generic initiating event frequency assessment).

Nevertheless, it is well recognized that the trend for initiating event frequencies has shown a steady decline since the 1980s when the NUREG/CR-3862 [2] data was collected. Generally, the initiating event frequencies have decreased by a factor of 4 or more.

This is sufficient to indicate that the future frequency for this initiating event is likely no higher than 0.02/yr (95% confidence upper bound) and is likely a factor of 4 lower, i.e., 5.0E-3/yr. Recognizing this trend in initiating event frequencies, reasonable engineering judgment based on these data trends supports the use of 0.02/yr as a conservative characterization of the Loss of Feedwater Heating initiating event frequency.

Table 15.0-21-1

**COMPARISON OF INITIATING EVENT FREQUENCIES CALCULATED FROM TWO DIFFERENT TIME PERIODS AND DETERMINATION OF THE TREND**

Category	NUREG/CR-5750 <sup>(2)</sup>			NUREG/CR-3862 <sup>(3)</sup>		
	Event Description	Frequency (per critical year)	Frequency <sup>(1)</sup> (per reactor year)	Event Description	Frequency (per reactor year)	Factor Decrease
1	Loss of Offsite Power	2.30E-02	1.73E-02	Loss of Offsite Power	8.00E-02	4.64
2	Stuck Open: 1 Safety/Relief Valve	4.70E-02	3.53E-02	Inadvertent Opening of a Safety/Relief Valve (Stuck)	1.40E-01	3.97
3	Inadvertent Closure of All MSIVs	3.30E-02	2.48E-02	Main Steam Isolation Valve Closure	2.70E-01	10.91
4	Loss of Condenser Vacuum	1.10E-01	8.25E-02	Loss of Normal Condenser Vacuum	4.10E-01	4.97
5	Turbine Bypass Unavailable	2.10E-03	1.58E-03	Turbine Bypass Fails Open	4.00E-02	297.14
				Turbine Bypass or Control Valves Cause Increased Pressure (closed)	4.20E-01	
				Electric Load Rejection With Turbine Bypass Valve Failure	4.00E-03	
				Turbine Trip with Turbine Bypass Valve Failure	4.00E-03	
				Total (Equals sum of the event frequencies for category 5)	4.68E-01	
6	Total Loss of Condenser Heat Sink	1.20E-01	9.00E-02	Total (Equals sum of categories 3, 4, and 5)	1.14E+00	12.67
7	Total Loss of Feedwater Flow	6.60E-02	4.95E-02	Loss of all Feedwater Flow	7.00E-02	1.41
8	General Transients (combined)	1.60E+00	1.20E+00	Electric Load Rejection	4.50E-01	
				Turbine Trip	8.70E-01	
				Inadvertent Closure of One MSIV	2.10E-01	
				Partial MSIV Closure	6.00E-02	
				Pressure Regulator Fails Open	8.00E-02	
				Pressure Regulator Fails Closed	1.00E-01	
8	General Transients (combined)			Recirculation Control Failure -- Increasing	1.80E-01	

Table 15.0-21-1

**COMPARISON OF INITIATING EVENT FREQUENCIES CALCULATED FROM TWO DIFFERENT TIME PERIODS AND DETERMINATION OF THE TREND**

		NUREG/CR-5750 <sup>(2)</sup>		NUREG/CR-3862 <sup>(3)</sup>		
Category	Event Description	Frequency (per critical year)	Frequency <sup>(1)</sup> (per reactor year)	Event Description	Frequency (per reactor year)	Factor Decrease
(cont'd)				Flow		
				Recirculation Control Failure -- Decreasing Flow	5.00E-02	
				Trip of One Recirculation Pump	6.00E-02	
				Trip of All Recirculation Pumps	3.00E-02	
				Abnormal Startup of Idle Recirculation Pump	2.00E-02	
				Recirculation Pump Seizure	4.00E-03	
				Feedwater -- Increasing Flow at Power	1.40E-01	
				Loss of Feedwater Heater	2.00E-02	
				Trip of One Feedwater Pump (or Condensate Pump)	2.00E-01	
				Feedwater -- Low Flow	4.90E-01	
				Low Feedwater Flow During Startup or Shutdown	1.20E-01	
				High Feedwater Flow During Startup or Shutdown	4.00E-02	
				Rod Withdraw at Power	1.00E-02	
				High Flux Due to Rod Withdrawal at Startup	5.00E-02	
				Inadvertent Insertion of Rod or Rods	6.00E-02	
				Detected Fault in Reactor Protection System	5.00E-02	
				Loss of Auxiliary Power (Loss of Auxiliary Transformer)	2.00E-02	
8	General Transients (combined)			Inadvertent Startup of HPCI/HPCS	1.00E-02	
(cont'd)				Scram Due to Plant Occurrences	5.80E-01	

Table 15.0-21-1

**COMPARISON OF INITIATING EVENT FREQUENCIES CALCULATED FROM TWO DIFFERENT TIME PERIODS AND DETERMINATION OF THE TREND**

		NUREG/CR-5750 <sup>(2)</sup>		NUREG/CR-3862 <sup>(3)</sup>		
Category	Event Description	Frequency (per critical year)	Frequency <sup>(1)</sup> (per reactor year)	Event Description	Frequency (per reactor year)	Factor Decrease
				Spurious Trip Via Instrumentation, RPS Fault	1.11E+00	
				Manual Scram -- No Out-of-Tolerance Condition	8.70E-01	
				Cause Unknown	6.00E-02	
				Total (Equals sum of the event categories for category 8)	5.94E+00	4.95
9	TOTAL	2.00E+00	1.50E+00		7.37E+00	5.68

(1) Frequency per reactor year is based upon the assumption of a criticality factor of 0.75 which is the NUREG/CR-5750 average for the BWR operating experience included in the model.

$$\text{Frequency/reactor year} = (\text{Frequency/critical year}) * \left( 0.75 \frac{\text{critical year}}{\text{reactor year}} \right)$$

(2) IE frequencies from NUREG/CR-5750 are taken from Table G-2.

(3) IE frequencies from NUREG/CR-3862 are taken from Table 33.

**GE Response to Item B:**

The mitigation systems to cope with a Loss of Feedwater Heating initiator have been modified to require failure of either Select Rod Insertion (SRI) or Selected Control Rod Run In (SCRRI). These systems are described in revised Section 15A.3.6.

Either method for inserting control rods failing will fail the mitigation function.

SRI will be assigned to different control rods versus SCRRI. There will be approximately 4 groups of SRI rods and 4 groups of SCRRI rods, with 4-32 rods per group.

The point is to have some rods insert fully fast (SRI) and some later, more slowly (SCRRI).

A simplified I&C diagram for the loss of FW heating with failure of selected control rod run-in is shown in Figure 15.0-21-1.

B(1) The FWCS can be postulated to have a latent failure that defeats its ability to sense the loss of FW heating. This potential common cause failure is added to the failure modes assessed in the RAI response to 15.0-25(B).

B(2) The treatment of the primary and backup signals is included in the revised calculation presented in response to RAI 15.0-25(B). No operator action is required for the hard-wired signals.

**Summary**

The Loss of Feedwater Heating with Failure of Selected Control Rod Run-in and Select Rod Insertion (Section 15A.3.6) is reassessed to incorporate more explicitly the items identified by the NRC in 15.0-21 and 15.0-25.

**References:**

- [1] Poloski, J.P., et al., for the U.S. Nuclear Regulatory Commission, "Rates of Initiating Events at U.S. Commercial Nuclear Plants; 1987 through 1995", NUREG/CR-5750, February 1999.
- [2] Mackowiak, D.P., et al., for the U. S. Nuclear Regulatory Commission, "Development of Transient Initiating Event Frequencies For Use in Probabilistic Risk Assessments", NUREG/CR-3862, May 1985.

**Affected Documents:**

DCD subsection 15A.3.6 and Table 15A-3 will be revised to reflect the addition of the SRI system to backup the SCRRI system.

### Loss of Feedwater Heating SCRRI & SRI

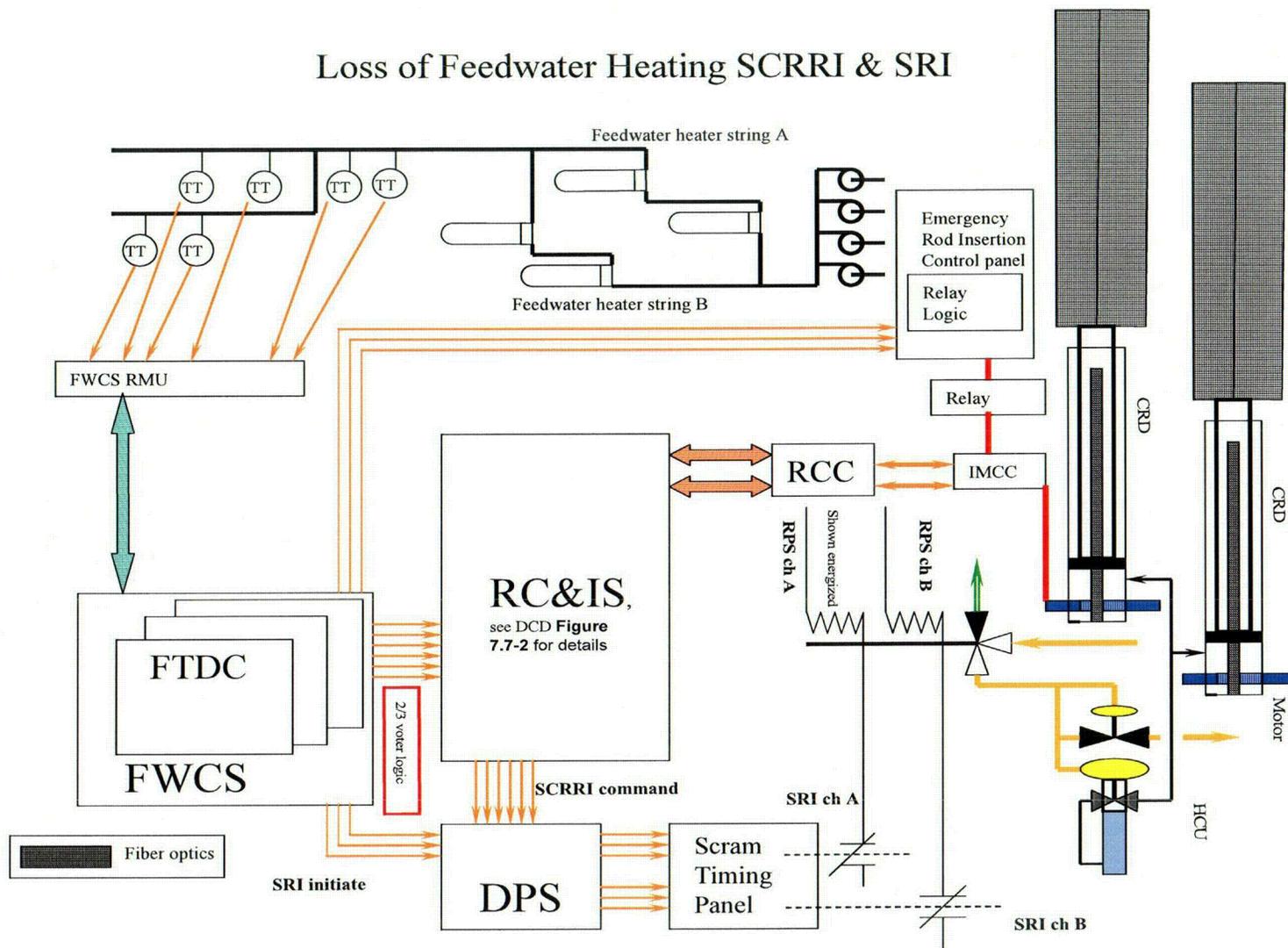


Figure 15.0-21-1 Loss of Feedwater Heating SCRRI & SRI

**NRC RAI 15.0-22:**

*Justify assumed interlock frequency (1E-3 per year) and operator error probability (1E-3) for "Inadvertent Shutdown Cooling Function Operation" (Section 15A.3.7).*

*The probability that the operator would inadvertently engage the RWCU/SDC system during power operation, given failure of the interlock feature, is assumed to be 1E-3. This may be a conservative value but no basis is provided in the analysis. It is stated that the RWCU/SDC system will have an interlock feature (no detailed design is available at this time) that will be shown (COL action item) to be single-failure proof. It is argued that the failure rate of a single-failure proof interlock feature is conservatively assessed to be 1E-3 per year. However, there is no basis provided to support the assumed interlock failure frequency. Additional justification is required. Alternatively, the proposed COL action item (to show that the interlock feature is single-failure proof) can be expanded to show, through a reliability analysis, that the mean time to failure (MTTF) is not higher than 1 in 1000 years, and to include the interlock in the D-RAP. Please discuss.*

**GE Response:**

This question relates to the frequency of Inadvertent Shutdown Cooling initiation. A technical basis is developed to provide a conservative characterization of the failure frequency assigned to the challenges to the SDC to RPV interface while the reactor is at power.

The postulated failure modes are identified in the fault tree of Figure 15.0-22-1 as follows (Top Gate SDC-E):

- Inadvertent SDC Function Initiation During Power Operations
- SDC Initiation During Interlock Testing (at-power)
- Valves Spuriously Open
- Automatic Actuation of SDC at-power

**Inadvertent SDC Function Initiation During Power Operations (SDC-E-F)**

This failure mode requires that the crew incorrectly manipulate the SDC controls while at-power and coincident with this that the interlock is failed. Gate: SDC-E-F describes this logic. The bases for the inputs to the logic diagram are as follows:

**Crew Error of Commission (SDOP-EOC-SDC--H--)**

Operating experience indicates that inadvertent operation of SDC while the reactor is at-power is unlikely. If we assume there are no such events that have occurred (assume 1 incipient failure) and there are 23 BWRs \* 20 years of operation, then the frequency of inadvertent SDC operation is less than 1/460 Rx Yr or 2.17E-03/RxYr.

$$F = 2.17E-03/RxYr$$

Alternatively, if we use the THERP analysis (NUREG/CR-1278 [1]) of the RWCU/SDC system and assume the SDC controls are not uniquely designated or

segregated from the RWCU controls, then the following errors could occur during a 2 year refuel period:

RWCU control manipulation once per week

Incorrect manipulation of the SDC controls 3E-3 (Table 20-12 Item (2) of NUREG/CR-1278)

Recovery from the inadvertent operation of the SDC controls 0.05 (Table 20-22 Item (3) of NUREG/CR-1278)

$$F = 52 \frac{\text{demands}}{\text{RxYr}} * 3E-03 * 5E-02 = 7.8E-03/\text{RxYr}$$

This can be approximated by 1E-2/RxYr as an upper bound.

#### Interlock Failure Probability (SDC-E-FA-C)<sup>(1)</sup>

The details of the SDC to RWCU interlock are not completed. The COL commitment is to provide a single failure proof interlock. A simplified model of the interlock is included to estimate a single failure proof design.

The failure probability of a single failure proof system can be estimated by a fault tree analysis. It is estimated here by two common cause failures:

Common cause miscalibration of sensors feeding the logic for the SDC interface valve logic estimated based on existing BWR PRAs and use of NUREG/CR-1278 [1] to be 8E-05.

Common cause failure of multiple logic circuits conservatively estimated as 1E-02/circuit and 0.05 common cause contribution.

#### SDC Initiation During Interlock Testing (at-power) (SDC-E-I)

The possibility of the SDC interlock being tested during power operation is considered remote. It is estimated as 0.1 probability per year. Given this test, the interlock is assumed bypassed. Coincident with this testing, the crew must incorrectly manipulate the valves for SDC. This treatment is under Gate SDC-E-I.

---

<sup>(1)</sup> There is a COL item in 15A.4 selected to providing a SDC interlock to prevent inadvertent SDC. The preliminary design of the interlock is as follows:

To prevent Inadvertent Shutdown Cooling Function Operation, the RWCU Shutdown mode is interlocked with Reactor operating mode to prevent increase in reactivity. During reactor normal Power operation operator cannot start or select the RWCU shutdown mode. Also additional interlocks are provided to prevent inadvertent operation of pumps at higher speed and higher flow and opening of RHX bypass valve. In all cases operator is alarmed if flow is higher than reactor normal operating mode flow when reactor is at power.

[Design description based on e-mail from Rasik Vagadia (GE) to Wingate, Gordon A. (GE Infra, Energy) and Poppel, Ira D. (GE Infra, Energy), dated February 3, 2007.]

This modeling is described as follows:

**SDIN-LOGICTST--:** This is the frequency that during power operation that the RWCU/SDC interlock would be in test. This frequency is judged small because the testing would likely be restricted to shutdown operational conditions, but is represented by a frequency of 0.1/yr.

**SDPH-RESPONSEH--:** This action is the conditional probability that during a test of the RWCU/SDC interlock while at-power the crew would be required to take actions to manipulate RWCU controls. Because these actions would likely be restricted during any such interlock tests, this conditional probability is judged to be quite low, but is conservatively estimated at 0.1.

**SDOP-SDCINIT-H--:** This is the Human Error Probability (HEP) that the crew while manipulating RWCU/SDC controls performs an incorrect series of operations that causes SDC initiation. This HEP is judged to be quite low based on the expected control design and expected crew training. Nevertheless, a conservative HEP of  $1E-2$  is used in the analysis. The error by the crew of  $1E-2$  is based on NUREG/CR-1278 Table 20-6 item (5).

#### Valves Spuriously Open (SDC-E-FA-V)

This gate is judged to double count the failure modes already addressed but is included at the design stage for completeness. It may subsequently be subsumed by more explicit modeling. The spurious open MOV frequency is  $5.0E-8/\text{hr}$  [2]. The CCF basic event is the frequency failure for the SDC function to inadvertently initiate given a full year of power operation (8760 hours). A conservative common cause factor of 0.1 (NRC common cause data is  $\sim 3E-2$  for 2 of 2 MOVs failing to operate) is applied and provides a result of  $5.00E-08/\text{hr} * 0.1 * 8760 \text{ hours/year} = 4.38E-05/\text{yr}$ .

#### Automatic Actuation of SDC At-Power (SDC-E-AUTO)

The SDC system is designed to automatically initiate given the following:

- Control rods fully inserted
- In addition to these initiation signals, the SDC interlocks must have failed. Gate SDC-E-AUTO provides the assessment of these combinations of failures.

Because of the preliminary nature of the design, the fault tree is rudimentary and the failure probabilities are upper bound estimates.

#### Result

The result of the fault tree analysis is a calculated frequency of inadvertent SDC operation at-power of approximately  $1.6E-04/\text{yr}$ , which includes interlock failure or bypass. The frequency of this failure is less than once in 6,250 years. Therefore, this event frequency meets the criterion for an infrequent event because it is less than once in 100 years. This is a conservative upper bound on the evaluation presented in section 15A.3.7.2 of the DCD. Therefore, this event frequency meets the criterion for an infrequent event because it is less than once in 100 years.

Section 15A.3.7.2 and Table 15A-3 of the DCD will be revised as needed to reflect these estimates and conclusions.

**References:**

- [1] Handbook of Human Reliability Analysis, NUREG/CR-1278
- [2] Eide, S.A. et al., Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs, EGG-SSRE-8875, February 1990.

**Affected Documents:**

DCD Tier (2), Figures will be added as 15A-3a, -3b, 3c and Subsection 15A.3.7, Table 15A-3, 15A.5 will be revised as needed.

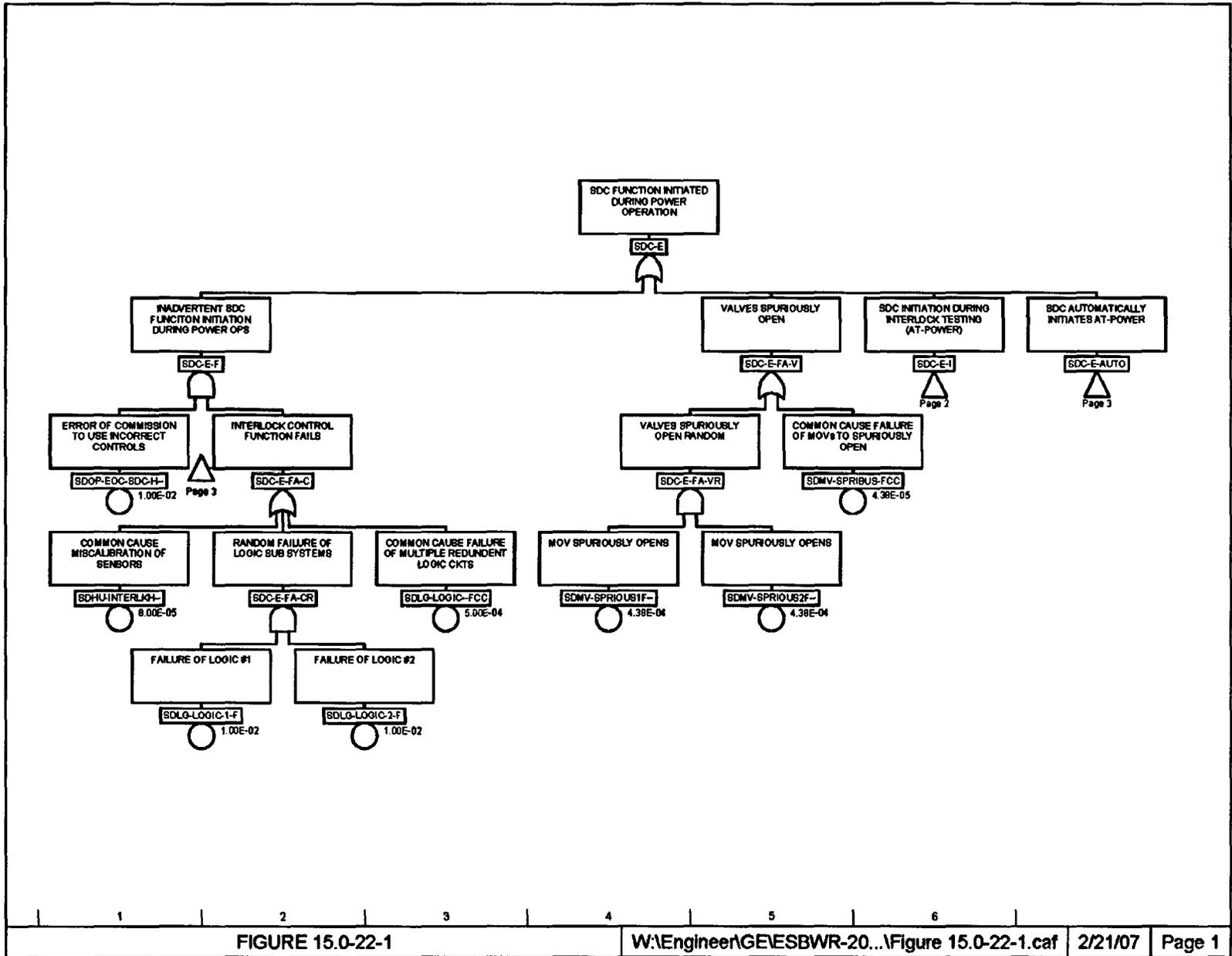


FIGURE 15.0-22-1

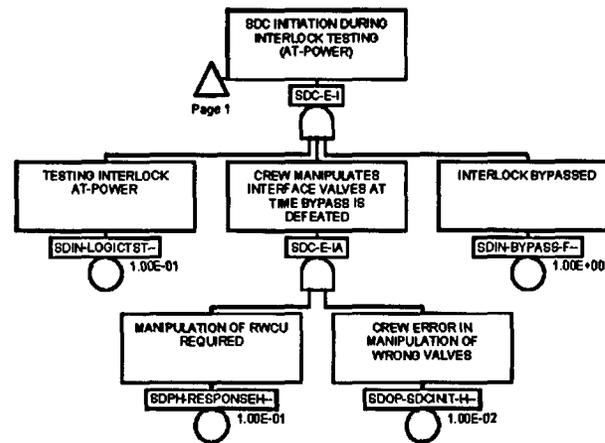


FIGURE 15.0-22-1

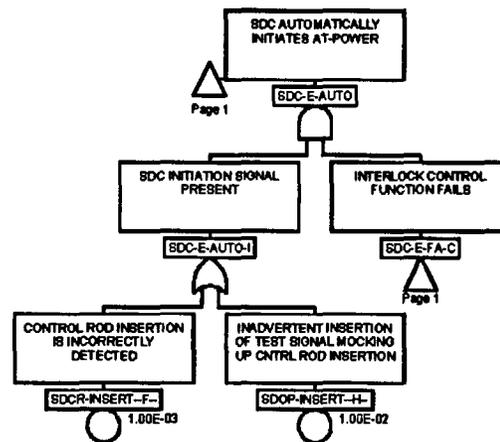


FIGURE 15.0-22-1

**NRC RAI 15.0-23:**

*Justify assumptions in frequency estimate for "Inadvertent Opening of a Safety/Relief Valve" frequency estimate (Section 15A.3.8).*

*Please provide additional information to justify and/or clarify assumptions and statements made in DCD Tier 2, Revision1, Sections 15A.3.8:*

*(A) It is stated (DCD Tier 2, Revision1, page 15A-12) that the probability of low setpoint setting or improperly locked setpoint spring, which goes undetected, is estimated to be negligible. However, no robust basis is provided to support this statement. Please provide historical data, if available, or use bounding arguments in a systematic analysis to estimate the probability of a human error that leads to an inadvertent opening of a relief valve (IORV) event.*

*(B) The probability of excess Nitrogen pressure leading to an IORV was estimated to be 1.5E-6 per year. This value is based on a proposed COL action item to confirm that no single failure in the nitrogen system can lead to IORV and the assumption of independence of failures. Please justify the assumption that no CCFs of the nitrogen supply system can lead to an IORV event. Otherwise assess the CCF contribution and revise the related probability. In addition, the assumed repair time of one week for a nitrogen supply system valve may not be a conservative value and needs to be justified in terms of requirements (e.g., Technical Specifications).*

*(C) It is stated (DCD Tier 2, Revision1, page 15A-12) that: "Per the analysis done for the DPV spurious actuation in Subsection 15A.3.9, the frequency of .....an IORV is 1.91E-04 per year." The staff could not find this frequency value in DCD Tier 2, Revision 1, Section 15A.3.9. Please explain.*

**GE Response to Item (a):**

There are three possible types of Inadvertent Opening of a Safety/Relief Valve (IORV) events that may be of interest:

- An IORV that occurs at power and leads to crew actions to close the valve and no subsequent challenge or shutdown results directly from the event.
- An IORV that occurs at power and results in sufficient associated issues that a manual or automatic scram is incurred, but eventually re-closes.
- An IORV that occurs at power and results in a scram but eventually re-closes.

Categories (b) and (c) are combined for this investigation. It is judged that events in Category (a) are not of interest and are not evaluated here.

The following failure modes are identified that may lead to an IORV:

Failure Modes	DCD Frequency (a)	Revised Frequency (b)	Revised Frequency References
Setpoint Error	0.0/yr	1E-4/valve/yr	NUREG/CR-1278 Table 20-7 Item (1) and Table 20-22 Item (4)
Vibration Induced	Not Identified	1E-5/valve/yr	Eng. Judg. <sup>(1)</sup>
Excess N <sub>2</sub>	1.5E-6/yr	2.29E-4/yr	See RAI 15.0-23(B)
Spring Relaxation	0.0/yr	Negligible	No change
Operator Error	0.0/yr	Negligible <sup>(2)</sup>	DCD 15A.3.9.2.1.2
Spurious Open Signal	1.9E-4/yr	6.0E-4/yr	DCD 15A.3.9 (Revised and summarized in RAI 15.0-23(C))

Failure frequencies associated with these failure modes are provided from: (a) DCD section 15A.3.9 ; and, (b) those that are recommended for use in calculating an upper bound frequency estimate of an IORV based on current BWR operating experience. This upper bound estimate is only for comparison purposes and to assess its impact on the categorization of the IORV event.

The total IORV frequency result given these failure modes when considered for the 18 installed SRVs is as follows:

Failure Mode	Upper Bound Frequency (per yr)
Setpoint Error	1.8E-03
Vibration Induced	1.8E-04
Excess N <sub>2</sub>	2.29E-04
Spring Relaxation	Negligible
Operator Error	Negligible
Spurious Open Signal	6.0E-04 (Applicable to 10 SRVs)
<b>TOTAL</b>	<b>2.81E-03</b>

<sup>(1)</sup> Operating experience with current SRVs in operating BWRs.

<sup>(2)</sup> The SRV inadvertent actuation due to operator error is evaluated in Section 15A.3.9.2.1.2 for the DPVs. The evaluation of operator error for the DPVs also applies to the SRV actuation due to operator error. The conclusion from this reassessment of operator error is that the probability of inadvertent opening of a DPV or an SRV due to operator error is insignificant compared with the probability of a spurious actuation signal.

Therefore, the upper bound frequency of 2.81E-03/yr still results in classification of the IORV as infrequent, i.e., less than 0.01/yr.

DCD Tier (2), Subsection 15A.3.8 will be revised to reflect this assessment as needed.

**GE Response to Item (b):**

The system for N<sub>2</sub> pressure to the SRVs has two pressure control valves in series. No single failure could be identified that would lead to SRV overpressurization. This configuration prevents a single random independent failure from causing overpressure to the SRVs.

The final design of the SRVs may result in a design that has the potential to open SRVs if a common cause failure of pressure control valves fail open causing nitrogen pressure to exceed 265 psig.

Figure 15.0-23(B)-1 summarizes the failure modes that may lead to SRV overpressurization including common cause failures.

**Random Independent Failures**

The pressure control valve failure rate is derived from NUREG/CR-4550 [15.0-23-2] as 5E-7/hr for transfer open that results in an annual failure frequency of 4.38E-3/yr.

The common cause failure of two pressure control valves transferring open results from applying a conservative 0.1 BETA factor to the independent failure frequency (4.38E-3/yr \* 0.1 = 4.38E-4/yr).

The most limiting upset sequence case is quantified at 2.19E-04/yr that includes this common cause failure probability. The overall failure probability (fault tree total) is 2.29E-04/yr and, therefore, the common cause failure of the pressure control valves upset contributes to ~95% of the IORV events occurring due to overpressurization.

**Repair Time**

The mean repair time for a valve from WASH-1400 [15.0-23-3] is 19 hours. For this calculation, a mean time to repair (MTTR) of 38 hours or twice that in WASH-1400 is used.

The probability of failure to repair,  $P_f = e^{-\lambda t}$

Where:

$$\lambda = 1/\text{MTTR} = 1/38 \text{ hrs.}$$

$$P_f = e^{-t/38 \text{ hrs}}$$

$$P_f = 1.2\text{E-}2$$

when  $t = 168$  hours

Therefore, it is found that there is a 98.8% probability of repair given the assumed 168 hour repair time. This is a conservative evaluation.

It is also noted that changes in the assumed repair time of factors of 2 or 3 make essentially no change in the calculated overall failure frequency of N<sub>2</sub> overpressure failure of the SRVs.

Conclusion

The revised total failure probability for SRV opening due to excess nitrogen pressure including the CCF is 2.29E-04/yr.

DCD Tier (2), Subsection 15A.3.8 will be revised to reflect this assessment as needed.

**Figure 15.0-23(B)-1**  
**SRV Overpressurization**  
**(2 Pages)**

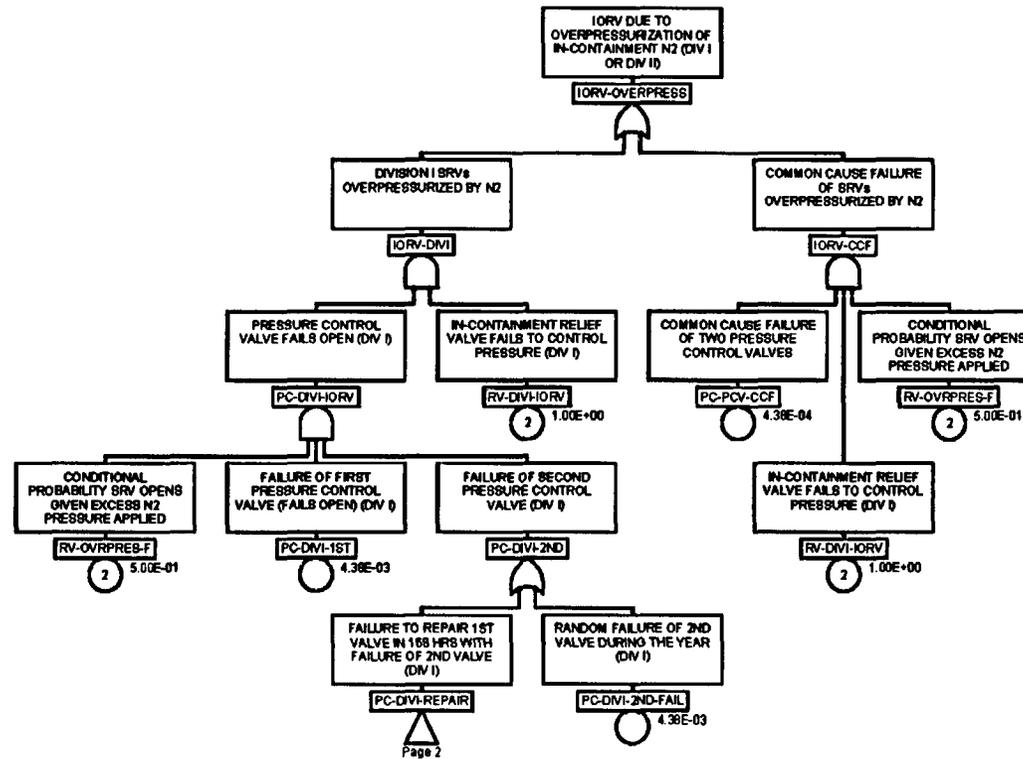
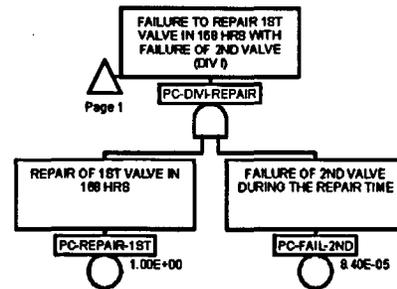


FIGURE 15.0-23(B)-1 SRV OVERPRESSURIZATION



**GE Response to item (C):**

DCD Tier 2, Revision 3, Subsection 15A.3.9 provides the quantification of the spurious opening of a DPV. This same approach is also used to assess the SRV spurious opening. The result of the calculation for the spurious opening of a DPV due to combinations of load driver and voter logic units is  $5.7E-04/\text{yr}$ . This analysis can be used to estimate the logic induced spurious opening of SRVs as approximately  $6E-4/\text{yr}$ .

This frequency is used in 15.0-23(A).

**Reference:**

- [15.0-23-1] Nonelectronic Parts Reliability Data, NPRD-95, Reliability Analysis Center, Rome Laboratory, Griffiss AFB, NY 13441-5700.
- [15.0-23-2] D.M. Ericson, Jr., Editor, et. al., Analysis of Core Damage Frequency Internal Events Methodology, NUREG/CR-4550, Vol. 1, Rev. 1, January 1990.
- [15.0-23-3] Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants Main Report, WASH-1400 (NUREG-75/014), October 1975.

**Affected Documents:**

DCD Tier (2), Subsections 15A.3.8, 15A.5 and Table 15A-3 will be revised to reflect this assessment as needed.

**NRC RAI 15.0-25:**

*Discuss the contribution of mechanical failures to the frequency of the events.*

*The contribution of mechanical failures to the frequency of the events is not discussed in many cases. Please discuss the reasons for not considering mechanical failures and clearly state any assumptions made in the analysis regarding mechanical failures.*

*(A) In discussing events "Pressure Regulator Failure - Opening of All Turbine and Control Bypass Valves" and "Pressure Regulator Failure - Closure of All Turbine Control and Bypass Valves" (DCD Tier 2, Sections 15A.3.1 and 15A.3.2, respectively), only the failure of the SB&PC Controller is considered. Please include a simplified flow diagram of the SB&PC system and discuss whether a mechanical failure of the Turbine Control Valves (TCVs) can cause opening or closure of all the Turbine Bypass Valves (TBVs).*

*(B) In discussing events "Loss of Feedwater Heating with Failure of Selected Control Rod Run-In" (DCD Tier 2, Section 15A.3-6) and "Control Rod Withdrawal Error - - during refueling, startup and power operation" (DCD Tier 2, Sections 15A.3.11, 15A.3.12 and 15A.3.13), mechanical failures are nowhere mentioned. In all of these cases a signal is sent to a system (or component) instructing it to perform a certain function but that system or component can be unavailable or fail mechanically.*

*Note: This question is related to RAIs 15.2-6, 15.2-8, and 15.2-10.*

**GE RESPONSE TO ITEM (A):**

Figures 15.0-25(A)-1 and 15.0-25(A)-2 provides the requested simplified flow diagrams for SB&PC.

It is correct that reliable control system design cannot preclude mechanical failures in the system being controlled. However, reliable control system design can significantly reduce the probability of failures that impact the entire system. In the case of the SB&PC system four Turbine Control Valves (TCVs) and twelve Turbine Bypass Valves (TBVs) are controlled. Single mechanical or control system failures can impact a single valve but only multiple failures causing failure of the SB&PC system can impact ALL valves. Therefore, a bounding subset of single valve events as AOOs (DCD Tier 2 Section 15.2) and a bounding subset of multiple failures that impact all valves as infrequent events (DCD Tier 2 Section 15.3) was analyzed. The evaluation of the bounding SB&PC system failure leading to infrequent events is found in DCD Tier 2 Subsections 15.3.3 through 15.3.6. The associated evaluation of the failure frequencies of the triplicated control system is presented in DCD Tier 2 Subsections 15A.3.1 through 15A.3.4. This DCD frequency analysis did not explicitly quantify multiple mechanical failures of all the valves to all open or all close at the same time because that probability is less than the probability of triplicated control system failures [15.0-25-1]. Therefore, the response to the RAI includes an evaluation of multiple mechanical failures. See below.

The response to RAI 15.2-8 [15.0-25-2] illustrates that the failures considered in AOO analysis envelope single mechanical and control system failures expected in the TCVs and TBVs. Note that no frequency evaluation is provided for these failures because they are evaluated in the highest frequency category, AOO.

Assessment of Mechanical Failures

**A. Pressure Regulator Failure – Opening of all Turbine Control and Bypass Valves**

For this event, the turbine control valves are open or partially open, but the TBVs are closed. In addition, the TBVs fail closed on loss of support systems.

No credible mechanical failures could be identified that would cause the opening of multiple, much less, all TBVs. There are, however, conservative probabilities for spurious opening of AOVs ( $5.0E-7/hr$ ) from NUREG/CR-4550. If these failure probabilities are used along with a conservative BETA factor of 0.01 for this failure mode, then the failure probability that would be added to the Control System failure of  $5E-4$  (developed in the DCD Subsection 15A.3.1) would be as follows:

Assume testing at each refueling:

TBV fail open failure rate:

$$\lambda T = 5.0E-7/hr * 8760 \text{ hrs/yr} = 4.38E-3/yr$$

F = Frequency of TBV fails open \* CCF of all TBVs Failing Open \* TCV Fail Open

$$F = 4.38E-3/yr * 0.01 * 3E-3/d$$

$$F_{Mech} = 1.31E-7/yr$$

This is negligible compared with the  $5E-4/yr$  frequency identified in the DCD Section 15A.3.1.

No changes to the DCD are required.

Affected Documents

None.

**B. Pressure Regulator Failure – Closure of all Turbine Control and Bypass Valves**

For this event, the turbine control valves are open or partially open, but the TBVs are closed. In addition, the TBVs fail closed on loss of support systems.

For this evaluation, an initiator of the TCV fail closed is assumed. This is based on the failure of either the turbine stop valve or turbine control valve to fail close.

Frequency of each =  $1.4E-7/hr$  from EPRI ALWR.

$$\text{Initiator Frequency} = 2 * (1.4E-7/hr * 8760 \text{ hr/yr}) = 2.45E-03/yr$$

Probability of TBVs fail closed (use 7 of 12 as the failure criteria) =  $4.4E-4/demand$

$$F = 2.45E-3/yr * 4.4E-4 = 1.1E-6/yr$$

This is negligible compared with the  $5E-4/yr$  frequency identified in the DCD Section 15A.3.1.

No changes to the DCD are required.

Conclusion

The mechanical failures are negligible contributors to the frequency determination for these events. Quantitative consideration of the mechanical failures would result in the frequency of both: (1) Pressure Regulator Failure with Opening of all Turbine and Control Bypass Valves; and, (2) Pressure Regulator Failure with Closure of all Turbine Control and Bypass Valves remaining classified as infrequent events with frequencies below 0.01/year.

References:

[15.0-25-1] RAI 15.2-6.

[15.0-25-2] RAI 15.2-8.

Figure 1 SB&PC Simplified Functional Block Diagram (Figure to be refined during COL)

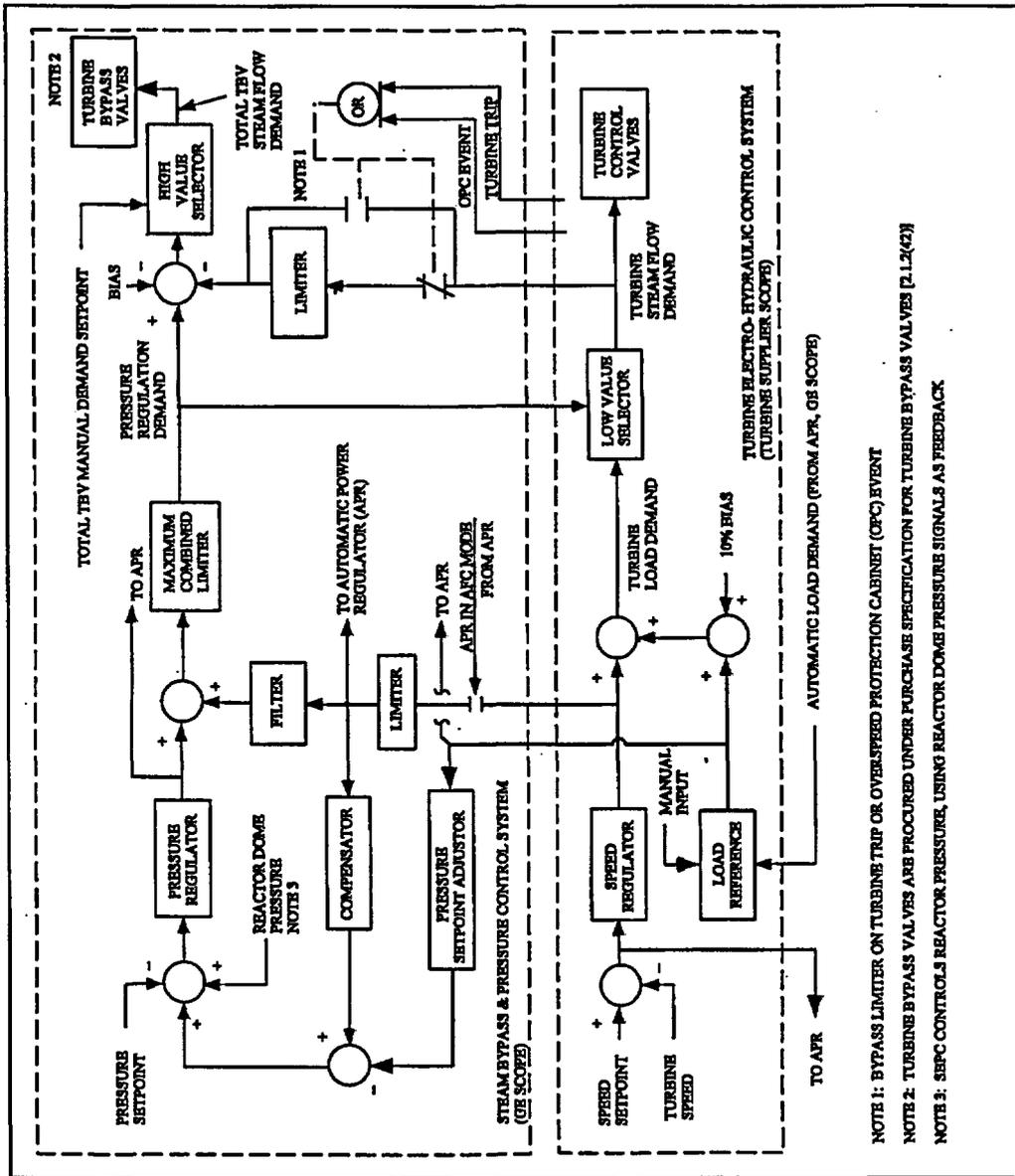


Figure 15.0-25(A)-1

Figure 8 Simplified Block Diagram of SB&PC FTDC and Supporting Components (To be refined during COL)

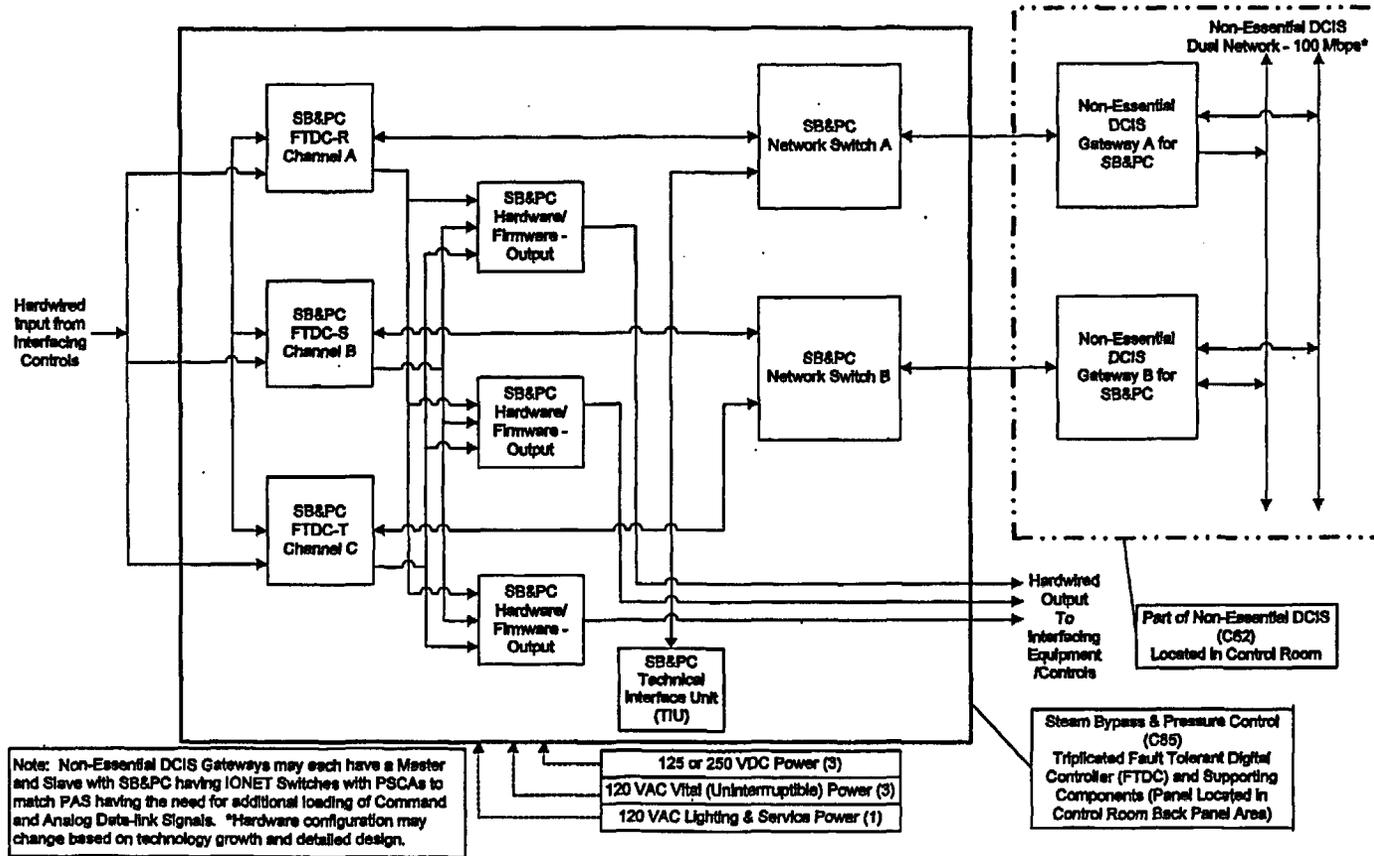


Figure 15.0-25(A)-2

**GE Response To Item B:**

Events "Loss of Feedwater Heating with Failure of Selected Control Rod Run-In" (DCD Tier 2, Section 15A.3-6) and "Control Rod Withdrawal Error - during refueling, startup and power operation" (DCD Tier 2, Subsections 15A.3.11, 15A.3.12 and 15A.3.13) have addressed control system failures as the dominant contributors to mitigation system failures.

Mechanical failures of components to operate could add some failure probability to the mitigation of the two identified "infrequent" events. This response provides an upper bound sensitivity assessment of possible mechanical failures that could add to the control system failures identified in the DCD, Appendix 15A.

**B.1 Loss of Feedwater Heating with Failure of Selected Control Rod Run-In (DCD Tier 2, Section 15A.3.6)**

The assessment of the mitigation capability given a loss of FW heating is estimated in Section 15A.3.6 of the DCD. This mitigation assessment is based on the failure of either of two functions: SCRRI or SRI. Failure of either method for inserting control rods would fail the mitigation function.

SRI will be assigned to different control rods versus SCRRI. There will be approximately 4 groups of SRI rods and 4 groups of SCRRI rods, with 4-32 rods per group.

The point is to have some rods insert fully fast (SRI) and some later, more slowly.

A simplified diagram of SCRRI and SRI is shown in Figure 15.0-21-1. (See RAI Response 15.0-21.)

The following discussion summarizes the prevention and mitigation failures that could lead to the Loss of Feedwater Heating with failure of selected control rod run in. These include:

- Random independent system failures
- Common logic or controller function failures
- Mechanical failures

**B.1.1 Random Independent System Failures**

Random independent system failures that could fail either of the two systems have not been assessed in detail at this stage of the design. Nevertheless, an estimate of the random independent logic or electrical failures that could defeat the system is estimated. Using values from current generation BWRs for logic and electrical support failures, results in a conservative estimate of system failure of 4E-3 per system. This conservative failure probability is used in estimating SRI and SCRRI independent failure probability:

System	Independent Failure Probability	Designator
SRI	4E-3	SRI-LOGIC
SCRRI	4E-3	SCRRI-LOGIC

**B.1.2 Common Logic or Controller Functions**

The common aspects of the failure modes for SCRRI and SRI are listed in the following table. The following table also compares the current DCD probability estimates with updated estimates of these failure probabilities that are also shown in the fault tree given in Figure 15.0-25-1.

Failures Accounted For	DCD 15A.3.6 Probability Estimate	DCD 15A.3.6 Revised Probability Estimate	Fault Tree Designator
Redundant Temperature Sensors	4.01E-5/d	4.01E-5/d	T-SIGNAL-F
FWCS Redundant Signals	ε	0.05	RWCS-SIG-F
RC&IS Controller Dual-Redundant	1E-3	1E-3	RCIS-SIG-F
Individual Rod Logic Panels to send hard wired signal to individual control rod logic	ε	1E-3	IRLF-SIG-F

The revised probability estimates are based on the following assessments:

**B.1.2.1 FWCS Redundant Signals**

For the upper bound sensitivity evaluation, the failure probability of the FWCS redundant signals are estimated at 0.05/d based upon possible common cause failures in the FWCS. This failure probability is multiplied by the redundant temperature sensor failure.

$$F_p = 4.01E-5/d * 0.05/d = 2.0E-6/d$$

**B.1.2.2 Hard Wired Signal**

For the hardwired signal, an upper bound circuit failure probability is estimated from IEEE-500 [15.0-25(B)-2]

$$F_p = 1E-3$$

**B.1.3 Control Rod Mechanical Failures**

Mechanical failure to insert control rods, from the previous DCD Subsection 15A.3.6 addressed failure to insert a large number of control rods as follows:

$$F_p = 1E-5$$

This estimate of mechanical control rods fail to insert is an assessment of the mechanical failure of a large number of control rods failing to insert consistent with NUREG-0460 and NUREG/CR-5500 Volume 3.

In addition, a sensitivity case that examines the impact of more conservative assumptions is developed in this response. The following postulated mechanical failure modes and their conservative failure probabilities are estimated to indicate the robust nature of the frequency estimate provided for the loss of feedwater heating with failure of selected control rod run-in.

Mitigation System	Failures Not Accounted For	Probability Estimate	Fault Tree Designator
SCRRI	Common Cause FMCRD Motor or Coupling Failures (Failure of 2 out of the Selected Control Rod Population demanded by SCRRI)	4.6E-2 <sup>(1)</sup>	FMCRD-F
SCRRI	Multiple Control Rods Stick (Fail to Insert two or more) (SCRRI Groups)	1E-2 <sup>(2)</sup>	SCRRI-CM-F
SRI	Common cause mechanical failure of multiple control rods to fail to insert from SRI group	1E-2 <sup>(2)</sup>	SRI-CM-F

- (1) Conservative estimate for common cause failure of frequently exercised motors. The conservative assessment is as follows:

$P_f$  = Failure of 2 or more FMCRD operating Successfully

Motor failure rate (standby) =  $1.0E-05/hr$

Time between "Tests" is monthly = 720 hrs.

CCF of a 2<sup>nd</sup> FMCRD failure = 0.1

32 rods/group

4 groups

Failure probability =  $P_{FMCRD}$

$$P_f = \lambda \frac{T}{2} * CCF * \frac{32 \text{ Combinations}}{\text{group}} * 4 \text{ groups}$$

$$P_f = 1E-5/hr * \frac{720 \text{ hrs}}{2} * 0.1 * 32 * 4$$

$$P_f = 4.61E-02$$

- (2) Operating experience at BWRs (conservative estimate).

#### B.1.4 Conclusion

The fault tree for the combined failure modes is given in Figure 15.0-25-1.

This leads to a total conditional mitigation failure probability of the control system and mechanical components of  $7.44E-2$  using the estimates for failure modes developed above in Section B.1.1, B.1.2, and B.1.3.

The frequency of the Loss of Feedwater Heating with the failure of Selected Control Rod Run-in is as follows:

$$F = \text{Loss of FW Heating} * \text{Failure of Control Rod Run-in}$$

Where,

$$\text{Loss of FW heating frequency} = 0.02/yr$$

Which is taken from Section 15A.3.6 and is also discussed in RAI Response 15.0-21.

The sensitivity evaluation to assess the upper bound effect of including mechanical component failures is an assessed frequency of

$$2E-2/yr * 7.44E-2 = 1.488E-3/yr$$

This remains below the AOO frequency of  $1E-2/yr$  and therefore this event remains classified as an infrequent event.

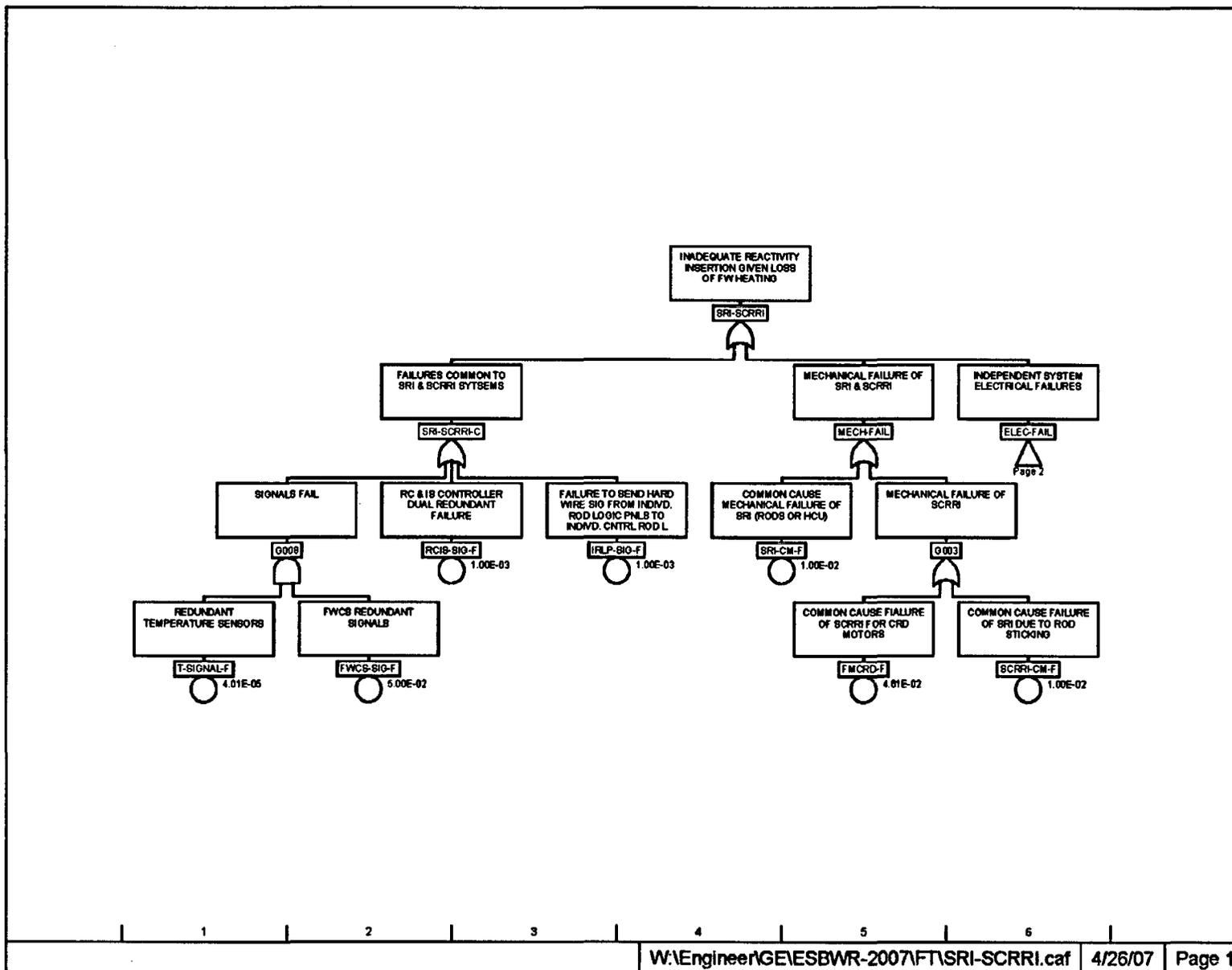


Figure 15.0-25-1 Fault Tree for Inadequate Reactivity Insertion Given a Loss of FW Heating (Page 1 of 2)

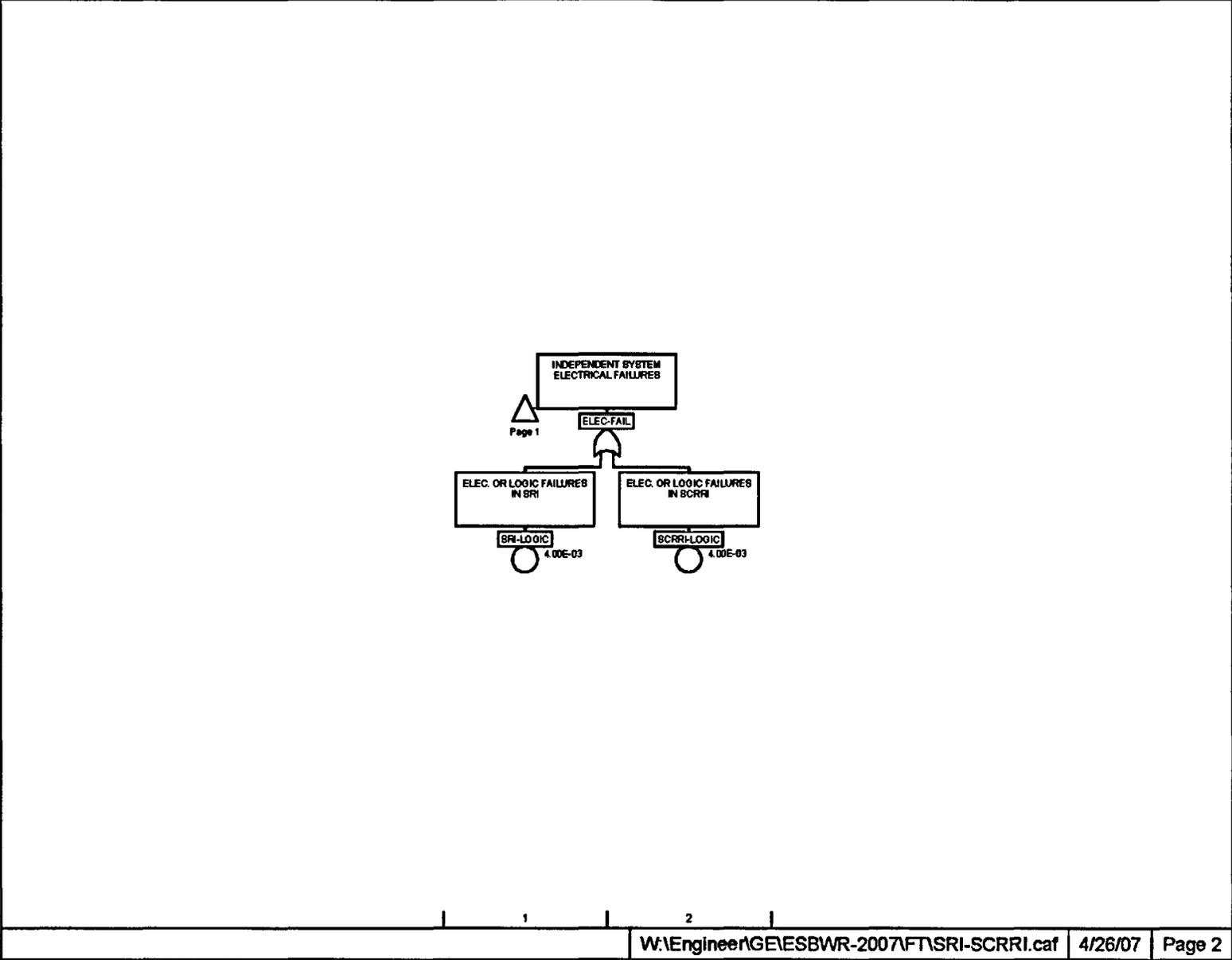


Figure 15.0-25-1 Fault Tree for Inadequate Reactivity Insertion Given a Loss of FW Heating (Page 2 of 2)

**B.2 Control Rod Withdrawal error during refueling, start up, and power operation (DCD Tier 2, Section 15A.3.11, 15A.3.12, 15A.3.13).**

The following discussion provides description of the interface with mechanical failures:

There are no identified mechanical components outside of the RC&IS whose failure has been identified that would result in a RWE.

The ESBWR FMCRDs are distinguished from the locking piston control rod drives (LPCRD) in that the control rods are moved electrically during normal operation. The LPCRDs are used in most BWRs prior to the ABWR, which uses the FMCRD. The FMCRD and LPCRD are inserted into the core hydraulically during emergency shutdown. However the FMCRD also has the electric motor to drive the control rod into the core even if the primary hydraulic system fails to do so.

Control rod insertion and withdrawal are controlled by the RC&IS. Some components of the RC&IS that involve mechanical type functions are relays (most of which are normally de-energized) and a few hard switches (pushbuttons in the control room). Mechanical failure of a single relay will not cause an inadvertent RWE. Additionally, failure of the contact of a single switch will not cause a RWE to occur. Therefore, the mechanically operated RC&IS equipment is single failure proof in regards to the RWE. Failure of electronic equipment in one channel of the dual redundant RC&IS equipment will not result in an inadvertent RWE, but could result in the inability to move the associated FMCRD by normal motor movement.

Several mechanical improvements to the CRD system are described here.

- The FMCRD is inserted hydraulically in response to a scram. Typical locking piston drives discharge the water from this type of hydraulic action in a scram discharge tank. This tank often causes maintenance and operational issues. The FMCRD discharges the volume of water to the reactor vessel thus eliminating the common mode failure source of the scram discharge tank.
- The FMCRD pistons have no seals, thus do not require maintenance.
- A pair of switches has been added to detect control rod separation. When the hollow piston is not properly seated on the ball nut or when the control rod separates from the hollow piston, a rod block is implemented.
- Latches have been added at axial intervals to prevent the control rod from dropping out of the core. There are also latches to hold the control rod full in after a scram until the ball-nut is run in to provide the normal support for the hollow piston and control rod.
- The control rod and hollow piston are coupled with a bayonet type coupling. This coupling is verified at refueling and during operation. The control rod can only be uncoupled from the FMCRD by relative rotation that is not possible during operation as it is always constrained between four fuel assemblies.

Electrical components that would be involved for a RWE to occur would be the FMCRD motor and brake. These are non-safety related components but have been qualified for operability by FMCRD design life testing. The brake is environmentally and seismically qualified to provide the holding function when not energized. If RWE occurs, the brake is electrically energized by the RC&IS (Rod Brake Controller) equipment.

RWE during refueling is prevented by ensuring subcriticality due to rod withdrawal interlocks and the shutdown margin in any given core configuration. A discussion of event probability is given in Chapter 15A. Since criticality is prevented, RWE during refueling will not be analyzed. Shutdown margin calculations are presented in DCD Section 4.3. In addition to ensuring subcriticality there are logics in RC&IS to prevent the withdrawal of more than one operable rod (i.e., all operable rods other than the one being withdrawn must be in full-in or rod block occurs). When in the SCRAM test mode of RC&IS, the RWM allows withdrawal of the two (or one rod for the central rod) rods associated with a single HCU. All other rods must be full-in for the movement of the two (or one) rods associated with one HCU to be withdrawn.

RWE at power is not analyzed due to the level of protection provided by the RWM and ATLM subsystems of RC&IS that terminate any spurious rod movement prior to operating limit violation. There are two RC&IS channels. Any disagreement between the two initiates a rod block (unless one is bypassed). Any one channel can signal rod block.

Detection of an out-of-sequence movement when the reactor power is below the Low Power setpoint by either channel of the RWM will cause an associated rod block to be enforced. If the spurious failure of one channel of RWM equipment is detected with the reactor below the Low Power Setpoint, with that channel not being bypassed, then a rod block is activated. The operator can bypass one channel of the RWM, but if the second channel is failed, then a rod block is activated. The operator can manually bypass one channel of the RWM; however, automatic control rod movement is prevented.

Above the Low Power Setpoint, the ATLM system monitors operating thermal limit protection function for either MCPR or MLHGR. The protection algorithms block further control rod withdrawal when there is potential for either (MCPR or MLHGR) operating limit to be violated. If spurious failure of one channel of ATLM equipment is detected with that channel not being bypassed, then a rod block is activated as with RWM. The operator can bypass one channel of the ATLM and if the second channel is failed then a rod block is initiated.

These systems are discussed in DCD Tier 2 Subsection 7.7.2.

RWE during startup has been identified as a COL Applicant Item.

The data for electronic system failure and the BETA factor used in frequency calculations for these events is from Reference 15.2-10-1 (Chapter 19, Table 19D.6-7, item Division 1 Transmission Network) as stated in DCD Tier 2 Subsection 15A.3.12.2.1. This reference documents the assessment of individual system failures.

### Conclusion

The mechanical failures are negligible contributors to the frequency determination for these events. Quantitative consideration of the mechanical failures would result in the frequency of Control Rod Withdrawal events remaining classified as infrequent events with frequencies below 0.01/year.

**References:**

- 15.0-25(B)-1 GE Nuclear Energy, "23A6100, ABWR Standard Safety Analysis Report"
- 15.0-25(B)-2 The Institute of Electrical and Electronics Engineers, Inc. (IEEE), "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations", IEEE Std. 500-1984.

**Affected Documents:**

The results of this RAI assessment are combined and incorporated in RAI 15.0-21 changes for DCD Tier (2), Subsections 15A.3.6.

**NRC RAI 15.4-21:**

*Section 4.4, "Main Steam Isolation Valve Leakage," of the General Electric Licensing Topical Report, NEDE-33279, "ESBWR Containment Fission Product Removal Evaluation Model, October 2006,"(LTR) states that the condensers are designed to meet the safe shutdown earthquake (SSE) requirements of the boiling water reactors owners group (BWROG) methodology.*

*DCD, Tier 1, Revision 2, Section 2.11.7, "Main Condenser," under "Design Description" states "the [main condenser] MC is classified as nonsafety-related. However, the supports and anchors for the MC are designed to withstand a safe shutdown earthquake [SSE]."*

*Please explain the discrepancy. If necessary, revise the DCD, Tier 1, Section 2.11.7, "Main Condenser," under "Design Description" to include that the MC must also be analyzed to the SSE loading conditions.*

**GE Response:**

No discrepancy exists between the GE Licensing Topical Report NEDE-33279 and DCD Tier 1 Subsection 2.11.7. The main condenser is used as a holdup volume for plateout and decay of fission products contained in MSIV leakage. The main condenser and the piping systems that comprise and are attached to the associated leakage path must be installed and fabricated such that they may be relied on in the event of a Safe Shutdown Earthquake (SSE).

The statement in NEDE-33279 "designed to meet the safe shutdown earthquake requirements of the boiling water reactors owners group (BWROG) methodology" may cause some misunderstanding as to compliance to the safe shutdown earthquake requirements. There is also potential for confusion with the requirements outlined in NRC approved documents related to this subject. Therefore, a review of pertinent documents for requirements and recommendations regarding condenser integrity, with respect to use of the isolated condenser method for MSIV leakage treatment, is provided in this response.

First, the statement from DCD Tier 1, Revision 2 quoted above in the text of the RAI was revised in DCD Tier 1, Revision 3 to state: "The MC is classified as nonsafety-related. However, the condenser supports and anchors are designed to *maintain condenser integrity* following a safe shutdown earthquake." This statement, when combined with piping design parameters outlined in DCD Tier 2, Revision 3, Figure 3.2-1, is consistent with NRC Paper SECY 93-087, entitled, "Policy, Technical, And Licensing Issues Pertaining To Evolutionary And Advanced Light-Water Reactor (ALWR) Designs." In this document, the authoring staff member(s) propose(s) that, ". . . seismic analyses be performed to ensure that the condenser anchorages and the piping inlet nozzle to the condenser are capable of maintaining their structural integrity during and after the SSE." Thus, with the statements made in the Design Description in DCD Tier 1 (and associated ITAAC), and the seismic category II design requirement for the drain and bypass piping to the condenser, this requirement is met.

GE Licensing Topical Report NEDE-33279, page 4-21, Section 4.4, "Main Steam Isolation Valve Leakage," 1st paragraph, second sentence, states, "To minimize the dose consequences from MSIV leakage many plants utilize a methodology developed by GE and the BWR Owner's Group (BWROG)." This methodology is documented in NEDO-31858, "BWROG Report for Increasing MSIV Leakage Rate Limits and Elimination of Leakage Control Systems." The

report continues this subject in the 3rd paragraph, 2nd sentence: "The condenser is of robust design, and it is designed to the Safe Shutdown Earthquake (SSE) requirements of the BWROG methodology."

The BWROG method of evaluating condenser design is outlined in NEDO-31858, Revision 2, "BWROG Report for Increasing MSIV Leakage Rate Limits and Elimination of Leakage Control Systems." In this document, several requirements for the condenser are listed. In short, seismic adequacy of the condenser is based on three design-related premises. First, empirical and historical data on condenser performance during seismic events is compiled in a database for the Seismic Qualification Utility Group (SQUG). The data shows that a range of condensers, including those not designed to resist earthquakes, exhibit substantial seismic ruggedness. Condensers similar in design to those in the database may therefore also be expected to withstand a Safe Shutdown Earthquake without gross structural failure. Secondly, the condenser is designed to industrial standards with significant margin. This margin results in a design that is unlikely to have the pressure boundary compromised by seismic events, i.e. the design is seismically rugged. Lastly, performing a plant-specific verification of the condenser's seismic adequacy provides reasonable assurance that the condenser will maintain structural integrity. The above design-related requirements are the basis of the BWROG methodology for ensuring condenser integrity following the Safe Shutdown Earthquake.

The ITAAC provided in DCD Tier 1, Revision 3, Section 2.11.7 related to condenser integrity states, "The condenser supports and anchors are designed to maintain condenser integrity following a safe shutdown earthquake." This design commitment is intended to confirm that the unit-specific condenser complies with the BWROG methodology for condenser seismic adequacy contained in NEDO-31858, Revision 2. Although this design commitment is consistent with the proposed requirements in SECY 93-087, the Design Description and ITAAC will be revised to provide clarity and obvious consistency with BWROG methodology.

The NRC's position and acceptance of the methodology presented in NEDO-31858, Revision 2, is provided in a Safety Evaluation Report ("Safety Evaluation By The Office of Nuclear Regulation, BWROG Generic Resolution For the BWR Main Steam Isolation Valve Leakage"). In this Report, the staff summarizes the condenser evaluation requirements in Section 5.7, stating that the BWROG methodology, "coupled with the plant-specific analytical evaluations for the condenser structural members and their associated anchorages, would provide an acceptable method to verify the seismic adequacy of the condenser design." In a later section of this same report, Section 6.0, the staff provides a limitation on use of NEDO-31858 methodology: "Individual licensees should demonstrate that the plant condenser design falls within the bounds of design characteristics found in the earthquake experience database."

In order to address the above limitation on use of NEDO 31858 and ensure that the licensee adheres to staff requirements, DCD Tier 1, Subsection 2.11.7 should address the NRC requirements associated with the above report and the staff's limitations on use of NEDO-31858 methodology. Therefore, the revision to this section in both the Design Description and associated ITAAC will address these limitations and requirements.

The proposed DCD revisions will require an analysis to confirm that the condenser structural members, supports, and anchors are designed to maintain condenser integrity following a Safe Shutdown Earthquake. The ESBWR Standard Plant condenser is a conventional, shell-and-tube, series, surface steam condenser. As a conventional condenser, it is expected to fall within the bounds of the design characteristics in the earthquake experience database. However, given the duty and resultant large size, it may not fall within these bounds. In addition, the DCD Tier 2 text allows the use of alternate condensers, such as one that may provide improved performance in the plant-specific environment. Therefore, acceptable means of performing the required analysis include evaluating the condenser design against the earthquake experience (SQUG) database and/or evaluating the structural members to ensure seismic adequacy, i.e. performing an analysis of the structural members to ensure that gross structural failure does not occur under SSE loading conditions.

**Affected Document Impact:**

DCD Tier 1, Section 2.11.7, Design Description, will be revised to include condenser structural members in the statement regarding condenser integrity following a Safe Shutdown Earthquake. In addition, an ITAAC will be provided that corresponds to the above statement. Finally, DCD Tier 2, Section 10.4.1.1.1 will be revised to maintain consistency with DCD Tier 1. These changes are provided on the attached markups.

**Enclosure 2**

**MFN 07-221**

**Response to Portion of NRC Request for Additional  
Information Letters, Nos. 77 and 90**

**Safety Analysis**

**DCD Markups**

**RAI Numbers 15.0-20 through 15.0-23, 15.0-25  
and 15.4-21**

## 10.4 OTHER FEATURES OF STEAM AND POWER CONVERSION SYSTEM

This section provides discussions of each of the principal design features of the Steam and Power Conversion System not described elsewhere in this chapter.

### 10.4.1 Main Condenser

The main condenser is the steam cycle heat sink. During normal operation, the main condenser receives, condenses, deaerates, and holds up for  $N^{16}$  decay, the main turbine exhaust steam. It performs the same functions for the turbine bypass steam whenever the turbine bypass system is operated. The main condenser is also a collection point for other steam cycle miscellaneous drains and vents.

The main condenser is utilized as a heat sink in the initial phase of reactor cooldown during a normal plant shutdown.

#### 10.4.1.1 Design Bases

##### 10.4.1.1.1 Safety (10 CFR 50.2) Design Bases

The main condenser does not perform, support or ensure any safety-related function, and thus has no safety bases. It is, however, designed with necessary shielding and controlled access to protect plant personnel from radiation. In addition, the main condenser hotwell provides a hold-up volume for MSIV fission product leakage. The condenser **structural members**, supports, and anchors are designed to maintain condenser integrity following a safe shutdown earthquake. [See Table 3.2-1 (N61).]

For evaluation against GDC 60, see Subsection 3.1.6.1.

##### 10.4.1.1.2 Non-Safety Power Generation Design Bases

- The main condenser is designed to function as the steam cycle heat sink and the collection point for miscellaneous drains and vents.
- The main condenser is designed to accommodate the turbine bypass steam flow following a full load rejection.
- The main condenser is designed to minimize air in-leakage and provides for the separation of noncondensable gases from the condensing steam and their removal by the main condenser air removal system (Subsection 10.4.2).
- At minimum normal operating hotwell water level, and normal full load condensate flow rate, the condenser provides a two-minute minimum condensate hold up time for  $N^{16}$  decay.
- The main condenser provides for deaeration of the condensate, such that condensate dissolved oxygen content does not exceed 15 ppb during normal operation above 50% load.
- The guidance provided in Reference 10.4-1 is considered in the condenser design.

## 2.11.7 Main Condenser

### Design Description

The Main Condenser (MC) condenses and deaerates the exhaust steam from the main turbine, provides a hold-up volume for  $N^{16}$  decay, provides a heat sink for the Turbine Bypass System (TBS), and is a collection point for other steam cycle drains and vents.

The MC hotwell provides a hold-up volume for main steam isolation valve (MSIV) fission product leakage.

The MC is classified as nonsafety-related. However, the condenser **structural members**, supports, and anchors are designed to maintain condenser integrity following a safe shutdown earthquake.

The MC is located in the Turbine Building.

The MC tubes are made from corrosion-resistant material.

The MC normally operates at a vacuum; consequently, air in-leakage is into the shell side of the MC. Circulating water leakage into the condenser shell is detected by measuring the conductivity of sample water extracted at select locations in the hotwell. In addition, conductivity monitor(s) in the condensate system provide alarms in the Main Control Room (MCR).

An increase in main condenser pressure above preset level(s) causes a MCR alarm, a turbine trip, reactor scram, bypass valve closure, and closure of the MSIVs.

### Inspections, Tests, Analyses and Acceptance Criteria

Table 2.11.7-1 provides a definition of the inspections, tests, and/or analyses, together with associated acceptance criteria for the Main Condenser.

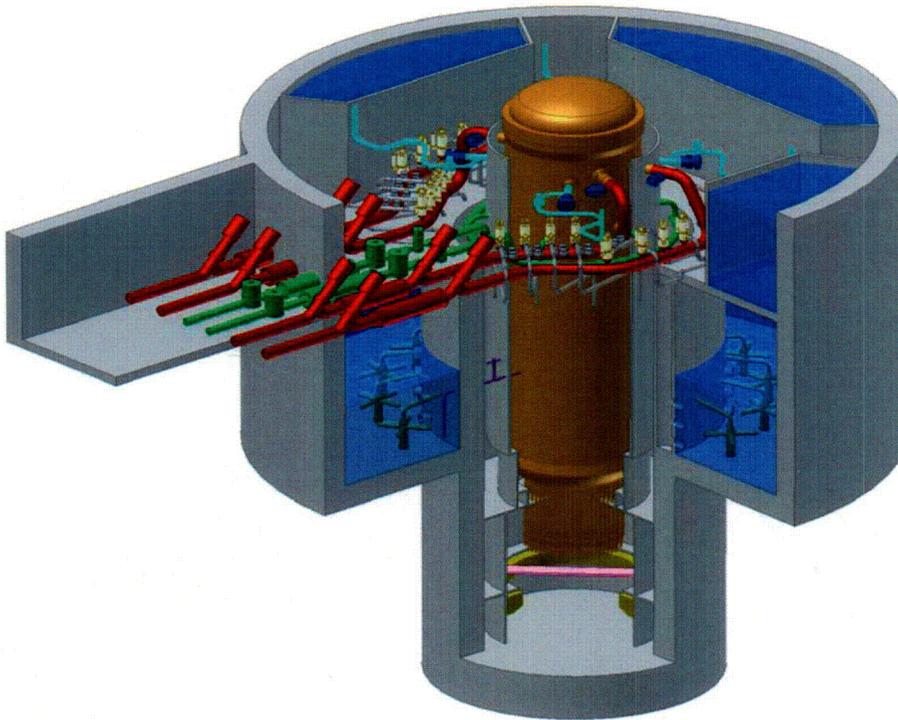
**Table 2.11.7-1**  
**ITAAC For The Main Condenser**

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
1. The condenser <b>structural members</b> , supports, and anchors are designed to maintain condenser integrity following a safe shutdown earthquake.	1. An analysis of the ability of the as-built condenser <b>structural members</b> , supports, and anchors to maintain condenser integrity following a safe shutdown earthquake will be performed.	1. An analysis report exists which concludes that the as-built main condenser <b>structural members</b> , supports, and anchors are able to maintain condenser integrity following a safe shutdown earthquake.
2. An increase in main condenser pressure above preset level(s) causes a MCR alarm, turbine trip, reactor scram, bypass valve closure, and closure of the MSIVs.	2. The main condenser pressure transmitters and associated logic will be tested with a simulated increase in main condenser pressure for HIGH condenser pressure function.	2. Tests of the main condenser pressure transmitters cause a MCR alarm, turbine trip, reactor scram, bypass valve closure, and closure of the MSIVs with a simulated increase in main condenser pressure above preset level(s).



**GE Energy Nuclear**

26A6642BP  
Revision 3  
February 2007



**ESBWR Design Control Document**  
**Tier 2**  
**Chapter 15**  
*Safety Analyses*



## 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.3.1.2 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. It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller 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.3.1.3 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. It is required that the Mean Time to Failure (MTTF) of the SB&PC Controller 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.3.3 Turbine Trip with Total Bypass Failure**

### ***15A.3.3.1 Introduction***

ESBWR is designed with 110% steam bypass capability, such that in case of a turbine trip event, the bypass valves open and send the steam to the main condenser thus avoiding a reactor trip. The bypass valves are part of the Turbine Bypass System (TBS) described in Subsection 10.4.4.

The TBS provides the capability to discharge main steam from the reactor to the condenser to minimize step load reduction transient effects on the Nuclear Boiler system. The outlets of TBVs are connected to the Main Condenser via piping with pressure reducers (orifice) to protect the condensers from overpressurization.

### ***15A.3.3.2 Analysis***

Turbine trip without bypass requires first a turbine trip to occur, and this is followed by failure of sufficient number of TBVs to open on demand. Turbine trip frequency is obtained from the ESBWR PRA. The failure of TBVs to open on demand depends upon the control signal failure, mechanical failure of TBVs to open and support system failure. Each of these items is discussed below:

**Turbine Trip Frequency:** The frequency of Generic Transients, 1.3 per year is conservatively assumed to represent the turbine trip frequency. The value is taken from Table 2.3-3 of Reference 15A-2.

**TBV Mechanical Failure:** Subsection 15.2.2.5 documents the safety analysis of the turbine trip with a single failure in the turbine bypass system. This analysis shows that even with a failure of 50% of the bypass capability, the safety analysis results are within acceptable limits. This means

that even with six of the twelve TBVs inoperable, results are within acceptable limits. Therefore, failure of seven or more out of twelve valves is considered unacceptable.

The ESBWR TBVs are designed to be significantly more reliable than the ones used in operating BWR and ABWR plants. The key improvement in the ESBWR TBVs is the use of separate hydraulic supply to each bypass valve (accumulator), such that no single hydraulic supply failure can cause multiple valves to open causing rapid depressurization of the reactor. This failure rate data is taken from the Reliability Data Base in Reference 15A-1. These also are the highest failure rate values of all types of valves in that database. The probability of random failure of seven valves, which involves the seventh power of a low number, is negligible compared to the common cause failure probability of seven valves. The common cause failure probability of seven valves is estimated by multiplying the individual TBV failure rate by a beta factor of 0.02. The value of 0.02 is judged to be a conservative value, especially since each valve is equipped with its own accumulator. Each group of 6 TBVs is actuated by hydraulic fluid from the main hydraulic lines. The hydraulic fluid for each group is isolated from other groups by check valves. If the hydraulic line for a particular group is lost for some reason, the accumulator in each of the TBVs is designed with sufficient capacity to open at least six times.. TBVs with individual accumulators is a design improvement made for the ESBWR and makes these TBVs less susceptible to common cause failures compared to the TBVs in operating BWR plants. The common cause failure probability is 0.02 times the TBV failure rate, which yields  $4.4E-4$  per demand.

**Signal Failure:** The TBVs are controlled by triple redundant signals from the Steam Bypass and Pressure Control System, whenever the actual steam pressure exceeds the preset steam pressure by a small margin. This occurs when the amount of steam generated by the reactor cannot be entirely used by the turbine. Triple-redundant, fault tolerant digital controllers (FTDC) using triplicated feedback signals from the reactor vessel dome pressure sensors generate command signals for the TBVs and pressure regulation demand signals used by the Turbine Generator Control System (TGCS) to generate valve position demand signals for the TCVs. The signal (instrumentation and control) reliability is generally significantly better than the mechanical component reliability. Since the controllers are required for continued plant operation, there is a high probability that the controller is available following a turbine trip event. The signal failure is judged to be negligible.

**Support System Failure:** The only relevant support system is the AC power and loss of AC power results in a different category of initiating event. Therefore, the failure of AC power is not considered in this evaluation.

**Operator action:** Operator action is not needed for TBVs to open and operator action cannot cause a failure of TBVs to open on demand. Therefore, operator error is not considered in this evaluation.

The failure probability of TBVs is  $4.4 E-4$  per demand, based on the above discussion.

#### **15A.3.3.3 Result**

The frequency of turbine trip without bypass event is evaluated as a product of the turbine trip frequency and probability of failure of TBVs. The event frequency = (1.3 events per year) ( $4.4E-4$  per demand) which is equal to  $5.72E-4$  per year. This translates to one event in over

1,700 years and therefore, the event frequency meets the criterion of being less than once in 100 years.

### 15A.3.4 Generator Load Rejection with Total Turbine Bypass Failure

#### 15A.3.4.1 Introduction

Following a load rejection, the Turbine Control Valves (TCVs) are commanded to close rapidly. At the same time the Steam Bypass and Pressure Control (SB&PC) System sends a signal to the Turbine Bypass Valves (TBVs) to open and throttle to maintain reactor pressure. The bypass valves are part of the Turbine Bypass System (TBS) described in Subsection 10.4.4. The SB&PC system is described in Subsection 7.7.5.

The TBS provides the capability to discharge main steam from the reactor to the condenser to minimize step load reduction transient effects on the Nuclear Boiler system. The outlets of TBVs are connected to the Main Condenser via piping with pressure reducers (orifice) to protect the condenser from over-pressurization.

#### 15A.3.4.2 Analysis

Generator load rejection with bypass failure event requires first a generator load rejection event to occur which is then followed by failure of sufficient number of TBVs to open on demand. The failure of TBVs to open on demand depends upon the control signal failure, mechanical failure of TBVs to open, and support system failure. Each of these items is discussed below.

Generator Load Rejection Frequency: The frequency of 0.45 per year is taken to represent the generator load rejection frequency. The value is taken from Table 9 of Reference 15A-5.

TBV Mechanical Failure: Subsection 15.2.2.5 documents the safety analysis of the turbine trip with a single failure in the turbine bypass system. This analysis shows that even with a failure of 50% of the bypass capability, the safety analysis results are within acceptable limits. This means that even with six of the twelve TBVs inoperable, results are within acceptable limits. Therefore, failure of seven or more out of twelve valves is considered unacceptable.

The ESBWR TBVs are designed to be significantly more reliable than the ones used in operating BWR and ABWR plants. The key improvement in the ESBWR TBVs is the use of separate hydraulic supply to each bypass valve (accumulator), such that no single hydraulic supply failure can cause multiple valves to open causing a rapid de-pressurization of the reactor. The probability of random failure of seven valves, which involves the seventh power of a low number, is negligible compared to the common cause failure probability of seven valves. The common cause failure probability of seven valves is estimated by multiplying the individual TBV failure rate by a beta factor of 0.02. The value of 0.02 is judged to be a conservative value, especially since each valve is equipped with its own accumulator. Each group of 6 TBVs is actuated by hydraulic fluid from the main hydraulic lines. The hydraulic fluid for each group is isolated from other groups by check valves. If the hydraulic line for a particular group is lost for some reason, the accumulator in each of the TBVs is designed with sufficient capacity to open at least six times. TBVs with individual accumulators is a design improvement made for the ESBWR and makes these TBVs less susceptible to common cause failures compared to the TBVs in operating BWR plants. The common cause failure probability is 0.02 times the TBV failure rate, which yields 4.4 E-4 per demand.

Signal Failure: The TBVs are controlled by triple redundant signals from the Steam Bypass and Pressure Control System, whenever the actual steam pressure exceeds the preset steam pressure by a small margin. This occurs when the amount of steam generated by the reactor cannot be entirely used by the turbine. Triple-redundant, fault tolerant digital controllers (FTDC) using triplicated feedback signals from the reactor vessel dome pressure sensors generate valve position command signals for the TBVs and pressure regulation demand signals used by the Turbine Generator Control System (TGCS) to generate demand signals for the TCVs. The signal (instrumentation and control) reliability is generally significantly better than the mechanical component reliability. Since the controllers are required for continued plant operation, there is a high probability that the controllers are available following a turbine trip event. The signal failure probability is judged to be negligible.

Support System Failure: The only relevant support system is the AC power and loss of AC power results in a different category of initiating event. Therefore, the failure of AC power is not considered in this evaluation.

Operator action: Operator action is not needed for TBVs to open and operator action cannot cause a failure of TBVs to open on demand. Therefore, operator error is not considered in this evaluation.

The failure probability of TBVs is  $4.4 \text{ E}^{-4}$  per demand, based on the above discussion.

#### **15A.3.4.3 Result**

The frequency of generator load rejection with bypass failure is evaluated as a product of the generator load rejection frequency and probability of failure of TBVs. The event frequency =  $(0.45 \text{ events per year}) \times (4.4 \text{ E}^{-4} \text{ per demand})$  which is equal to  $1.98 \text{ E}^{-4}$  per year. This translates to one event in over 5,000 years and therefore, the event frequency meets the criterion of 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. It is required that the Mean Time to Failure (MTTF) of the Feedwater System Controller 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.3.6 Loss of Feedwater Heating with Failure of Selected Control Rod Run-In and Select Rod Insertion**

#### **15A.3.6.1 Introduction**

The loss of feedwater heating causes the feed temperature to go down which increases the reactivity level. The ESBWR is designed such that the loss of feedwater results in insertion of selected control rods, so the reactivity level is adjusted appropriately. The failure of feedwater heating followed by the failure of the selected control rods to insert is the event of concern. **The assessment of the mitigation capability given a loss of FW heating is estimated based on the failure of either of two functions: SCRRI or SRI. Failure of either method for inserting control rods would fail the mitigation function.**

#### **15A.3.6.2 Analysis**

The loss of feedwater heating can occur at any given time during normal power range operation (e.g. the feedwater heaters are not operational during low power startup/shutdown conditions when the main turbine is not operational). When this event happens, the feedwater temperature goes down. This is detected by redundant temperature sensors in the feedwater piping lines that lead to the reactor pressure vessel that provide input signals to the Feedwater Control System (FWCS). The description of the FWCS is provided in Subsection 7.7.3. The primary purpose of the FWCS is to maintain proper reactor pressure vessel water level in the operating range. In addition, the FWCS sends signals to the Rod Control and Information System (RC&IS), via the Nonsafety DCIS equipment to insert selected control rods to mitigate the consequence of the loss of feedwater heating event. The description of the RC&IS is provided in Subsection 7.7.2. The

RC&IS equipment in the control room back panel area sends signals to individual control rod logic implemented in the local RC&IS equipment in the reactor building in order to complete the run-in of each of the selected control rods to its associated, pre-defined Selected Control Rod Run-In and Select Rod Insertion (SCRRI/SRI) target position.

The RC&IS is equipped with dual-redundant, digital controller equipment including power supplies, and input/output signals. The design consists of two parallel processing channels, each containing the hardware and software for execution of the control algorithms. The controller equipment is designed to a high degree of reliability.

The RC&IS is also equipped with an Emergency Rod Insertion Control Panel and two associated Emergency Rod Insertion Panels that provide a parallel, redundant set of hardwired-based relay logic that also receives redundant signals from the FWCS (via the Nonsafety-Related DCIS equipment) when the loss of feedwater heating event is detected. For each control rod, one hardwired signal is provided from an associated Emergency Rod Insertion Panel to the individual control rod logic equipment that also must be activated in order for the individual local control rod logic to accomplish the selected control rod run-in of that control rod.

Therefore, in order to accomplish the selected control rod run-in of an individual control rod, the dual-channel logic must send the required command signals to the individual local control rod logic; and the Emergency Rod Insertion Panel must send the hardwired discrete signal to the individual local control rod. For the dual-redundant logic portion, if one channel is manually bypassed or if an operational channel detects the other channel has failed, there is logic in the operational channel that accomplishes bypass of the other channel so that the selected run-in function can still be accomplished as long as the hardwired discrete signal from the Emergency Rod Insertion Panel is operable. For this analysis it is assumed that, if a failed redundant channel situation exists, it has been manually bypassed by the operator to allow continued plant operation.

In parallel with the SCRRI the RC&IS will generate a Select Rod Insert (SRI) signal that will be processed through an independent path in the Diverse Protection System (DPS) and then through the Scram Timing Panels to pre set selection switches for the rod pairs that will be scrambled in using the scram solenoids.

Failure of the power supply to the individual rod controller equipment can also cause this failure event, but it is not considered in this analysis since it is considered to be a more significant initiating event, which is addressed separately in the design.

Failure of the Feedwater Heating: The frequency of feedwater heater failure in BWR plants is 0.02 per year based on operating experience, as reported in Table 9 of Reference 15A 5, the trend for initiating event frequencies has shown a steady decline since the 1980s when the Reference 15A 5 data was collected. Generally, the initiating event frequencies have decreased by a factor of 4. This is sufficient to indicate that the future frequency for this initiating event is likely no higher than 0.02/yr (95% confidence upper bound) and is likely a factor of 4 lower, i.e., 5 E-3/yr. Recognizing this trend in initiating event frequencies, reasonable engineering judgment based on these data trends supports the use of 0.02/yr as a conservative characterization of the Loss of Feedwater Heating initiating event frequency.

Failure of Temperature Sensors: The failure of the redundant temperature sensors to detect the loss of feedwater heater(s) is estimated to be small. The failure rate of a temperature transmitter is  $3.5E-7$  per hour, as documented in Table A.3-1 of Reference 15A-1. Even though the temperatures are displayed in the main control room, no credit is taken in this analysis for detection by the operator of sensor failure. Assuming that these sensors are tested during refueling outages every two-years, the probability that each sensor is unavailable is failure rate times the test interval divided by two =  $(3.5 E-7)*(17,520 / 2) = 3.07 E-3$ . The probability that both sensors fail upon demand is the product of unavailability of individual sensors, which is equal to  $(3.07 E-3)*(3.07 E-3) = 9.42 E-6$  per demand. In addition, common cause failure (CCF) is estimated based on a beta factor of 0.01. Thus the unavailability due to CCF is  $(0.01)*(3.07 E-3) = 3.07 E-5$  per demand. The combined unavailability =  $9.42 E-6 + 3.07 E-5$  per demand, which is equal to  $4.01 E-5$  per demand.

Failure of FWCS: Since the FWCS is required for continued plant operation, there is a high probability that the controller is available following a loss of feedwater heater event. The failure of the FWCS to generate the select control rod run-in signals (and provide the redundant signals to the RC&IS equipment via the Nonsafety-Related (DCIS)) is judged to be negligible. **However to establish an upper bound failure probability sensitivity the FWCS redundant signals are estimated at 0.05/d based upon possible common cause failures in the FWCS. This failure probability is multiplied by the redundant temperature sensor failure.**

- $FP = 4.01E-5/d * 0.05/d = 2.0E-6/d$

Failure of RC&IS Dual-redundant Channel Signals: The RC&IS has dual-redundant controller equipment of which only one is required for continued plant operation. When a failure occurs in one of the controllers, the failure is announced and the other controller continues to operate **thus** the plant operator can bypass the failed equipment and then repair or replace the failed part. For the RC&IS to fail, the second failure has to occur during the time when the first failed controller is being repaired while in the bypass condition, generally within a shift. The failure of the both controllers in this short period is very low, especially compared to the hardwired signal, which is also required – see below.

Failure of RC&IS Hardwired Signals (via the Emergency Rod Insertion Control Panel and Emergency Rod Insertion Panels): The RC&IS provides hard-wired signals to individual control rod logic equipment. Even though the failure of this signal not to actuate when required is not announced, failure of one hard-wired signal only impacts the run-in function for one control rod and redundant relays are used for actuation of each hardwired output signal to the individual control rod logic equipment. The failure probability of the hard-wired signal is conservatively estimated to be better than, (i.e., lower than), 0.001 per demand. (For reference, failure rate of a single relay is  $1.0E-4$  for demand). A detailed analysis is expected to show a much better, (i.e., lower), number.

Failure of Individual Control Rod Logic Equipment to Insert Selected Rods: The capability for movement of all control rods by the individual control rod logic equipment is tested during the monthly double-notch movement surveillance testing. Therefore, the only credible failure mode that prevents multiple control rods from being inserted upon command is considered to be loss of electrical power. However, the loss of power is a separate event, with associated alarm logic, analyzed more conservatively and is therefore not considered here.

The following discussion summarizes the prevention and mitigation failures that could lead to the Loss of Feedwater Heating with failure of selected control rod run in. These include:

- Random independent system failures
- Common logic or controller function failures
- Mechanical failures

#### Random Independent System Failures

Random independent system failures that could fail either of the two systems have not been assessed in detail at this stage of the design. Nevertheless, an estimate of the random independent logic or electrical failures that could defeat the system are estimated. Using values from current generation BWRs for logic and electrical support failures, results in a conservative estimate of system failure of 4E-3 per system. This conservative failure probability is used in estimating SRI and SCRRI independent failure probability:

System	Independent Failure Probability	Designator
SRI	4E-3	SRI-LOGIC
SCRRI	4E-3	SCRRI-LOGIC

The common aspects of the failure modes for SCRRI and SRI are listed in the following table.

Failures Accounted For	Probability Estimate	Fault Tree Designator
Redundant Temperature Sensors	4.01E-5/d	T-SIGNAL-F
FWCS Redundant Signals	0.05	RWCS-SIG-F
RC&IS Controller Dual-Redundant	1E-3	RCIS-SIG-F
Individual Rod Logic Panels to send hard wired signal to individual control rod logic	1E-3	IRLF-SIG-F

**Mechanical** failure of more than one control rod to insert when commanded is estimated based on the following:

Mitigation System	Failures Not Accounted For	Probability Estimate	Fault Tree Designator
SCRRI	Common Cause FMCRD Motor or Coupling Failures (Failure of 2 out of the Selected Control Rod Population demanded by SCRRI)	4.6E-2 <sup>(1)</sup>	FMCRD-F
SCRRI	Multiple Control Rods Stick (Fail to Insert two or more) (SCRRI Groups)	1E-2 <sup>(2)</sup>	SCRRI-CM-F
SRI	Common cause mechanical failure of multiple control rods to fail to insert from SRI group	1E-2 <sup>(2)</sup>	SRI-CM-F

(1) Conservative estimate for common cause failure of frequently exercised motors. The conservative assessment is as follows:

For the SCRRI function - Common Cause FMCRD Motor or Coupling Failures (Failure of 2 out of the Selected Control Rod Population demanded by SCRRI)

Pf = Failure of 2 or more FMCRD operating Successfully

Motor failure rate (standby) = 1.0E-05/hr

Time between "Tests" is monthly = 720 hrs.

CCF of a 2nd FMCRD failure = 0.1

32 rods/group

4 groups

Failure probability = PFMCRD

$$Pf = \lambda \frac{T}{2} * CCF * \frac{32 \text{ Combinations}}{\text{group}} * 4 \text{ groups}$$

$$Pf = 1E-5/\text{hr} * \frac{720 \text{ hrs}}{2} * 0.1 * 32 * 4$$

$$Pf = 4.61E-02$$

(2) Operating experience at BWRs (conservative estimate)

For the SCRRI function - Multiple Control Rods Stick (Fail to Insert two or more) (SCRRI Groups) 1E-2 based on Operating experience at BWRs (conservative estimate)

For the SRI function - Common cause mechanical failure of multiple control rods to fail to insert from SRI group 1E-2 based on Operating experience at BWRs (conservative estimate).

The fault tree for the combined failure modes is given in Figure 15A-4.

This leads to a total conditional mitigation failure probability of the control system and mechanical components of  $7.44\text{E-}2$ .

The frequency of the event of concern is obtained by multiplying the frequency of loss of FW heater (0.02/year), by the probability of failure of **the total conditional mitigation failure probability**.

The event frequency =  $(0.02) * (7.44\text{E-}2) = 1.488\text{E-}3$  per year. This translated to one failure in more than 600 years.

### **15A.3.6.3 Result**

The frequency of the failure of feedwater heating followed by the failure of the selected control rods to insert is less than once in more than 600 years and therefore, this 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. 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 postulated failure modes are identified in the fault tree of Figure 15A-3a as follows (Top Gate SDC-E):

**Inadvertent SDC Function Initiation During Power Operations**

**SDC Initiation During Interlock Testing (at-power)**

**Valves Spuriously Open**

**Automatic Actuation of SDC at-power**

**Inadvertent SDC Function Initiation During Power Operations (SDC-E-F)**

This failure mode requires that the crew incorrectly manipulate the SDC controls while at-power and coincident with this that the interlock is failed. Gate: SDC-E-F describes this logic. The bases for the inputs to the logic diagram are as follows:

Crew Error of Commission (SDOP-EOC-SDC--H--)

Operating experience indicates that inadvertent operation of SDC while the reactor is at-power is unlikely. If we assume there are no such events that have occurred (assume 1 incipient failure) and there are 23 BWRs \* 20 years of operation, then the frequency of inadvertent SDC operation is less than 1/460 Rx Yr or 2.17E-03/RxYr.

$$F = 2.17E-03/RxYr$$

Alternatively, if we use the THERP analysis Reference 15A-7 of the RWCU/SDC system and assume the SDC controls are not uniquely designated or segregated from the RWCU controls, then the following errors could occur during a 2 year refuel period:

RWCU control manipulation once per week

Incorrect manipulation of the SDC controls 3E-3 (Table 20-12 Item (2) of Reference 15A-7)

Recovery from the inadvertent operation of the SDC controls 0.05 (Table 20-22 Item (3) of Reference 15A-7)

$$F = 52 \frac{\text{demands}}{\text{RxYr}} * 3E-03 * 5E-02 = 7.8E-03/RxYr$$

This can be approximated by 1E-2/RxYr as an upper bound.

Interlock Failure Probability (SDC-E-FA-C)

The details of the SDC to RWCU interlock are not completed. The COL commitment is to provide a single failure proof interlock. A simplified model of the interlock is included to estimate a single failure proof design.

The failure probability of a single failure proof system can be estimated by a fault tree analysis. It is estimated here by two common cause failures:

Common cause miscalibration of sensors feeding the logic for the SDC interface valve logic estimated based on existing BWR PRAs and use of Reference 15A-7 to be 8E-05.

Common cause failure of multiple logic circuits conservatively estimated as 1E-02/circuit and 0.05 common cause contributions.

SDC Initiation During Interlock Testing (at-power) (SDC-E-I)

The possibility of the SDC interlock being tested during power operation is considered remote. It is estimated here as 0.1 probability per year. Given this test, the interlock is assumed bypassed. Coincident with this testing the crew must incorrectly manipulate the valves for SDC. This treatment is under Gate SDC-E-I.

This modeling is described as follows:

SDIN-LOGICTST--: This is the frequency that during power operation that the RWCU/SDC interlock would be in test. This frequency is judged small because the testing would likely be restricted to shutdown operational conditions, but is represented by a frequency of 0.1/yr.

**SDPH-RESPONSEH--:** This action is the conditional probability that during a test of the RWCU/SDC interlock while at-power the crew would be required to take actions to manipulate RWCU controls. Because these actions would likely be restricted during any such interlock tests, this conditional probability is judged to be quite low, but is conservatively estimated at 0.1.

**SDOP-SDCINIT-H--:** This is the Human Error Probability (HEP) that the crew while manipulating RWCU/SDC controls performs an incorrect series of operations that causes SDC initiation. This HEP is judged to be quite low based on the expected control design and expected crew training. Nevertheless, a conservative HEP of  $1E-2$  is used in the analysis. The error by the crew of  $1E-2$  is based on Reference 15A-7.

#### Valves Spuriously Open (SDC-E-FA-V)

This gate is judged to double count the failure modes already addressed but is included at the design stage for completeness. It may subsequently be subsumed by more explicit modeling. The spurious open MOV frequency is  $5.0E-8/hr$ . Reference 15A-8. The CCF basic event is the frequency failure for the SDC function to inadvertently initiate given a full year of power operation (8760 hours). A conservative common cause factor of 0.1 (NRC common cause data is  $\sim 3E-2$  for 2 of 2 MOVs failing to operate) is applied and provides a result of  $5.00E-08/hr * 0.1 * 8760 \text{ hours/year} = 4.38E-05/yr$ .

#### Automatic Actuation of SDC At-Power (SDC-E-AUTO)

The SDC system is designed to automatically initiate given the following:

Control rods fully inserted

In addition to these initiation signals, the SDC interlocks must have failed. Gate SDC-E-AUTO provides the assessment of these combinations of failures.

Because of the preliminary nature of the design, the fault tree is rudimentary and the failure probabilities are upper bound estimates.

#### Result

The result of the fault tree analysis is a calculated frequency of inadvertent SDC operation at-power of approximately  $1.6E-04/yr$ , which includes interlock failure or bypass. The frequency of this failure is less than once in 6,200 years. Therefore, this event frequency meets the criterion for an infrequent event because it is less than once in 100 years.

#### **15A.3.7.3 Result**

The frequency of the inadvertent SDC function operation is estimated to be  $1.60E-4$  per year. The event frequency is one in 6,200 years, and therefore, the event frequency meets the criterion of being less than once in 100 years.

### 15A.3.8 Inadvertent Opening of a Safety Relief Valve

#### 15A.3.8.1 Introduction

ESBWR is equipped with four Isolation Condensers and eighteen Safety Relief valves (SRVs). ESBWR is designed with the capability to handle reactor overpressurization using only the Isolation Condensers.

Subsection 5.2.2 states “For overpressure protection, the Isolation Condensers have sufficient capacity to preclude actuation of the SRVs, during normal operational transients.” The SRVs are therefore a backup to the Isolation condensers and are also needed for ATWS conditions. Of the 18 SRVs, ten SRVs discharge through lines routed to quenchers in the suppression pool. The remaining eight SRVs are arranged in two groups of four. Each group discharges to a horizontal header that has a rupture disc at the end. Each header has a discharge line that is routed to a quencher in the suppression pool. These SRVs discharge through the rupture discs to the drywell or through the discharge line to the suppression pool.

The SRVs provide two main protection functions:

- Overpressure relief function (all 18 SRVs are actuated by the inlet steam pressure to prevent nuclear steam overpressurization); and
- Depressurization operation (ten SRVs are actuated by the Automatic Depressurization System, (ADS), as part of the ECCS).

Eight of the SRVs are opened by steam pressure if the direct and increasing static inlet steam pressure overcomes the restraining spring and the frictional forces acting against the inlet steam pressure at the main or pilot disk and the main disk moves in the opening direction at a faster rate than corresponding disk movements at higher or lower inlet steam pressures.

The remaining ten of the SRVs are opened by either of the following two modes of operation:

- The safety (steam pressure) mode of operation is initiated by the direct and increasing static inlet steam pressure as described above for the eight SRVs.
- The ADS (power) mode of operation is initiated when an electrical signal is received at any of the solenoid valves located on the pneumatic actuator assembly. The solenoid valve(s) open, allowing pressurized pneumatic fluid to enter the lower side of the pneumatic cylinder piston, which pushes the piston and the rod upwards.

The power-actuated SRVs can be operated individually by remote manual controls from the main control room. Remote manual actuation of the SRVs from the control room is recommended to minimize the total number of these discharges with the intent of achieving extended valve seat life.

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) **Vibration Induced**
- (3) Excess nitrogen pressure
- (4) Spring relaxation
- (5) Spurious opening signal
- (6) 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, is** 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 estimate **based on Reference 15A-7 (Table 20-7 Item (1) and Table 20-22 Item (4)).**

**Vibration induced error: This value is based operating experience with current SRVs in operating BWRs.**

**Excess Nitrogen Pressure:** Excess nitrogen pressure could result in inadvertent valve opening. 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 **at 2.29 E-04.**

**Spring Relaxation:** Spring relaxation of solenoid valve with normal nitrogen pressure can potentially lead to an IORV event. However, this has never occurred in the operating BWR history, and hence it is judged that this even has a negligible probability of occurrence.

**Spurious Actuation Signal:** Spurious actuation can occur from a failure in the control logic of the SRVs. There are 10 SRVs actuated by ADs. The other 8 SRVs are opened only by steam pressure overcoming a restraining spring; therefore, not subject to spurious signal actuation. The ADS logic was analyzed for spurious actuation in Subsection 15A.3.9 for the DPV inadvertent opening, resulting in a frequency of 5.75E-04 per year. This frequency is increased to 6.04E-04 **to estimate** the SRVs, to account for the fact that there are 10 SRVs, and only 8 DPVs.

**Operator Error:** The power-actuated SRVs can be operated individually by remote manual controls from the main control room. The operator is expected to use this feature only after the SRVs open initially, with the intent of minimizing total number of discharges. He should not be opening the SRVs inadvertently and he cannot do it accidentally because a deliberate action is required to open the SRVs. Since the primary means of controlling reactor overpressure in the ESBWR is the Isolation Condenser, the operator does not have a reason to actuate SRVs to relieve reactor pressure. The probability of an IORV resulting from an operator action is judged to be negligible.

In summary, the frequency of an IORV, based on the above discussion is as follows:

Incorrect setpoint or spring adjustments:	1.8 E-03 per year
<b>Vibration Induced:</b>	<b>1.8 E-04 per year</b>
Excess nitrogen pressure:	2.29E-04 per year

## ESBWR

Spring relaxation:	0.0 per year
Spurious opening signal:	6.0E-04 per year
Operator error:	0.0 per year
Total:	2.81E-03 per year

The resulting IORV frequency is  $-2.81 \text{ E-}03$  per year, or one event in over 300 years.

**15A.3.8.3 Result**

The ESBWR IORV frequency is less than once in 300 years of operation. Thus the event frequency meets the criterion of being less than once in 100 years.

**15A.3.9 Inadvertent Opening of a Depressurization Valve****15A.3.9.1 Introduction**

The Depressurization Valves (DPVs) are part of the Automatic Depressurization System (ADS). ADS consists of 10 SRVs and 8 DPVs and their associated instrumentation and controls.

The DPVs are described in Subsection 6.3.2.8.2. In summary, the DPVs are of a non-leak/non-simmer/non-maintenance design. They are straight-through, squib-actuated, non-reclosing valves with a metal diaphragm seal. The DPV is closed with a cap covering the inlet chamber. The cap shears off when pushed by a valve plunger that is actuated by the explosive initiator-booster.

Four initiators (igniter charges or squibs), singly or jointly, ignite a buster assembly explosive charge, which drives the shearing plunger. Each initiator is activated by an independent firing circuit. The firing of one initiator is adequate to ignite the buster, and open the valve.

The firing circuits of three DPV initiators are actuated by the ADS logic, which is part of the Engineered Safety Features (ESF) systems. In addition, the Diverse Protection System (DPS) can independently actuate the fourth DPV firing circuits. The DPS is implemented as a Nonsafety-Related system. The ESF and DPS logics are presented in Chapter 7, sections 7.3.1.1, and 7.8.1.2, respectively.

A simplified diagram of the DPV initiation logic is shown schematically in Figure 15A-1.

The conceptual design shown in Figure 15A-1, with two 2-out-of-4 logics and two load drivers per initiating (firing) circuit is generic for ECCS, including the SRV portion of ADS. The DPV actuation includes a third load driver (controlled by a third 2-out-of-4 logic) in the firing circuit for increased reliability against spurious actuation. For generality and conservatism, the analysis in this section, regarding the inadvertent opening of a DPV, is performed for the case of only two 2-out-of-4 logics and two load drivers per DPV firing circuit.

The safety-related ADS logic is implemented in four divisions. Each division has an instrument channel consisting of a level transmitter, trip-decision-making logic, and 10-second timer. All four divisions share the trip decision generated by each instrument channel. Each of the four divisions makes a 2-out-of-4 trip decision from each of the four divisional trip decisions. The system has single-channel bypass capability, that is, one channel at a time can be manually

removed from the voting logic for maintenance purposes. In this case, the trip decision process reverts to a 2-out-of-3 logic.

Each division has two trains of 2-out-of-4 trip logic to support the requirement that single divisional failures do not inadvertently open any ADS valve. These trains are named Voting Logic Units (VLUs) for the purpose of this analysis. As shown in Figure 15A-1, each pair of VLUs actuates one pair of series-connected load drivers in one firing circuit of each of six DPVs. Before reaching the load drivers, the trip signals from the VLUs initiate timers, one per load driver. These timers are set such that predetermined groups of SRVs and DPVs open at staggered times, to minimize reactor water level swell. These timers are not shown in Figure 15A-1, but are accounted for in the analysis by including their failure rate in the Load Driver (LD) reliability component.

The information received from the four safety-related instrument channels is compared for consistency at each VLU input, and inconsistencies are annunciated. Any one load driver trip in a firing circuit of a DPV is also annunciated.

The non-safety DPS logic actuates one pair of series-connected load drivers in one firing circuit of each DPV. Each load driver is actuated by a dedicated 2-out-of-3 voting logic. The voting is performed between the trip decisions generated by the three instrument channels of a Nonsafety-Related controller. This triplicate channel controller is a complex piece of equipment, with high reliability due to its ability to share information between channels at different stages of the process. A reliability analysis performed by a vendor is available for a controller of this type. Therefore, the triplicate channel controller is represented as a single reliability component in Figure 15A-1 for the purpose of this analysis.

### **15A.3.9.2 Analysis**

#### **15A.3.9.2.1 Analysis of Failure Causes**

Inadvertent opening of a DPV can occur due to one of the following causes:

- Local failure mechanisms at the DPV level, leading to ignition of the initiator-buster without any of the load drivers in the firing circuit having been closed
- Operator error
- Spurious actuation signals

Each one of these causes is discussed in the following subsections.

##### **15A.3.9.2.1.1 Local failure mechanisms at the DPV level**

The DPV has undergone engineering development testing using a prototype to demonstrate the proper operability, reliability, and flow capability of the design. Functional tests were performed to assure proper operability and the adequacy of the initiator-booster to operate the valve assembly.

The initiator used for the DPV actuation is also used in the automotive industry to actuate the airbag restraint system. Data obtained by GE from the manufacturer of initiators shows that between 1987 and 1993 there were no reported problems of any kind in more than 15,000,000 automotive initiators that were delivered. Because the initiators were delivered over a period of

6 years, and probably more in the later part of this period, it is assumed that the average operating time for one initiator is 2 years. Based on this data, i.e., 15,000,000 initiators operating with no failure over a time period of 2 years, the estimated failure frequency for one initiator is  $1/(15,000,000*2) = 3.3E-8/\text{year}$ . Based on this estimate, and the fact that the propellant used in the buster is more stable than the initiator, it is assessed that the contribution from local failure mechanisms at the DPV level is insignificant.

#### **15A.3.9.2.1.2 Operator Error**

The DPV control system is designed to minimize the possibility of accidental manual actuation.

Each firing circuit of a DPV includes a key-lock switch, which has to be open when testing the load drivers in that circuit. Although the load drivers are tested sequentially, and one load driver actuation alone cannot open the DPV, the key-lock switch offers additional protection against accidental firing of an initiator-buster.

Manual actuation of the DPVs can be performed from video display units (VDU) in the main control room. Safety-related and nonsafety-related VDUs can provide a display format that allows the operator to manually open each DPV independently. Each display utilizes an “arm/fire” configuration that requires at least two deliberate operator actions. Operator use of the “arm” portion of the display causes a plant alarm. Also, ADS can be manually initiated as a system to open all SRVs and DPVs, instead of each valve individually. To perform this action, each safety-related VDU can provide a display with an “arm/fire” switch (one per division). If the operator uses any two of the four switches, the ADS sequence seals in, and starts the ADS valve sequencing. This requires at least four deliberate operator actions. For all of the manual initiations, operator use of the “arm” portion of the display causes a plant alarm.

Based on the design described above, it is considered that the probability of inadvertent opening of a DPV due to operator error is insignificant compared to the probability of a spurious actuation signal.

#### **15A.3.9.2.1.3 Spurious Actuation Signals**

This failure mechanism includes spurious initiation signals, and inadvertent closure of load drivers. This failure cause is considered dominant, and analyzed in the following subsections of this report.

#### **15A.3.9.2.2 Analysis of Spurious Actuation Signal Frequency**

A fault tree was developed based on the schematic diagram shown in Figure 15A-1. Figure 15A-2 shows the fault tree modeling the inadvertent opening of one or more DPVs. The calculation of the frequency of inadvertent opening of one or more DPVs is performed by first calculating the frequencies for the different categories of failures shown on the left-hand side of Table 15A-1, based on the corresponding scenarios resulting from the failure combinations shown on the right-hand side of Table 15A-1. The following presents frequency calculations for the different combinations of failures. The input failure data used in these calculations are presented in Table 15A-2.

#### 15A.3.9.2.2.1 Frequency contribution of combinations of Load Drivers (LD) failures, and combinations of LD and Voter Logic Unit (VLU) failures

Table 15A-1 shows 3 LD combinations and 6 LD/VLU combinations for each DPV. Each combination leads to 2 scenarios resulting in inadvertent DPV opening. There are a total of 8 DPVs. Therefore:

$$F_1 = 8*[6*F(LD)*P(LD) + 6*F(LD)*P(VLU) + 6*F(VLU)*P(LD)] = \\ = 48*[F(LD)*P(LD) + F(LD)*P(VLU) + F(VLU)*P(LD)]$$

where:

F(LD) and F(VLU) are the yearly failure frequencies for the LD and VLU shown in Table 15A-2.

P(LD) and P(VLU) are the unavailabilities of the LD and VLU shown in Table 15A-2.

Therefore,

$$F_1 = 48*(8.76E-3*1.0E-5 + 8.76E-3*5.0E-5 + 4.38E-2*1.0E-5) = 4.36E-05/year$$

#### 15A.3.9.2.2.2 Frequency contribution of VLU failure combinations

$$F_2 = 8*F(VLU)*P(VLU) = 1.75E-05/year$$

#### 15A.3.9.2.2.3 Frequency contribution of Instrument Channel (IC) failure combinations, with failure to detect first IC failure

$$F_3 = 12*F(IC)*P(IC\_F)*P(FD) = 2.32E-6/year$$

where:

F(IC): Yearly failure frequency of the IC

P(IC\_F): Unavailability of an IC when its failure is detected only during the channel functional test

P(FD): Probability of failing to automatically detect an IC failure

#### 15A.3.9.2.2.4 Frequency contribution of IC failure combinations, with first IC failure detected and bypassed

$$F_4 = 12*F(IC)*P(IC)^2 = 1.05E-8/year$$

#### 15A.3.9.2.2.5 Frequency contribution of Triplicate Channel Controller(IC\_T)

$$F_5 = F(IC\_T) = 2.65E-04/year$$

#### 15A.3.9.2.2.6 Frequency contribution of LD and Voter Logic (LDV) failure combinations

$$F_6 = 16*F(LDV)*P(LDV) = 5.05E-5/year$$

#### 15A.3.9.2.2.7 Frequency contribution of Common Cause Failures (CCFs)

To account for failure modes that are not well understood (e.g., CCF due to software), CCFs of groups of redundant and identical components were included in the model. Three groups of components subject to CCF were identified for the ESF part of the design, and one for the non-

safety part of the design. A beta-factor of 1.0E-3 was assumed for the calculation of these CCF probabilities, applied to the failure rate of each type of component listed in Table 15A-2. The following are the four CCFs used in the analysis.

CCF of 2 or more LDs (LDccf):	8.76E-06/year
CCF of 2 or more VLUs (VLUccf):	4.38E-05/year
CCF of ICs (ICccf):	8.76E-05/year
CCF of 2 or more LDVs (LDVccf):	5.26E-05/year

The frequency contribution of the CCF of ESF and non-safety components is as follows:

$$F_7 = F(\text{LDccf}) + F(\text{VLUccf}) + F(\text{ICccf}) = 1.40\text{E-}4/\text{year}$$

$$F_8 = F(\text{LDVccf}) = 5.26\text{E-}5/\text{year}$$

### 15A.3.9.3 Results

The total frequency of inadvertent opening of one or more DPVs due to Instrumentation and Control failures is:

$$F = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + F_7 + F_8 = 5.75\text{E-}04/\text{year}$$

The frequency of 5.75E-04 per year translates to one DPV inadvertent opening in more than 1,700 years. Thus the event frequency meets the criterion of being less than once in 100 years.

## 15A.3.10 Stuck Open Relief Valve

### 15A.3.10.1 Introduction

ESBWR is equipped with four Isolation Condensers and eighteen Safety Relief valves (SRVs). ESBWR is designed with the capability to handle reactor overpressurization using only the Isolation Condensers.

Subsection 5.2.2 states “For overpressure protection, the Isolation Condensers have sufficient capacity to preclude actuation of the SRVs, during normal operational transients.” The SRVs are therefore a backup to the Isolation condensers and are also needed for ATWS conditions. Of the 18 SRVs, ten SRVs discharge through lines routed to quenchers in the suppression pool. The remaining eight SRVs are arranged in two groups of four. Each group discharges to a horizontal header that has a rupture disc at the end. Each header has a discharge line that is routed to a quencher in the suppression pool. These SRVs discharge through the rupture discs to the drywell or through the discharge line to the suppression pool.

The SRVs provide two main protection functions:

- Overpressure relief function (all 18 SRVs are actuated by the inlet steam pressure to prevent nuclear steam overpressurization)
- Depressurization operation (ten SRVs are actuated by the Automatic Depressurization System, (ADS), as part of the ECCS.

Even though the SRVs are not required or expected to open during a transient, under some rare conditions when all the Isolation Condensers not available, one or two SRVs may open. When

the SRVs are opened, there is a chance that they will get stuck in the open position. The event in which the SRV sticks open is identified as a Stuck Open Relief Valve (SORV) event, and its frequency is evaluated in this subsection.

There is a potential for SRVs to stick open if the SRVs are tested at power. However, as stated in Subsection 5.2.2.4, "It is not practical to test the SRV setpoints while the reactor is at power. Therefore, the potential for an SORV to occur following a SRV test at power is not considered.

#### ***15A.3.10.2 Analysis***

For an SORV event to occur, first, there should be a transient event in which there is a potential for reactor over pressurization, and second, one of the Isolation Condensers which is designed to actuate on demand does not open, and third, a number of SRVs open to relieve the pressure, and then finally, one of the SRVs fails to reclose after opening. It is assumed that four SRVs open when the Isolation Condenser is unavailable following a pressurization transient.

From Table 2.3-3 of Reference 15A-2, the following events are identified as overpressurization events:

- Transient with PCS unavailable: 3.74E-1 events /year
- Loss of Feedwater: 9.25 E-2 events/year
- Loss of Preferred Power: 4.6E-2 events/year
- Total 5.125E-1 events/year

The probability that Isolation Condenser System is not available on demand is conservatively estimated to be 0.1. The actual value is expected to be significantly lower.

In Reference 15A-6, there are five SORV events occurred in BWR plants (it is noted that only one of these instances were with direct-acting SRVs, so therefore this is a conservative approach to getting the frequency of SORV). The number of overpressurization events in BWRs in that database is estimated by adding the frequency of total loss of heat sink (122 events) with loss of offsite power (33 events), a total of 155 events. The assumption of four SRVs opened during each overpressurization transient (note: lower number gives a conservative value), results in a total of 620 SRV actuations which resulted in five SORV events. Therefore, the conditional probability of any SRV sticking open after it opens initially = 5 divided by 620, which is equal to 0.0016 per valve opening.

The ESBWR overpressurization frequency in which SRVs are likely to open is obtained by multiplying the frequency of over pressurization transient by probability that the Isolation Condensers are unavailable, which is  $5.125 \text{ E-1 times } 0.1 = 5.125 \text{ E-2 events per year}$ .

The expected number of SRV actuations =  $5.125 \text{ E-2 times four} = 2.05 \text{ E-1 SRV actuations per year}$ .

The frequency of SORV =  $2.05\text{E-1 times } 0.0016 = 0.000328$  per year.

The frequency of SORV can also be expressed as once in over 3000 reactor years.

### ***15A.3.10.3 Result***

The ESBWR SORV frequency is less than once in 3000 years of operation. Thus the event frequency meets the criterion of being less than once in 100 years.

## **15A.3.11 Control Rod Withdrawal Error During Refueling**

### ***15A.3.11.1 Introduction***

The control rod withdrawal error event during refueling involves inadvertent criticality due to the complete withdrawal or removal of the most reactive rod (or pair of control rods associated with the same Control Rod Drive system hydraulic control unit) during refueling. Two channels of instrumentation are provided to sense the position of each of the control rods. In addition, redundant signals for the position status of the refueling machine and the loading of the refueling machine main hoist are provided to both channels of the RC&IS logic. With the reactor mode switch in the refueling position, the indicated conditions are combined in redundant RC&IS logic circuits to determine if all restrictions on refueling equipment operations and control rod withdrawal are satisfied. The reactor mode switch status is sensed by four channels (i.e. divisions) of safety logic with each channel providing separate, isolated status inputs into the two channels of non-safety Rod Control and Information System (RC&IS). A rod withdrawal block based upon this redundancy in either RC&IS channel will provide a control rod withdrawal block to all control rods.

While in the refueling mode, detection of an operable control rod not being at its full-in position results in activation of interlock signals being provided from the RC&IS to the refueling equipment that prevent operating the equipment over the reactor core when loaded with a fuel assembly. Conversely, when the refueling equipment is located over the core and loaded with fuel, the refueling equipment provides redundant interlock signals to the RC&IS that generates a control rod withdrawal block signal in the RC&IS to prevent withdrawing a control rod.

This event is initiated by one or more operator errors followed by failure of the refueling equipment interlocks.

### ***15A.3.11.2 Analysis***

The following is an analysis of the operational conditions during refueling that could lead to a potential control rod withdrawal error.

#### **15A.3.11.2.1 Fuel Insertion with Control Rod Withdrawn**

All operational control rods are fully inserted when fuel is being loaded into the core to minimize the possibility of loading fuel into a cell containing no control rod. Refueling interlocks associated with both rod withdrawal and movement of the refueling platform back up this requirement. When the mode switch is in the REFUEL position, the interlocks prevent the platform from being moved over the core if a control rod is withdrawn and fuel is in the hoist. Likewise, if the refueling platform is over the core and fuel is on the hoist, control rod withdrawal is blocked by associated RC&IS logic. In addition, the control rod scram function provides backup mitigation action should a criticality occur during refueling. Since the scram function and refueling interlocks may be suspended, alternate backup protection required by Technical Specifications is obtained by assuring that an array of control rods, centered on the

withdrawn control rod, are inserted and are incapable of being withdrawn (by insertion of a control rod block). Since this event requires operator error in loading the fuel plus the failure of the multiple refueling interlocks and redundant RC&IS logic or not following the procedures required by Technical Specifications, this event frequency is assessed to be significantly less than once in 1,000 years.

The capability to place individual control rods in the inoperable bypass status in the RC&IS logic can be used to allow multiple (e.g., more than one control rod or control rod pair) control rod withdrawals, control rod blade replacement, associated control rod drive (CRD) removal or repair, or any combination of these, provided all fuel has been removed from the cell if the control rod blade does not remain fully inserted. With no fuel assemblies in the core cell, the associated control rod has no reactivity control function and is not required to remain fully inserted. Prior to reloading fuel into the cell, however, the associated control rod must be inserted to ensure that an inadvertent criticality does not occur. There is a special case when loading fuel into the core with multiple control rods withdrawn under administrative controls. Special spiral reload sequences are used to ensure adequate detection of the neutron flux level by the Startup Range Neutron Monitor equipment, as such reload sequences are being performed (e.g. for providing monitoring capability for inadvertent criticality). Spiral reloading encompasses reloading a cell (four fuel locations immediately adjacent to a control rod) on the edge of a continuous fueled region (the cell can be loaded in any sequence). The occurrence of an inadvertent criticality event under this special case is assessed to be less than 0.00000001 per year or one event in 10,000,000 years based on GE SIL 372 (Reference 15A-3).

#### **15A.3.11.2.2 Second Control Rod Removal or Withdrawal**

When the platform is not over the core (or fuel is not on the hoist), and the mode switch is in the REFUEL position, only one operable control rod can be withdrawn when the RC&IS SINGLE/GANG switch is in the SINGLE position. When the RC&IS switch is in the GANG position, only one operable control rod pair associated with the same HCU may be withdrawn. Any attempt to withdraw an additional rod results in a rod block by the redundant RC&IS logic. Because the core is designed to meet shutdown requirements with one such control rod pair (associated with the same HCU) of the maximum reactivity worth, OR one rod of maximum reactivity worth withdrawn, the core remains subcritical even with one such control rod pair (of control rod) withdrawn. Withdrawal of a second control rod or a second rod pair (with the same HCU) would require an operator error and failure of the redundant RC&IS rod withdrawal block logic and failure of the scram function. The frequency of this type of event is assessed to be significantly less than once per 1,000 years based on the multiple failures required for this event to occur.

#### **15A.3.11.2.3 Control Rod Removal Without Fuel Removal**

The installed design of the control rod incorporates a bayonet coupling system that without disassembly of the control rod drive equipment in the under-vessel area, it is physically impossible to accomplish the upward removal of the control rod blade without:

- The simultaneous or prior removal of the four adjacent fuel bundles, and
- Decoupling of the control rod blade by physical rotation of the blade relative to the associated coupling spud of the hollow piston tube.

Therefore, based on the required conditions for this event to occur, this event is considered not credible.

### **15A.3.11.3 Results**

The frequency of a rod withdrawal error during refueling is evaluated to be significantly less than once in 1,000 years based the multiple failures that are required for this event to occur. This event therefore meets the criterion of less than one event in 100 years.

## **15A.3.12 Control Rod Withdrawal Error During Startup**

### **15A.3.12.1 Introduction**

It is postulated that, during reactor startup, a single control rod is inadvertently withdrawn continuously due to a procedural error by the operator during manual rod withdrawal, or a gang of control rods is inadvertently withdrawn due to a malfunction in the automated rod movement control system (ganged rod operation) of the Plant Automation System (PAS), when in the automatic startup mode. Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the reference rod pull sequence (RRPS), when the RC&IS is in either the automatic or semi-automatic rod movement mode. The RC&IS is described in Subsection 7.7.2.

The RC&IS has a dual channel rod worth minimizer (RWM) function that prevents withdrawal of any out-of-sequence rods from 100% to 50% control rod density, i.e., for Group 1 to Group 4 rods. It also has ganged withdrawal sequence restriction constraints such that, if the withdrawal sequence constraints are violated, the rod worth minimizer function of the RC&IS initiates a rod block. The RWM sequence restriction constraints are in effect from 100% control rod density up to the low power setpoint.

The Plant Automation System includes triple-redundant process controllers. It provides rod movement demand signals to the RC&IS to accomplish automatic positioning of the control rods during an automatic startup, shutdown or during automatic power range maneuvers. The Plant Automation System is described in Subsection 7.7.4.

In addition, the startup range neutron monitors (SRNMs), a subsystem of the Neutron Monitoring System (NMS), has a "period withdrawal permissive" automatic rod withdrawal interlock for each of twelve SRNM instruments, three SRNMs per NMS division. It is also possible to bypass one SRNM in each core quadrant, or all three SRNMs in one NMS division. When any of the unbypassed SRNM channels senses that the reactor period reaches the rod withdrawal block setpoint due to erroneous control rod withdrawal, control rod withdrawal is blocked and automatic control rod operation by the PAS is interrupted. As a result, continuous control rod withdrawal is stopped. If the reactivity addition by the rod withdrawal error is large enough, the SRNM scram function will also be initiated (i.e. if the unbypassed SRNMs of two or more NMS divisions detect the reactor period has reached the associated scram function setpoint). The SRNM setpoints are so selected that no violation of the applicable thermal margins occurs during this event. The NMS is described in Subsection 7.2.2.

Because both the RC&IS and Plant Automation System include either a dual channel or triple-redundant processors, no single failure can cause this event to occur.

### 15A.3.12.2 Analysis

#### 15A.3.12.2.1 Automatic Rod Movement during Startup

During a typical plant startup, the PAS automated rod movement control function provides command signals to the RC&IS that withdraws the rod gangs. If there were erroneous ganged rod withdrawal initiated by the PAS that result in a flux excursion with the measured SRNM period for an unbypassed SRNM shorter than 20 seconds during rod withdrawal, the SRNM function and associated redundant RC&IS logic initiates the associated rod withdrawal block function. If there is a measured flux excursion shorter than 10 seconds, as detected by the unbypassed SRNMs of two NMS divisions, a scram is initiated. Therefore, an unmitigated rod withdrawal error during the automatic startup would require a failure in the PAS automated rod movement control function followed by a failure of the SRNM rod block trip and SRNM scram initiation. Triple-redundant fault-tolerant digital controllers and redundant system controllers would have to fail to cause loss of the PAS and RC&IS control logic functions. In addition, all unbypassed channels of SRNM system and the redundant RC&IS logic would have to fail to cause loss of the rod block function. The unbypassed SRNMs of 3 of 4 NMS divisions would have to fail to cause loss of the period-based scram function. The frequency of an automatic control rod withdrawal error during startup can be calculated as:

Annual Frequency of Automatic Control Rod Withdrawal Error =

(Number of startups/year) times

(Probability of failure of redundant PAS control logic) times

(Probability of failure of both SRNM rod block trip channels)

Because of the multiple failures required for this event, it can be expected that this frequency is significantly less than 1/100 years. To demonstrate this without a detailed analysis of the systems involved, a bounding calculation was performed. The number of starts per year was conservatively assumed to be 5 starts per year. The actual number of starts based on the ESBWR design can be expected to be no more than 2 starts per year. It is assumed that the probability of failure of both the redundant PAS and redundant SRNM channels is conservatively bounded by a common cause failure that disables both systems. The failure rate for electronic processors (from Reference 15A-4, Chapter 19, Table 19D.6-7, item Division 1 Transmission Network) is  $1.0E-5/\text{hour}$ . Assuming 24 hours per startup, the probability of failure/startup is  $(1.0E-05) \times 24 = 2.4E-04/\text{startup}$ . Applying a beta-factor of  $1.0E-03$ , the probability of a common cause failure disabling both systems is  $(2.4E-04 \times 1.0E-03) = 2.4E-07/\text{startup}$ . The beta factor is also obtained from the page 19N-3 of Reference 15A-4. The final calculation of the frequency of a control rod withdrawal error during a startup using the automatic rod movement system is  $(5 \text{ starts/year}) \times (2.4E-07/\text{start}) = 1.2E-06/\text{year} = 1 \text{ event}/8.3E+05 \text{ years}$ .

#### 15A.3.12.2.2 Manual Rod Movement during Startup

This event consists of an operator or procedural error during a single or ganged rod group withdrawal. The dual channel RWM enforces specific control rod sequences to limit the potential amount and rate of reactivity increase during control rod withdrawals. Control rod withdrawal is blocked when there is an out of sequence control rod withdrawal. The frequency of an automatic control rod withdrawal error during startup can be calculated as:

Annual Frequency of manual Control Rod Withdrawal Error =  
 (Number of startups/year) times  
 (Probability of operator or procedural error per startup) times  
 (Probability of the RWM to block control rod movement)

To demonstrate the low frequency without a detailed analysis of the systems involved, a bounding calculation was performed similar to the previous section. It was conservatively assumed that there would be 5 starts per year. The probability of an operator or procedural error per startup is conservatively assumed to be 1 event in 10 startups (0.1 per startup). The final results are insensitive to these two assumptions. As in the previous section, the failure rate for electronic processors (Reference 15A-4) is  $1.0E-5$ /hour. Assuming 24 hours per startup, the probability of failure/startup of a single channel in the RWM ( $1.0E-05$ ) X 24 =  $2.4E-04$ /startup. The probability of both channels failing is  $(2.4E-04)^2 = 5.8E-08$ /startup. This failure probability assumes that the first channel is not repaired during the 24-hour period. If it can be repaired in less than 24 hours, then the probability would be even lower.

Using the same beta-factor as in the previous section, the probability of a common cause failure of both RWM channels is  $(2.4E-04 \times 1.0E-03) = 2.4E-07$ /startup. The total failure probability for a startup is  $(5.8E-08) + (2.4E-07) = 3.0E-07$ . The final calculation of the frequency of a control rod withdrawal error during a startup using manual rod withdrawal is  $(5 \text{ starts/year}) \times (0.1) \times (3.0E-07) = 1.5E-07$ /year = 1 event/6.7E+06 years.

### **15A.3.12.3 Results**

The frequency of a rod withdrawal error due to automatic or manual startup is evaluated to be less than once in 741,000 years based the multiple failures that are required for this event to occur. Therefore, the event frequency meets the criterion of being less than one in 100 years.

## **15A.3.13 Control Rod Withdrawal Error During Power Operation**

### **15A.3.13.1 Introduction**

The causes of a potential rod withdrawal error (RWE) at power are either a procedural error by the operator in which a single control rod or a gang of control rods is withdrawn continuously, or a malfunction of the automated rod withdrawal sequence control logic during automated operation in which a gang of control rods is withdrawn continuously. In either case, the operating thermal limits rod block function blocks any further rod withdrawal when the operating thermal limit is reached. That is, the withdrawal of rods is stopped before the operating thermal limit is reached. The performance of the automated thermal limit monitor (ATLM) subsystem of the RC&IS prevents the RWE event from occurring. The core and system performance are not affected by such an operator error or control logic malfunction.

In the ESBWR, the ATLM subsystem performs the rod block monitoring function. The ATLM is a dual channel subsystem of the RC&IS. Each ATLM channel has two thermal limit monitoring functions. One function monitors the MCPR limit and protects the operating limit MCPR, and the other function monitors the MLHGR limit and protects the operating limit of the MLHGR. The rod block algorithm and setpoint of the ATLM are based on actual on-line core

thermal limit information. If any one of the limits is reached, such as due to control rod withdrawal, control rod withdrawal block is initiated.

### **15A.3.13.2 Analysis**

#### **15A.3.13.2.1 Automatic Rod Movement during Power Operation**

The analysis of the rod withdrawal error during power operation is similar to the bounding analysis for startup operation. The frequency of an automatic control rod error during power operation is calculated as follows:

Annual frequency of automatic control rod error during power operation =

(Frequency of failure of redundant PAS control logic/year) times

(Probability of failure of the dual channel ATLM subsystem)

It is assumed the failure of both redundant PAS control logic channels is dominated by common cause failure. Using the same failure rate and beta-factor as used for the startup control rod withdrawal error, the frequency of a common cause failure of the PAS control logic channels causing a gang of control rods to be withdrawn continuously is  $(1.0E-05 \text{ failures per hour}) \times (8760 \text{ hours/year}) \times (\text{Beta factor } 1.0E-03)$ . This is  $(8.76E-02/\text{year}) \times (1.0E-03) = 8.76E-05/\text{year}$ . As in the previous section for startup operation, the failure rate for electronic processors (from ABWR PRA) is  $1.0E-5/\text{hour}$ . The probability of failure of both ATLM channels is calculated based on a 92 day Technical Specification test interval and no annunciation of failures or repair. This is very conservative since failures are normally annunciated and the failed channel restored in less than 12 hours. The probability of both ATLM channels being unavailable is  $(1.0E-05 \times 24 \text{ hours} \times 92 \text{ days}/2)^2 = 1.22E-04$ . The probability of a common cause failure using a beta-factor of  $1.0E-03$  is  $(1E-05 \times 1E-03 \times 24 \text{ hours} \times 92 \text{ days}/2) = 1.1E-05$ . The final calculation of the frequency of an automatic control rod withdrawal error during power operation is  $(8.76E-05/\text{year} \times 1.33E-04) = 1.2E-09/\text{year} = 1 \text{ event}/8.3E+8 \text{ years}$ .

#### **15A.3.13.2.2 Manual Rod Movement during Power Operation**

The frequency of a manual control rod error during power operation is calculated as follows:

Annual frequency of manual control rod error during power operation =

(Frequency of operator error /year) times

(Probability of failure of the dual channel ATLM subsystem)

The frequency of operator control rod withdrawal error is dependent on the number of times an operator performs manual control rod withdrawals within a year. It is assumed that an operator makes a control rod withdrawal error 1 time every 5 years. This is considered conservative since the ESBWR design provides the operator with information on the main control panel to assist in control rod withdrawal and reduce the potential of a procedural error. Also, the results and conclusions are not very sensitive to this assumption. Using probability of failure of the dual channel ATLM subsystem from the previous section for automatic control rod withdrawal, the final calculation of the frequency of a manual control rod withdrawal error during power operation is  $(1 \text{ event}/5 \text{ years}) \times (1.22E-04) = 2.44E-05/\text{year}$  or  $1 \text{ event}/40,984 \text{ years}$ . This calculated frequency should be recognized as a very conservative bounding value. A more

realistic analysis, taking into consideration the ESBWR designed test features that provides annunciation of failures and allows the restoration of a failed logic channel in a reasonable short period, could reduce the calculated frequency by one or more orders of magnitude.

### ***15A.3.13.3 Results***

The frequency of a rod withdrawal error during startup is calculated to be one in 40,984 years based the multiple failures that are required for this event to occur. This event therefore meets the criterion of less than one event in 100 years.

## **15A.3.14 Fuel Assembly Loading Error, Mislocated Bundle**

### ***15A.3.14.1 Introduction***

The loading of a fuel bundle in an improper location with subsequent operation of the core requires three separate and independent errors:

- A bundle must be placed into a wrong location in the core.
- The bundle that was supposed to be loaded where the mislocation occurred is also put in an incorrect location or discharged.
- The misplaced bundles are overlooked during the core verification process performed following core loading.

Proper location of the fuel assembly in the reactor core is readily verified by visual observation and assured by verification procedures during core loading. GE provides recommended fuel assembly loading instructions for the initial core as part of the Startup Test Instructions (STIs). It is expected that the plant owners use similar procedures during subsequent refueling operations. Verification procedures include inventory checks, current bundle location logs, serial number verifications and visual or photographic inspection of the loaded core. The verification procedures are designed to minimize the possibility of the occurrence of the mislocated bundle accident.

### ***15A.3.14.2 Analysis***

The likelihood of operating the core with a mislocated bundle is low because multiple errors are required. The likelihood of a mislocation resulting in a reduced thermal margin is also low. In an initial core most mislocations do not cause adverse effects on thermal margin. For reload cores, at least two bundles have to be mislocated and fuel locations are verified. Verification procedures include inventory checks, current bundle location logs, serial number verifications and visual or photographic inspection of the loaded core.

Current operating plants have provided the basis for changing this event from an AOO event to an infrequent event. With improved design features, the ESBWR is expected to be as good as or better than current operating experience in preventing this event. Event calculations based on actual plant operating experience supports the infrequent event classification. A 2004-2005 utility survey indicates there has been no confirmed mislocated bundle events based on 25 years of operating experience for 29 plants (a total of 725 years). The estimated failure frequency based on 0 failures and 725 years at the 50% confidence interval is 0.00096 per year or 1 event in 1,046 years.

### ***15A.3.14.3 Results***

The frequency of a mislocated fuel assembly during power operation is estimated to be 1 event in 1,046 years. Thus the event frequency meets the criterion of being less than once in 100 years.

## **15A.3.15 Fuel Assembly Loading Error, Misoriented Bundle**

### ***15A.3.15.1 Introduction***

Proper orientation of fuel assemblies in the reactor core is readily verified by visual observation and assured by verification procedures during core loading. Five separate visual indications of proper fuel assembly orientation exist:

- The channel fastener assemblies, including the spring and guard used to maintain clearances between channels, are located at one corner of each fuel assembly adjacent to the center of the control rod.
- The identification boss on the fuel assembly handle points toward the adjacent control rod.
- The channel spacing buttons are adjacent to the control rod passage area.
- The assembly identification numbers that are located on the fuel assembly handles are all readable from the direction of the center of the cell.
- There is cell-to-cell replication.

### ***15A.3.15.2 Analysis***

Current operating plants have provided the basis for changing this event from an AOO event to an infrequent event. With improved design features, the ESBWR is expected to be as good as or better than current operating experience in preventing this event. Event calculations based on actual plant operating experience supports the infrequent event classification. A 2004-2005 utility survey indicates there has been three confirmed misoriented bundle events that went undetected based on 25 years of operating experience for 29 plants (a total of 725 years). The actual frequency based on 3 errors in 725 years is 4.1 E-03 per year or 1 event in 242 years. This estimate is considered conservative since improved core verification procedures have been adopted by utilities. Zero errors during the most recent period from June 1995 to January 2005, representing 290 years of operating, confirms the effectiveness of the improved core verification procedures. Based on 0 errors and 290 years of operation, the 50% confidence estimate is 0.0024 failures per year or 1 event in 418 years.

### ***15A.3.15.3 Results***

The frequency of a misoriented fuel assembly during power operation is 1 event in 418 years based on improved core verification procedures. Thus the event frequency meets the criterion of being less than once in 100 years.

### 15A.3.16 Liquid-Containing Tank Failure

#### 15A.3.16.1 Introduction

A description of this event is provided in Subsection 15.3.16.

#### 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.

**15A.5 REFERENCES**

- 15A-1 Electric Power Research Institute, "Advanced Light Water Reactor Utility Requirements Document, Volume II, Chapter 1 Appendix A, PRA Key Assumptions and Groundrules", Revision 6, December 1993.
- 15A-2 GE Nuclear Energy, "ESBWR Certification Probabilistic Risk Assessment", NEDO-33201, scheduled March 2006.
- 15A-3 GE Nuclear Energy, "Recommended Technical Specifications for Fuel Loading", SIL 372, June 1982.
- 15A-4 GE Nuclear Energy, "23A6100, ABWR Standard Safety Analysis Report"
- 15A-5 USNRC, "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments", NUREG/CR-3862, May 1985.
- 15A-6 USNRC, "Rates of Initiating Events at US Nuclear Power Plants: 1987-1995", NUREG/CR-5750, February 1999
- 15A-7 USNRC, "Handbook of Human Reliability Analysis", NUREG/CR-1278, August 1983.
- 15A-8 Eide, S.A. et al., Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs, EGG-SSRE-8875, February 1990.
- 15A-9 Nonelectronic Parts Reliability Data, NPRD-95, Reliability Analysis Center, Rome Laboratory, Griffiss AFB, NY 13441-5700.
- 15A-10 D.M. Ericson, Jr., Editor, et. al., Analysis of Core Damage Frequency Internal Events Methodology, NUREG/CR-4550, Vol. 1, Rev. 1, January 1990.
- 15A-11 Reactor Safety Study; An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants Main Report, WASH-1400 (NUREG-75/014), October 1975.
- 15A-12 The Institute of Electrical and Electronics Engineers, Inc. (IEEE), "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations", IEEE Std. 500-1984.

**Table 15A-1**  
**I&C Failures Leading to Inadvertent Opening of DPVs**

Category		Combinations of Failures		
ESF Portion of DPV Control	Common Cause Failures	IC CCF		
		LD CCF		
		VLU CCF		
	Combinations of Load Driver Failures and Combinations of Load Driver and VLU Failures	DPV 1	LD11	LD12
			LD11	VLUA2
			LD12	VLUA1
			LD13	LD14
			LD13	VLUB2
			LD14	VLUB1
			LD15	LD16
			LD15	VLUC2
			LD16	VLUC1
		DPV 2	LD21	LD22
			LD21	VLUB2
			LD22	VLUB1
			LD23	LD24
			LD23	VLUC2
			LD24	VLUC1
			LD25	LD26
			LD25	VLUD2
			LD26	VLUD1
		DPV 3	LD31	LD32
			LD31	VLUC2
			LD32	VLUC1
			LD33	LD34
			LD33	VLUD2
			LD34	VLUD1
			LD35	LD36
			LD35	VLUA2
		DPV 4	LD36	VLUA1
			LD41	LD42
			LD41	VLUD2
			LD42	VLUD1
			LD43	LD44
			LD43	VLUA2
			LD44	VLUA1
			LD45	LD46
		LD45	VLUB2	
			LD46	VLUB1

Table 15A-1

I&C Failures Leading to Inadvertent Opening of DPVs (continued)

Category		Combinations of Failures		
ESF Portion of DPV Control (continued)	Combinations of Load Driver Failures and Combinations of Load Driver and VLU Failures (continued)	DPV 5	LD51	LD52
			LD51	VLUA2
			LD52	VLUA1
			LD53	LD54
			LD53	VLUB2
			LD54	VLUB1
			LD55	LD56
			LD55	VLUC2
			LD56	VLUC1
		DPV 6	LD61	LD62
			LD61	VLUB2
			LD62	VLUB1
			LD63	LD64
			LD63	VLUC2
			LD64	VLUC1
			LD65	LD66
			LD65	VLUD2
		DPV 7	LD66	VLUD1
			LD71	LD72
			LD71	VLUC2
			LD72	VLUC1
			LD73	LD74
			LD73	VLUD2
			LD74	VLUD1
			LD75	LD76
			LD75	VLUA2
		DPV 8	LD76	VLUA1
			LD81	LD82
			LD81	VLUD2
			LD82	VLUD1
			LD83	LD84
			LD83	VLUA2
			LD84	VLUA1
			LD85	LD86
			LD85	VLUB2
		LD86	VLUB1	

**Table 15A-1  
I&C Failures Leading to Inadvertent Opening of DPVs (continued)**

Category		Combinations of Failures				
ESF Portion of DPV Control (continued)	Combinations of VLU Failures		VLUA1	VLUA2		
			VLUB1	VLUB2		
			VLUC1	VLUC2		
			VLUD1	VLUD2		
	Combinations of Instrument Channel Failures	Failure of First Channel is not Detected	ICA F	ICB F	FD	
			ICA F	ICC F	FD	
			ICA F	ICD F	FD	
			ICB F	ICC F	FD	
			ICB F	ICD F	FD	
			ICC F	ICD F	FD	
		First Failed Channel is Bypassed	ICA	ICB	ICC	
			ICA	ICB	ICD	
			ICA	ICC	ICD	
			ICB	ICC	ICD	
Non-Safety (DPS) Portion of Control	Triplicate Controller		IC T			
	Load-Driver/Voter CCF		LDV CCF			
	Combinations of Load-Driver/Voter Failures - One per DPV -		LDV17	LDV18		
			LDV27	LDV28		
			LDV37	LDV38		
			LDV47	LDV48		
			LDV57	LDV58		
			LDV67	LDV68		
			LDV77	LDV78		
			LDV87	LDV88		

NOTE: Naming of failure events is based on schematic diagram in Figure 15A-1. The combinations of failures result from the fault tree in Figure 15A-2.

**Table 15A-2**  
**Failure Data**

Component / Event		Failure Rate [h]	Failure Frequency [y]	MTTR [h]	Test Interval [h]	Unavailability
Description	Acronym					
Load Driver	LD	1.00E-06	8.76E-03	10		1.00E-05
Voting Logic Unit	VLU	5.00E-06	4.38E-02	10		5.00E-05
Instrument Channel	IC	1.00E-05	8.76E-02	10		1.00E-04
IC with Failure not Detected	IC_F	1.00E-05	8.76E-02		4416	2.21E-02
Load Driver CCF	LDccf	1.00E-09	8.76E-06			
Voting Logic Unit CCF	VLUccf	5.00E-09	4.38E-05			
Instrument Channel CCF	ICccf	1.00E-08	8.76E-05			
Failure to Detect IC Failure	FD					P = 1.0E-04
LD and Voter Group	LDV	6.00E-06	5.26E-02	10		6.00E-05
LDV CCF	LDVccf	6.00E-09	5.26E-05			
Triplicate Channel Controller	IC_T	3.03E-08	2.65E-04			

References and Notes for Table 15A-2:

Load Driver (LD). This component includes the actual load driver and associated timer. Per Reference 15A-1, Page A.A-28, the failure rate for a solid-state relay spurious operation is 2.0E-07/h, and the failure rate of a solid-state time-delay relay premature operation is 5.0E-07/h. The failure rate of the LD component, for the purpose of this calculation, was conservatively assumed 1.0E-06/h, or 8.76E-03/y. Actuation of a load driver is annunciated. Therefore, the unavailability of the LD component is calculated based on its Mean Time to Repair (MTTR). Assuming an MTTR of 10 hours, the LD unavailability is 1.0E-05.

Voting Logic Unit (VLU). The failure rate of the VLU generating a spurious signal is conservatively assumed to be 5.0E-06/h, or 4.38E-2/y. This is a conservative estimate, based on reliability requirements in Reference 15A-4. This value assumes there are multiple circuit boards included in this reliability component. The VLU unavailability, based on a 10 hour MTTR is 5.0E-5.

Instrument Channel (IC). This component includes the level transmitter, trip-decision-making logic, and associated timers. Based on its complexity, a failure rate twice the value of the VLU failure rate was assumed. The failure rate used for the IC generating a spurious signal is 1.0E-05/h, or 8.76E-02/y. The failure of an instrument channel is normally detected immediately, by comparing the inputs to the VLUs. In this case, the IC unavailability, assuming an MTTR of 10 hours is 1.0E-4. If the IC failure was not detected, it is assumed it is detected and repaired during the channel functional test, once every 184 days, or 4416 hours. In this case, the IC unavailability is 2.21E-02.

Failure to Detect an IC Failure (FD). The failure detection mechanism for a faulty trip signal generated by one of the instrument channels is fairly simple. It consists of annunciating any inconsistency between the inputs to the VLUs. There are four VLUs, each getting all four IC inputs from the four ESF divisions. The failure to detect an inconsistency should be negligible.

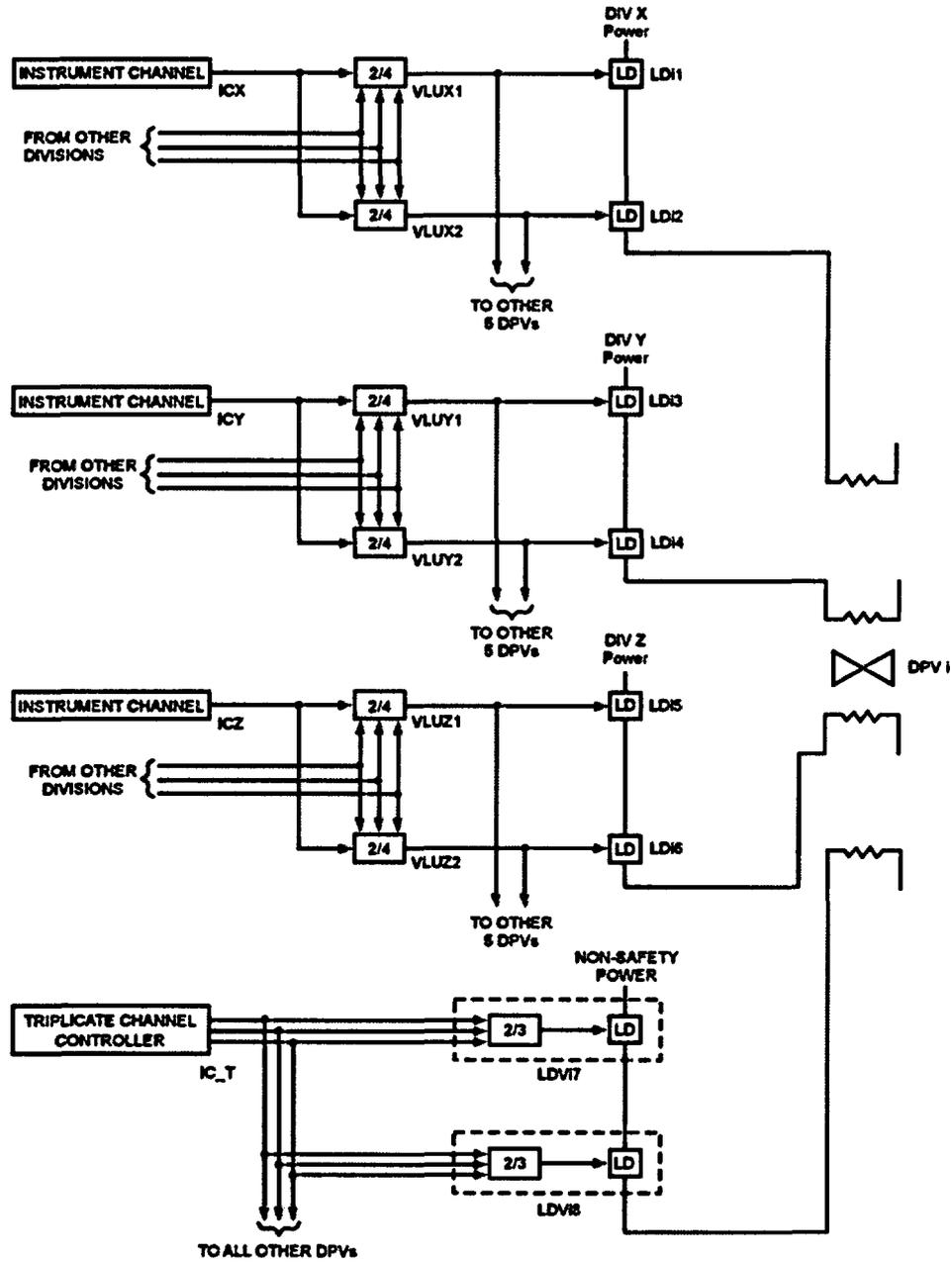
However, for the purpose of this conservative analysis, a failure probability of  $1.0E-4$  was assumed.

Load Driver and Voter (LDV). Compared to the LD component, this component also includes a dedicated two-out-of-three voting logic. Its failure rate is assumed to be the sum of the LD and VLU failure rates described above. Therefore, a failure rate of  $6.0E-06/h$ , or  $5.26E-2/y$  was assumed for this component. The unavailability of the LDV, based on a 10 hour MTTR, is  $6.0E-05$ .

Triplicate Channel Controller (IC\_T). A reliability analysis was performed by the vendor of a similar controller. The result of that analysis was assumed applicable to this controller. Therefore, the failure rate for IC\_T inadvertently opening the DPVs is assumed to be  $3.03E-8/h$ , or  $2.65E-04/y$ .

**Table 15A-3**  
**Summary of Event Frequency Estimates**

Section Number	Event	Event Frequency
15A.3.1	Pressure Regulator Failure – Opening of All Turbine Control and Bypass Valves	1 Event in 2,000 Years
15A.3.2	Pressure Regulator Failure – Closure of All Turbine Control and Bypass Valves	1 Event in 2,000 Years
15A.3.3	Turbine Trip with Total Turbine Bypass Failure	1 Event in 1,700 Years
15A.3.4	Generator Load Rejection with Total Turbine Bypass Failure	1 Event in 5,000 Years
15A.3.5	Feedwater Controller Failure – Maximum Demand	1 Event in 2,000 Years
15A.3.6	Loss of Feedwater Heating With Failure of Selected Control Rod Run-In	1 Event in 600 Years
15A.3.7	Inadvertent Shutdown Cooling Function Operation	1 Event in 6,200 Years
15A.3.8	Inadvertent Opening of a Safety Relief Valve	1 Event in 300 Years
15A.3.9	Inadvertent Opening of a Depressurization Valve	1 Event in 1,700 Years
15A.3.10	Stuck Open Safety Relief Valve	1 Event in 3,000 Years
15A.3.11	Control Rod Withdrawal Error During Refueling	1 Event in 1,000 Years
15A.3.12	Control Rod Withdrawal Error During Startup	1 Event in 741,000 Years
15A.3.13	Control Rod Withdrawal Error During Power Operation	1 Event in 40,900 Years
15A.3.14	Fuel Assembly Loading Error, Mislocated Bundle	1 Event in 1,046 Years
15A.3.15	Fuel Assembly Loading Error, Misoriented Bundle	1 Event in 418 Years
15A.3.16	Liquid-Containing Tank Failure	1 Event in 3,000 Years



NOTES: This figure shows only 2 (instead of 3) VLUX/LDs per firing circuit for consistency with the conservative analysis performed  
 'T' represents the DPV number  
 'X,' 'Y,' and 'Z' represent the divisions assigned to each DPV

i	1	2	3	4	5	6	7	8
X	A	B	C	D	A	B	C	D
Y	B	C	D	A	B	C	D	A
Z	C	D	A	B	C	D	A	B

Figure 15A-1. DPV Initiation Logic

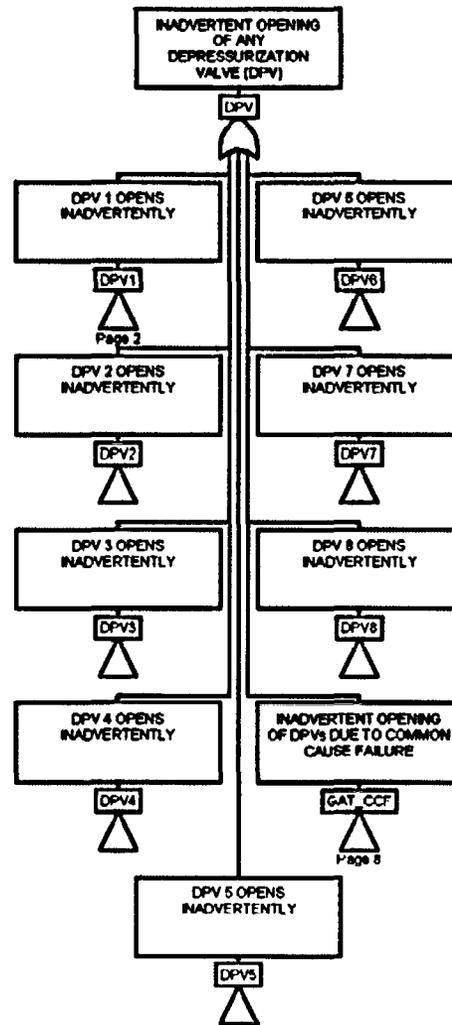


Figure 15A-2a. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 1 of 8)

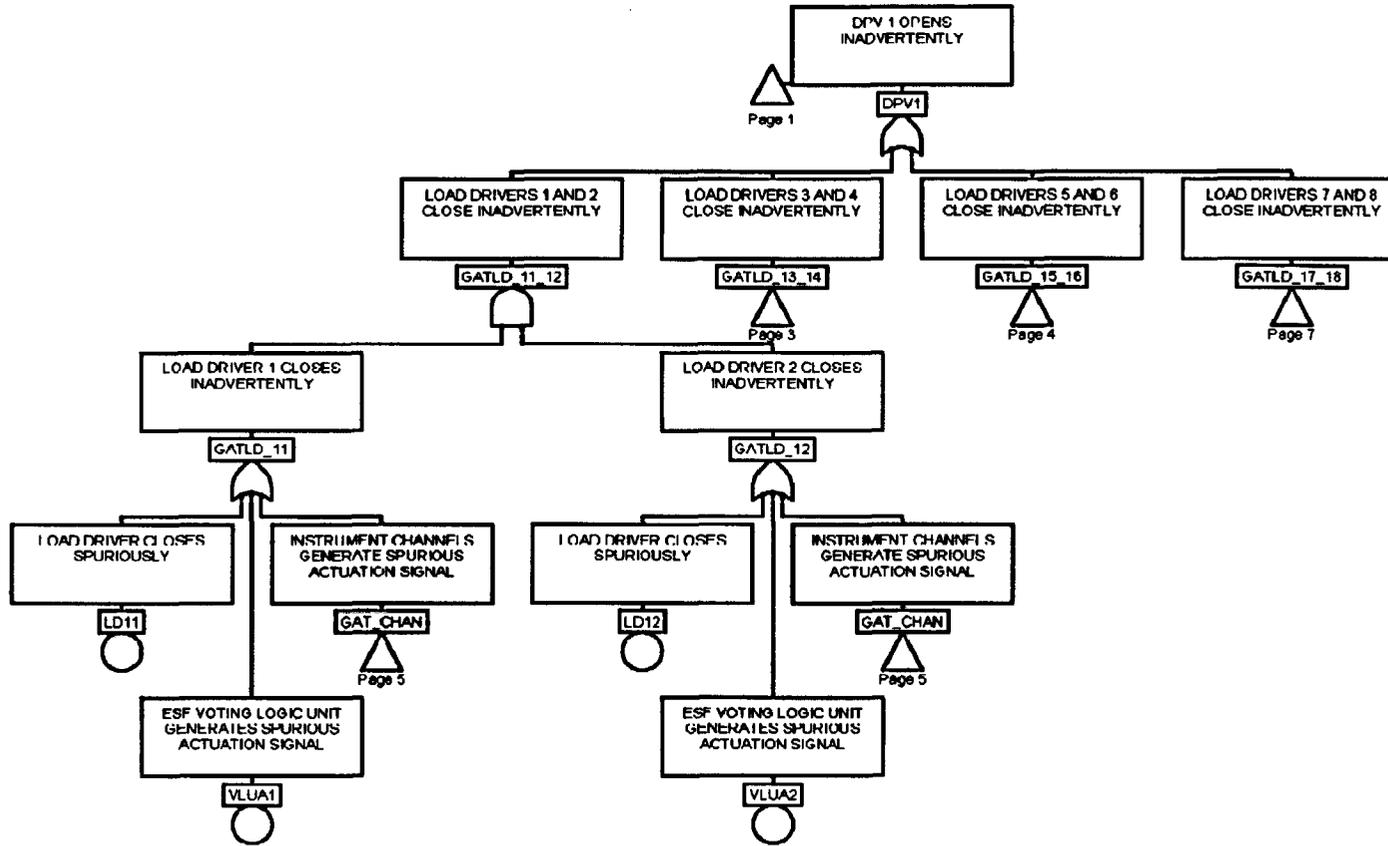


Figure 15A-2b. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 2 of 8)

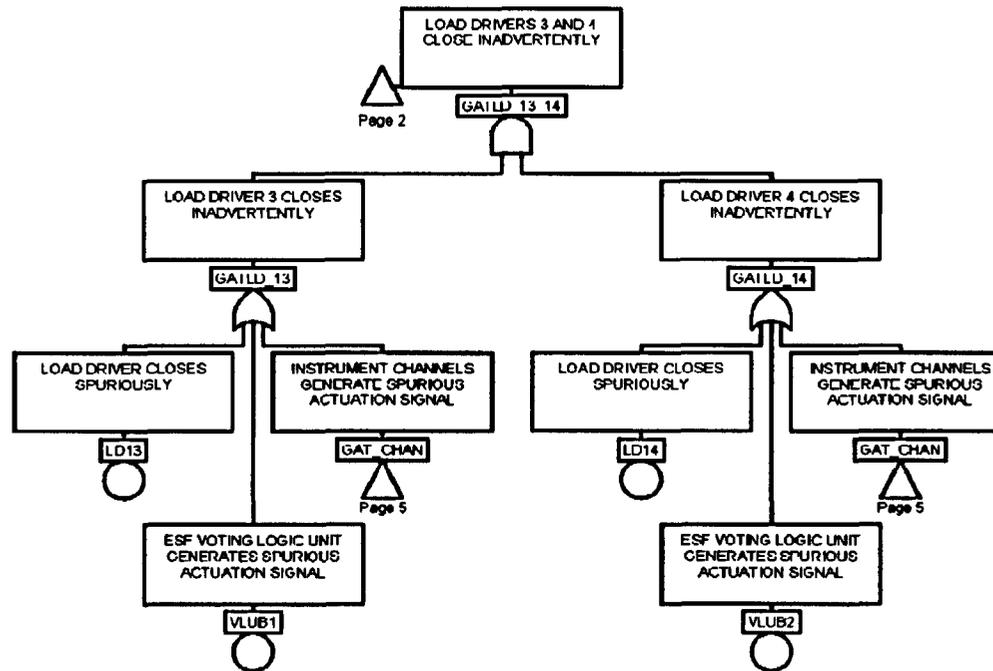


Figure 15A-2c. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 3 of 8)

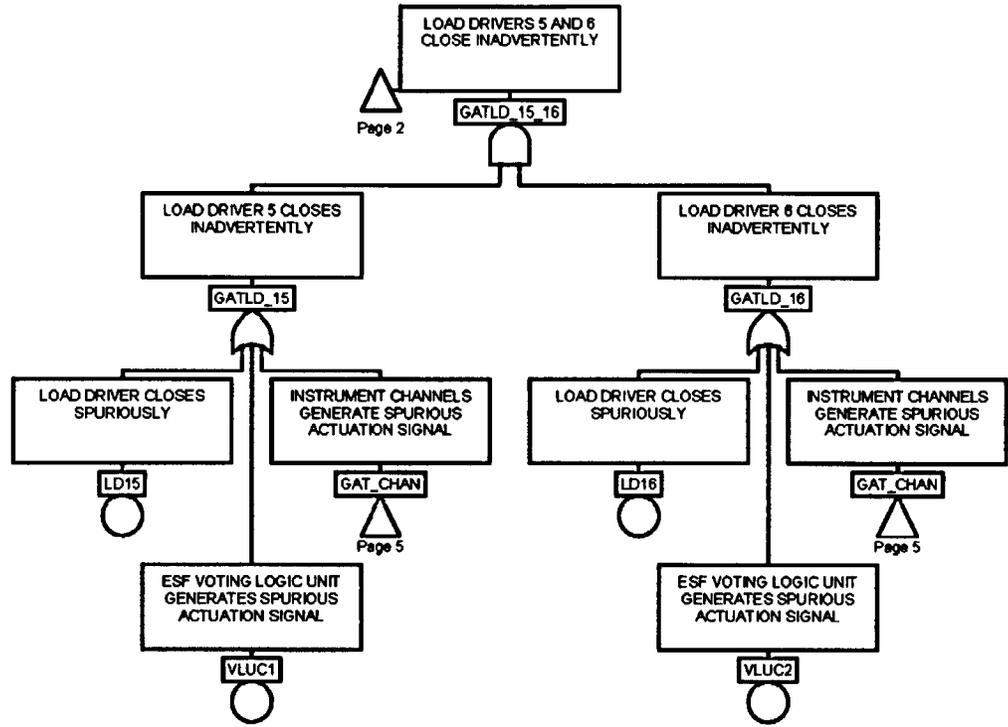


Figure 15A-2d. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 4 of 8)

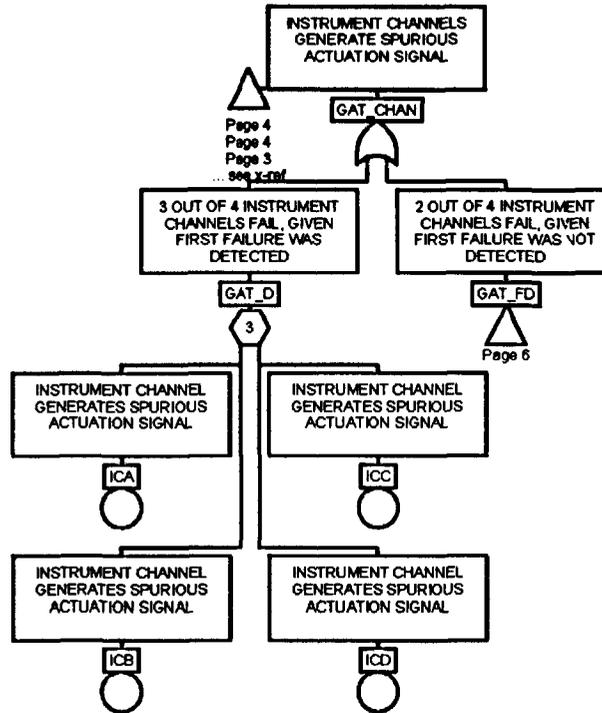


Figure 15A-2e. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 5 of 8)

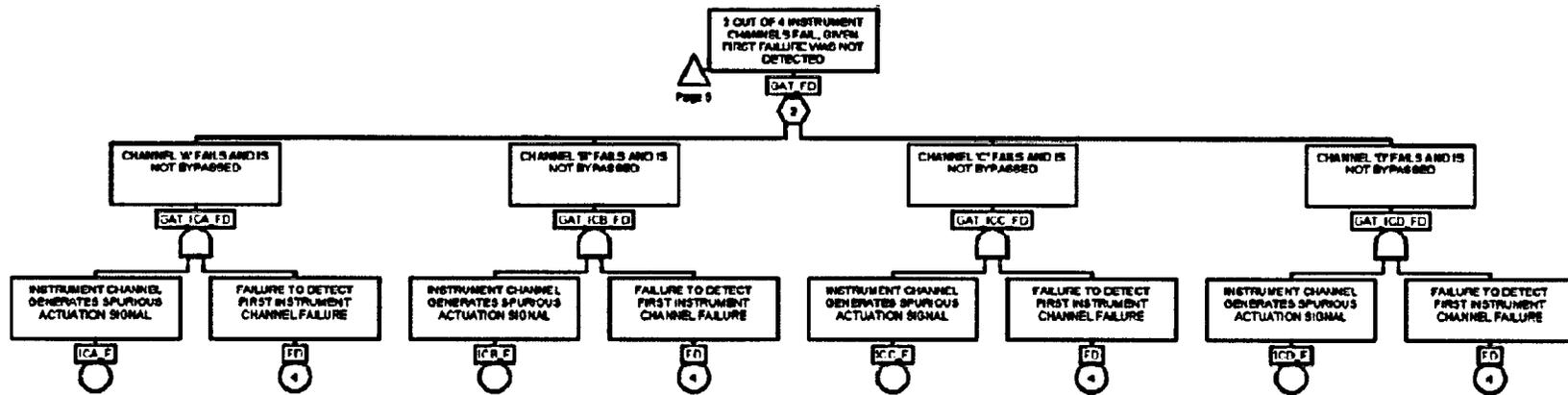


Figure 15A-2f. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 6 of 8)

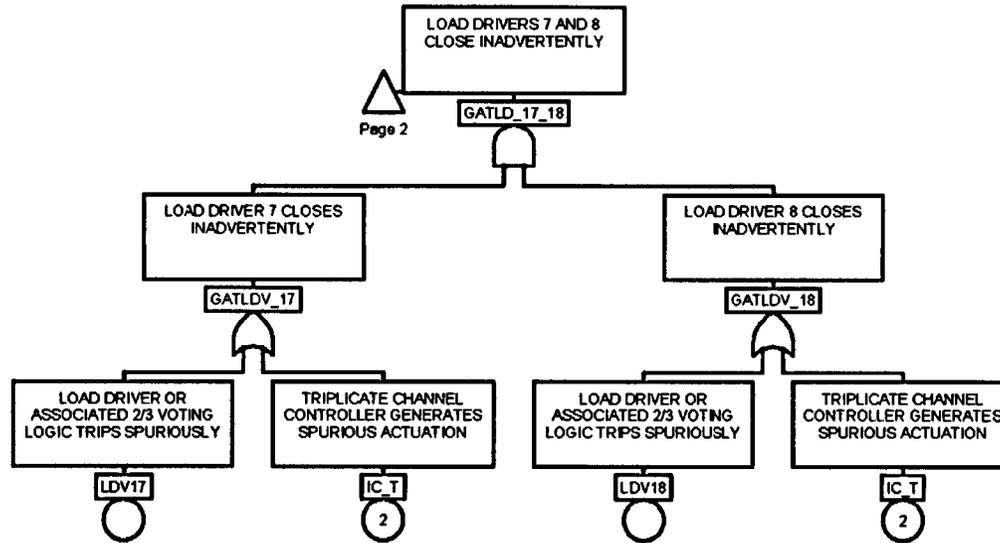


Figure 15A-2g. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 7 of 8)

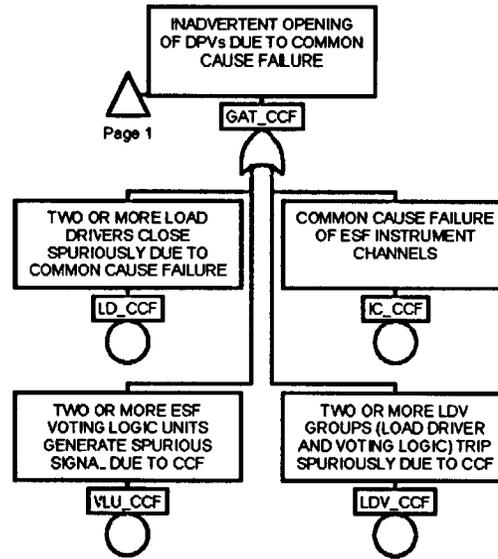


Figure 15A-2h. Fault Tree – Inadvertent Opening of a Depressurization Valve (page 8 of 8)

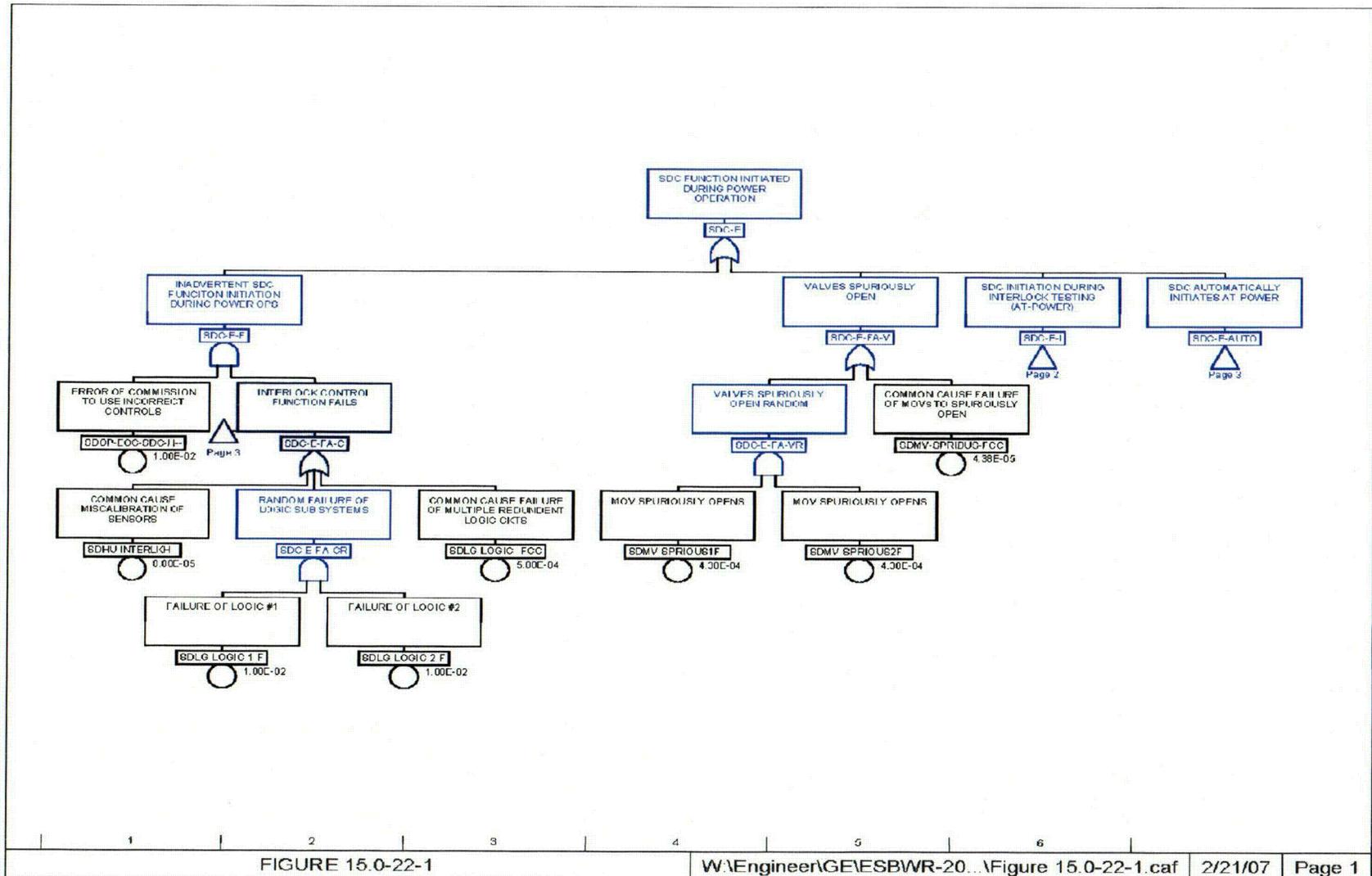


Figure 15A-3a. Fault Tree – Inadvertent Shutdown Cooling Function Operation (page 1 of 3)

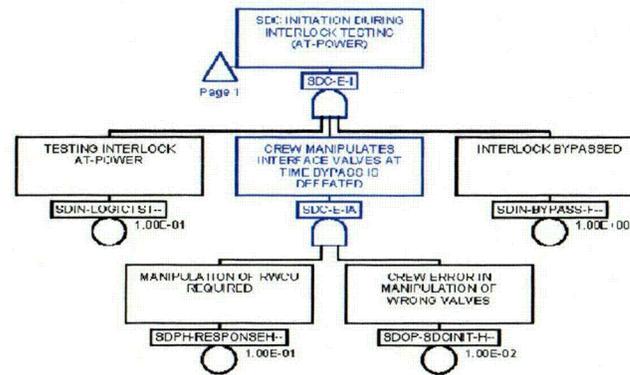


FIGURE 15.0-22-1

**Figure 15A-3b. Fault Tree – Inadvertent Shutdown Cooling Function Operation (page 2 of 3)**

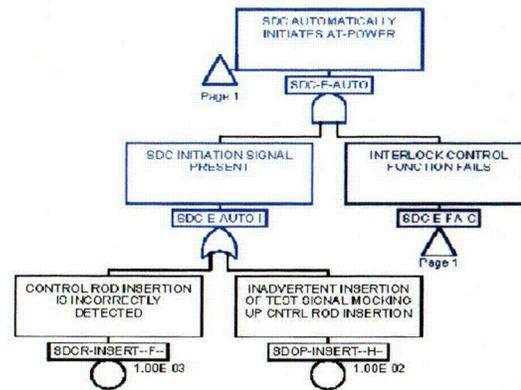


FIGURE 15.0-22-1

Figure 15A-3c. Fault Tree – Inadvertent Shutdown Cooling Function Operation (page 3 of 3)

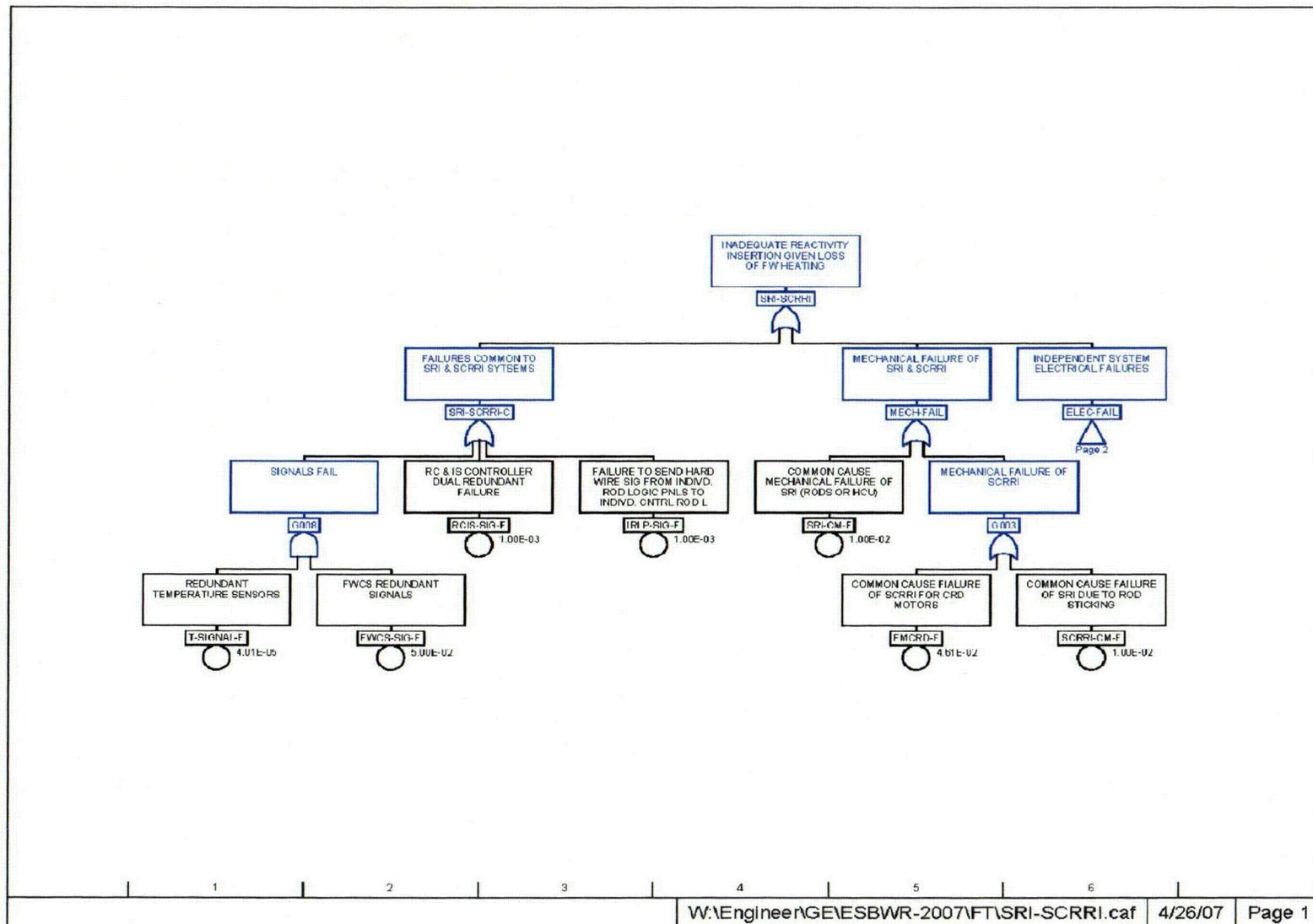
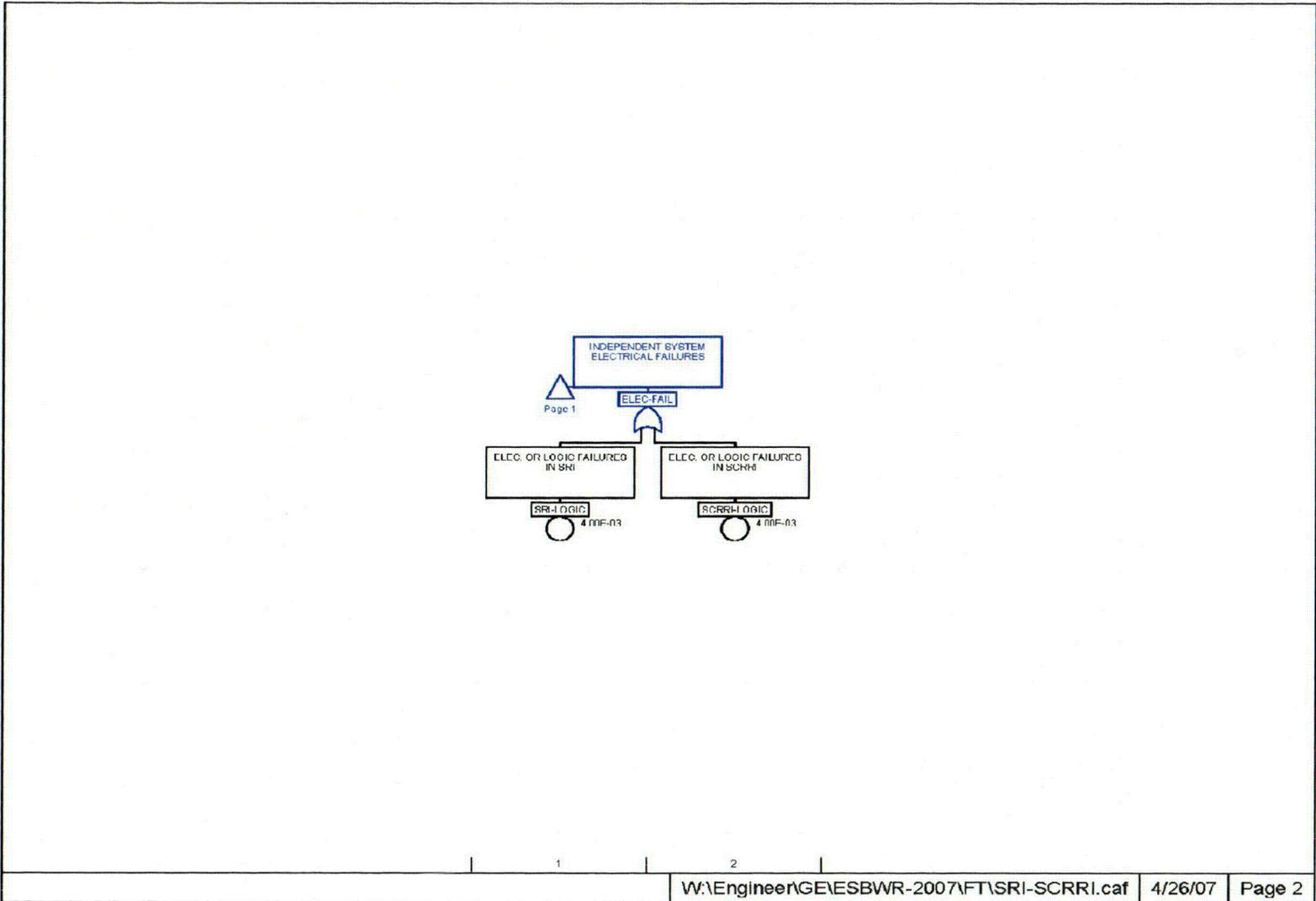


Figure 15A-4. Fault Tree for Inadequate Reactivity Insertion Given a Loss of FW Heating (page 1 of 2)



**Figure 15A-4. Fault Tree for Inadequate Reactivity Insertion Given a Loss of FW Heating(page 2 of 2)**