



March 21, 2011  
NRC:11:026

52-020

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

**ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report",  
Revision 2**

Ref. 1: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC),  
"Submittal of Revision 1 to ANP-10304, U.S. EPR Diversity and Defense-in-Depth  
Assessment Technical Report " NRC:09:115, December 4, 2009.

Proposed changes to the instrumentation and controls (I&C) architecture were communicated to the NRC staff in the February 15, 2011, public meeting. The U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report previously provided in Reference 1 has been revised to incorporate the revised I&C architecture. The revised report "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report" (ANP-10304), Revision 2, is enclosed with this letter.

AREVA NP has incorporated this revised report by reference in the U.S. EPR Final Safety Analysis Report (FSAR). The conforming changes to U.S. EPR FSAR will be transmitted to the NRC consistent with the schedule communicated in the February 15, 2011, public meeting. AREVA NP requests that the NRC incorporate the review of this revised report into the evaluation of the instrumentation and controls design in the safety evaluation report for the U.S. EPR FSAR in a manner consistent with other reports which are incorporated by reference in the U.S. EPR FSAR.

Also enclosed is a copy of the revised report showing a mark-up of the changes to facilitate the NRC review. If you have any questions related to this submittal, please contact me by telephone at 434-832-2369 or by e-mail to [sandra.sloan@areva.com](mailto:sandra.sloan@areva.com).

Sincerely,

A handwritten signature in cursive script that reads "Sandra M. Sloan".

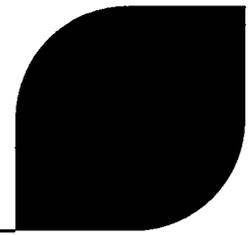
Sandra M. Sloan  
Regulatory Affairs Manager, New Plants  
AREVA NP Inc.

Enclosure

cc: G. Tesfaye  
Docket No. 52-020

**AREVA INC.**  
3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935  
Tel.: 434 832 3000 [www.aveva.com](http://www.aveva.com)

D077  
NRD



---

# **U.S. EPR Diversity and Defense-in-Depth Assessment**

ANP-10304  
Revision 2

## **Technical Report**

March 2011.

AREVA NP Inc.

---

(c) 2011 AREVA NP Inc.

**Copyright © 2011**

**AREVA NP Inc.  
All Rights Reserved**



**Contents**

	<u>Page</u>
1.0 INTRODUCTION.....	1-1
1.1 Purpose .....	1-1
1.2 Background.....	1-1
2.0 U.S. EPR I&C ARCHITECTURE .....	2-3
2.1 HMI Systems .....	2-3
2.2 Automation Systems & Instrument and Actuator Interface Systems .....	<del>2-52</del> 4
2.3 Dedicated I&C Systems .....	<del>2-72</del> 6
2.4 U.S. EPR I&C Defense-In-Depth Concept.....	<del>2-72</del> 6
2.5 Comparison of U.S. EPR I&C Defense-in-Depth Concept and NUREG/CR-6303 Echelons of Defense.....	<del>2-82</del> 7
3.0 DIVERSITY AND DEFENSE-IN-DEPTH FEATURES OF THE U.S. EPR I&C ARCHITECTURE .....	3-1
3.1 Features that Prevent a CCF of the I&C Safety Systems (Main Line of Defense).....	3-1
3.1.1 Equipment Design.....	3-1
3.1.2 Safety I&C System Design .....	3-3
3.1.3 Application Software Development Process .....	3-4
3.2 Features that Mitigate a Postulated SWCCF of the Protection System.....	<del>3-53</del> 4
3.2.1 Diversity between the Main Line of Defense and the Risk Reduction Line of Defense.....	3-5
4.0 DIVERSITY AND DEFENSE-IN-DEPTH ASSESSMENT.....	4-1
4.1 Guideline 1: Choosing Blocks .....	4-1
4.2 Guideline 2: Determining Diversity.....	<del>4-44</del> 3
4.3 Guideline 3: System Failure Types .....	<del>4-134</del> 12
4.4 Guideline 4: Echelon Requirement .....	<del>4-144</del> 13
4.5 Guideline 5: Method of Evaluation .....	<del>4-144</del> 13

4.6	Guideline 6: Postulated Common-Mode Failure of Blocks .....	<del>4-154-13</del>
4.7	Guideline 7: Use of Identical Hardware and Software Modules .....	<del>4-154-14</del>
4.8	Guideline 8: Effect of Other Blocks .....	<del>4-154-14</del>
4.9	Guideline 9: Output Signals .....	<del>4-164-15</del>
4.10	Guideline 10: Diversity for Anticipated Operational Occurrences .....	<del>4-164-15</del>
4.11	Guideline 11: Diversity for Accidents .....	<del>4-164-15</del>
	4.11.1 Identification of Credible SWCCF .....	<del>4-174-16</del>
	4.11.2 Establishing Boundaries for the Effects of Postulated SWCCFs .....	<del>4-194-18</del>
4.12	Guideline 12: Diversity among Echelons of Defense .....	<del>4-224-21</del>
4.13	Guideline 13: Plant Monitoring .....	<del>4-244-22</del>
4.14	Guideline 14: Manual Operator Action .....	<del>4-244-23</del>
4.15	Conclusions .....	<del>4-254-23</del>
5.0	REFERENCES .....	5-1
5.1	U.S. Regulations .....	5-1
5.2	U.S. Regulatory Guidance .....	5-1
5.3	Regulatory Review Precedent .....	5-1
5.4	AREVA NP Documents.....	5-2
<b>APPENDIX A DIVERSITY AND DEFENSE-IN-DEPTH PLANT RESPONSE ANALYSIS .....</b>		
		<b>A-1</b>
A.1	Introduction .....	A-2
A.2	D3 Plant Response analysis approach .....	A-5
	A.2.1 Method .....	A-5
	A.2.2 I&C Functions Available to Cope with SWCCF .....	<del>A-7A-6</del>
	A.2.3 Postulated Events .....	A-10
	A.2.4 Acceptance Criteria.....	A-10
	A.2.5 Evaluation Models and Methods .....	<del>A-12A-11</del>
A.3	Evaluation Results .....	<del>A-18A-17</del>
	A.3.1 General .....	<del>A-18A-17</del>
	A.3.2 Increase in Heat Removal by Secondary System .....	<del>A-18A-17</del>

---

A.3.3	Decrease in Heat Removal by Secondary System.....	<del>A-40A-39</del>
A.3.4	Decrease in RCS Flow Rate .....	<del>A-53A-52</del>
A.3.5	Reactivity and Power Distribution Anomalies .....	<del>A-67A-66</del>
A.3.6	Increase in RCS Inventory .....	<del>A-95A-94</del>
A.3.7	Decrease in RCS Inventory.....	<del>A-97A-95</del>
A.3.8	Containment Integrity .....	<del>A-118A-115</del>
A.3.9	Radiological consequences .....	<del>A-119A-116</del>
A.4	Conclusion .....	<del>A-122A-118</del>
A.5	References .....	<del>A-122A-119</del>

### List of Tables

Table 2-1—I&C Systems and Associated Technology .....	<del>2-102-9</del>
Table 2-2—U.S. EPR Lines of Defense .....	<del>2-102-9</del>
Table A.2-1—U.S. EPR Initiating Events.....	<del>A-14A-13</del>
Table A.2-2—DNBR and PLPD Limits .....	<del>A-15A-14</del>
Table A.2-3—Signals and PS/DAS Setpoints and Delays.....	<del>A-16A-15</del>
Table A.2-4—Best Estimate Vs. FSAR Chapter 15 Parameters .....	<del>A-17A-16</del>
Table A.3.2-1— $K_{eff}$ Summary for MSLB Event.....	<del>A-26A-25</del>
Table A.3.2-2—Reactivity Parameters Comparison .....	<del>A-26A-25</del>
Table A.3.4-1—Complete Loss of RCS FLOW – Sequence of Events.....	<del>A-55A-54</del>
Table A.3.4-2—D3 Rotor Seizure Event Parameters– Comparison FSAR Tier 2, Chapter 15 versus D3.....	<del>A-56A-55</del>
Table A.3.5-1—RCCA Withdrawal at Power – Sequence of Events .....	<del>A-75A-74</del>
Table A.3.5-2—Radial Power Peaking Factors (FDH) for Single RCCA Drop and RCCA Bank A Drop .....	<del>A-75A-74</del>
Table A.3.5-3—RCCA Ejection Event: Core Performance Results .....	<del>A-76A-75</del>
Table A.3.5-4—Sequence of Events for Rod Ejection for Case with No Break..	<del>A-76A-75</del>
Table A.3.5-5—Sequence of Events for Rod Ejection for Case with 0.025 ft <sup>2</sup> Break	<del>A-77A-76</del>
Table A.3.5-6—Sequence of Events for Rod Ejection for Case with 0.048 ft <sup>2</sup> Break	<del>A-77A-76</del>

### List of Figures

Figure 2-1—U.S. EPR I&C Architecture .....	2-3
Figure 2-2—Lines of Defense and I&C Functions .....	2-3
Figure 4-1—Block Diagram for D3 Assessment.....	<u>4-264-25</u>
Figure 4-2—Block Diagram with Diversity Attributes .....	<u>4-274-26</u>
Figure 4-3—Credible SWCCF Concurrent with AOO or PA .....	<u>4-284-27</u>
Figure 4-4—TXS Software .....	<u>4-294-28</u>
Figure 4-5—TXS System Software and Application Software .....	<u>4-304-29</u>
Figure A.3.2-1—Increase in Steam Flow Event: Indicated and Actual Reactor Power .....	<u>A-27A-26</u>
Figure A.3.2-2—Increase in Steam Flow Event: Indicated RCS Four-Loop- Average Temperatures.....	<u>A-28A-27</u>
Figure A.3.2-3—Increase in Steam Flow Event: Indicated Pressurizer Pressure	<u>A-29A-28</u>
Figure A.3.2-4—Increase in Steam Flow Event: Indicated Pressurizer Liquid Level	<u>A-30A-29</u>
Figure A.3.2-5—Increase in Steam Flow Event: Indicated SG Steam Line Pressure .....	<u>A-31A-30</u>
Figure A.3.2-6—Increase in Steam Flow Event: Steam Generator Level (NR)..	<u>A-32A-31</u>
Figure A.3.2-7—Increase in Steam Flow Event: Indicated Steam Generator Level (WR).....	<u>A-33A-32</u>
Figure A.3.2-8—Increase in Steam Flow Event: Main Feedwater Flow Rate.....	<u>A-34A-33</u>
Figure A.3.2-9—Increase in Steam Flow Event: Total TBS Flow Rate.....	<u>A-35A-34</u>
Figure A.3.2-10—Increase in Steam Flow Event: MSSV Flow Rate .....	<u>A-36A-35</u>
Figure A.3.2-11—Increase in Steam Flow Event: Normalized DNBR and LHGRA	<u>A-37A-36</u>
Figure A.3.2-12—Increase in Steam Flow Event: Power Response for Case Stabilizing under the High Neutron Flux Setpoint .....	<u>A-38A-37</u>
Figure A.3.2-13—Increase in Steam Flow - DNBR and Linear Heat Generation Rate for Case Stabilizing under the High Neutron Flux Setpoint	<u>A-39A-38</u>
Figure A.3.3-1—MSIVC Event: Indicated and Actual Reactor Power .....	<u>A-46A-45</u>
Figure A.3.3-2—MSIVC Event: RCS Average Temperatures .....	<u>A-47A-46</u>

Figure A.3.3-3—MSIVC Event: Maximum RCS Pressure (bottom of RPV).....	<u>A-48A-47</u>
Figure A.3.3-4—MSIVC Event: SG Pressure at Top of Tubesheet Below Cold-Side Downcomer .....	<u>A-49A-48</u>
Figure A.3.3-5—MSIVC Event: Steam Generator Wide Range Levels .....	<u>A-50A-49</u>
Figure A.3.3-6—MSIVC Event: Steam Generator Narrow Range Levels.....	<u>A-51A-50</u>
Figure A.3.3-7—MSIVC Event: MSSV Flow.....	<u>A-52A-51</u>
Figure A.3.4-1—Complete Loss of Forced RCS Flow Event: Mass Flow Rates	<u>A-57A-56</u>
Figure A.3.4-2—Complete Loss of RCS Flow – RCS Flow Coastdown Comparison .....	<u>A-58A-57</u>
Figure A.3.4-3—Complete Loss of Forced RCS Flow Event: RCS Temperatures	<u>A-59A-58</u>
Figure A.3.4-4—Complete Loss of Forced RCS Flow Event: Pressurizer Pressure	<u>A-60A-59</u>
Figure A.3.4-5—Complete Loss of Forced RCS Flow Event: Core Average Heat Flux.....	<u>A-61A-60</u>
Figure A.3.4-6—Complete Loss of RCS Flow – Plot of Minimum DNBR Normalized to SAFDL.....	<u>A-62A-61</u>
Figure A.3.4-7—Complete Loss of Forced RCS Flow Event: Pressurizer Liquid Level.....	<u>A-63A-62</u>
Figure A.3.4-8—Complete Loss of Forced RCS Flow Event: Steam Generator Wide Range levels.....	<u>A-64A-63</u>
Figure A.3.4-9—Complete Loss of Forced RCS Flow Event: Steam Generator Narrow Range Levels .....	<u>A-65A-64</u>
Figure A.3.4-10—Complete Loss of Forced RCS Flow Event: Turbine Bypass Flows .....	<u>A-66A-65</u>
Figure A.3.5-1—Uncontrolled RCCA Withdrawal at Power Event: Indicated and Actual Reactor Power.....	<u>A-78A-77</u>
Figure A.3.5-2—Uncontrolled RCCA Withdrawal at Power Event: RCS Temperatures .....	<u>A-79A-78</u>
Figure A.3.5-3—Uncontrolled RCCA Withdrawal at Power Event: Steam line Pressure .....	<u>A-80A-79</u>
Figure A.3.5-4—Uncontrolled RCCA Withdrawal at Power Event: Steam Generator Narrow range Level .....	<u>A-81A-80</u>
Figure A.3.5-5—Bank A Drop at EOC Event: Reactor power.....	<u>A-82A-81</u>

Figure A.3.5-6—Bank A Drop at EOC Event: RCS Temperatures .....	<u>A-83A-82</u>
Figure A.3.5-7—Bank A Drop at EOC Event: Pressurizer Pressure.....	<u>A-84A-83</u>
Figure A.3.5-8—Bank A Drop at EOC Event: Steam Line Pressure .....	<u>A-85A-84</u>
Figure A.3.5-9—Boron Dilution at Power Event: Indicated and Actual Reactor Power .....	<u>A-86A-85</u>
Figure A.3.5-10—Boron Dilution at Power Event: RCS Temperatures .....	<u>A-87A-86</u>
Figure A.3.5-11—Boron Dilution at Power Event: Pressurizer Pressure .....	<u>A-88A-87</u>
Figure A.3.5-12—Boron Dilution at Power Event: Steam Line Pressure .....	<u>A-89A-88</u>
Figure A.3.5-13—Boron Dilution at Power Event: Steam Generator Narrow Range Levels .....	<u>A-90A-89</u>
Figure A.3.5-14—RCCA Ejection - No Rupture Event: Indicated and Actual Reactor Power.....	<u>A-91A-90</u>
Figure A.3.5-15—RCCA Ejection - No Rupture Event: RCS Temperatures.....	<u>A-92A-91</u>
Figure A.3.5-16—RCCA Ejection - No Rupture Event: Pressurizer Pressure ....	<u>A-93A-92</u>
Figure A.3.5-17—RCCA Ejection - No Rupture Event: Steam Generator NR Level	<u>A-94A-93</u>
Figure A.3.7-1—Steam Generator Tube Rupture – Reactor Power .....	<u>A-105A-102</u>
Figure A.3.7-2—Steam Generator Tube Rupture – Pressurizer Pressure ....	<u>A-106A-103</u>
Figure A.3.7-3—Steam Generator Tube Rupture – Pressurizer Level .....	<u>A-107A-104</u>
Figure A.3.7-4—Steam Generator Tube Rupture – Steam Generator Pressure	<u>A-108A-105</u>
Figure A.3.7-5—Steam Generator Tube Rupture – Steam Generator Wide Range Level.....	<u>A-109A-106</u>
Figure A.3.7-6—Steam Generator Tube Rupture – Steam Generator Narrow Range Level .....	<u>A-110A-107</u>
Figure A.3.7-7—Steam Generator Tube Rupture – Affected Steam Generator Liquid Volume.....	<u>A-111A-108</u>
Figure A.3.7-8—Steam Generator Tube Rupture – Break Mass Flow Rate...	<u>A-112A-109</u>
Figure A.3.7-9—Comparison of PCT: RCP NO Trip (New) vs. RCP TRIP FSARA	<u>A-113A-110</u>
Figure A.3.7-10—SBLOCA 6.5 inch diameter Break: Loop Seal Clearing Time	<u>A-114A-111</u>
Figure A.3.7-11—SBLOCA 6.5 inch diameter Break: Primary/ Secondary System Pressure .....	<u>A-114A-111</u>

Figure A.3.7-12—SBLOCA 6.5 inch diameter Break: Hot Assembly Collapsed  
Liquid Level ..... A-115A-112

Figure A.3.7-13—SBLOCA 2.5 inch diameter Break: Primary/ Secondary System  
Pressure ..... A-115A-112

Figure A.3.7-14—SBLOCA 2.5 inch diameter Break: EFW System Mass Flow  
Rate..... A-116A-113

Figure A.3.7-15—SBLOCA 2.5 inch diameter Break: Loop Seal Void Fraction A-116A-113

Figure A.3.7-16—SBLOCA 2.5 inch diameter Break: RCS/ RV Mass Inventory A-117A-114

Figure A.3.7-17—SBLOCA 2.5 inch diameter Break: Chemical and Volume  
Control System Flow Rate..... A-117A-114

## Nomenclature

<b>Acronym</b>	<b>Definition</b>
ADM	Anti-Dilution Mitigation
ALWR	Advanced Light Water Reactor
AOO	Anticipated Operational Occurrence
APU	Acquisition and Processing Unit
<u>ARI</u>	<u>All Rods In</u>
ATWS	Anticipated Transient Without Scram
BDBE	Beyond Design Basis Event
BOC	Beginning-of-Cycle
CCF	Common-Cause Failure
CHF	Critical Heat Flux
CoPP	Communication-Priority Pair
CRDCS	Control Rod Drive Control System
CVCS	Chemical and Volume Control System
D3	Diversity and Defense-in-Depth
DAS	Diverse Actuation System
DBE	Design Basis Event
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
EBS	Extra Borating System
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
EFWS	Emergency Feedwater System
EOC	End-of-Cycle
ESF	Engineered Safety Feature
FHA	Fuel Handling Accident
FLCV	Full Load Control Valve
FWLB	Feedwater Line Break
<u>HFP</u>	<u>Hot Full Power</u>
HMI	Human-Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
<u>ID</u>	<u>Inner Diameter</u>
IOPSRV	Inadvertent Opening of Pressurizer Safety Relief Valve
IRWST	In-Containment Refueling Water Storage Tank

<b>Acronym</b>	<b>Definition</b>
LLCV	Low Load Control Valve
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPD	Linear Power Density
MCR	Main Control Room
MDNBR	Minimum Departure from Nucleate Boiling Ratio
MFW	Main Feedwater
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSRT	Main Steam Relief Train
MSSV	Main Steam Safety Valve
MTC	Moderator Temperature Coefficient
NI	Nuclear Island
<u>NR</u>	<u>Narrow Range</u>
OS	Operating System
PA	Postulated Accident
PACS	Priority and Actuator Control System
PAM	Post Accident Monitoring
PAS	Process Automation System
PICS	Process Information and Control System
PCT	Peak Clad Temperature
PDIL	Power-Dependent Insertion Limit
PLD	Programmable Logic Device
PLPD	Peak Linear Power Density
PRA	Probabilistic Risk Assessment
PS	Protection System
PSRV	Pressurizer Safety Relief Valve
PZR	Pressurizer
QDS	Qualified Display System
<del>RAU</del>	<del>Remote Acquisition Unit</del>
RBWMS	Reactor Boron and Water Make-Up System
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance, and Limitation System

<b>Acronym</b>	<b>Definition</b>
RHR	Residual Heat Removal
RSS	Remote Shutdown Station
RTS	Reactor Trip System
RT	Reactor Trip
SA	Severe Accident
SAFDL	Specified Acceptable Fuel Design Limit
SA I&C	Severe Accident Instrumentation and Control
SAS	Safety Automation System
SBLOCA	Small Break LOCA
SBO	Station Blackout
<u>SCDS</u>	<u>Signal Conditioning and Distribution System</u>
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SICS	Safety Information and Control System
SIS	Safety Injection System
SIVAT	Simulation-based VAlidation Tool
SRM	Staff Requirements Memorandum
SSSS	Standstill Seal System
SWCCF	Software Common-Cause Failure
TBS	Turbine Bypass System
TG I&C	Turbine Generator Instrumentation and Control
TI	Turbine Island
TSC	Technical Support Center
TXS	TELEPERM XS
UV	Undervoltage
V&V	Verification and Validation
<u>WR</u>	<u>Wide Range</u>

## 1.0 INTRODUCTION

### 1.1 *Purpose*

The purpose of this report is to assess the adequacy of the U.S. EPR™ (U.S. EPR) instrumentation and control (I&C) architecture with respect to diversity and defense-in-depth (D3). Specifically, this report assesses conformance with the four point staff position on D3 found in NUREG-0800 BTP 7-19 (Reference 3).

To support the assessment, this report describes the I&C systems that compose the overall I&C architecture. The U.S. EPR defense-in-depth concept is discussed, and is compared to the echelons of defense discussed in NUREG/CR-6303 (Reference 7). Design features that minimize the potential for occurrence of a common-cause failure (CCF) of the safety I&C systems, and features that mitigate the effects of a postulated software CCF (SWCCF) in the protection system, are presented. Additionally, each of the 14 guidelines in NUREG/CR-6303 are discussed with respect to the U.S. EPR I&C architecture.

Appendix A presents the results of the U.S. EPR D3 plant response analysis, which concludes that the U.S. EPR design contains adequate diversity and defense-in-depth to mitigate the effects of an SWCCF in the protection system during an anticipated operational occurrence (AOO) or Postulated Accident (PA).

### 1.2 *Background*

CCFs of analog protection systems were not postulated in previous designs of safety I&C systems for nuclear power plants. This was based on the nature of the equipment, steps taken to preclude certain types of CCFs (e.g., equipment qualification, periodic testing), and years of operating experience with the technology. In modern I&C system designs, digital equipment is used because of its many advantages over analog technology, including features such as self-monitoring, reliability, availability, and ease of installation and maintenance. Despite many of the advantages that digital systems provide over analog systems, there are concerns that errors in software of digital I&C systems could cause CCFs that affect multiple redundant divisions of safety systems.

An early attempt to address these types of CCF was provided in NUREG-0493 (Reference 6). Subsequently, in SECY 91-292 (Reference 5), the staff included discussion of its concerns about ~~common-cause failure~~ CCFs in digital systems used in nuclear power plants. As a result of the reviews of advanced light water reactor (ALWR) design certification applications for designs that use digital protection systems, the NRC documented its position with respect to ~~common-cause failure~~ CCFs in digital systems and defense-in-depth. This position was documented as Item II.Q in SECY 93-087 (Reference 8) and was subsequently modified in the associated staff requirements memorandum (SRM), (Reference 9). BTP 7-19 was developed to provide further guidance and clarification of D3 design and acceptance criteria.

With the advent of a new generation of nuclear power plants, the I&C systems will be implemented based on current technology digital platforms, such as the AREVA NP TELEPERM XS (TXS). As such, these new plants will need to demonstrate adequate D3 within their design; especially relative to postulated ~~software common-cause failures~~ SWCCF.

## 2.0 U.S. EPR I&C ARCHITECTURE

The I&C architecture for the U.S. EPR is depicted in Figure 2-1~~Figure 2-4~~. The I&C architecture is arranged into three levels—Human Machine Interface (HMI) Systems, Automation Systems & Instrument and Actuator Interface Systems, and Dedicated I&C Systems, Level 2 (Supervisory Control), Level 1 (System Level Automation), and Level 0 (Process Interface). In general, functions (both automatic and manual) are allocated to the various Level 1 Automation Systems ~~systems~~ depending on the safety classification of the function, and what the function is designed for (e.g., rod cluster control assembly control, initiation of safety injection). Interfaces are provided between the HMI Systems and Automation Systems Level 2 and Level 1 I&C systems for manual functions. The intended platforms for each of the major U.S. EPR I&C systems are shown in Table 2-1~~Table 2-4~~.

### 2.1 HMI Systems~~Level 2—Supervisory Control~~

Level 2 HMI Systems contains two systems: the process information and control system (PICS) and the safety information and control system (SICS).

The PICS is used for monitoring and control during all conditions of plant operation, including normal operation, anticipated operational occurrences, postulated accidents, and beyond design basis events (DBE). Most plant equipment can be monitored and controlled via the PICS. PICS equipment is located in the main control room (MCR) and the remote shutdown station (RSS). View-only PICS displays are located in the technical support center (TSC). The PICS consists of equipment such as computer-based displays, input devices (e.g., mouse, keyboard), databases, network hardware, and data archival systems. The PICS is a non-safety-related system and will be implemented with a-an industrial digital I&C platform other than digital I&C platform diverse from-TXS.

The SICS is provided as a backup ~~human-machine interface (HMI)~~ used in the unlikely event that the PICS is unavailable. The SICS contains both safety-related and ~~non-safety-related~~ non-safety-related equipment located in both the MCR and RSS. The functions are location-specific and are as follows:

- ~~Monitoring and control of essential non-safety-related systems to provide for safe, steady-state plant operation for a limited time, and to reach and maintain hot standby (MCR only).~~
- Monitoring and control of safety-related systems. This includes the following capabilities:
  - System-level actuation of reactor trip (RT) (MCR and RSS).
  - System-level actuation of engineered safety features (ESF) systems (MCR ~~only~~).
  - ~~Monitoring and Control~~ of safety systems to reach and maintain safe shutdown (MCR and RSS).
  - Component-level control of safety-related actuators (MCR).
- ~~Monitoring and control of non-safety-related~~ non-safety-related systems. This includes the following capabilities:
  - Diverse means of a system-level actuation of reactor trip RT (MCR).
  - Diverse means of system-level actuations of critical safety functions (MCR).
- Monitoring and control of plant equipment necessary to mitigate a severe accident (MCR only). These controls are hardwired to the PACS and bypass the computer systems.
- Display of Types A-C Post-Accident Monitoring (PAM) variables.

For the initiation of protective actions at the system level (e.g., reactor trip, safety injection), conventional means (e.g., buttons, switches) are provided on the SICS. For RT initiation and ESF system-level initiations, these signals are acquired by protection system (PS) computers and combined with the automatic actuation logic. The RT signals are also hardwired directly to the reactor trip RT devices, bypassing the PS computers. -Diverse manual system-level actuation of critical safety functions and RT is available to the operator on the SICS. The way in which these diverse initiation signals are combined with the automatic actuation logic in the

~~diverse actuation system (DAS) in a similar fashion is similar to the PS logic. For reactor trip (RT) initiation, the signals are hardwired directly to the reactor trip devices, bypassing the PS computers.~~

The SICS also contains qualified display system (QDS) video display units. These are provided, in addition to the required hardwired SICS indications, to provide trending and graphing capabilities of a limited number of plant parameters to improve operator situational awareness. The QDS displays receive input from the PS for display and do not have control capabilities.

~~For other functions, conventional I&C equipment or the qualified display system (QDS) may be used. The QDS is a video display unit capable of both indication and control, and it is part of the family of TXS components. In either case, the signals to and from these interfaces are processed with TXS computers that interface to the various Level 1 I&C systems.~~

The safety-related portions of the SICS are designed to the requirements of 10 CFR 50.55a(h) (Reference 1) The design of U.S. EPR I&C systems conforms to IEEE 603-1998 in lieu of IEEE 603-1991 based on an alternative request pursuant to 10 CFR 50.55a(a)(3)(i).

## **2.2 Automation Systems & Instrument and Actuator Interface Systems Level 1— System Level Automation**

The PS is a safety-related integrated RT and ESF actuation system. The PS detects the conditions indicative of an AOO or PA and actuates the plant safety features to mitigate these events. This is accomplished primarily through the execution of automatic safety I&C actuation functions; specifically, RT and actuation of ESF systems. The PS has four redundant, independent divisions. Each division is located in a physically separated Safeguards Building. Each division of the PS contains two independent subsystems to support implement signal diversity. The PS utilizes the TXS platform and is designed to the requirements of 10 CFR 50.55a(h) subject to the alternative request described in Section 2.1.

The safety automation system (SAS) is a safety-related system. The SAS processes automatic control functions, and manually initiated control functions, to mitigate AOOs and postulated accidents and to reach and maintain safe shutdown. The SAS has four independent divisions. Each division is located in a physically separated Safeguards Building. Additional SAS

equipment is located in the two physically separated Emergency Diesel Generating Buildings and the four Essential Service Water Pump Structures. For maximum reliability, there are redundant controllers within each division of the SAS. The SAS utilizes the TXS platform and is designed to the requirements of 10 CFR 50.55a(h) subject to the alternative request described in Section 2.1.

~~The severe accident I&C (SA I&C) system is provided to perform those risk reduction I&C functions related to the monitoring and control of plant equipment required to mitigate severe accidents. The SA I&C utilizes the TXS platform and is a non-safety-related system.~~

The reactor control, surveillance, and limitation system (RCSL) performs core-related operational and limitation I&C functions. It is a redundant (master - hot standby) control system with physical separation of redundant equipment located in separate Safeguard Buildings. The RCSL utilizes the TXS platform and is a non-safety-related system.

The process automation system (PAS) executes the majority of plant control functions. Specifically, it performs operational and limitation I&C functions, except those performed by RCSL. ~~It consists of three main subsystems:~~

- ~~•Nuclear Island (NI) PAS.~~
- ~~•Turbine Island (TI) PAS.~~
- ~~•Balance of Plant (BOP) PAS.~~

The PAS is a non-safety-related system and is implemented with an industrial control platform other than TXS. ~~a digital I&C platform.~~

~~The diverse actuation system (DAS) executes those risk reduction I&C functions required to mitigate BDBEs other than severe accidents, including anticipated transient without scram (ATWS), station blackout (SBO), and SWCCF of the protection system PS. The DAS is a non-safety-related system and is implemented with a non-microprocessor based I&C system, digital I&C platform diverse from TXS.~~

The priority and actuator control system (PACS) is a safety-related system. It performs the following functions: priority control, drive actuation, drive monitoring, and essential component protection. ~~The PACS is implemented in four independent divisions; each division is located in~~

~~a physically separate Safeguards Building.~~ Each safety-related actuator is associated with one PACS communication-priority pair (CoPP). Each CoPP consists of two modules: a safety-related priority logic module, and a non-safety-related communication module. The priority module is subject to 100 percent combinatorial testing and is therefore not subject to an SWCCF. The priority module is designed to the requirements of 10 CFR50.55a(h) subject to the alternative request described in Section 2.1.

The Signal Conditioning and Distribution System (SCDS) is a safety-related system provided to condition and distribute safety-related sensor signals, and non-safety-related sensor signals that are required in functions allocated to SICS, DAS or RC SL. It is segmented within each division to include safety-related and non-safety-related equipment for the conditioning and distribution of safety-related and non-safety-related instrumentation, respectively. The SCDS receives inputs from process sensors and black box I&C systems and provides a conditioned, standard analog output signal to the Automation Systems and HMI Systems. The SCDS is implemented with a non-microprocessor based I&C system.

### **2.3 Dedicated I&C Systems Level 0—Process Interface**

The process interface level consists of the actuators, sensors, and signal processing equipment necessary to monitor and control the various plant processes. Examples include in-core instrumentation, level sensors, pressure sensors, electrical switchgear, motor-operated valves, and pumps.

### **2.4 U.S. EPR I&C Defense-In-Depth Concept**

AREVA NP has established three lines of defense within the I&C architecture. These lines of defense are:

- Preventive Line (RC SL and PAS).
- Main Line (PS and SAS).
- Risk Reduction Line (DAS and SA I&C).

The various lines of defense, as well as the I&C systems and functions that support the defense-in-depth concept, are shown in Figure 2-2 ~~Figure 2-2~~.

The preventive line of defense attempts to cope with deviations from normal operation and prevent their evolution into accidents. Operational and limitation I&C functions are executed by the RCSL and PAS, within the preventive line of defense.

The main line of defense mitigates the effects of AOOs and postulated accidents and prevents their evolution into severe accidents. Safety I&C functions are implemented in the PS (RT and ESF actuation), and the SAS (ESF control) to mitigate AOOs and postulated accidents, and to reach safe shutdown.

The risk reduction line of defense is used to limit the consequences of a complete loss of the PS due to SWCCF, concurrent with a design-basis event DBE. Risk reduction I&C functions are executed by the DAS, RT and ESF, and also help preserve the integrity of the containment in the case of severe accidents by special core melt retention and cooling devices. Risk reduction I&C functions are executed by the DAS, to mitigate the effects of BDBEs, and by the SA I&C, to specifically mitigate the effects of severe accidents.

In general, the lines of defense apply to the architecture A automation S systems & and I instrument and A actuator I interface S systems Level 1 automation systems. The PACS prioritizes actuation requests from I&C systems within each of the lines of defense; therefore, it supports all lines of defense. I Because the SCDS provides information from the D dedicated I&C S systems to the A automation S systems in each of the lines of defense; therefore, it supports all lines of defense. The prioritization of actuation requests incorporates the D3 concepts and is described in U.S. EPR FSAR Tier 2, Section 7.1. The PICS is used as long as it is available, and the SICS implements a backup Class 1E human-machine interface (HMI) that is always available for use even when the PICS is unavailable. The PICS and SICS support all lines of defense.

## **2.5 Comparison of U.S. EPR I&C Defense-in-Depth Concept and NUREG/CR-6303 Echelons of Defense**

The original concept of "Echelons of Defense" was discussed in NUREG-0493. This study identified three conceptual, functional echelons of defense (control, RT, and ESF) that were to be used to an acceptable degree so that the postulated CCF events do not lead to unacceptable consequences. This approach was expanded in NUREG/CR-6303 by using four echelons of defense designated:

1. Control.
2. RT.
3. ESF.
4. Monitoring and indication.

The U.S. EPR lines of defense are compared to these four echelons of defense discussed in NUREG/CR-6303 in Table 2-2 ~~Table 2-2~~. The control echelon is comparable to the preventive line of defense; although, the preventive line of defense includes limitation I&C functions that provide additional mitigation capability beyond control functions. The RT echelon and the ESF actuation echelon are both part of the main line of defense. The PS executes both functions. The monitoring and indication echelon is part of all three lines of defense (preventive, main, and risk reduction).

The risk reduction line of defense contains the following features beyond the four echelons of defense described in NUREG/CR-6303:

- Functions to mitigate BDBEs that have associated regulatory significance (ATWS and SBO).
- ~~Functions to mitigate safety significant sequences identified by the probabilistic risk assessment (PRA) or operational experience (e.g., complete loss of main feedwater and emergency feedwater).~~
- Functions to mitigate an SWCCF of the PS as discussed in BTP 7-19.

**Table 2-1—I&C Systems and Associated Technology Platforms**

<b>System</b>	<b>Platform <u>Technology</u></b>
Process Information and Control System	Computerized, <u>industrial platform</u> ; <del>not diverse from</del> TXS
Safety Information and Control System	<u>Hardwired / TXS (QDS)</u> <del>TXS (QDS) / Hardwired</del>
Protection System	TXS
Safety Automation System	TXS
Priority and Actuator Control System	TXS (Programmable Logic Device-based)
<u>Signal Conditioning and Distribution System</u>	<u>Non-computerized, Hardwired</u>
<del>Severe Accident Instrumentation and Control</del>	TXS
Reactor Control, Surveillance, and Limitation System	TXS
Process Automation System	Computerized industrial platform, <u>not TXS</u>
Diverse Actuation System	<u>Non-microprocessor based</u> <del>Computerized, diverse from</del> TXS

**Table 2-2—U.S. EPR Lines of Defense**

<b>NUREG/CR-6303 Echelon of Defense</b>	<b>U.S. EPR Line of Defense</b>		
	<b>Preventive</b>	<b>Main</b>	<b>Risk Reduction</b>
Control	x		
RT		x	
ESF		x	
Monitoring and Indication	x	x	x

Figure 2-1—U.S. EPR I&C Architecture

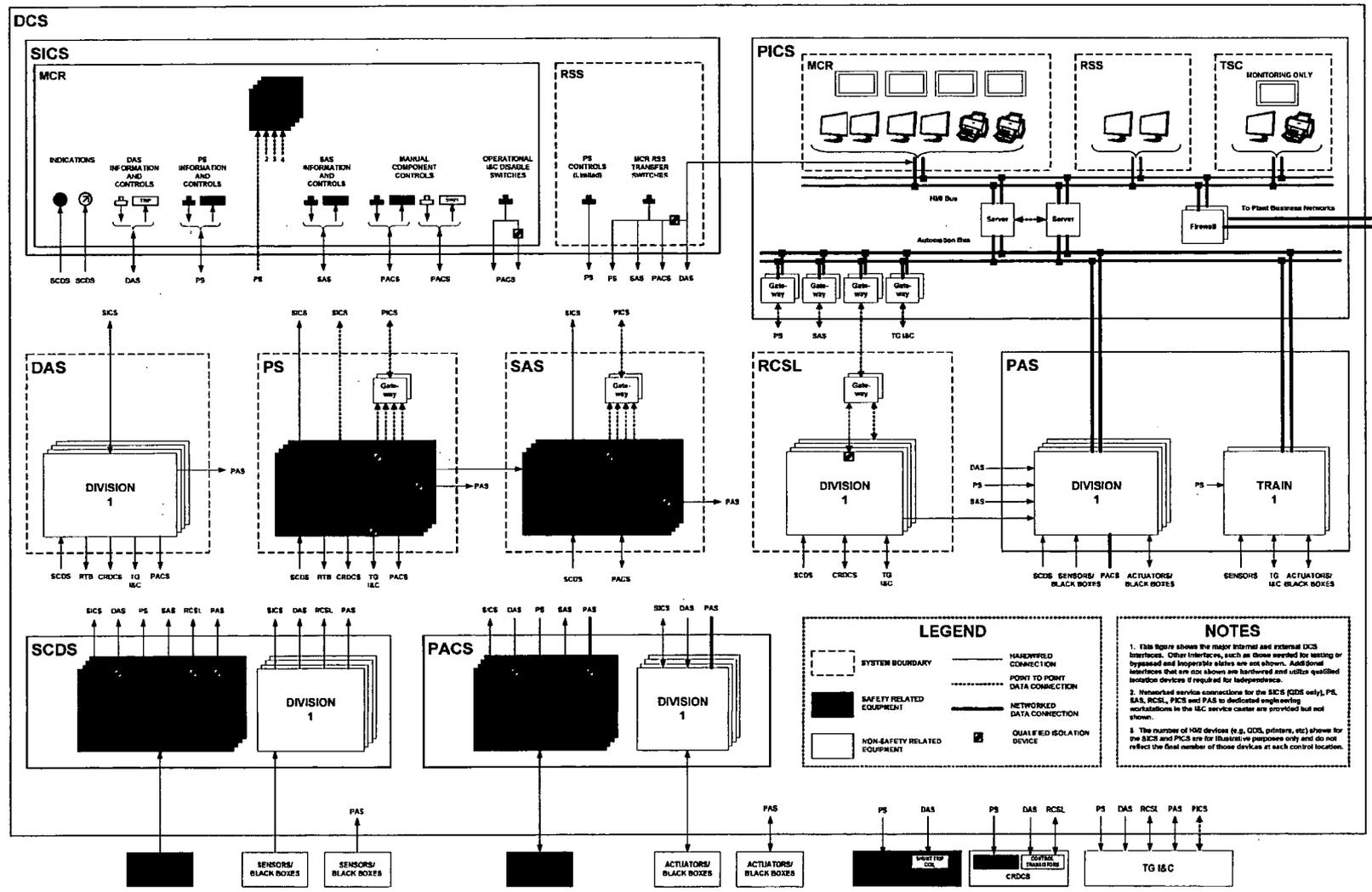
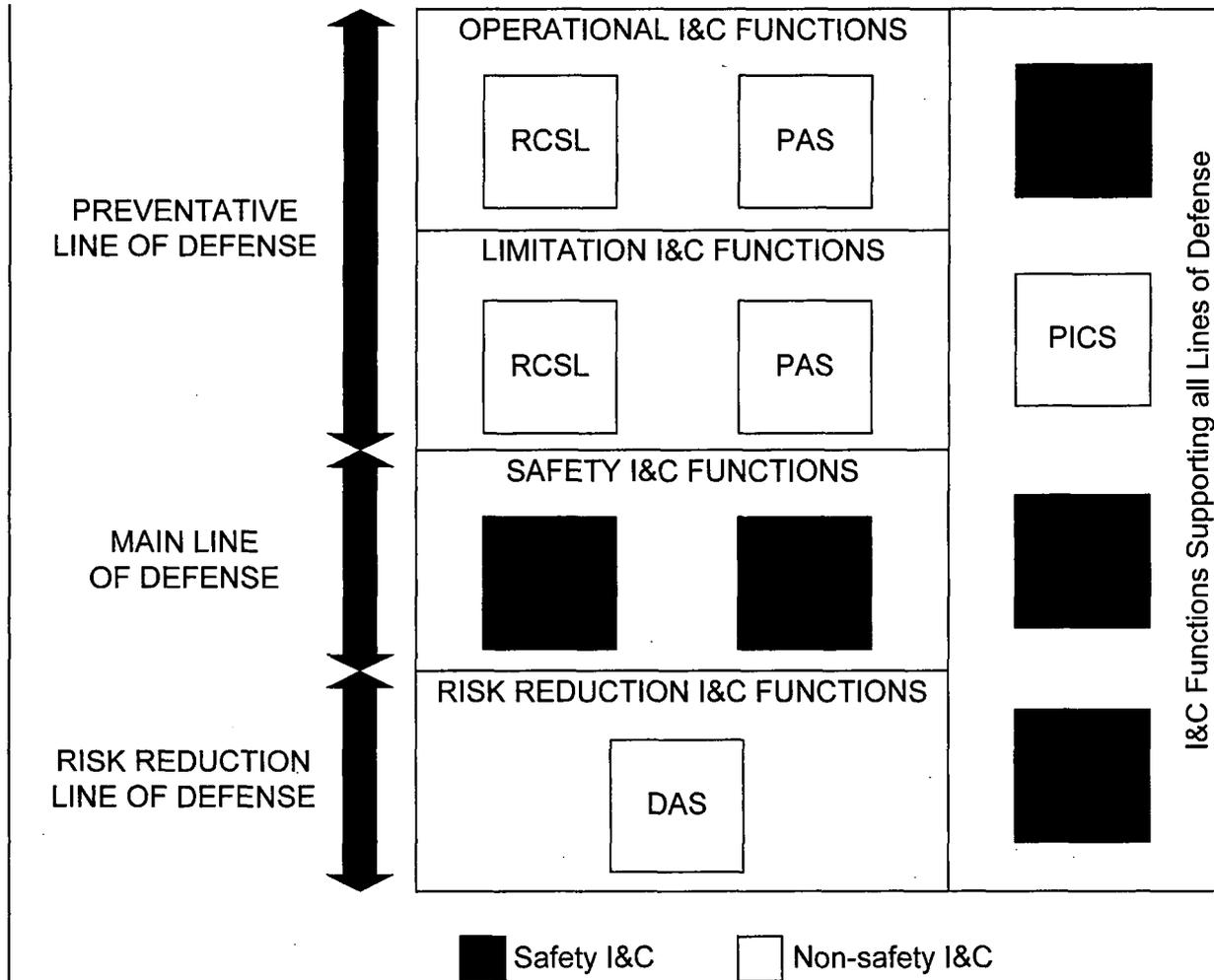


Figure 2-2—Lines of Defense and I&C Functions



### **3.0 DIVERSITY AND DEFENSE-IN-DEPTH FEATURES OF THE U.S. EPR I&C ARCHITECTURE**

The U.S. EPR I&C architecture withstands the effects of various CCFs that could prevent performance of the required safety functions. In general, the design utilizes two types of features:

- Features that prevent a CCF that could disable a safety function.
- Features that mitigate the effects of a postulated SWCCF that prevents the PS from responding to an AOO or PA.

#### **3.1 *Features that Prevent a CCF of the I&C Safety Systems (Main Line of Defense)***

##### **3.1.1 Equipment Design**

###### **3.1.1.1 TXS Platform**

TXS is a digital I&C platform designed specifically for use in safety systems in nuclear power plants. The TXS platform is used for the implementation of the PS and the SAS, as well as the ~~computerized portions QDS~~ of the SICS QDS. The NRC staff has approved the TXS platform for use in safety-related applications (Reference 10).

The TXS platform is designed with many features that enhance reliability and availability. These features are described in detail in Siemens Topical Report EMF-2110 (NP)(A), Revision 1 (Reference 13) and Siemens Topical Report EMF-2267(P), Revision 0 (Reference 14).

The following list summarizes the features of TXS that are designed to prevent a CCF of the platform and the reference where that feature is described further.

- Cyclic, deterministic, asynchronous operation—refer to Section 2.4.3.4 of Reference 13 and Sections 9.1 and 9.3 of Reference 14.
- Interference-free communications—refer to Section 2.9 of Reference 13 and Section 9.1 of Reference 14.
- Independence of the TXS platform operation (including both hardware and system software) from the application software program—refer to Section 2.4.2.2.1 of Reference 13 and Section 9.4 of Reference 14.

- Fault tolerance—refer to Section 2.7 of Reference 13.
- Equipment and system software qualification—refer to Section 2.2 of Reference 13
- The use of a standard library of application function blocks with operating experience—refer to Section 2.1.3.1 of Reference 13.

An analysis of postulated failures of the TXS platform is performed in Section 2.4.2 of Reference 13. The result of this analysis shows that random single failures are the dominant failure mode based on the system design features.

Additionally, a review of the TXS design features and various failure mechanisms are described in Section 9 of Reference 14. The results of this review, as discussed in Section 9.5 of Reference 14, demonstrate that a CCF is very unlikely, if appropriate design and testing measures are taken.

The TXS platform benefits from extensive operating experience. Internationally, TXS has been in use for over 10 years with over 62 million processor hours of operation. Section 5.2 of Reference 13 describes a configuration management plan, including a change control process. According to problem reports gathered as a result of the change control process, there have been no reported CCFs of the TXS platform system software to date.

#### **3.1.1.2 PACS Design**

The PACS is a prioritization system that is part of the TXS product family, and meets the requirements of 10 CFR 50.55a(h). The PACS operates independently of, and diverse to, the operational principles of the digital TXS platform discussed in Section 3.1.1.1. As previously mentioned, the safety-related priority module used in the PACS is subject to 100 percent combinatorial testing, to preclude consideration of SWCCF. Further descriptions of the PACS design and the 100 percent combinatorial testing methodology are found in Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report (Reference 11).

#### **3.1.1.3 SCDS Design**

The signal conditioning and distribution system (SCDS) is a conditioning and distribution system that is part of the TXS product familyline, and meets the requirements of 10 CFR 50.55a(h) subject to the alternative request described in Section 2.1. The SCDS operates independently

of, and diversely to, the operational principles of the digital TXS platform discussed in Section 3.1.1.1. The SCDS contains only analog conditioning and distribution equipment and is not considered subject to a SWCCF.

### **3.1.2 Safety I&C System Design**

#### **3.1.2.1 PS System Design**

Section 2.2 contains a general description of the PS. A detailed description of the PS architecture is provided in U.S. EPR Digital Protection System Technical Report (Reference 12). The PS is implemented with the TXS platform. In addition to the features inherent to TXS, the PS design incorporates the following features that are designed to prevent a CCF of the system:

- Signal diversity Subsystems within each division - Errors in requirement specification or application software design are potential sources of SWCCF. Separate subsystems that implement different reactor trip RT functions can prevent a design error in one reactor trip RT function from disabling another reactor trip RT function in the other subsystem that utilizes a diverse input parameter.
- Fail safe/fault tolerant design - A failure in one division is accommodated by voting logic in the other divisions so that those divisions remain capable of performing the safety function.
- Independence - Electrical isolation, physical separation, and communication isolation are implemented between divisions to prevent a failure in one division from propagating to redundant divisions.
- Diversity of RT devices - Multiple sets of RT devices, with each set capable of achieving the RT function, prevent a CCF of one set of devices from disabling the RT function.

~~The design of the PS is the direct result of the experience AREVA NP has developed in the area of digital protection systems installed internationally. This experience demonstrates that the dominant CCF mode for digital I&C systems is because of errors in the specification of the requirements (i.e., application software), not in the platform itself (i.e., hardware and system operating software). To specifically address this type of CCF, signal diversity is implemented in the design of the PS. The CCF prevention features discussed in Section 3.1.1.1 prevent a CCF~~

~~associated with application software from impacting the operating system software and propagating to diverse functions.~~

### **3.1.2.2 SAS System Design**

The SAS is implemented with the TXS platform. In addition to the features inherent to TXS, the design provides for independence between the four divisions of the SAS and between the SAS and interfacing non-safety systems. The characteristics of this independence are physical separation, electrical isolation, and communications independence, as described in U.S. EPR FSAR Tier 2, Section 7.1.

### **3.1.2.3 PACS System Design**

PACS 100 percent combinatorial testing demonstrates that the priority modules in PACS are not subject to SWCCF. Additionally, the design provides for independence between the four divisions of the PACS, and between the PACS and interfacing non-safety systems. The characteristics of this independence are physical separation, electrical isolation, and communications independence, as described in U.S. EPR FSAR Tier 2, Section 7.1.

### **3.1.3 Application Software Development Process**

The processes used to develop, test, and maintain application software for the I&C safety systems using TXS processors are described in Software Program Manual for TELEPERM XS Safety System Topical Report (Reference 15). These processes include the following:

- Software Quality Assurance Plan.
- Software Safety Plan.
- Software Verification and Validation Plan.
- Software Configuration Management Plan.
- Software Operations and Maintenance Plan.

Taken together, these plans provide a rigorous approach to the lifecycle management of application software in digital safety I&C systems that reduces the probability of a CCF disabling a safety function.

The TXS platform provides important tools to implement the software development processes and reduce the likelihood of a programming error. Function block programming and automatic code generation significantly reduce the complexity of the application software programming task, as compared to manual programming. The Simulation-based Validation Tool (SIVAT) provides the ability to test the application software against its requirements to verify proper functionality. ~~These tools are described in detail in Reference 15.~~

### **3.2 Features that Mitigate a Postulated SWCCF of the Protection System**

The features described in Section 3.1 reduce the likelihood of a CCF. However, it is postulated that an SWCCF occurs in the PS that prevents it from responding to an AOO or PA. This postulated SWCCF is such that the design features discussed in Section 3.1 are ineffective at preventing the failure. A system diverse from PS is provided to cope with this scenario. That system, the DAS, automatically initiates reactor trip and ESF functions, or allows manual execution of certain functions by the operator.

Additionally, substantial diversity attributes exist in several other I&C systems such that they can be demonstrated not to be subject to the same SWCCF postulated to occur in the PS concurrent with an AOO or PA. ~~These other systems may assist in event mitigation in case the postulated PS failure occurs.~~

Section 4.2 describes the diversity attributes that exist throughout the I&C architecture relative to the PS.

#### **3.2.1 Diversity between the Main Line of Defense and the Risk Reduction Line of Defense**

Only the portion of the risk reduction line of defense provided to directly mitigate the loss of the PS is required to be diverse from PS. In the U.S. EPR I&C design, the DAS performs these functions, and is implemented with a non-microprocessor based I&C platform. ~~digital I&C platform diverse from TXS.~~ Additionally, in conformance with BTP 7-19 Position 4, the PICS SICS is required to be diverse from the PS for system-level initiation of critical safety functions.

With respect to the TXS platform used to implement the PS, the platforms used for the DAS and PICS SICS exhibit the following attributes:

- The design architecture will be different.
- The design organization, management, designers, programmers, and testing engineers will be different.
- A non-computerized, hardwired platform will be used to implement the I&C functions.
- ~~The microprocessor CPU, input/output circuit boards, and bus structure will be from different manufacturers.~~
- The AC/DC power supplies, and DC/DC power supplies will be from different manufacturers.
- ~~The computer languages will be different.~~
- ~~The software operating systems will be different.~~
- ~~The software development tools will be different.~~
- ~~The software validation tools will be different.~~
- ~~The software algorithms, logic, program architecture, timing, and order of execution will be different.~~

### 3.2.1.1 Reactor Trip

The PS is the primary means of initiating RT. Assuming a postulated SWCCF renders the PS inoperable, there are two diverse means of initiating a RT. If an RT is required to be automatically initiated, it is performed by the DAS. If automatic initiation is not required, a manual, ~~hardwired~~ means of initiating an RT is provided on the SICS from either the MCR or RSS. The ~~hardwired~~ controls on SICS to initiate RT, as discussed in Section 2.1, are provided to address Point 4 of NUREG-0800, BTP 7-19. These controls consist of four switches; each is assigned to a division of DAS, an independent safety division. The controls are diverse; a software failure of the PS safety systems will not affect the operation of the ~~hardwired~~ controls.

For high reliability of the ~~reactor trip~~RT function, the power supply for the RCCAs can be interrupted in several diverse ways. The safety-related ~~reactor trip~~RT breakers contain both an undervoltage (UV) coil and a diverse shunt trip coil. Power to the UV coil can be interrupted by a signal from either the PS or the SICS in the MCR. The shunt trip coil receives signals from the DAS and the ~~reactor trip switch~~ in the RSS. The safety-related trip contactors are diverse

from the trip breakers, and receive actuation signals from the PS ~~or the SICS in the MCR~~. The non-safety-related control logic gates in the control rod drive control system (CRDCS) are diverse from the trip breaker and trip contactors, and receive a signal to interrupt power from the DAS, PS or the SICS in the MCR.

### 3.2.1.2 ESF Actuation

The PS is the primary means of performing ESF actuations. Assuming a postulated SWCCF renders the PS inoperable, there are ~~two~~ diverse means of performing an ESF actuation. If an ESF actuation is required to be automatic, it is performed by the DAS. If automatic actuation is not required, manual means of actuating an ESF system are provided from the PICS Additionally, manual system-level initiation of critical safety functions is available from the SICS, which is required to be diverse from the PS. The manual commands from SICS are combined with the automatic actuation logic in DAS.

### 3.2.1.3 Indications and Alarms

Diversity is provided for the processing and display of indications and alarms necessary to alert the operator to abnormal plant conditions, including type A, B and C post-accident monitoring variables, as defined in Regulatory Guide 1.97 (Reference 4). ~~The PS and SAS are~~ SCDS is the credited means of processing these variables, and the SICS is the credited means for display. ~~Since this display path bypasses any microprocessor-based systems; therefore, a diverse display is not required.~~ The PAS DAS provides redundant diverse-processing of sensor information because the DAS obtains sensor information independently of the PS and SAS software. and the PICS, which is used during all plant conditions, while it is available, provides a redundant diverse display. The indications provided via DAS and PICS conform to NRC guidance on diversity for post-accident monitoring in Regulatory Guide 1.97 and guidance on diverse indications per Point 4 of NUREG-0800, BTP 7-19.

## 4.0 DIVERSITY AND DEFENSE-IN-DEPTH ASSESSMENT

The guidance of NUREG-0800, BTP 7-19 recommends that, for designs that use digital ~~protection system~~ PSs, the applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to ~~common-cause failure~~ CCFs have been adequately addressed. BTP 7-19 guidance also states that NUREG/CR-6303 describes an acceptable method for performing such assessments. NUREG/CR-6303 contains 14 guidelines for performing a complete D3 assessment. The following sections describe the U.S. EPR D3 assessment relative to each NUREG/CR-6303 guideline.

### 4.1 *Guideline 1: Choosing Blocks*

It is clear from the stated purposes of BTP 7-19 and NUREG/CR-6303 that the focus of the D3 assessment is the ~~protection system~~ PS. The PS is shown as a system-level block diagram in U.S. EPR FSAR Figure 7.1-6. Based on NUREG/CR-6303, Guideline 1, the U.S. EPR PS system-level block diagram is already divided into appropriate blocks to perform the D3 assessment.

NUREG/CR-6303, Guideline 1 states: "the main criterion for selecting blocks (previously defined in Section 2.5) is that the actual mechanism of failure inside a block should not be significant to other blocks."

This criterion is satisfied by the U.S. EPR FSAR Tier 2, Figure 7.1-6 block diagram because each block contains all the equipment needed for that block to perform its function (e.g., I/O cards, communication modules, function processors). Essentially, any block can be removed from the diagram and all other blocks can still perform their function (as demonstrated by the system-level FMEA summary presented in U.S. EPR FSAR Tier 2, Sections 7.2 and 7.3).

Therefore, the system-level diagram of the U.S. EPR PS constitutes a block representation consistent with the intent of NUREG/CR-6303, Guideline 1.

However, AREVA NP recognizes that use of the PS system level diagram to perform the D3 assessment would naturally result in taking credit for portions of the PS to function correctly when other portions of the PS are impaired by SWCCF. For example, acquisition and processing unit (APU) A2 would be assumed to function in all four divisions if APU A1 failed in

all four divisions because APU A1 and APU A2 would not be viewed as "identical" blocks per Guideline 7. AREVA NP believes this approach, while consistent with the intent of NUREG/CR-6303, would result in an extensive and lengthy NRC review, which is undesirable. Additionally, the U.S. EPR design includes a diverse actuation system conservatively designed to mitigate AOOs and PAs, assuming a complete PS failure. The U.S. EPR design can satisfy D3 criteria without credit taken for any portion of the PS functioning correctly. Therefore, AREVA has chosen a more conservative block representation to use in performing the D3 assessment.

Because I&C systems outside the PS will be used to demonstrate adequate D3, these other systems are established as blocks in the diagram, and the PS is simplified to only two blocks, subsystem A and subsystem B. The subsystems within the PS are maintained as separate blocks, because they are functionally independent of each other, and they are designed specifically to implement signal diversity between them. Signal diversity for RT functions implemented in the subsystems of the PS is not credited to mitigate any events in the D3 plant response analysis. The subsystems are maintained as separate blocks simply to illustrate that signal diversity exists in the design to address type 3 failures as defined in NUREG/CR-6303. Section 4.11 addresses type 3 failures relative to the D3 plant response analysis for SWCCF of the PS.

The resulting block diagram used to perform the U.S. EPR D3 assessment is shown in Figure 4-1 ~~Figure 4-1~~. The connections in ~~Figure 4-1~~ that are numbered (1 thru 3) represent ~~connections where one I&C system initiates a specific function to be performed by a second I&C system. Those that are not numbered are general purpose interfaces between systems that~~ represent connections to perform all of the interfacing functions between those systems.

Note that not all major I&C systems are shown in the block diagram. The major I&C systems that ~~are excluded~~ are not included in the diagram may still be modeled in the D3 plant response analysis under best estimate assumptions to accurately model progression of an event, but are not needed to demonstrate the ability to terminate the events (see Section A.2.2); credited in the D3 assessment for various reasons:

**Severe Accident I&C**

~~The SA I&C is a system designed to perform very limited functionality, specifically, to mitigate a severe accident. These functions are not required to demonstrate adequate response to a design basis event. As such, SA I&C is not credited in the D3 assessment.~~

**Safety Information and Control System**

~~In the D3 assessment, no failures beyond the SWCCF of the PS are postulated. Therefore, PICS is considered operational and the operator is assumed to be controlling and monitoring the plant using PICS. Additionally, the PICS is required to be diverse from the PS because it is credited to satisfy BTP 7-19 position 4; so, it can clearly be credited in the D3 assessment to mitigate SWCCF of the PS. For these reasons, the SICS as a whole is not credited in the D3 assessment. Note that the hardwired RT on SICS is available to satisfy BTP 7-19 position 4, even though the SICS system is not represented on the block diagram.~~

**Reactor Control Surveillance and Limitation System**

The RCSL performs core control and limitation functions designed to prevent disturbances from requiring protective action. This functionality could be very useful, if credited in the D3 assessment to mitigate a PS SWCCF. RCSL is implemented in the same technology as the PS and acquires many of the same measurements as the PS, but has significantly different functionality than the PS. This results in very different application software and allows a sound argument to be made that RCSL would not be subject to the same SWCCF as the PS, concurrent with a DBE. However, because of the multiple similarities between PS and RCSL, a conservative decision is made not to credit the RCSL to terminate events in the D3 assessment.

**Process Information and Control System**

In the D3 assessment, no failures are postulated beyond the SWCCF of the PS are postulated. Therefore, PICS is therefore considered operational and the operator is assumed to be controlling and monitoring the plant using PICS. This assumption allows the event progression to be accurately modeled. All manual control functions that are credited in the D3 analysis are performed in SICS.

### **Process Automation System**

In the D3 assessment, no failures beyond the SWCCF of the PS are postulated. Therefore, PAS is therefore considered operational. As part of best estimate assumptions, normally operating control functions in PAS, such as (e.g., pressurizer level control, and pressurizer pressure control,) continue to operate following a SWCCF. The only PAS function that relies on a PS output is the Partial Gcooldown Aactuation. Because it relies on a PS output, this function is not assumed to be operational in the D3 analysis. This assumption allows the event progression to be accurately modeled taking into account the effects on plant systems caused by the normally operating PAS functions.

#### **4.2 Guideline 2: Determining Diversity**

The next step of the assessment involves establishing diversity attributes, for each block in the diagram, relative to the PS. The diversity attributes of the PS subsystems are established relative to each other.

NUREG/CR-6303, Guideline 2 defines the following six diversity attributes:

- Design diversity.
- Equipment diversity.
- Functional diversity.
- Human diversity.
- Signal diversity.
- Software diversity.

Guideline 2 also defines, for each diversity attribute, design characteristics that can be used to establish the existence and strength of the diversity attribute. In NUREG/CR-6303, these design characteristics are listed in decreasing order of effectiveness.

Commitments made in the U.S. EPR FSAR regarding I&C system architectures and functionality and the commitments relative to platform diversity made in Section 3.2.1 are used to define design characteristics that establish diversity attributes for each I&C system, relative to the PS. For each block in the diagram, the established diversity attributes are placed into one of

two categories: those supported by one of the more effective design characteristics (higher on the NUREG/CR-6303 list); and, those supported by one of the less effective design characteristics (lower on the NUREG/CR-6303 list).

The diversity attributes exhibited by each block in the diagram are discussed below.

### **PS Subsystems:**

The PS subsystems, A and B, exhibit the following diversity attributes, relative to each other:

- **Design diversity**—Subsystems A and B have different architectures. For example, ~~Subsystem A contains remote acquisition units (RAU) while Subsystem B does not.~~ Subsystem A contains three APUs while Subsystem B contains two APUs. These architectural differences result in different network topologies and different communication patterns between the functional units within a subsystem. Different architecture is a “less effective”, but still relevant, characteristic of design diversity.
- **Signal diversity**—Subsystems A and B acquire measurements from different sensors measuring different process parameters, to perform RT functions that can protect against the same events. For example, one subsystem performs an RT on low reactor coolant system (RCS) flowrate, while the other subsystem performs an RT on low reactor coolant pump (RCP) speed. Using different reactor or process parameters sensed by different physical effects is a “more effective” characteristic of signal diversity.
- **Software diversity**—Subsystems A and B perform different algorithms and logic. The standard TXS software blocks are configured differently, to perform the different logical functions that compose each protective action. Different algorithms and logic is a “more effective” characteristic of software diversity. However, because the same or similar standard software blocks are used to achieve different logic, a conservative decision has been made to credit this type of different logic as a “less effective”, but still relevant, characteristic of software diversity.

### **Safety Information and Control System:**

The SICS exhibits the following diversity attributes relative to the PS:

- Design diversity—The control functions and indications provided in SICS are performed by hardwired, analog components. The PS uses digital processors to implement its functions. Including different technology in the design is a “more effective” characteristic of design diversity.
- Equipment diversity—At a minimum, the SICS equipment will be of fundamentally different design than the PS equipment. Section 3.2.1 identifies this commitment. The use of fundamentally different designs is a “more effective” characteristic of equipment diversity.
- Functional diversity—The SICS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The SICS is a human-machine interface system that allows the operator to monitor and control plant operation. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Different purpose and function is a “more effective” characteristic of functional diversity.
- Human diversity—At a minimum, different engineers will be responsible for the design of the SICS and PS. It is likely that different design organizations will be responsible for the design of the equipment of the two systems, which is ~~the strongest~~ most effective characteristic of human diversity, but ~~this won't be known for certain~~ will not be determined until the detailed design of these systems is in progress ~~underway~~. ~~To be conservative,~~ As a conservative measure, only the use of different engineers is credited in human diversity, which constitutes a “less effective”, but still relevant, characteristic of human diversity.
- Software diversity—The SICS uses a hardwired, analog I&C platform to implement a human-machine interface. There is no software running in the SICS, ~~(with exception of the QDS, which is for display purposes only and is not credited in the D3 analysis.)~~ This constitutes a “more effective” characteristic of software diversity.

#### Process Information and Control System:

The PICS exhibits the following diversity attributes relative to the PS:

- Design diversity—The PICS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. Different architecture is a “less effective”, but still relevant, characteristic of design diversity.

- ~~Equipment diversity~~—At a minimum, the PICS equipment will be of fundamentally different design than the PS equipment. Section 3.2.1 identifies this commitment. The use of fundamentally different designs is a “more effective” characteristic of equipment diversity.
- ~~Functional diversity~~—The PICS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The PICS is a human-machine interface system that allows the operator to monitor and control plant operation. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Two systems with different purposes and functions require significantly different application software structures. This greatly reduces the risk of the same latent software defect existing in the two systems. Different purpose and function is a “more effective” characteristic of functional diversity.
- ~~Human diversity~~—At a minimum, different engineers will be responsible for the design of the PICS and PS. It is likely that different design organizations will be responsible for the software design of the two systems (the ~~strongest-most effective~~ characteristic of human diversity. ~~), but (This won't be known for certain will not be determined~~ until the detailed software design of these systems is ~~in progress~~ underway. ~~To be conservative~~ As a conservative measure, only the use of different engineers is credited, which constitutes a “less effective”, but still relevant, characteristic of human diversity.
- ~~Signal diversity~~—The PICS does not directly acquire signals from process measurement sensors. Inputs to the PICS are in the form of manual commands from the operator and incoming data messages from the various I&C systems. The PICS ~~clearly senses~~ different reactor or process parameters (i.e., ~~PICS doesn't directly sense these parameters at all~~) than the PS, which is a “more effective” characteristic of signal diversity.
- ~~Software diversity~~—Because of its different purpose and function, the PICS uses completely different algorithms and logic than the PS; and, PICS functions are built from a non-TXS set of standard software blocks. This constitutes a clear case of different algorithms and logic, which is a “more effective” characteristic of software diversity.

**Process Automation System:**

The PAS exhibits the following diversity attributes relative to the PS:

- Design diversity—The PAS system architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. Most significantly, PAS is redundant within a division, while the PS is redundant between divisions. Also, PAS is a single layer system (only a control unit layer) while the PS is a multi-layer system (RAU, APU, actuation logic unit). Different architecture is a “less effective”, but still relevant, characteristic of design diversity.
- Equipment diversity—The PAS equipment is specified to be an industrial control platform other than TXS. This means the PAS equipment will be of fundamentally different design than the PS equipment. The use of fundamentally different designs is a “more effective” characteristic of equipment diversity.
- Functional diversity—The PAS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The PAS performs automated control functions to regulate the majority of the plant systems. The PAS also processes commands from the PICS, to allow the operator to manually control the majority of plant actuators. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Two systems with different purposes and functions require significantly different application software structures. This greatly reduces the risk of the same latent software defect existing in the two systems. Different purpose and function is a “more effective” characteristic of functional diversity.
- Human diversity—At a minimum, different engineers will be responsible for the design of the PAS and PS. It is likely that different design organizations will be responsible for the software design of the two systems (the strongest-most effective characteristic of human diversity), but ~~it~~ will not be determined until the detailed software design of these systems is underway. To be conservative, only the use of different engineers is credited, which constitutes a “less effective”, but still relevant, characteristic of human diversity.
- Signal diversity—The vast majority of sensors acquired by the PAS are not acquired by the PS, and vice versa. A small set of sensors may be used by both systems; however,

those signals would be used for fundamentally different purposes (e.g., signal selection algorithms for closed loop control in PAS vs. coincidence voting logic for actuation in PS). The PAS largely uses different process sensor measurements than the PS, which is a "more effective" characteristic of signal diversity.

- Software diversity—The PAS uses completely different algorithms and logic than the PS (because of its different purpose and function) that are built from a non-TXS set of standard software blocks. This constitutes a clear case of different algorithms and logic, which is a "more effective" characteristic of software diversity.

### **Safety Automation System:**

The SAS exhibits the following diversity attributes relative to the PS:

- Design diversity—The SAS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and is clearly different from the PS architecture. Most significantly, SAS is a single layer system (only a control unit layer) while the PS is a multi-layer system (RAU, APU, actuation logic unit). Different architecture is a "less effective", but still relevant, characteristic of design diversity.
- Functional diversity—The SAS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The SAS performs automated control functions of safety-related plant systems, to regulate those systems during normal operation. The SAS also processes commands from the PICS and SICS to allow the operator to manually control the safety-related plant systems. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Two systems with different purposes and functions require significantly different application software structures. This greatly reduces the risk of the same latent software defect existing in the two systems. Different purpose and function is a "more effective" characteristic of functional diversity.
- Signal diversity—The vast majority of sensors acquired by the SAS are not acquired by the PS, and vice versa. A small set of sensors is used by both systems; however, those signals are used for fundamentally different purposes (e.g., signal selection algorithms for closed loop control in SAS vs. coincidence voting logic for actuation in PS). Additionally, the functions in SAS that use the same sensors as the PS rely on PS

outputs for initiation and are therefore not credited to mitigate a PS failure in the D3 assessment. The use of different process parameters as inputs is a "more effective" characteristic of signal diversity.

- **Software diversity**—The SAS performs different algorithms and logic than the PS. The standard TXS software blocks are configured differently in each system to perform the different algorithms and logical functions. Different algorithms and logic is a "more effective" characteristic of software diversity. However, because the same or similar standard software blocks are used to achieve different logic, a conservative decision has been made to credit this type of different logic as a "less effective", but still relevant, characteristic of software diversity.

#### **Diverse Actuation System:**

The DAS exhibits the following diversity attributes relative to the PS:

- **Design diversity**—~~Though the equipment used in the DAS, is while considered digital, it is a fundamentally different approach to digital technology than employed that in the PS. For instance (e.g., the programmable logic device or discrete electronics in DAS vs. versus processors running application software in the PS). This constitutes a different approach within a technology, as listed in Guideline 2. Additionally, the DAS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. This combination of multiple design characteristics establishes a "more effective" case of design diversity. The DAS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. Most significantly, DAS is a single layer system (only a diverse actuation unit layer), while the PS is a multi-layer system (RAU, APU, actuation logic unit). Different architecture is a "less effective", but still relevant characteristic of design diversity.~~
- **Equipment diversity**—At a minimum, the DAS equipment will be a fundamentally different design than the PS equipment. Section 3.2.1 identifies this commitment. The use of a fundamentally different design is a "more effective" characteristic of equipment diversity.
- **Functional diversity**—The DAS is designed with the intent of allowing the PS to actuate before the DAS, in response to a ~~design basis event~~ DBE. This results in different

setpoint parameters and delay times for the DAS functions, compared to the PS. Different response timescale is a "less effective", but still relevant, characteristic of functional diversity.

- ~~Human diversity~~—At a minimum, different engineers will be responsible for the design of the DAS and PS. It is likely that different design organizations will be responsible for the ~~software~~ design of the two systems (the ~~strongest-most effective~~ characteristic of human diversity. ~~), but t~~This won't be known for certain will not be determined until the detailed ~~software~~ design of these systems is underway in progress. To be conservative, only the use of different engineers is credited, which constitutes a "less effective", but still relevant characteristic of human diversity.
- ~~Software diversity~~—While the DAS uses similar functional logic as the PS, the DAS uses non-microprocessor based technology to implement its functions. There is no software running in the DAS. This implementation in a different platform dictates that the DAS logic will be built from a non-TXS set of standard software blocks. Additionally, the program architecture will be different, the timing of the systems will be different, and a different operating system will be used. This combination of multiple design characteristics establishes a "more effective" case of software diversity.

#### **Priority and Actuator Control System:**

The PACS exhibits the following diversity attributes relative to the PS:

- ~~Design diversity~~—The equipment used in the priority module of the PACS, while considered digital, is a fundamentally different approach to digital technology than employed in the PS (i.e., programmable logic device in PACS vs. processors running application software in the PS). This constitutes a different approach within a technology, as listed in Guideline 2. Additionally, the PACS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. Most significantly, a standalone portion of the PACS is dedicated to each safety-related plant actuator, while the PS uses its whole architecture to affect groups of actuators. This combination of multiple design characteristics establishes a "more effective" case of software design diversity.

- Equipment diversity—The PACS equipment is of fundamentally different design than the PS equipment (i.e., programmable logic device in PACS vs. processors running application software in the PS). Regardless of whether a different manufacturer is used, a fundamentally different equipment design is a “more effective” characteristic of equipment diversity.
- Functional diversity—The PACS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The PACS performs priority logic on signals from multiple I&C systems, so that each safety-related actuator is in the proper state for the current plant condition. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Different purpose and function is a “more effective” characteristic of functional diversity.
- Signal diversity—The PACS does not acquire any input sensors that are acquired by the PS. The use of different process sensor measurements is a “more effective” characteristic of signal diversity.
- Software diversity—Unlike the function processors of the PS, the priority modules in the PACS do not utilize application software; they are pre-configured to perform static logic functions. The PACS exhibits all of the design characteristics that support software diversity from the PS, which is clearly a “more effective” case of software diversity.

#### **Signal Conditioning and Distribution System:**

The SCDS exhibits the following diversity attributes relative to the PS:

- Design diversity—The signal conditioning and distribution functions performed by the SCDS are done by analog modules. The PS uses digital processors to implement its automated functions. Different technology is a “more effective” case of design diversity.
- Equipment diversity—The SCDS equipment is of fundamentally different design than the PS equipment (i.e., analog signal conditioning modules in the SCDS vs. processors running application software in the PS). Regardless of whether a different manufacturer is used, a fundamentally different equipment design is a “more effective” characteristic of equipment diversity.

- Functional diversity—The SCDS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The SCDS performs signal conditioning and distribution on signals from the sensors and black box systems. The PS performs automatic actuation functions specifically designed to respond to AOOs or PASAs. Different purpose and function is a “more effective” characteristic of functional diversity.
- Human diversity—At a minimum, different engineers will be responsible for the design of the SCDS and PS. It is possible that different design organizations will be responsible for the equipment design of the two systems (the strongest most effective characteristic of human diversity). ~~T, but this won't be known for certain~~ will not be determined until the detailed design of these systems is ~~underway~~ in progress. To be conservative, only the use of different engineers is credited, which constitutes a “less effective”, but still relevant, characteristic of human diversity.
- Software diversity—The SCDS uses hardwired, analog equipment to implement signal conditioning and distribution. There is no software running in the SCDS. This constitutes a “more effective” case of software diversity.

Following the Guideline 2 diversity assessment, each block in the block representation is updated to include its diversity attributes, as described above. If the diversity attribute was determined to be “more effective”, it is listed in red. Those diversity attributes that were determined to be “less effective”, but still relevant, are listed in blue. The updated block diagram is shown in ~~Figure 4-2~~ Figure 4-2.

### 4.3 **Guideline 3: System Failure Types**

NUREG/CR-6303 defines three failure types to be addressed in the assessment:

#### **Type 1 Failures**

This type of failure occurs when a plant transient is induced by a failure in the control system, and, because of some interaction between the control and ~~protection system~~ PSs (e.g., common sensors as inputs), the protective functions required to mitigate the transient also fail.

NUREG/CR-6303 states that assessment of type 1 failures is required by Guideline 12.

Therefore, U.S. EPR mitigation of type 1 failures is discussed in Section 4.12.

## Type 2 Failures

This type of failure occurs when the PS simply fails to respond to occurrence of a ~~design-basis event~~DBE, due to a ~~software common-cause failure~~SWCCF in redundant portions of the PS. NUREG/CR-6303 states that assessment of type 2 failures is required by Guidelines 10 and 11. Therefore, U.S. EPR mitigation of type 2 failures is discussed in Sections 4.10 and 4.11.

## Type 3 Failures

This type of failure occurs when a common mode failure of redundant input sensors prevents the PS from responding to occurrence of a ~~design-basis event~~DBE. NUREG/CR-6303 states that assessment of type 3 failures is required by Guidelines 10 and 11. Therefore, U.S. EPR mitigation of type 3 failures is discussed in Sections 4.10 and 4.11.

### 4.4 *Guideline 4: Echelon Requirement*

Section 2 describes the U.S. EPR I&C architecture. Section 2.4 describes the lines of defense within the I&C architecture and Section 2.5 compares these lines of defense to the echelons of defense defined in NUREG/CR-6303 Guideline 4.

### 4.5 *Guideline 5: Method of Evaluation*

In accordance with NUREG/CR-6303, when performing the SWCCF assessment, the PS is treated as a black box and all PS outputs are assumed to fail. For the purpose of evaluating an SWCCF, no credit is taken for one subsystem of the PS to function correctly, if the other fails (i.e., the PS is treated as one block). The subsystems are treated as separate blocks only when considering common-cause sensor failures. The following assumptions are used to define the PS failure modes resulting from a postulated SWCCF concurrent with a ~~design-basis event~~DBE:

- The PS functions credited in the U.S. EPR FSAR Tier 2, Chapter 15 safety analysis to protect against a given AOO or PA do not respond. Two scenarios are possible:
  - Complete failure—No PS outputs credited in the U.S. EPR FSAR Tier 2, Chapter 15 event respond.
  - Partial failure—Some PS outputs credited in the U.S. EPR FSAR Tier 2, Chapter 15 event respond correctly, but others do not.

- PS outputs that are not credited to mitigate the U.S. EPR FSAR Tier 2, Chapter 15 event do not fail in a manner to worsen the consequences of the event.
- “Smart” failures (i.e., the worst possible combinations of multiple failures) are assumed not to occur.

#### **4.6 Guideline 6: Postulated Common-Mode Failure of Blocks**

NUREG/CR-6303 Guideline 6 states that: “Analysis of defense-in-depth should be performed by postulating concurrent failures of the same block or identical blocks (as defined in Guideline 7) in all redundant divisions.”

Guideline 6 was taken into account in developing the block diagram shown in Figure 4-2Figure 4-2. The block diagram already combines all divisions of the PS into one block so that, when that block is failed, all divisions are assumed to fail.

#### **4.7 Guideline 7: Use of Identical Hardware and Software Modules**

NUREG/CR-6303 Guideline 7 recommends that blocks are to be considered identical, when the likelihood of SWCCF affecting them simultaneously is acceptably low. Guideline 7 is taken into account in the development of the block diagram shown in Figure 4-2Figure 4-2, mainly by making two conservative assumptions:

- All of the functional units in each subsystem of the PS (e.g., RAU, APU, actuation logic unit.) are considered identical, although the NUREG/CR-6303 guidance would support their use as separate, non-identical blocks.
- The RCSL is considered identical to the PS, although the NUREG/CR-6303 guidance would support its use as a separate, non-identical block.

The diversity attributes in Guideline 2 are used to establish the non-identical nature of the other blocks in the diagram relative to the PS. Section 4.2 describes the diversity attributes that are established for each block.

#### **4.8 Guideline 8: Effect of Other Blocks**

Guideline 8 indicates that signals from failed blocks should be propagated to downstream blocks that function correctly in response to the possibly erroneous signals. In the block

diagram shown in ~~Figure 4-2~~Figure 4-2, the signals from the PS to downstream blocks are shown. It should be noted that, for signals from the PS in response to an AOO or PA, only hardwired connections are used. This feature is important because it limits failure propagation modes to "physical" (as defined in NUREG/CR-6303 Guideline 1) and excludes the possibility of "logical" failure propagation.

In the U.S. EPR D3 assessment, downstream blocks are assumed to function correctly in response to the PS output failures defined in Section 4.5. Essentially, the PS fails to respond to the AOO or PA; so, any follow on actions normally taken by downstream blocks do not occur.

#### **4.9      *Guideline 9: Output Signals***

In accordance with Guideline 9, the U.S. EPR assessment assumes that failures do not propagate backwards into an output of a previous block.

In the block diagram shown in Figure 4-2, no block output is influenced by a failure of equipment connected to another output of the same block.

#### **4.10      *Guideline 10: Diversity for Anticipated Operational Occurrences***

NUREG/CR-6303 Guideline 10 indicates that each AOO should be analyzed in conjunction with the postulated ~~common-cause failure~~CCFs. Appendix A presents the results of such an analysis (referred to hereafter as the "D3 plant response analysis").

A detailed discussion of what types of ~~common-cause failure~~CCFs are postulated to occur simultaneously with a ~~design-basis event~~DBE (AOO or PA) is presented in Section 4.11, and it is applicable to both the Guideline 10 and Guideline 11 analysis.

#### **4.11      *Guideline 11: Diversity for Accidents***

NUREG/CR-6303 Guideline 11 indicates that each PA should be evaluated in conjunction with the postulated ~~common-cause failure~~CCFs. Appendix A presents the results of such an analysis.

The D3 plant response analysis is performed to assess conformance to BTP 7-19, using NUREG/CR-6303 as guidance for the analysis methodology. NUREG/CR-6303 Guidelines 10 and 11 suggest performing the plant response analysis considering type 2 and type 3 failures.

However, BTP 7-19 is clear that the need for performing this analysis is based solely on concerns regarding SWCCF in digital ~~protection system~~ PSs. Therefore, type 3 failures (common failure of sensors) are outside the scope of the analysis required by BTP 7-19, if no software-based sensors are used. The U.S. EPR design does not use software-based sensors as inputs to the PS. For this reason, the D3 plant response analysis is performed assuming only type 2 SWCCFs concurrent with AOOs and PAs.

Although type 3 failures are not considered in the D3 plant response analysis, it should be noted that the U.S. EPR design includes signal diversity for RT functions utilizing ~~between~~ the subsystems of the PS. This design feature is described in Reference 12. Signal diversity is provided specifically to mitigate type 3 failures. Additionally, signal selection and/or voting logic within the PS contributes to mitigating failures of multiple, redundant sensors.

To perform the D3 plant response analysis using a best estimate approach (as allowed by BTP 7-19), the analysis must identify the I&C functionality it assumes to remain available following the postulated SWCCF of the PS concurrent with an AOO or PA. This is done so that functions that would remain available, but are not credited in the U.S. EPR FSAR Tier 2, Chapter 15 safety analysis, can be modeled and credited appropriately in the D3 plant response analysis.

The approach to identify I&C functionality that is unaffected by the postulated SWCCF of the PS consists of three steps.

1. Identify SWCCFs that could credibly occur in the PS concurrent with an AOO or PA..
2. Define boundaries for the effects of the postulated SWCCFs.
3. Assess the other I&C systems with respect to the credible SWCCFs to identify I&C functionality that is unaffected.

#### **4.11.1 Identification of Credible SWCCF**

Three premises are used as the basis to identify credible SWCCFs that could occur in the PS concurrent with an AOO or PA. Each premise is discussed below.

##### **Premise #1**

For a ~~common-cause failure~~ CCF to occur, two conditions must be present:

1. An identical, latent defect must exist in multiple redundancies of a system.
2. A triggering condition must occur, in multiple redundancies, that exposes the latent defect.

If one of the two conditions in premise #1 does not exist, a failure does not occur. This premise is useful in defining boundaries for the effects of a postulated SWCCF. If it is established that two I&C systems are not likely to contain identical latent defects, or that two I&C systems are not subjected to the same triggering condition, then those two I&C systems are not subject to the same SWCCF.

### **Premise #2**

Only latent software defects and triggering conditions that could expose software defects are considered concurrently with occurrence of an AOO or PA.

This premise essentially eliminates hardware defects and triggering conditions that could only reveal hardware defects. Premise #2 is consistent with the BTP 7-19 explanation of the basis for performing the D3 plant response analysis:

The above four point position is based on the NRC concern that software design errors are a credible source of ~~common-cause failure~~ CCFs. Software cannot typically be proven to be error-free and is therefore considered susceptible to ~~common-cause failure~~ CCFs because identical copies of the software are present in redundant channels of safety-related systems.

### **Premise #3**

A triggering condition that is not related to occurrence of an AOO or PA will not expose a latent defect simultaneously with occurrence of an AOO or PA.

This premise means that only combinations of triggering conditions that are directly related to occurrence of an AOO or PA, and the latent defects that could be revealed by those triggers, are considered to exist concurrent with an AOO or PA. Premise #3 is the logical conclusion of progressive reasoning:

- A postulated SWCCF (latent defect in multiple redundancies exposed by a corresponding trigger) in the PS is a rare event. This is based on extensive operating experience of the TXS platform, with no such failure occurring.
- A postulated SWCCF in the PS (rare event) that is triggered by an AOO or PA is an extremely rare event because it requires existence of a specific defect that is subject to a specific AOO or PA trigger.
- A postulated SWCCF in the PS concurrent with an AOO or PA (extremely rare event) where the trigger is unrelated to occurrence of the AOO or PA would require:
  - a latent defect to exist.
  - occurrence of a specific triggering condition that reveals the defect but is unrelated to occurrence of an AOO or PA..
  - occurrence of an AOO or PA.

The existence of these three conditions simultaneously is incredible.

A simple matrix can be constructed by applying the three premises discussed above. This matrix is shown in Figure 4-3 and illustrates the category of SWCCF that can credibly be assumed to occur in the PS concurrent with an AOO or PA.

As shown in Figure 4-3, triggering conditions can be placed into one of two categories: those that result from occurrence of an AOO or PA, and those that do not. Likewise, latent software errors can be placed into one of two categories: those that could be exposed by an AOO or PA trigger, and those that could not. As indicated in Figure 4-3, only those SWCCFs that can credibly be assumed to occur in the PS concurrent with an AOO or PA are considered in the D3 plant response analysis.

#### **4.11.2 Establishing Boundaries for the Effects of Postulated SWCCFs**

Section 4.11.1 identifies the category of credible SWCCFs that could occur in the PS concurrent with an AOO or PA. Boundaries for the effects of those credible SWCCFs can be established by examining the nature of relevant triggering conditions, and fundamental characteristics of the TXS platform.

**Triggering Conditions:**

There are only three ways in which the computerized portion of the PS can be influenced by interfaces with the remainder of the power plant:

- Through sensor measurements that change as a function of the process parameter they measure.
- Through information received from a human-machine interface system reflecting any operator commands.
- Through the physical environment where the system resides (e.g., temperature, humidity).

The occurrence of an AOO or PA could result in the PS “seeing” changes at any one of these interface points.

Any triggering conditions involving a change in the physical environment cannot reveal a latent software defect, only a hardware defect. Therefore, according to Premise #2, environmental triggers are not considered in the D3 plant response analysis. This leaves the first two interfaces (i.e., sensor inputs and manual inputs) as the triggering conditions of concern that could reveal a latent software defect concurrent with an AOO or PA.

**TELEPERM XS Software Characteristics:**

The TXS software is described in Reference 13. For convenience, ~~Figure 4-4~~ ~~Figure 4-4~~ is a reproduction of Figure 3.5 from Reference 13. As shown in ~~Figure 4-4~~ ~~Figure 4-4~~, the TXS software can be divided into three layers: Operating system software layer, platform software layer, and application software layer.

The operating system software layer and the platform software layer together constitute the “system software”; that is, the portion of TXS software that is not configured differently to suit each specific application (e.g., U.S. EPR PS application). The application software layer is configured uniquely for each TXS processor to perform its required functions relative to plant operation (i.e., functional requirements). This distinction is made to highlight the fact that there is no interface between the system software and the power plant. The application software

layer is responsible for performing all logical functions that use sensor measurements or manual commands as inputs. ~~Figure 4-5~~Figure 4-5 illustrates this principle.

A fundamental design requirement of TXS to ~~ensure~~verify deterministic behavior is to prevent interference by plant process data on the system software (Reference 13). The following are key characteristics of TXS that exist to satisfy this requirement:

- The operating system is kept simple.
- Only basic, uncomplicated multi-tasking is used.
- No plant or application-dependent interrupts are used. Only a simple timer interrupt exists.
- Strictly cyclic processing is employed.
  - A constant number of input/output parameters are processed each cycle.
  - A constant number of data messages are transferred each cycle. Each message is a fixed length.
  - Data messages are transferred in a fixed sequence each cycle.
- The "system software" performs no interpretation of data values processed by the application software layer.
- There is no increase or decrease in communication loading as plant conditions change.

These characteristics are discussed in further detail in Reference 13.

To summarize, the TXS "system software" is in continuous use and performs its functions the same way every processing cycle, regardless of external plant conditions. By design, it does not change its behavior in response to occurrence of an AOO or PA. It can therefore be reasonably concluded that any latent software error existing in the "system software" is not subject to an AOO or PA triggering condition. This is not to say that an SWCCF cannot occur in the TXS "system software"; a triggering condition unrelated to occurrence of an AOO or PA could reveal a latent error in the "system software". However, per premise #3, it is incredible that such a triggering condition could exist concurrently with an AOO or PA. Further, given that the "system software" continuously performs its functions in the same manner every processing

cycle, such a failure would be self-revealing (likely on system start-up) and would not remain latent until occurrence of an AOO or PA.

Based on the discussion above, it is concluded that boundaries for the effects of a postulated SWCCF in the PS concurrent with a ~~design basis event~~DBE are as follows:

- The failure originates because of a change in inputs (i.e., sensor measurement or manual command) resulting from an AOO or PA that reveals a latent defect in the PS application software layer.
- The failure does not affect the TXS "system software."
- If the PS and a separate TXS-based system do not have the same sensor measurements or manual commands as inputs, the failure does not affect the application software layer of the other system.
- If common sensor inputs are used between the PS and a separate TXS-based system, the failure does not affect the other system if strong functional or software diversity characteristics are exhibited by the other system
- If an I&C system implemented in technology different from TXS exhibits strong functional or software diversity characteristics, then the failure does not affect those systems, even if they use the same sensor measurements as inputs.

Based on the discussion of diversity attributes in Section 4.2, it is concluded that these boundaries correspond to the boundaries of the PS in the block diagram in Figure 4-2  
4-2.

A reasonable input assumption for the D3 plant response analysis is that a postulated SWCCF in the PS concurrent with an AOO or PA does not affect I&C functions outside of the PS, if those functions do not rely on a PS output.

#### **4.12 Guideline 12: Diversity among Echelons of Defense**

NUREG/CR-6303 Guideline 12 focuses on control systems and identifies three roles that those systems play in defense-in-depth. The U.S. EPR design addresses each of these three roles.

- They prevent the need for protective action by controlling disturbances.

- They could fail, resulting in the need for protective action (type 1 failure from Guideline 3).
- They could assist in event mitigation in case of a CCF of the PS.

The RCSL and PAS perform control functions during normal operation that are designed to maintain key plant parameters in ranges that preclude the need for protective action. The RCSL also includes limitation functions specifically designed to take more aggressive action (e.g., partial reactor trip) if the normal controls are ineffective at controlling a disturbance.

Regarding control system failures, Guideline 12 indicates that type 1 failures are addressed by compliance with GDC 24. The guideline states that, "the control system and the protection system~~PS~~ should not be disabled by the same single failure." In the U.S. EPR design, compliance to GDC 24 and mitigation of type 1 failures is provided by:

- Independence between the PS and the control systems
- Signal selection algorithms in the control systems
- Redundancy, fault detection and voting logic in the PS

With respect to event mitigation following a PS CCF, Guideline 12 states that, "Only in the third role is the control system actively involved as a third echelon of defense ...." As described in Section 4.1, the U.S. EPR design does not credit the RCSL system to perform in this role. This is a conservative assumption given that the RCSL is designed to perform this type of function, and an argument can be made that RCSL would not be subject to the same SWCCF as the PS.

While the PAS system is not credited in the D3 plant response analysis to directly mitigate the events, perform in this third role. the nature of its diversity attributes (described in Section 4.2) and the fact that it is in continuous operation (i.e., a failure in PAS would be self-revealing before occurrence of an AOO or PA) dictate that control functions in the PAS, that do not rely on a PS output, can be assumed to function normally following a PS SWCCF concurrent with an AOO or PA. For this reason, the best estimate assumption that the PAS is operational allows enables more accurate modeling of the AOO or PA to be more accurately modeled.

It should be noted that NUREG/CR-6303 Guideline 12 was written without acknowledgement of a diverse actuation system provided specifically to cope with PS CCF. The U.S. EPR design

contains such a system, which provides a layer of defense, diverse to the PS, beyond the echelons addressed in Guidelines 4 or 12.

#### **4.13 Guideline 13: Plant Monitoring**

NUREG/CR-6303 Guideline 13 contains three major points:

1. Plant monitoring systems should not significantly reduce the reliability or increase the complexity of the PS.
2. Failure of the monitoring systems should not influence the functioning of the PS.
3. If failure of the monitoring system induces incorrect operator action to cause a transient, the PS should protect against that transient.

The first point is addressed by PS compliance with reliability requirements and adherence to the PS application design process. These topics are addressed in Section 7.1 of the U.S. EPR FSAR.

The second point is addressed by PS compliance with GDC 24 and IEEE-603 independence requirements. These topics are addressed in Section 7.1 of the U.S. EPR FSAR.

The third point is addressed by the design characteristic differences diversity between the PICS and PS as discussed in Section 4.2. The diversity attributes dictate that the same failure is not likely to occur in the two systems. Therefore, the a failure in PICS does not occur in the PS, and the PS remains available to mitigate any transient caused by erroneous operator action. Additionally, as discussed in U.S. EPR FSAR Tier 2, Section 7.1, there is no data communication from the PICS to the PS—is independent from the PICS, so a PICS failure does not prevent the PS from performing its function.

#### **4.14 Guideline 14: Manual Operator Action**

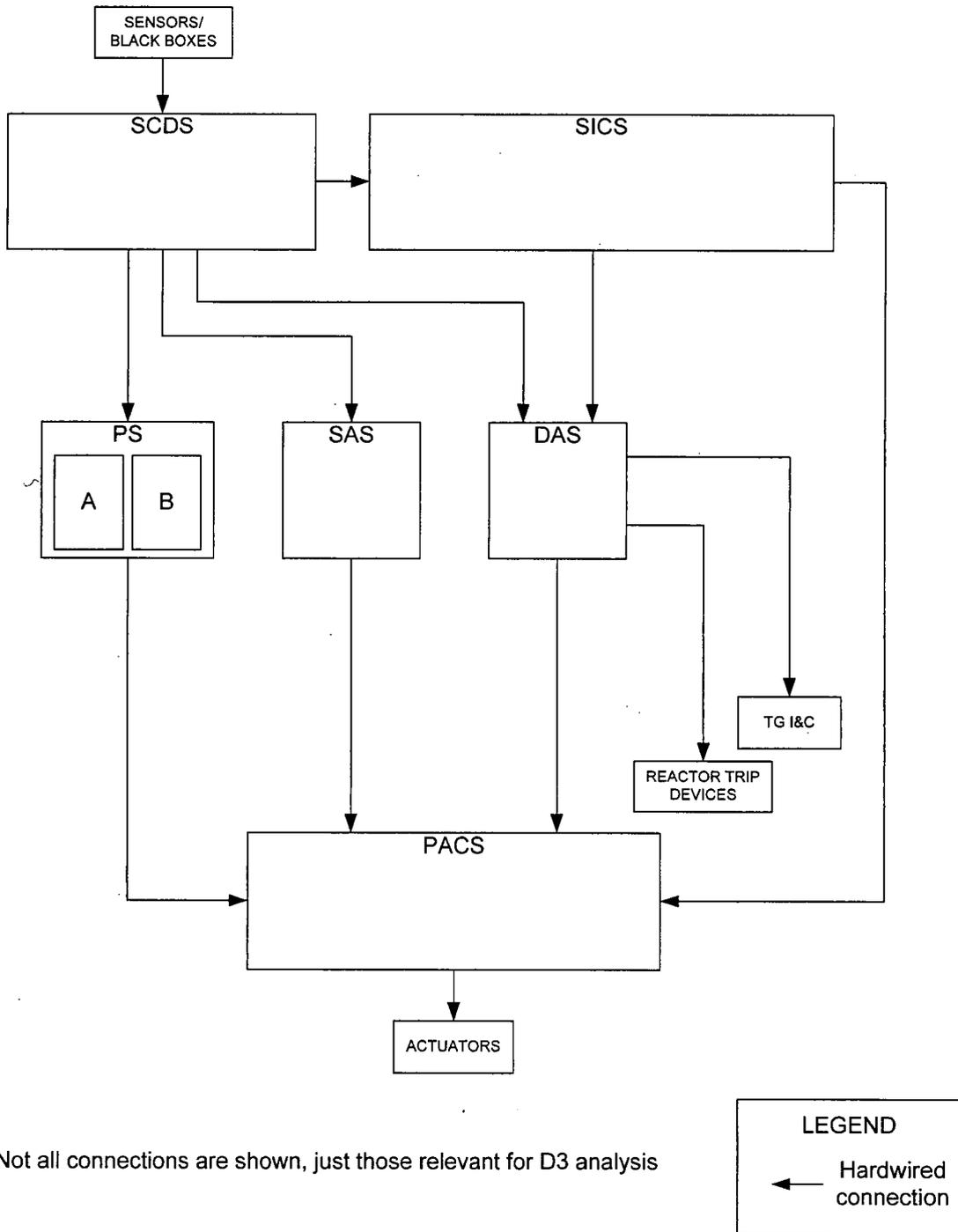
NUREG/CR-6303 Guideline 14 is similar to BTP 7-19 position 4 and indicates that independent and diverse displays and manual controls should be available for system level actuation of critical safety functions. The U.S. EPR design includes these system level actuations from PICS-SICS via the DAS, both are diverse from the PS. These manual actions are discussed further in U.S. EPR FSAR Tier 2, Section 7.8.

#### 4.15 *Conclusions*

The assessment of the U.S. EPR design against the 14 guidelines in NUREG/CR-6303 demonstrates that adequate D3 exists in the design as recommended by BTP 7-19. The key results obtained in performing the assessment are as follows:

- The block representation (~~Figure 4-1~~Figure 4-4) used to perform the assessment was constructed using conservative assumptions and decisions. Other than the PS, the I&C systems shown in the block representation are those that can be credited in the D3 plant response analysis.
- Significant diversity attributes are present throughout the I&C architecture, even after applying conservative assumptions relative to what types of diversity are credited.
- The I&C architecture contains multiple lines of defense, consistent with the traditional "echelons of defense."
- The risk reduction line of defense provides an extra layer of protection, beyond the traditional "echelons of defense."
- An analysis of postulated SWCCF in the PS, concurrent with an AOO or PA, provides confidence that the effects of such a failure do not affect I&C functions outside of the PS, if those functions do not rely on a PS output.

Figure 4-1—Block Diagram for D3 Assessment

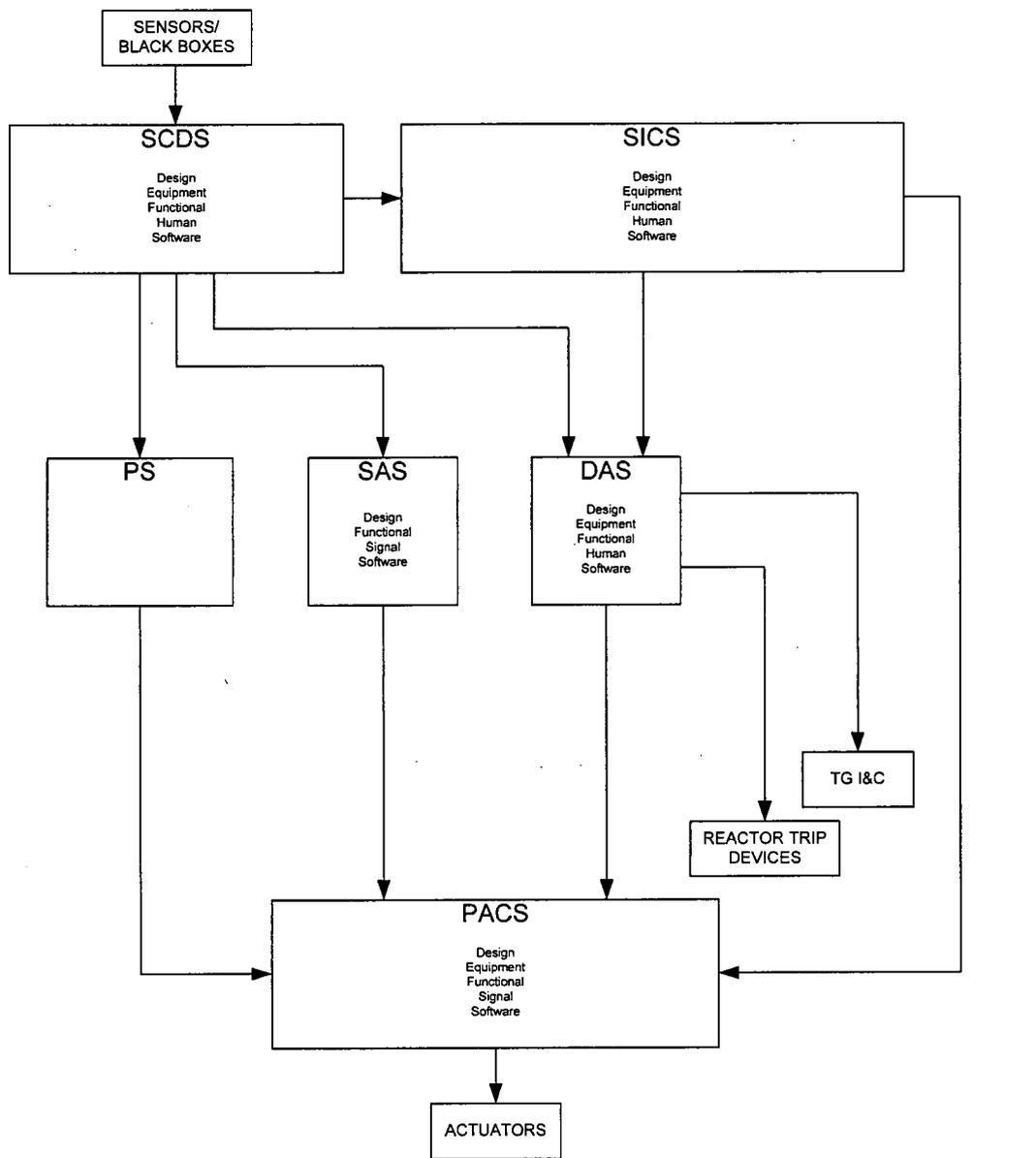


Note: Not all connections are shown, just those relevant for D3 analysis

**LEGEND**

← Hardwired connection

Figure 4-2—Block Diagram with Diversity Attributes



Note: Not all connections are shown, just those relevant for D3 analysis

**LEGEND**

← Hardwired connection

Red text = "more effective" diversity attribute  
Blue text = "less effective" diversity attribute

**Figure 4-3—Credible SWCCF Concurrent with AOO or PA**

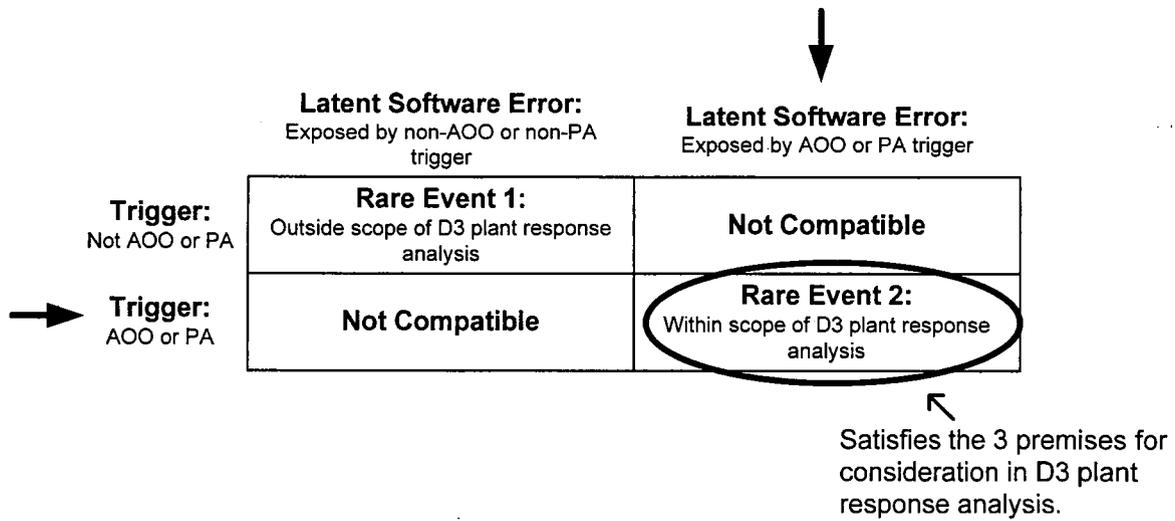


Figure 4-4—TXS Software

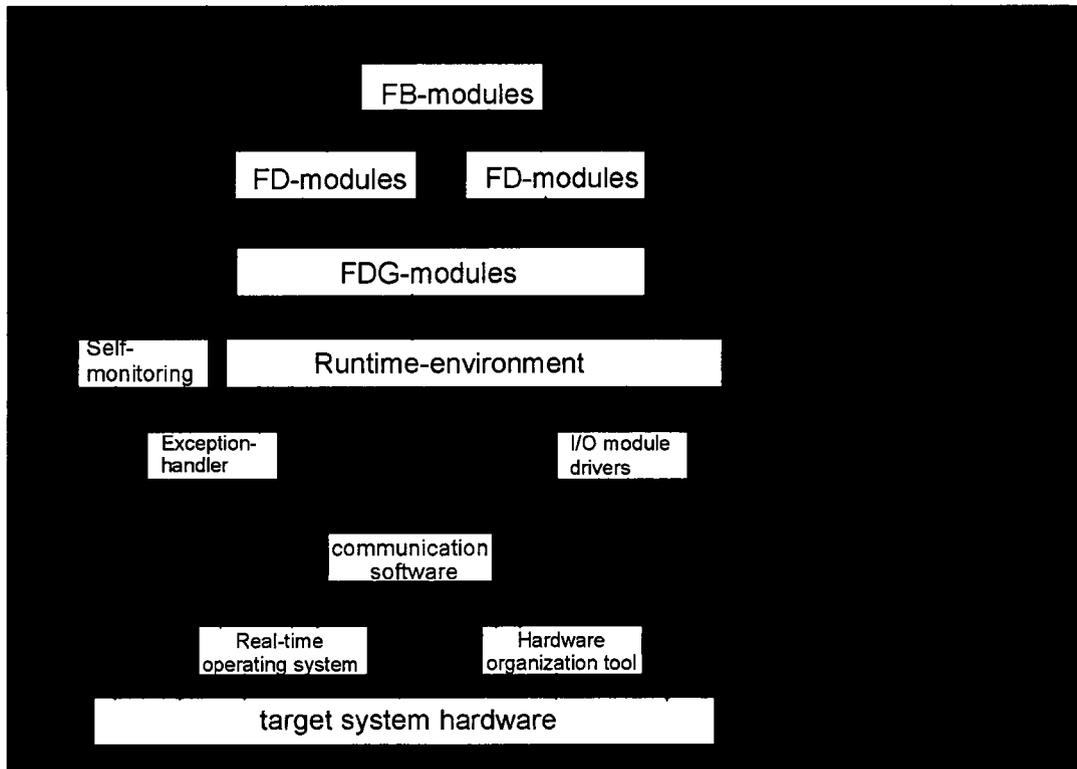
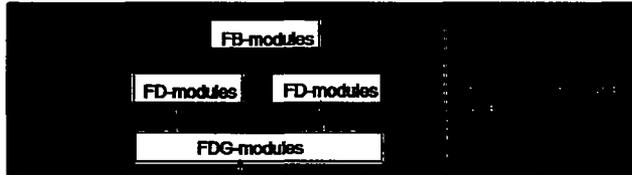
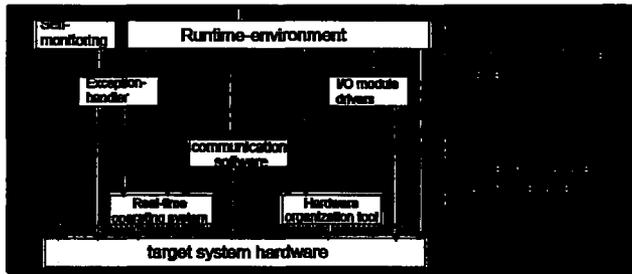


Figure 4-5—TXS System Software and Application Software



**Application Software**

- Implements the plant's functional requirements
- Unique design for each TXS application
- Subjected to measurements of plant processes (i.e., data trajectories).



**System Software**

- Implements the TXS platform requirements
- Same design for each TXS application
- Unaffected by measurements of plant processes (i.e., data trajectories).

## **5.0 REFERENCES**

### **5.1 U.S. Regulations**

1. 10 CFR 50.55a(h), "Protection and Safety Systems."
2. 10 CFR 100, "Reactor Site Criteria."

### **5.2 U.S. Regulatory Guidance**

3. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 5, March 2007.
4. Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Revision 4, June 2006.
5. SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," September 1991.
6. NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.
7. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
8. SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993.
9. Staff Requirements Memorandum on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993.

### **5.3 Regulatory Review Precedent**

10. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, 'Acceptance for Referencing of Licensing

Topical Report EMF-2110 (NP), Revision 1', "TELEPERM XS: A Digital Reactor Protection System" (TAC NO. MA1983) May 2000.

#### 5.4 **AREVA NP Documents**

11. AREVA NP Technical Report, ANP-10310P, Revision 01, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report," AREVA NP Inc., ~~October 2009~~ March 2011.
12. AREVA NP Technical Report, ANP-10309P, Revision 01, "U.S. EPR Digital Protection System Technical Report," AREVA NP Inc., ~~November 2009~~ March 2011.
13. Siemens Topical Report, EMF-2110 (NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," May 2000.
14. Siemens Topical Report, EMF-2267(P), Revision 0, "Siemens Power Corporation Methodology Report for Diversity and Defense-In-Depth," September 1999.
15. AREVA NP Topical Report, ANP-10272, Revision 02, "Software Program Manual TELEPERM XS™ Safety Systems Topical Report," ~~December 2006~~ May 2010.

## **APPENDIX A**

### **DIVERSITY AND DEFENSE-IN-DEPTH PLANT RESPONSE ANALYSIS**

## A.1 INTRODUCTION

U.S. NRC Standard Review Plan, Branch Technical Position 7-19 (BTP 7-19, Reference A-1) recommends a D3 assessment of the proposed digital I&C system to demonstrate that ~~common-cause failure~~CCFs have been adequately addressed. Part of that assessment includes an analysis of ~~design-basis event~~DBEs. If a postulated ~~common-cause failure~~CCF could disable a safety function that is required to respond to a ~~design-basis event~~DBE, a diverse means of effective response is necessary. The ~~I&C~~ diverse means may be an automatic or manual non-safety system, if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The method of assessment used is to analyze, assuming an SWCCF in the PS, the ~~design-basis events (DBEs)~~ analyzed in the U.S. EPR FSAR safety analysis. The DBEs are identified in Section A.2.3. ~~In this analysis credit is taken for the DAS (see Section A.2.5) and I&C systems that do not rely on the PS. All systems credited are described in Section A.2.2.~~

The purpose of this appendix is to present the U.S. EPR D3 plant response analysis that assesses conformance with Point 2 of NUREG-0800 BTP 7-19. The D3 plant response analysis entails a quantitative evaluation of U.S. EPR FSAR Chapter 15 AOOs and PAs in the presence of an SWCCF that renders the PS ineffective.

The quantitative evaluation consists of engineering arguments and engineering analysis to demonstrate that the U.S. EPR I&C design mitigates an SWCCF in the PS concurrent with an AOO or PA. Realistic assumptions (best estimate) are used and the acceptance criteria for the analyses are consistent with the guidance of BTP 7-19.

An assessment of SWCCF modes is presented in Section 4 of this report. That assessment concludes that a postulated SWCCF in the PS, concurrent with an AOO or PA, does not affect I&C functions outside of the PS, if those functions do not rely on a PS output. Complete failures (i.e., no credited PS outputs respond) and partial failures (i.e., some credited PS outputs respond, others do not) are considered. Partial failures are considered when the activation of a PS function results in more severe consequences. The operation of a PS function is not credited when it produces more favorable results. In most cases the complete failure of the PS is limiting.

Additionally, 10CFR50.62 requires that an ATWS mitigation system be composed of equipment that is diverse from the reactor trip system (RTS). The ATWS mitigation system for the U.S. EPR is the DAS. The D3 plant response analysis started with the DAS functions developed for ATWS and added additional functions where needed to satisfy the acceptance criteria for D3. The difference in required DAS functionality, between ATWS and D3, results from the fact that ATWS addresses AOOs with the failure of the ~~reactor trip system (RTS)~~ while D3 addresses AOOs and PAs with a failure of the PS (RTS and ESFs). In this sense, ATWS functions are a subset of D3.

Section A.2 describes the method used in the D3 plant response analysis. This includes assumptions regarding initial conditions, plant systems available for mitigation, postulated events analyzed, acceptance criteria, DAS functions, evaluation models and methods, and assumed operator actions.

Section A.3 presents the analysis of each postulated event, including an assessment of whether the containment integrity and radiological consequences satisfy the BTP 7-19 acceptance criteria.

This appendix provides a review of the U.S. EPR safety analysis in support of D3. The scope of the review included the U.S. EPR FSAR safety analysis (U.S. EPR FSAR Tier 2, Chapter 15), radiological consequence analysis (U.S. EPR FSAR Tier 2, Chapter 15) and the containment analysis (U.S. EPR FSAR Tier 2, Chapter 6). This review was performed to disposition the various analyses assuming an ~~software common-cause failure (SWCCF)~~ in the ~~protection system~~ PS. A number of DAS functions were identified in the course of the review to demonstrate that, in the event of an SWCCF in the PS, the acceptance criteria of BTP-7-19 are met. Events were found acceptable by engineering argument or specific engineering analysis. Events where additional analyses were performed include:

- Single main steam isolation valve (MSIV) closure to determine the need for a high steam generator (SG) pressure ~~reactor trip~~ RT.
- Increase in steam flow to determine the effectiveness of high neutron flux ~~reactor trip~~ RT.
- Complete loss of flow to confirm departure from nucleate boiling (DNB) margins.

- Rod cluster control assembly (RCCA) withdrawal and RCCA drop in the absence of a low departure from nucleate boiling ratio (DNBR) trip function.
- RCCA ejection to determine the effectiveness of the high neutron flux trip.
- Boron dilution to determine the response of the plant with manual RCCA control under best estimate conditions.
- Steam Generator Tube Rupture (SGTR) to assess the margin to overfill.
- Small break loss of coolant accident (SBLOCA) to determine the need for an automatic RCP trip.
- Large break loss of coolant accident (LBLOCA) to confirm that continuous RCP operation has a negligible impact.
- Radiological analysis to determine the need for automatic control room isolation.

The DAS functions established from this review are provided in Table A.2-2~~Table A.2-2~~. These functions are inclusive of those required to support ATWS. Operator actions that were necessary to support the conclusions include:

- Manual RT (~~steam generator tube rupture~~SGTR). Note that this action makes the event response more severe. Under normal conditions without an automatic reactor trip RT operators would maneuver the plant through a controlled shutdown.
- Manual ~~Diesel~~generator loading (emergency diesel generators or SBOs) (Loss of AC power).
- Manual emergency feedwater (EFW) actuation (Loss of AC power).
- Manual operation of EFW for long-term ~~steam generator (SG)~~ level control.
- Manual safety injection (SI) switchover to hot leg injection (loss of coolant accident).
- Manual actions associated with an ~~steam generator tube rupture~~SGTR identified in Section A.3.7.2 (MSIV closure, feedwater isolation, initiate and control medium head safety injection, extend partial cooldown, depressurize RCS using pressurizer sprays to terminate leak, and actuate extra borating system (EBS)).

- Manual control room heating, ventilation, air conditioning (HVAC) reconfiguration on high intake activity signal (radiological events).
- Manual chemical and volume control system (CVCS) isolation on boron dilution indication ~~for loss of shutdown margin, or high pressurizer level (boron dilution, CVCS malfunction).~~
- Manual main steam relief train (MSRT) (for long-term heat removal).

The U.S. EPR design, including DAS functions, available plant control systems, and manual operator actions, are determined to be sufficient in maintaining the acceptance criteria of BTP 7-19 for an SWCCF in the PS during U.S. EPR ~~design-basis-event~~DBEs, which include AOOs and PAs.

## **A.2 D3 PLANT RESPONSE ANALYSIS APPROACH**

### **A.2.1 Method**

The method used in this analysis is to review the U.S. EPR ~~design-basis-event~~DBEs analyzed in the U.S. EPR FSAR safety analysis, assuming an SWCCF in the PS that renders the PS ineffective. The events considered are identified in Section A.2.3. The D3 plant response analysis considers the I&C functionality as described in Section A.2.2. ~~The D3 plant response analysis credits DAS functions, and it credits I&C systems other than the PS, if those systems do not rely on the PS for actuation. A detailed description of the credited systems is in Section A.2.2.~~

The D3 plant response analysis consists of both engineering analysis and engineering arguments to demonstrate that the acceptance criteria of BTP 7-19 are met (see Section A.2.4). The engineering analysis, where applied, utilizes best estimate models and methods based on the NRC-approved S-RELAP5 code (References A-2 and A-3). These models and methods are described in Section A.2.5. The engineering arguments utilize results from the U.S. EPR FSAR safety analysis to establish the plant response, with an SWCCF in the PS. The engineering arguments draw on the fact that the DAS and other available plant systems have functions that provide a similar level of protection as the PS.

The analysis assumes the plant is operating under full power nominal conditions (no uncertainties) with all equipment available (i.e., no preventative maintenance and no single

failures). RCCAs are maintained in their normal full power position (i.e., all RCCAs are out, with the lead control bank slightly inserted). The analysis employs best estimate core neutronic parameters and power distributions expected at full power conditions (hot channel factors accounting for engineering uncertainties, RCCA bow, or assembly bow are excluded). The best estimate parameters assumed in the D3 assessments are compared to design parameters assumed in the FSAR Chapter 15 analyses in Table A.2-4~~Table A.2-4~~. The core neutronic parameters correspond to nominal conditions (no uncertainty) for an equilibrium cycle and are considered representative during full power steady-state operation. An equilibrium cycle is selected because it represents parameters that correspond to conditions where the plant is expected to operate most of the time. Differences between the first cycle and the equilibrium cycle do not affect the conclusions of this report. For example, the equilibrium cycle moderator temperature coefficient (MTC) and Doppler are more conservative at end-of-cycle (EOC), for overcooling events, than the first cycle. The scram worth for the equilibrium cycle is also more conservative than the first cycle. The MTC at beginning-of-cycle (BOC) for the first cycle is slightly less negative than for the equilibrium cycle. The analysis considers variation in the core neutronic parameters, as a function of cycle lifetime. Offsite power remains available; on reactor trip, all RCCAs insert (i.e., the analysis assumes no stuck RCCAs).

The plant response analysis considers the response of the plant to the point where a stable controlled condition is achieved. A "stable controlled condition" is defined as:

- Reactor is subcritical and remains subcritical.
- Core is covered.
- Decay heat is being removed from the RCS.
- Secondary inventory levels are sufficient to maintain RCS temperatures.
- During large break LOCA, SI is maintaining core temperatures.

For most events discussed herein, the end state corresponds to hot shutdown. There are some cases that reach a new steady-state condition without a reactor trip~~RT~~. These are also considered a stable controlled condition. For a LOCA, the end-state corresponds to a depressurized RCS with SI providing make-up for maintaining RCS inventory and core cooling. For an steam generator tube rupture (SGTR), after initial stabilization, the plant is required to

cool down and establish residual heat removal (RHR) cooling. Sufficient plant systems remain available such that cooldown and depressurization is achieved in the normal fashion.

### **A.2.2 I&C Functions Available to Cope with SWCCF**

The U.S. EPR I&C architecture is described in Section 2 of this report. The plant response analysis assumes an SWCCF in the PS that renders the PS ineffective during a ~~design-basis event~~ DBE. ~~Functions of the remaining I&C systems are available to mitigate the consequences of the event if they do not rely on the PS for initiation.~~ Functions that require initiation from the PS are assumed to be lost as a result of the SWCCF (i.e., partial cooldown). The analysis assumes that normally operating SAS and PAS functions that do not rely on a PS output continue to operate ~~control functions continue to operate~~. The analysis conservatively assumes the RCSL is not available as a credited mitigation system. RCSL is assumed to function during an event when its correct operation would make the response of the event more severe. The assessment of the I&C systems that reaches these conclusions is presented in Section 4.

~~Listed below~~ The following list provides ~~are the specific I&C functions credited to remain available either assumed to operate normally (SAS and PAS functions) or provided specifically as a diverse means to mitigate events in the D3 evaluation with~~ of an SWCCF in the PS during a postulated design-basis event ~~DBE~~. These functions are ~~credited~~ described in the evaluation presented in Section ~~9A.3~~. Essential auxiliary support systems required for these functions are either in continuous operation (controlled by SAS or PAS and not affected by PS SWCCF), or are initiated as part of the DAS actuation of the associated ESF function. The operator actions listed below are not assumed to occur until 30 minutes after the initiating event, unless otherwise noted. ~~The credited functions are identified in each event discussion.~~

Automatic control functions:

- ~~PAS/PACS~~ —main feedwater (MFW) flow control and steam generator ~~SG level control (FLCVs and LLCVs).~~
- ~~PAS/PACS~~ —pressurizer pressure (heaters and spray) and level control (CVCS charging and letdown).
- ~~PAS/PACS~~ —pressurizer level limitation function to isolate charging on high level, isolate letdown and start second charging pump on low level.

- PAS/PACS—: ~~steam generator~~SG level and turbine load (pressure control) control.
- PAS/PACS—: main steam pressure control (Turbine Bypass).
- SAS/PACS—: EFW flow control (limits flow to a depressurized SG).

## Manual functions:

- SICS/DAS—: manual RT<sup>1</sup>.
- SICS/PACS—: manual EDG start.
- SICS/DAS/PACSPICS & PAS—: manual diesel generator loading (emergency diesel generators or SBOs).
- SICS/DAS/PACSPICS & DAS—: manual EFW actuation<sup>1</sup>.
- SICS/PACSPICS & PAS—: manual operation of EFW for long-term SG level control.
- SICS/PACSPICS & PAS—: manual SI switchover to hot leg injection.
- SICS/PACSPICS & PAS—: manual MSIV closure.
- SICS/PACSPICS & PAS—: manual feedwater isolation (MFW and EFW).
- SICS/DAS/PACSPICS & DAS—: manual initiation of medium head safety injection (MHSI)<sup>1</sup>.
- SICS/PACSPICS & PAS—: manual control of MHSI.
- SICS/PACSPICS & PAS—: manually extend partial cooldown.
- SICS/PACS: Manual depressurize RCS with pressurizer sprays.
- SICS/PACSPICS & PAS—: manual actuation of ~~extra borating system~~ (EBS).
- SICS/PACSPICS & PAS—: manual control room HVAC reconfiguration.
- SICS/PACSPICS & PAS—: manual CVCS isolation.
- SICS/PACSPICS & PAS—: manual MSRT<sup>1</sup>.
- SICS/DAS/PACS—: manual Stage 1 cContainment Isolation<sup>1</sup>.

---

<sup>1</sup> BTP 7-19 Point 4

- ~~SICS/DAS/PACS~~ - manual opening of containment H<sub>2</sub> mixing dampers<sup>1</sup>.

## Automatic DAS functions:

- ~~DAS/PACS~~ - RT on low SG pressure ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on low SG level ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on high SG level ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on low RCS flow (two loops) ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on low-low RCS flow (one loop) ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on high neutron flux (power range) ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on low hot leg pressure ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - RT on high pressurizer pressure ~~(DAS/PACS)~~.
- ~~DAS/TG I&C~~ - Turbine trip on RT ~~(DAS/TG I&C)~~.
- ~~(DAS/PACS)~~ - EFWS actuation on low SG level ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - Safety injection system (SIS) actuation on low pressurizer pressure ~~(DAS/PACS)~~, with signal to PAS to generate partial cooldown through turbine bypass system (TBS).
- ~~(DAS/PACS)~~ - Main steam isolation on low SG pressure ~~(DAS/PACS)~~.
- ~~(DAS/PACS)~~ - Containment Isolation on high activity ~~(DAS/PACS)~~. (This includes functions that cascade from containment isolation: annulus ventilation and Safeguards Building HVAC reconfiguration.)
- ~~DAS/PACS~~ - MFW isolation on low SG pressure (affected SG) ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - MFW isolation on high SG level (affected SG) ~~(DAS/PACS)~~.
- ~~DAS/PACS~~ - Opening of containment H<sub>2</sub> mixing dampers on high containment pressure, or a differential pressure between the equipment rooms and the operational rooms ~~(DAS/PACS)~~.
- ~~DAS~~ - Start SBO Diesel generators ~~(DAS)~~.

The setpoints and time delays for the PS and DAS functions are listed in Table A.2-3~~Table A.2-3~~. DAS setpoints are selected to provide reasonable assurance they are reached only after the corresponding PS setpoint is reached. The delay times are composed of several components. Differences between the PS and DAS delay times result from the response time of the channel (RT) or signal application to actuators (ESF). These DAS functions are credited in the analysis presented in Section 0A.3. These functions are enabled/disabled by separate permissives.

Table A.2-3~~Table A.2-3~~ includes the ~~diverse actuation system (DAS)~~ setpoint values used in the ~~diversity and defense-in-depth (D3)~~ transient analysis. The DAS setpoints represent nominal values and were used directly in the S-RELAP5 simulations for ~~these~~ the events ~~wherefor~~ which specific analysis was performed. This approach differs from that used in the safety analysis supporting the design basis. For the design basis, ~~protection system (PS)~~ setpoints are derived from the analytical limits used in the safety analysis. From the analytical limits, the limiting trip setpoints, which correspond to the limiting safety system settings defined in 10 CFR 50.36, take into account total instrumentation channel uncertainty, such as calibration tolerance, drift, and basic sensor accuracy. The D3 analysis uses best-estimate assumptions for the DAS setpoints. These represent expected setpoints dialed-in the plant instrumentation. Because the dialed-in setting meets the Technical Specification limit, it is typically set well below the analytical limit used in the safety analysis and including uncertainties as well as administrative margin. In the D3 analysis, the DAS setpoints used represent conditions that are closer to actual plant conditions.

### **A.2.3 Postulated Events**

The ~~design basis event~~DBEs analyzed in the presence of an SWCCF of the PS are those evaluated in the U.S. EPR FSAR safety analysis. Also included are analyses of radiological consequences and containment integrity. The postulated events evaluated for D3 are given in Table A.2-1~~Table A.2-1~~.

### **A.2.4 Acceptance Criteria**

The acceptance criteria applied in this analysis are those of BTP 7-19. This results in the following for AOOs and PAs:

- AOOs: Radiation release must not exceed 10 percent of the 10CFR100 guideline; and, The integrity of the reactor coolant system boundary must be maintained.
- PAs: Radiation release must not exceed the 10CFR100 guideline; The integrity of the reactor coolant system boundary must be maintained; and, The integrity of the containment must be maintained.

For some events, more conservative acceptance criteria are applied to assure conformance to the radiological acceptance criteria of BTP 7-19. Those criteria are elaborated on in the individual evaluations of Section 0.

The analysis assumes RCS boundary integrity is maintained, if RCS pressure is maintained within 120 percent of design (This is consistent with ASME service level C limits and is consistent with criteria applied for ATWS). The RCS design pressure is 2535 psig. Although BTP 7-19 does not specifically address a secondary pressure limit, to determine if the integrity of the secondary system is maintained during events that may challenge secondary system pressure limits, a similar criteria consistent with ASME service level C limits is applied (i.e., 120 percent of design pressure). The main steam system design pressure is 1435 psig.

Containment integrity is maintained for pressures well above containment design pressure. The ultimate pressure below which containment integrity is ~~ensured~~ provided is 156 psig, which is 2.52 times the containment design pressure. Therefore, in this analysis, if containment pressure remains below 156 psig, the conclusion is that containment integrity is maintained. The containment ultimate capacity deterministic analysis was performed in accordance with the guidance provided in U.S. NRC Standard Review Plan (SRP) Section 3.8.1.II.4.K (Revision 2 – March 2007). The ultimate pressure capacity of 156 psig corresponds to the loss of structural integrity of the equipment hatch, the limiting containment structural component.

The analysis of core thermal-hydraulic performance consists of an assessment of the DNBR and peak linear power density (PLPD) for all events that can challenge limits for DNB, fuel centerline melt, or clad strain. The evaluation of these parameters is performed with best estimate conditions.

The applicable limits for minimum DNBR are the design limits for the critical heat flux (CHF) correlations used and are provided in Table A.2-2 ~~Table A.2-2~~. The applicable limit for PLPD is

the minimum of the fuel centerline melt and clad strain limits, also provided in Table A.2-2 ~~Table A.2-2~~. As long as these limits are respected throughout a transient, fuel integrity is assured.

This assessment is conservatively used to determine failed fuel fractions for input to radiological analysis against the BTP 7-19 criteria.

#### **A.2.5 Evaluation Models and Methods**

The computer codes used for this analysis are the same as those used in the U.S. EPR FSAR safety analysis. Minor changes to the S-RELAP5 computer code have been made to reflect improved heat transfer in the ~~steam generator~~ SG secondary system.

Additionally, the D3 analyses utilize best estimate modeling assumptions that differ from the U.S. EPR FSAR analysis. The system modeling is changed to reflect available systems and expected behavior during best estimate conditions versus design basis.

The following systems are included in the S-RELAP5 best-estimate non-LOCA model. These systems are not included in the U.S. EPR FSAR Tier 2, Chapter 15 analysis, unless the operation of these systems provides a more adverse response.

- Automatic RCCA control system (RCCA control is evaluated in both automatic and manual mode, depending on which produces the most limiting consequences).
- Pressurizer pressure and level control systems.
- ~~Steam generator~~ SG blowdown system.
- Turbine-bypass-specific secondary system overpressure relief system.

The best-estimate SBLOCA model (i.e., S-RELAP5) is essentially the same as that in Reference A-2, except for changes to reflect available systems and expected behavior during best-estimate conditions versus design basis. The secondary side model is consistent with the non-LOCA model described above.

For the LBLOCA, the model used in the RCP study is identical to the model in Reference A-3.

This analysis uses the LYNXT computer model to perform DNB analysis. LYNXT is also used in the U.S. EPR FSAR analysis. In this analysis, best estimate boundary conditions are used from S-RELAP5 and best estimate power distributions are used to represent core peaking.

This analysis assesses core performance for RCCA ejection in a manner similar to the U.S. EPR FSAR analysis. It consists of an assessment of fuel rod thermal performance, including DNBR, peak clad temperatures, peak fuel rod temperatures, and fuel enthalpy conditions. The evaluation of these parameters is performed with best estimate conditions.

**Table A.2-1—U.S. EPR Initiating Events**

Category	Event	Type	Section
Increase in Heat Removal By Secondary System	Decrease in feedwater temperature	AOO	A.3.2.1
	Increase in feedwater flow	AOO	A.3.2.2
	Increase in steam flow	AOO	A.3.2.3
	Inadvertent opening of SG relief or safety valve	AOO	A.3.2.4
	Steam system piping failures	PA	A.3.2.5
Decrease in Heat Removal By Secondary System	Loss of external load/turbine trip	AOO	A.3.3.1
	Loss of condenser vacuum	AOO	A.3.3.1
	Closure of MSIV	AOO	A.3.3.2
	Loss of non-emergency AC power	AOO	A.3.3.3
	Loss of normal feedwater flow	AOO	A.3.3.4
	Feedwater system pipe break	PA	A.3.3.5
Decrease in RCS Flow Rate	Partial loss of forced reactor coolant flow	AOO	A.3.4.1
	Complete loss of forced reactor coolant flow	AOO	A.3.4.2
	RCP rotor seizure or RCP shaft break	PA	A.3.4.3
Reactivity & Power Distribution Anomalies	Uncontrolled RCCA withdrawal from subcritical or low power startup condition	AOO	A.3.5.1
	Uncontrolled RCCA withdrawal at power	AOO	A.3.5.2
	Single RCCA withdrawal	AOO	A.3.5.3
	RCCA misalignment / RCCA drop	AOO	A.3.5.3
	Startup of RCP in inactive loop	AOO	A.3.5.4
	Inadvertent decrease in boron concentration in RCS	AOO	A.3.5.5
	RCCA ejection	PA	A.3.5.6
Increase in RCS Inventory	Inadvertent operation of SIS or EBS	AOO	A.3.6.1
	CVCS malfunction that increases reactor coolant inventory	AOO	A.3.6.2
Decrease in RCS Inventory	Inadvertent opening of PSRV	AOO	A.3.7.1
	<del>Steam generator tube rupture</del> SGTR	PA	A.3.7.2
	Small break LOCA	PA	A.3.7.3.2
	Large break LOCA	PA	A.3.7.3.1
Radioactive Release From A Subsystem Or Component	Failure of small line carrying primary coolant outside containment	PA	A.3.9
	LOCA	PA	A.3.9
	SG tube failure	PA	A.3.9
	MSL failure outside containment	PA	A.3.9

Category	Event	Type	Section
	Feedwater line break	PA	A.3.9
	RCP locked rotor / RCP broken shaft	PA	A.3.9
	RCCA ejection	PA	A.3.9
	Fuel handling accident	PA	A.3.9
Containment Evaluation	LOCA	PA	A.3.8.1
	Main steam line break	PA	A.3.8.2

1. Minor leaks or breaks are considered AOOs.

**Table A.2-2—DNBR and PLPD Limits**

Parameter		Limit
DNBR	ACH-2 CHF Correlation for the U.S. EPR	1.25
	BWU-N BWU CHF Correlation	1.21
PLPD	Fuel Centerline Melt	20.45 kW/ft
	Clad Strain	17.20 kW/ft

**Table A.2-3—Signals and PS/DAS Setpoints and Delays**

Signal	PS setpoint (uncertainty)	PS Delay (sec)	DAS setpoint	DAS delay (sec)
RT, Low SG pressure	724.7 (30, 75 for harsh conditions) psia	1.3	684.7 psia (670 psig)	1.8
RT, Low SG level	20 (3.5)% NR	1.9	15 % NR	2.4
RT, Low-Low RCS flow (one loop)	54 (4)% NF	1.05	44% NF	1.30
RT, Low RCS flow (two loops)	90 (4)% NF	1.05	80% NF	1.30
RT, High neutron flux (power range)	None	0.7	115% RTP	1.0
RT, Low hot leg pressure	2005 (25, 55 for harsh conditions) psia (pressurizer pressure)	1.3	1964.7 psia (1950 psig)	1.8
RT, High pressurizer pressure	2414.9 (25) psia	1.3	2454.7 psia (2440 psig)	1.8
RT, High SG level	69 (9.5) % NR	1.9	79 % NR	2.4
Turbine trip, on RT	NA	1.0	NA	1.0
MFW Isolation, High SG level (w/ RT) (affected SG)	65 (9.5) % NR for 10 sec	1.5	75% NR for 10 sec	2.0
MFW Isolation, Low SG pressure (affected SG)	579.7 (30) psia	0.9	539.7 psia (525 psig)	1.4
EFW actuation, Low SG level	40 (2) % WR	1.5 (plus 15 sec for EFW delivery)	37% WR	2.0 (plus 15 sec for EFW delivery)
SI actuation / SG partial cooldown (via TBS), Low pressurizer pressure	1667.9 (25) psia	1.5 (plus 15 sec for SI delivery)	1627.7 psia (1613 psig)	2.6 (plus 15 sec for SI delivery)
MSIV isolation on low SG pressure	724.7 (30, 75 for harsh conditions) psia	0.9	684.7 psia (670 psig)	1.4
Open H2 mixing dampers / high containment pressure exceeding delta pressure	2.7 (0.5) psig 0.5 (0.1) psi delta pressure	18	4.0 psig 0.95 psi delta pressure	
Containment Isolation / high containment activity	100 x background		120 x background	

**Table A.2-4—Best Estimate Vs. FSAR Chapter 15 Parameters**

<u>Parameter</u>	<u>Best Estimate (Equilibrium Cycle)</u>	<u>FSAR Chapter 15</u>
<u>MTC (pcm/°F)</u>		<u>0</u>
<u>BOC, HFP</u>	<u>-11.38</u>	<u>-50</u>
<u>EOC, HFP</u>	<u>-39.4</u>	
<u>DTC (pcm/°F)</u>		<u>-1.17</u>
<u>BOC, HFP</u>	<u>-1.40</u>	<u>-1.85</u>
<u>EOC, HFP</u>	<u>-1.63</u>	
<u>Scram (pcm)</u>		<u>6161</u>
<u>BOC, HFP</u>	<u>9449</u>	<u>7353</u>
<u>EOC, HFP</u>	<u>10349</u>	
<u>Initial Core Power (MWt)</u>	<u>4590</u>	<u>4612</u>
<u>T<sub>avg</sub> (°F)</u>	<u>594</u>	<u>594 ± 4</u>
<u>Pressure (psia)</u>	<u>2250</u>	<u>2250 ± 50</u>
<u>Reactor coolant System Flow Per loop (gpm)</u>	<u>124,741</u>	<u>119,692</u>
<u>Decay Heat</u>	<u>ORIGEN based <sup>1</sup></u>	<u>ANS 1973</u>
<u>F<sub>d</sub><sup>2</sup> BOC</u>	<u>1.695 (2.1 SBLOCA)</u>	<u>2.6</u>
<u>EOC</u>	<u>1.613</u>	
<u>FΔH<sup>2</sup> BOC</u>	<u>1.476 (1.557 SBLOCA)</u>	<u>1.70</u>
<u>EOC</u>	<u>1.425</u>	

1) % enrichment, 40 GWD/MTU including actinides2) Limiting for all Cycles

## **A.3 EVALUATION RESULTS**

### **A.3.1 General**

Each DBE identified in Section A.2.3 and ~~Table A.2-1~~Table A.2-4 is analyzed assuming an SWCCF in the PS. -The acceptance criteria used to assess whether the U.S. EPR I&C design adequately addresses ~~common-cause-failure~~CCFs are identified in Section A.2.4. The analysis uses a combination of engineering word arguments based on previous analysis and additional engineering analysis when required to draw conclusions of the adequacy of DAS functions, available plant equipment, and operator actions in coping with the SWCCF. The word arguments use the design basis response, operator actions, and available plant equipment in the presence of an SWCCF to draw the conclusion that the design basis is bounding or representative. The results of the analysis are presented below.

### **A.3.2 Increase in Heat Removal by Secondary System**

#### **A.3.2.1 Decrease in Feedwater Temperature**

The Decrease in Feedwater Temperature event is defined as the inadvertent opening of a feedwater heater bypass valve, which decreases the temperature of the feedwater to the ~~steam generator~~SGs. In turn, this increases the heat removed from the RCS, lowering the temperatures of the RCS. The decreased RCS temperatures, coupled with a negative MTC, increase reactor power. In the U.S. EPR FSAR analysis, this event is terminated by a PS-initiated low DNBR reactor trip. However, in this D3 analysis, with an SWCCF in the PS, power increases and, depending on the time in core life, the power increase may stabilize at a slightly higher power or increase until the DAS reactor trip on excore high neutron flux setpoint is reached.

Following the DAS reactor trip, normal pressurizer pressure and level controls maintain RCS pressure and pressurizer level. The normal MFW control system reacts to control SG level. Depending on the speed of control of the MFW to match decay heat, MFW may be isolated on high SG level (a DAS function). If MFW is isolated, EFW actuates once SG level decreases to the low level DAS setpoint. The operator then controls SG level, to remove decay heat using the EFW system. It takes more than 60 minutes for the level to recover from the EFW actuation setpoint, giving the operator sufficient time to manually control SG level. After RT, the ~~TBS~~

turbine bypass system (TBS) opens, to maintain secondary system pressure. This post-trip response is similar for many events.

The increase in the load removed by the secondary system, with the accompanying decrease in RCS temperatures and increase in core power, is much less for this event than for the Increase in Steam Flow event. Therefore, DNB consequences for this event are bounded by the Increase in Steam Flow event presented in Section A.3.2.3.

### **A.3.2.2 Increase in Feedwater Flow**

Failure or misoperation of the MFW control system can increase flow to a single SG. The most severe event is a rapid full opening of a MFW full-load line control valve. This increases the heat removed from the RCS, lowering the temperatures of the RCS. The decreased RCS temperatures, coupled with a negative MTC, increase reactor power. The primary PS reactor trip for this event is high SG level. The PS isolates MFW on high level, shortly after RT. DAS also has high SG level RT and MFW isolation functions. In the presence of an SWCCF in the PS, DAS provides an equivalent but diverse means of protection. The acceptance criteria are met, and the U.S. EPR design is ~~determined adequate~~determined to be adequate for an SWCCF in the PS, during the Increase in Feedwater Flow event.

Following the DAS reactor trip, normal pressurizer pressure and level controls maintain RCS pressure and pressurizer level. Because MFW is isolated DAS actuates EFW when SG level decreases to the low level DAS setpoint. The operator controls the EFW system manually to maintain SG level and remove decay heat. It takes approximately 60 minutes for the SG level to recover to its nominal value from the EFW actuation setpoint. This provides the operator adequate time to manually control SG level. After RT, the TBS opens, to control primary pressure through the maintenance of secondary system pressure in a stable, controlled condition.

### **A.3.2.3 Increase in Steam Flow**

The Increase in Steam Flow event is defined as an increase in main steam flow above steady state demand. The magnitude can range from a small increase, caused by the opening of the turbine control valves, to a large increase, caused by the opening of the turbine bypass valves. The increased steam flow increases the heat removed from the RCS, lowering RCS

temperatures. Decreased RCS temperatures, coupled with a negative MTC, increase reactor power.

In the U.S. EPR FSAR analysis, cases run from hot full power (HFP) trip the reactor on low DNB, high SG pressure drop, or high core power (based on measured thermal power), depending on the magnitude of the steam demand. The corresponding RT in DAS is on excore high neutron flux. Therefore, in the case of an SWCCF in the PS, core power increases to a higher level than in the U.S. EPR FSAR analysis, until the DAS RT on excore high neutron flux setpoint is reached. The excore neutron flux signal is decalibrated by the reduction in downcomer temperatures, further delaying RT. This results in more adverse conditions for DNB. The increase in DNB margins, obtained using best estimate assumptions, is sufficient to balance the reduction in minimum departure from nucleate boiling ratio (MDNBR) due to the more adverse thermal hydraulic conditions. However, because DAS provides RT on excore high neutron flux and does not contain a low DNBR or core power level trip, a specific analysis of this event is performed.

The temperature decalibration factors used in the analysis are determined by an independent adjoint calculation. This adjoint calculation uses the Oak Ridge National Laboratory (ORNL) programs Group-Organized Cross-Section Input Program (GIP) and Discrete Ordinates Transport (DORT). The GIP program generates 47 group neutron cross sections for the materials internal and adjacent to the U.S. EPR pressure vessel. The DORT program calculates the adjoint fluxes necessary to obtain the desired excore detector response factors for a 25°F temperature variation around the nominal inlet coolant temperature. In addition, due to because the uncertainty in the exact location of the excore detector has not been determined, the factor is calculated for three different excore detector locations. The temperature decalibration factor (DF) for all the locations is calculated to be 0.51% percent/ per °Fdegree Fahrenheit.

In the S-RELAP5 best estimate model used for diversity and defense-in-depth (D3) analysis, the decalibration factor is applied as follows:

$$IndicatedPower(\%) = reactorPower(\%) \times \left\{ 1 + \frac{\left[ \Delta T(^{\circ}F) \times DF\left(\frac{\%}{^{\circ}F}\right) \right]}{100(\%)} \right\}$$

$$where \quad \Delta T(^{\circ}F) = T_{calibration}^{Downcomer} - T_{current}^{Downcomer}$$

When the temperature decreases, as in the Increase in Steam Flow event, the correction

$T(^{\circ}F) \times DF\left(\frac{\%}{^{\circ}F}\right)$  is negative, the indicated reactor power is therefore lower than the current

reactor power, and the reactor trip RT on high neutron flux is delayed.

The limiting Increase in Steam Flow event is the case with all turbine bypass valves inadvertently opened at BOC conditions under manual RCCA control. The combination of rapid cooling and neutron flux decalibration with a lower BOC MTC causes the reactor to reach its highest power, without challenging the DAS excure high neutron flux RT.

Core power peaks at 131.1 percent in 825 seconds, but power is fairly constant at a value of approximately 130 percent power, from 130 seconds until the transient is terminated by the operator. For this event, reactor trip does not occur. Indicated core power does not reach a level high enough to cause a DAS-initiated reactor trip on excure high neutron flux. Instead, the system moves to a higher steady-state power level. ~~Steam generator SG~~ levels are maintained during the transient, even with actual core power at 130 percent. The MFW pumps are able to match the demand, due to the decreased pressure on the secondary side. (This is a conservative assumption because matching the demand results in the highest core power.)

Figure A.3.2-1~~Figure A.3.2-1~~ through Figure A.3.2-11~~Figure A.3.2-11~~ provide the response of key parameters for the limiting Increase in Steam Flow event.

Under best estimate conditions, the feed train likely trips, as a result of the reduced feedwater system pressures. If the MFW pumps are unable to keep up with demand, SG levels decrease and the reactor trips on low SG level. MSIV closure and MFW isolation will be initiated by DAS on low SG pressures. DAS will then actuate EFW on low SG level to provide long term cooling. The operator controls EFW manually to maintain SG level. For long-term heat removal, manual operation of the MSRTs is available.

Actual reactor power reaches a higher value than in the U.S. EPR FSAR analysis, as a result of the decalibration of the excore neutron flux signal used by DAS for RT. However, no fuel failure is predicted. Any degradation in safety system functionality, due to the SWCCF in the PS, is more than offset by the best estimate initial conditions analyzed within the core, as illustrated in Figure A.3.2-11—Increase in Steam Flow Event:

Normalized DNBR and LHGR~~Figure A.3.2-11—Increase in Steam Flow Event:~~

Normalized DNBR and LHGR, Normalized performance of DNBR and LHGR.

These results presented above were based on an evaluation of BOC and EOC cases. It is possible that between EOC and BOC, reactivity kinetic conditions could lead to the stabilization of the indicated neutron flux signal just under the DAS reactor trip RT setpoint. An additional analysis was performed with reactivity conditions that lead to an indicated power just below the DAS reactor trip RT setpoint. Figure A.3.2-12~~Figure A.3.2-12~~ shows the indicated power and reactor power response for this case. Figure A.3.2-13~~Figure A.3.2-13~~ presents the DNBR and LHGR response.

Consequently, the acceptance criteria for D3 are met and the U.S. EPR design is assessed as adequate to meet an SWCCF in the PS, for the Increase in Steam Flow event.

#### **A.3.2.4 Inadvertent Opening of an MSRT or MSSV**

Opening an MSRT or MSSV valve increases the steam removed from the SGs. This increases heat removal from the RCS, lowering the temperatures of the RCS. The decreased RCS temperatures, coupled with a negative MTC, increases reactor power. The U.S. EPR FSAR safety analysis addresses cases for both MSRT and main steam safety valve (MSSV) opening. An MSRT has a greater flow capacity than an MSSV, but the MSRT can be isolated by the PS, so both scenarios are analyzed. The Inadvertent Opening of an MRST or MSSV event is an AOO.

The response of the plant to an inadvertent opening of an MSRT or MSSV (along with an SWCCF in the PS) is analyzed in two parts. The first part is prior to RT by DAS. The excess capacity of a single failed open MSRT is 50 percent of full steam load in one loop. This is greater than the capacity of a failed open MSSV, which is 25 percent of full steam load in one loop. However, the MSRT and MSSV capacities are both less than the excess capacity of failing all the turbine bypass valves, which is 60 percent of full steam load from all four loops.

Therefore, the increase in the load removed by the secondary system, with the accompanying decrease in RCS temperatures and increase in core power, is less than for the Increase in Steam Flow event discussed in Section A.3.2.3. Therefore, the pre-RT DNB consequences for this event are bounded by the results of the Increase in Steam Flow event.

For the D3 evaluation, DAS will initiate a RT on low SG pressure. The post-RT response and potential return to power, are bounded by the post-RT ~~main steam line break (MSLB)~~ response. Applying AOO criteria to the steam line break (Section A.3.2.5) for the post-trip response demonstrates that the D3 acceptance criteria are met for an Inadvertent Opening of an MRST or MSSV event.

### A.3.2.5 Steam System Piping Failures

A steam line rupture causes an increase in the steam removed from the SGs. This increases the heat removed from the RCS, lowering the temperatures of the RCS. Decreased RCS temperatures, coupled with a negative MTC, increase reactor power.

The U.S. EPR FSAR analyzes a spectrum of different break sizes at different power levels, for both pre-RT and post-RT conditions. In all cases, the FSAR analyses credit the EFW flow control (SAS) to limit EFW flow to a depressurized steam generator SG. The operator is assumed to isolate EFW to the affected steam generator SG after 30 minutes. For the period up to RT, the U.S. EPR FSAR analyzes three break sizes, 10 percent, 50 percent, and 100 percent of steam line area.

The main steam line break (MSLB) event was not specifically analyzed with S-RELAP5 for the diversity and defense-in-depth (D3) assessment, but was evaluated by a quantitative comparison to the FSAR Tier 2, Chapter 15 analysis using best estimate assumptions. Hot full power (HFP) was assumed as the initial condition in all the D3 assessments. HFP represents the normal plant operating condition and is consistent with best estimate conditions.

For these cases, RT occurs on high core power (based on thermal power), low DNB, or high SG pressure drop. For the case with an SWCCF in the PS at full power, the available DAS RT functions are excure high neutron flux or low SG pressure.

The 10 percent break cases act essentially the same as the increased steam flow events. (See Section A.3.2.3.) The conclusions and cases analyzed for these events cover the 10 percent break area cases for MSLB for the pre-RT period.

Larger break sizes quickly lead to RT and MSIV closure, on low SG pressure. The use of best estimate neutronics parameters, particularly MTC, limits the power increase. Therefore, DNB does not occur; no fuel failures occur, and the radiological dose limits are respected.

After RT, flow to the turbine is isolated. However, if the break is located between the SG outlet and the MSIV, steam flow through the break continues. The long term cooldown aspects involve a potential return to power and a possible challenge to DNBR limits.

For the post-RT period, the U.S. EPR FSAR analysis considers a spectrum of breaks, initiated from various power levels. In the FSAR analysis, the case initiated from hot zero power HZP is limiting with respect to return to power. For cases initiated from HFP, RT and MSIV closure is on high SG pressure drop. For an SWCCF in the PS at full power, DAS initiates RT on low SG pressure, as discussed above. DAS subsequently isolates MFW in the affected SG on a lower SG pressure. It actuates EFW on low SG level. After 30 minutes, the operator terminates EFW flow to the affected SG.

The value of MTC is a dominant parameter for MSLB, because it determines the positive reactivity feedback from the cooldown. The use of a best estimate MTC significantly reduces the positive reactivity feedback and the potential return to power. Additionally, by crediting best estimate scram and shutdown margin worths (including no stuck RCCA), a significantly larger negative reactivity must be overcome by the cooldown feedback to result in a return to criticality. With best estimate neutronics, including scram worth and excess shutdown margin, the core does not return to criticality, even after an extended cooldown. ~~Assuming all RCCAs in after scram (no stuck RCCA) with best estimate neutronics, it is calculated the RCS could cool to 105°F before the core returns to criticality.~~ To establish whether the core would return to critical following an MSLB from HFP with a SWCCF of the PS, the temperature at which the core would be critical under best-estimate assumptions was determined. For this calculation, the PRISM reactor analysis tool was used to determine the reactor state ( $k_{eff}$ ) as a function of temperature with all rods in (ARI), HFP xenon, and at end of cycle (EOC). The cases employ both thermal and Doppler feedback mechanisms to determine the reactivity response as a function of inlet

temperature at isothermal conditions. Assuming all RCCAs in after scram (no stuck RCCA) with best estimate neutronics, it is calculated the RCS could cool to 105°F before the core returns to criticality. This limiting set of conditions coincides with an equilibrium cycle, and the results are summarized in Table A.3.2-1Table A.3.2-1.

These data illustrate that the temperature at which a return to critical is expected to occur post-MSLB is ~ 105°F under best-estimate core conditions at EOC, ARI with HFP xenon conditions. This is the basis for the conclusion that a return to power would not occur following an MSLB considering an ~~software common cause failure (SWCCF).~~

Because this temperature is well below the saturation temperature at atmospheric pressure, the SGs cannot cool the RCS to this level. With no return to criticality, there are no fuel failures and radiological dose criteria are met. Therefore, the U.S. EPR design is adequate in addressing an SWCCF in the PS, for a spectrum of MSLBs. As discussed in Section A.3.2.4, because there is no fuel failure, this conclusion also applies to the Inadvertent Opening of an MRST or MSSV event.

Once the affected SG dries-out because of isolation of the MFW and EFW, long term heat removal is accomplished by feeding the unaffected SGs with MFW or EFW and venting steam out of the MSRTs. In this scenario, the operator manually controls the MSRTs.

The difference between this analysis and that documented in the U.S. EPR FSAR Tier 2, Chapter 15 ~~involves the use of best estimate moderator temperature coefficient (MTC), Doppler fuel temperature coefficient (DTC), and scram reactivity. The difference in these parameters between the best estimate and FSAR Tier 2, Chapter 15 values are given in Table A.3.2-2Table A.3.2-2.~~

The U.S. EPR FSAR Tier 2, Chapter 15 values include biases and account for calculational uncertainties. The best estimate values are determined from the core analysis models for projected Cycle 1 and the equilibrium cycle. The scram reactivity used in the D3 analysis does not assume a stuck rod.

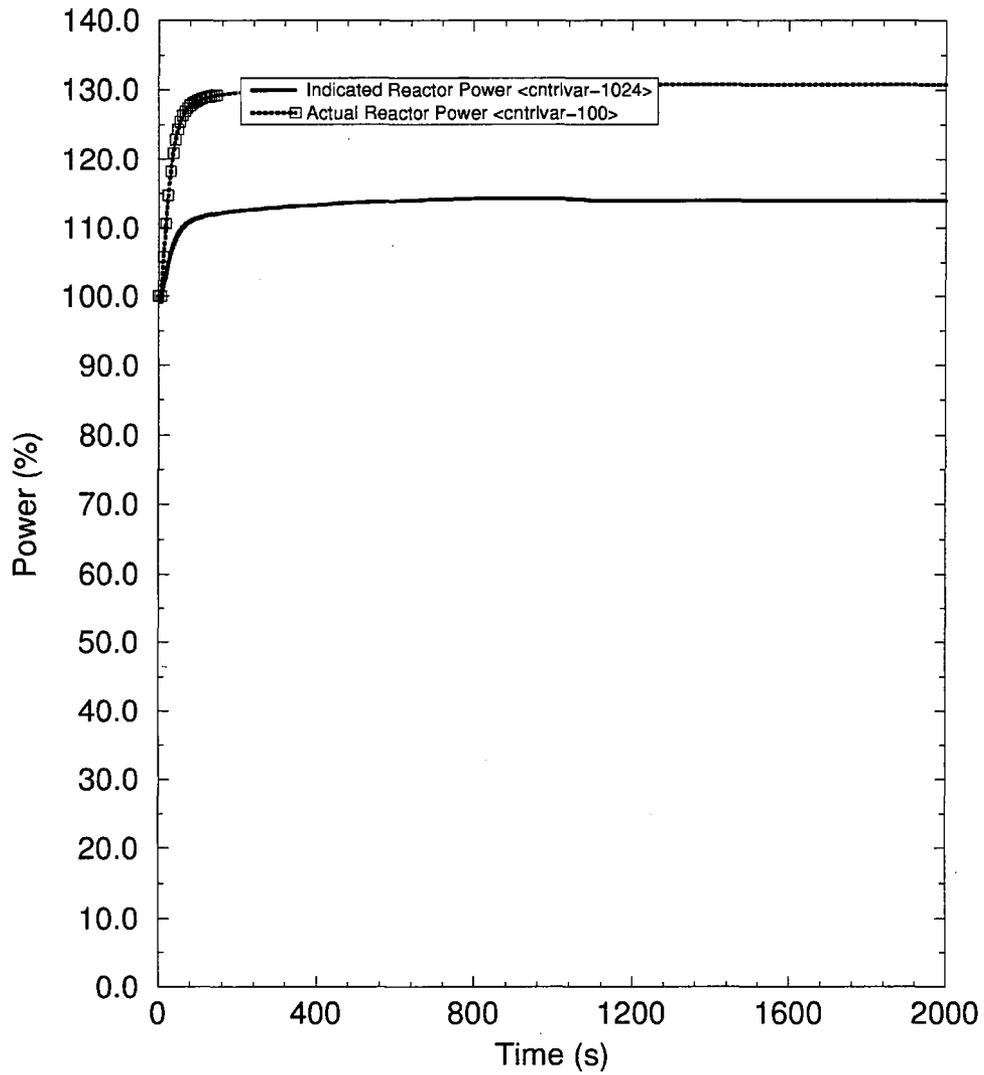
**Table A.3.2-1— $K_{eff}$  Summary for MSLB Event**

<u>Moderator Temperature</u> <u>(°F)</u>	<u>Effective Multiplication</u> <u>Factor (<math>k_{eff}</math>)</u>	<u>Reactivity</u>	
		<u>(<math>\Delta k/k</math>)</u>	<u>(pcm)</u>
<u>596.15</u>	<u>0.924745</u>	<u>-.081380</u>	<u>-8138</u>
<u>600</u>	<u>0.923059</u>	<u>-0.083354</u>	<u>-8335</u>
<u>500</u>	<u>0.953973</u>	<u>-0.048248</u>	<u>-4825</u>
<u>400</u>	<u>0.971725</u>	<u>-0.029097</u>	<u>-2910</u>
<u>300</u>	<u>0.983901</u>	<u>-0.016362</u>	<u>-1636</u>
<u>200</u>	<u>0.993078</u>	<u>-0.006971</u>	<u>-697</u>
<u>100</u>	<u>1.00018</u>	<u>0.000178</u>	<u>18</u>

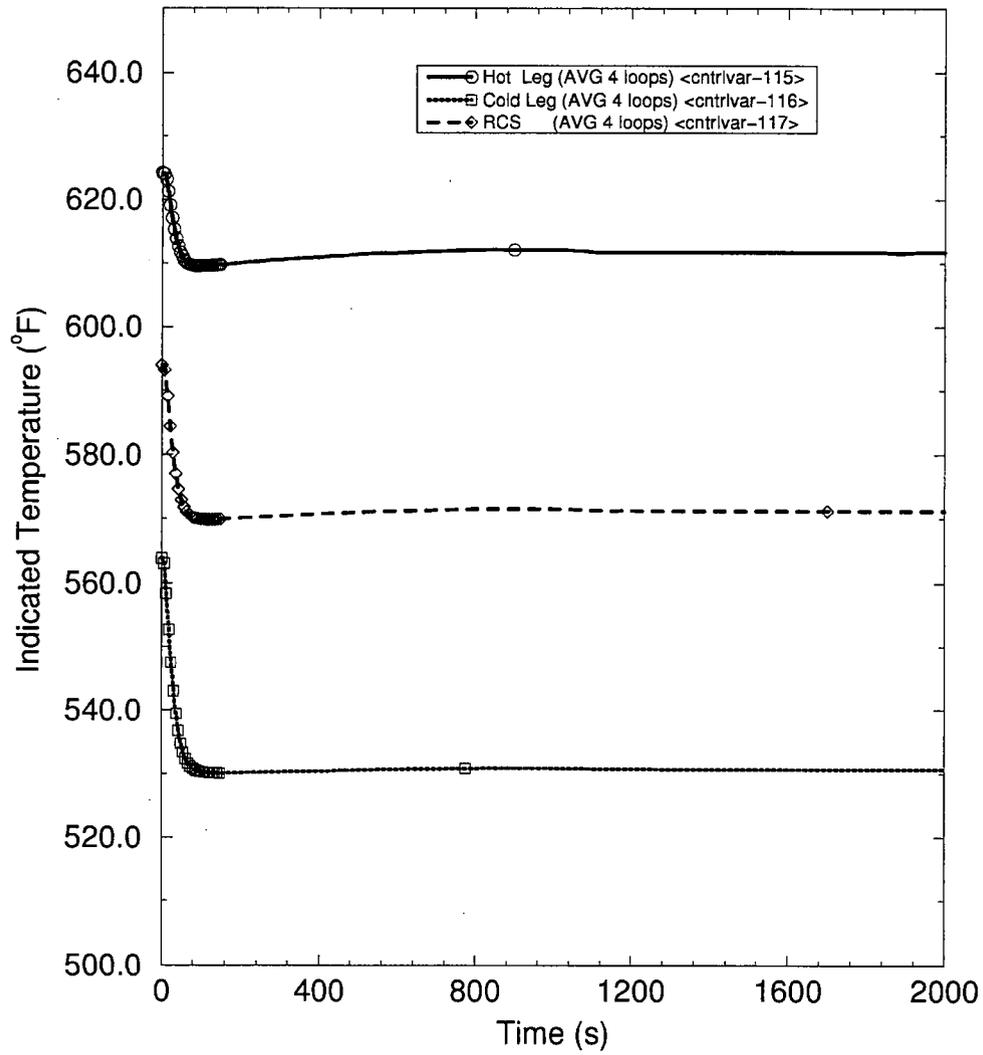
**Table A.3.2-2—Reactivity Parameters Comparison**

<u>Parameter</u>	<u>Best Estimate</u> <u>(Equilibrium Cycle)</u>	<u>U.S. EPR™ FSAR Tier 2,</u> <u>Chapter 15</u>
<u>MTC (pcm/°F) EOC HFP</u>	<u>-39.4</u>	<u>-50</u>
<u>DTC (pcm/°F) EOC HFP</u>	<u>-1.63</u>	<u>-1.85</u>
<u>Scram (pcm) EOC HFP</u>	<u>10349</u>	<u>7353</u>

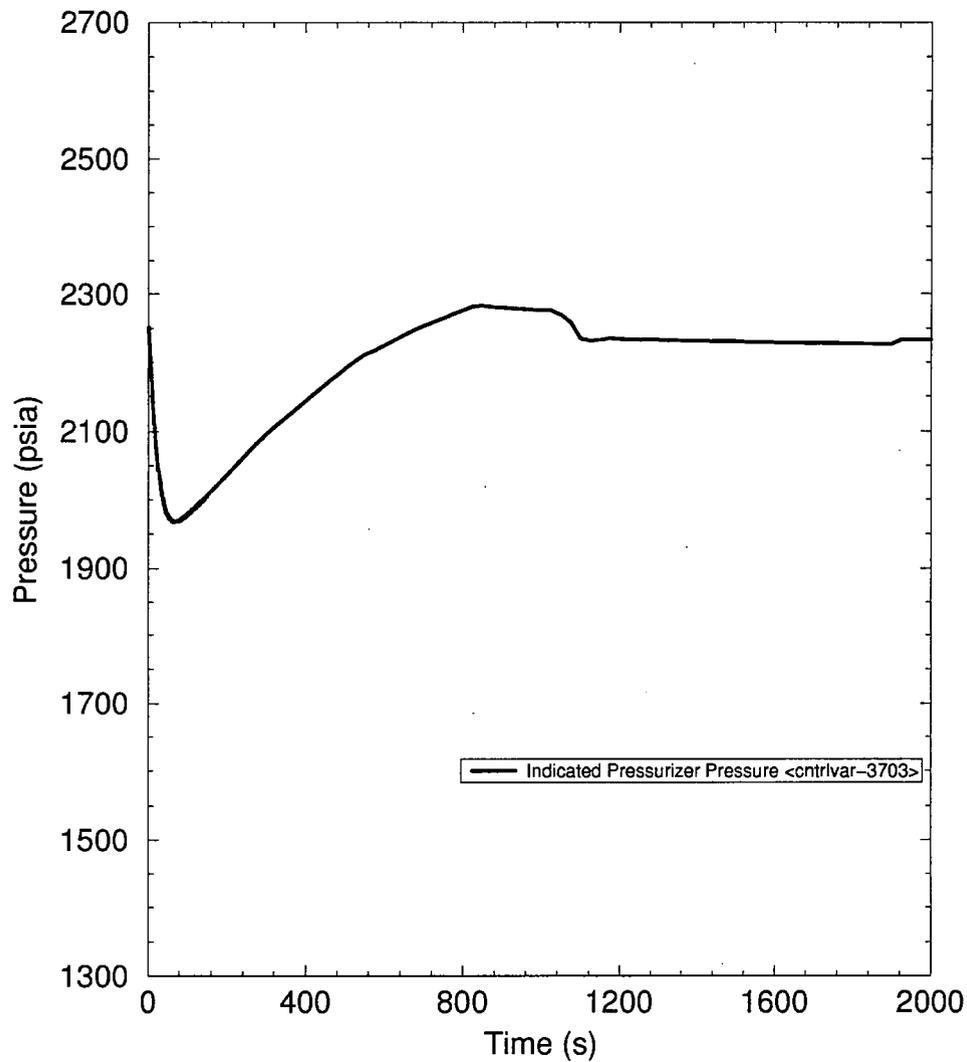
**Figure A.3.2-1—Increase in Steam Flow Event:  
Indicated and Actual Reactor Power**



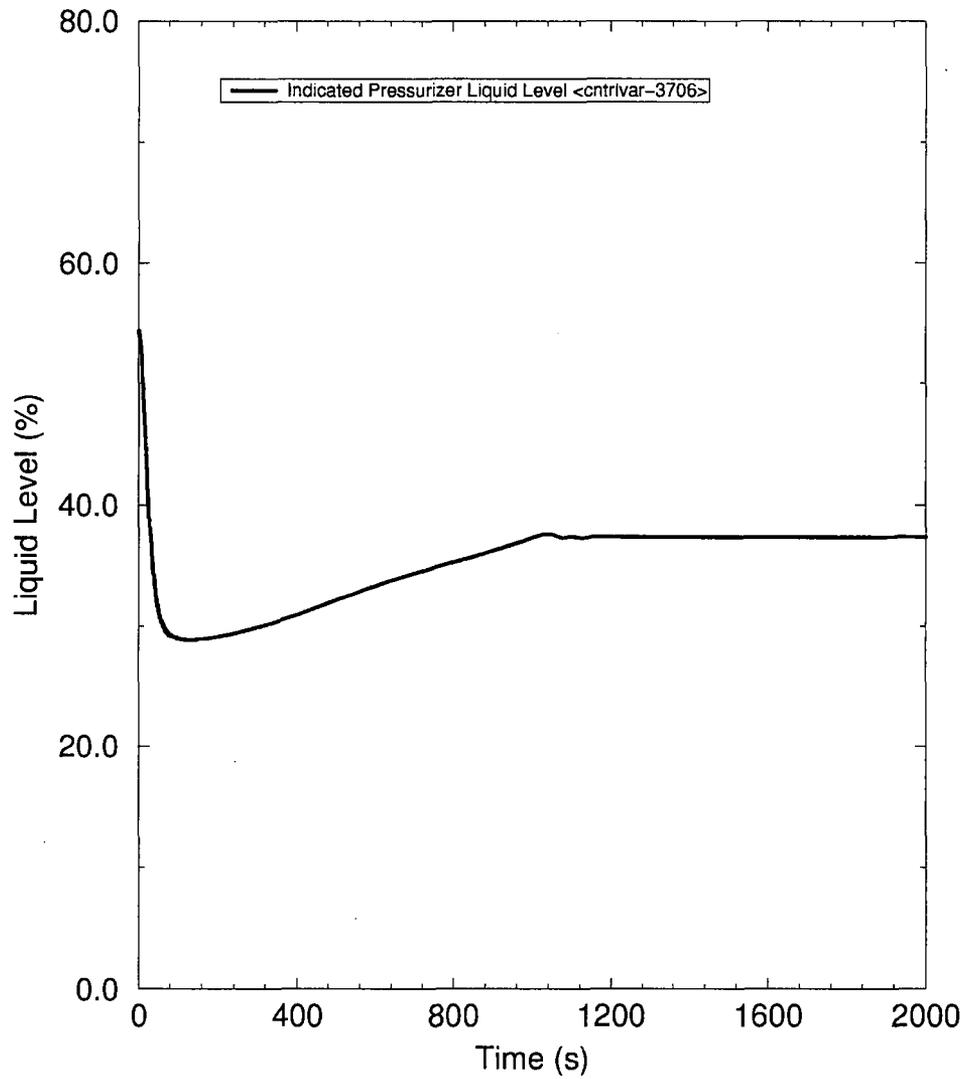
**Figure A.3.2-2—Increase in Steam Flow Event:  
Indicated RCS Four-Loop-Average Temperatures**



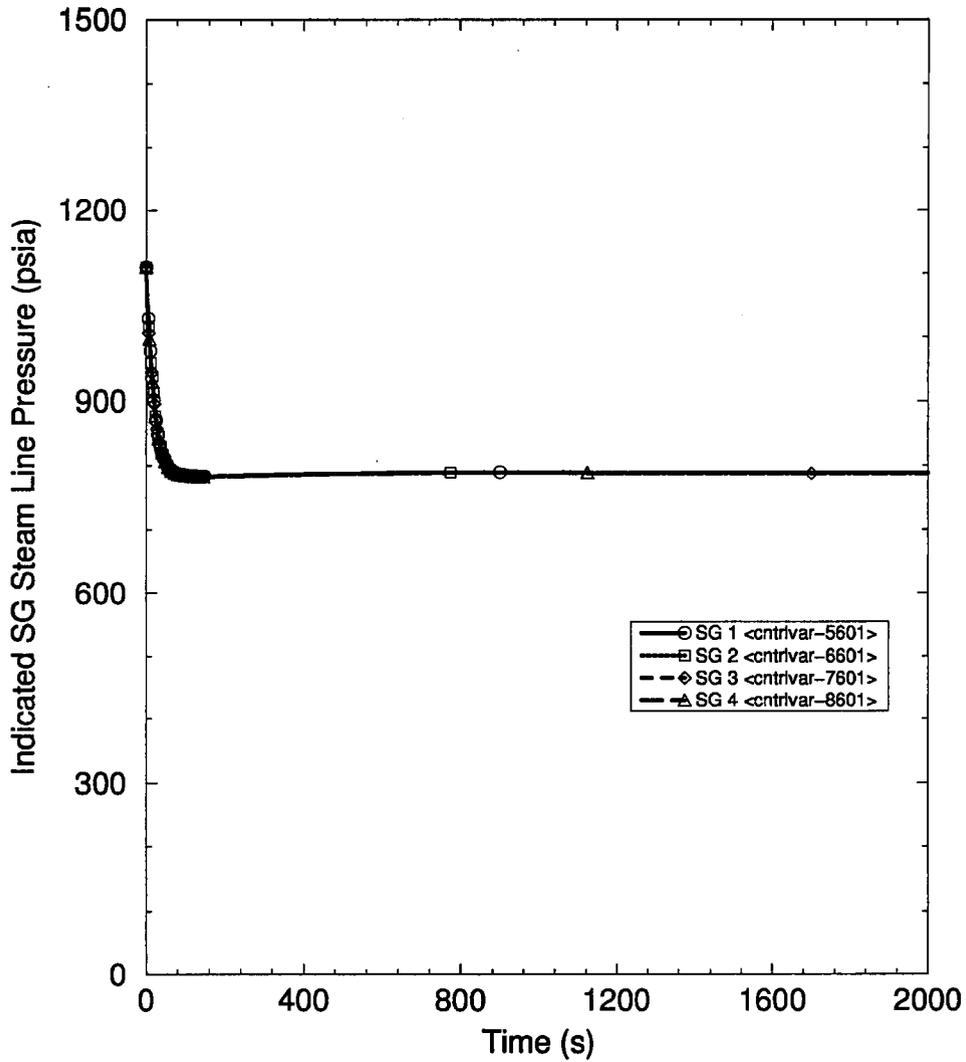
**Figure A.3.2-3—Increase in Steam Flow Event:  
Indicated Pressurizer Pressure**



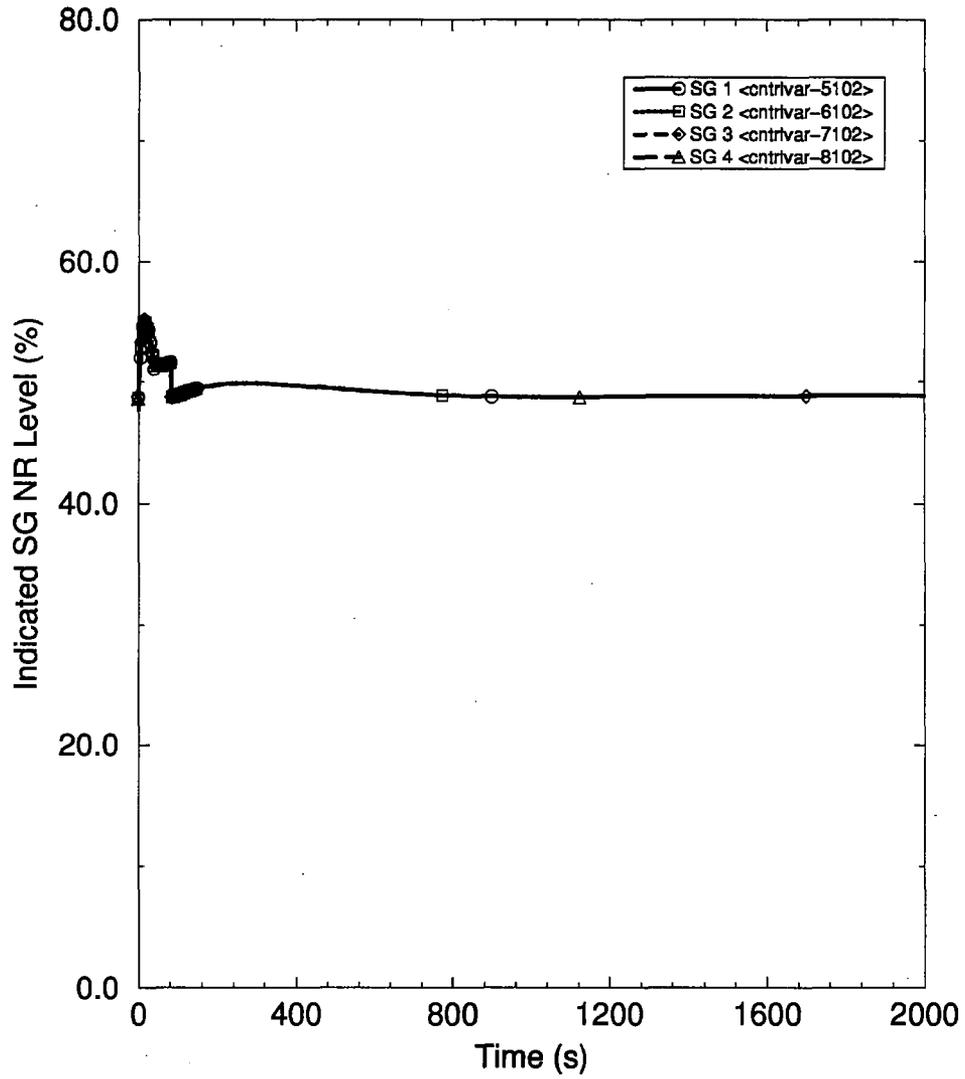
**Figure A.3.2-4—Increase in Steam Flow Event:  
Indicated Pressurizer Liquid Level**



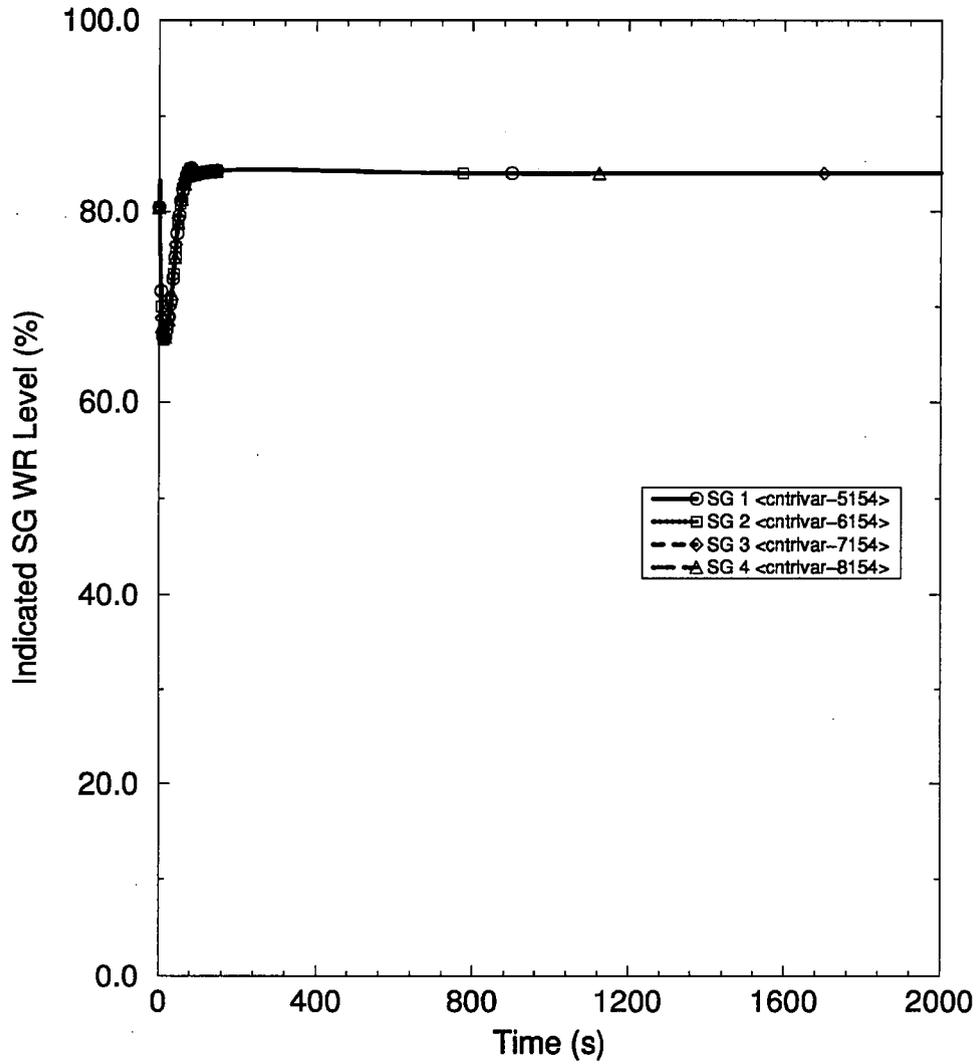
**Figure A.3.2-5—Increase in Steam Flow Event:  
Indicated SG Steam Line Pressure**



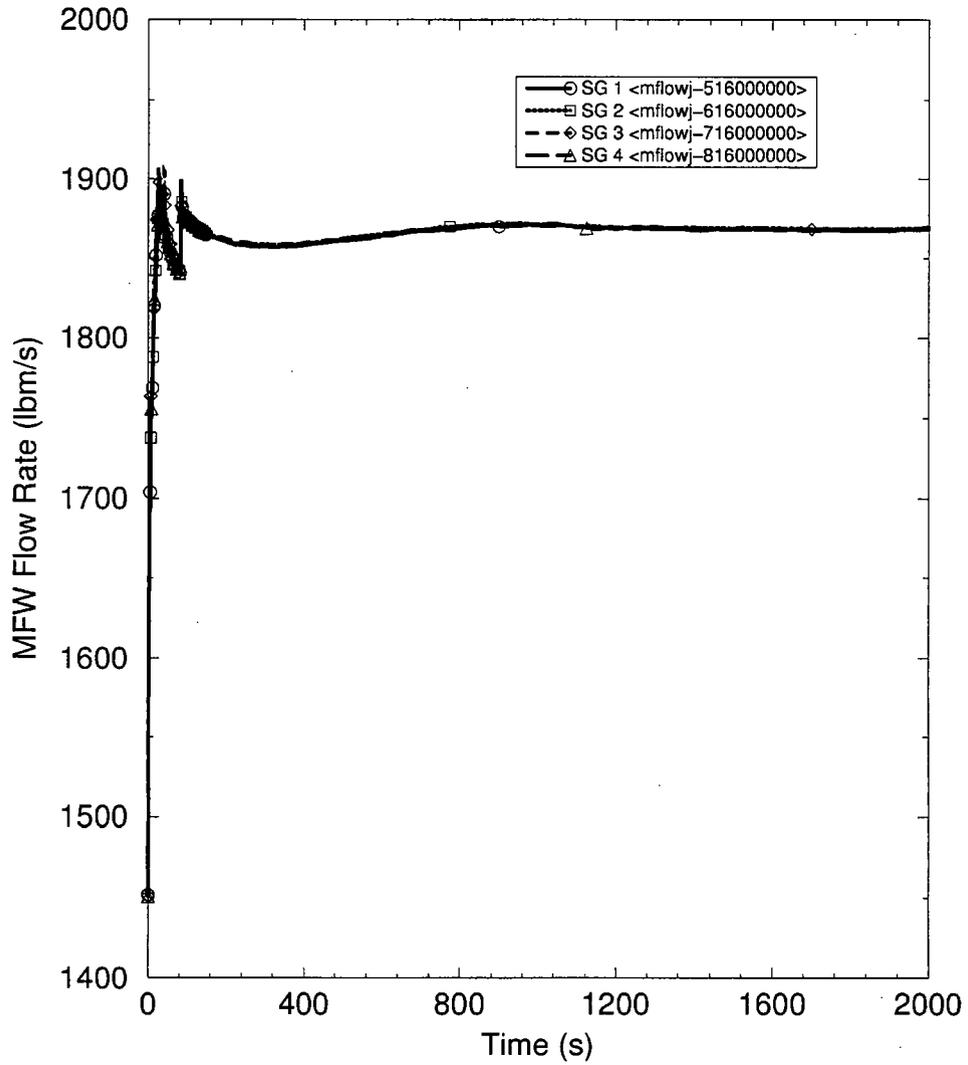
**Figure A.3.2-6—Increase in Steam Flow Event:  
Steam Generator Level (NR)**



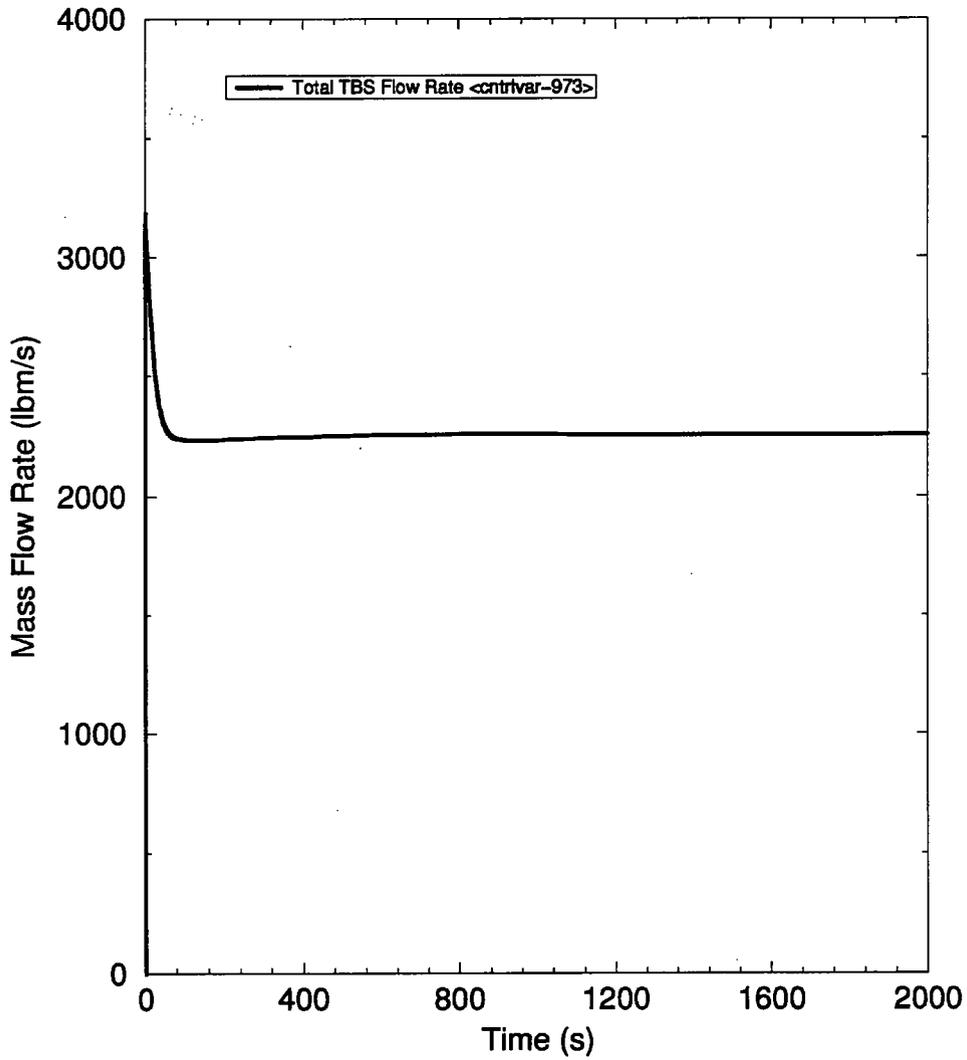
**Figure A.3.2-7—Increase in Steam Flow Event:  
Indicated Steam Generator Level (WR)**



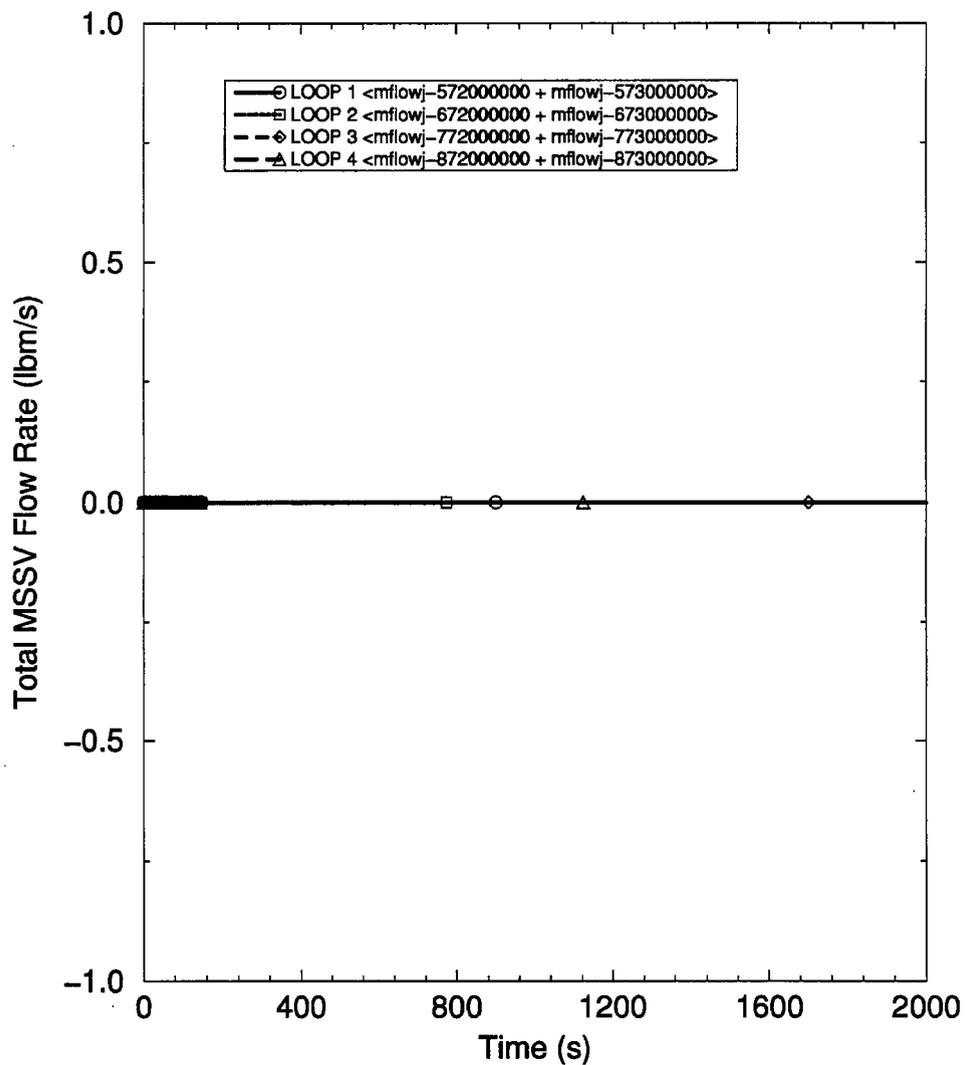
**Figure A.3.2-8—Increase in Steam Flow Event:  
Main Feedwater Flow Rate**



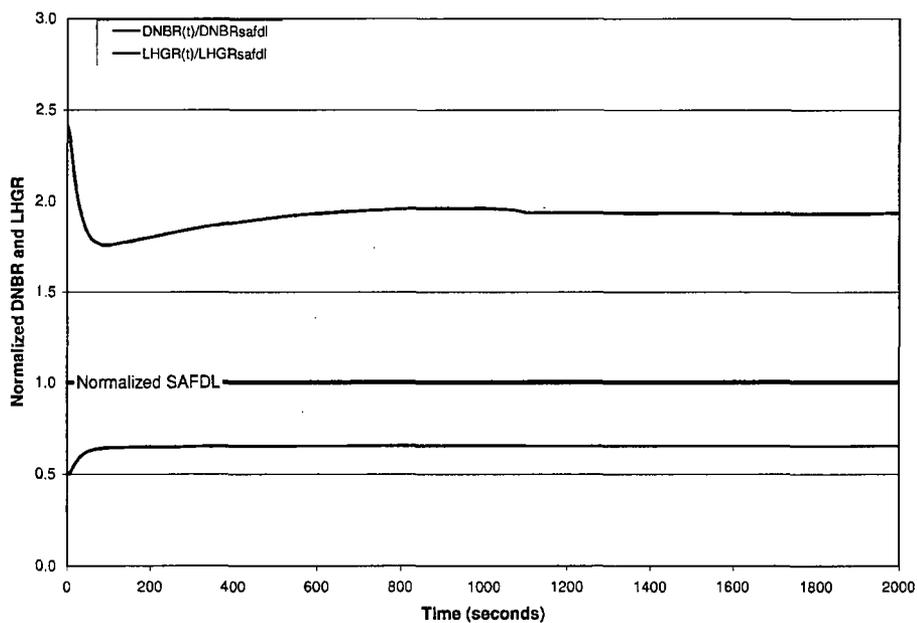
**Figure A.3.2-9—Increase in Steam Flow Event:  
Total TBS Flow Rate**



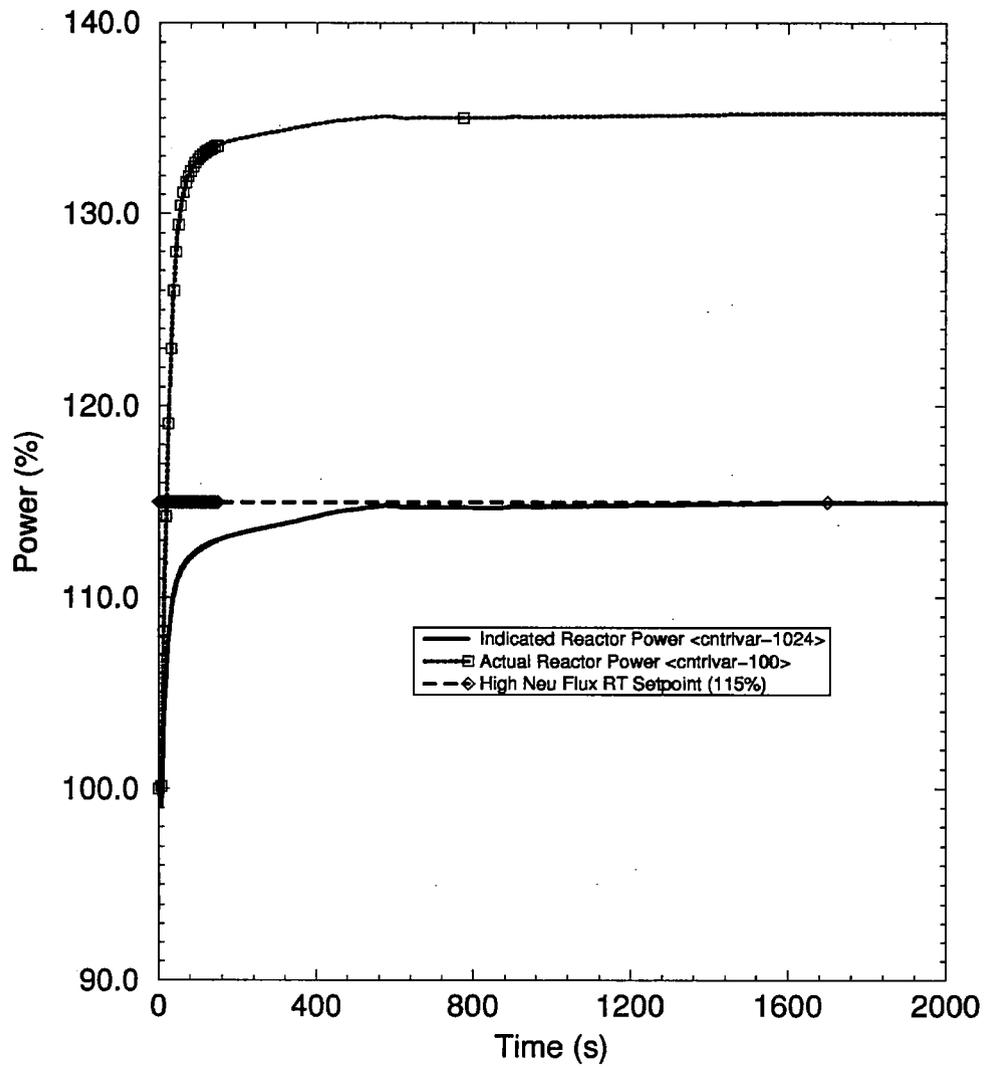
**Figure A.3.2-10—Increase in Steam Flow Event:  
MSSV Flow Rate**



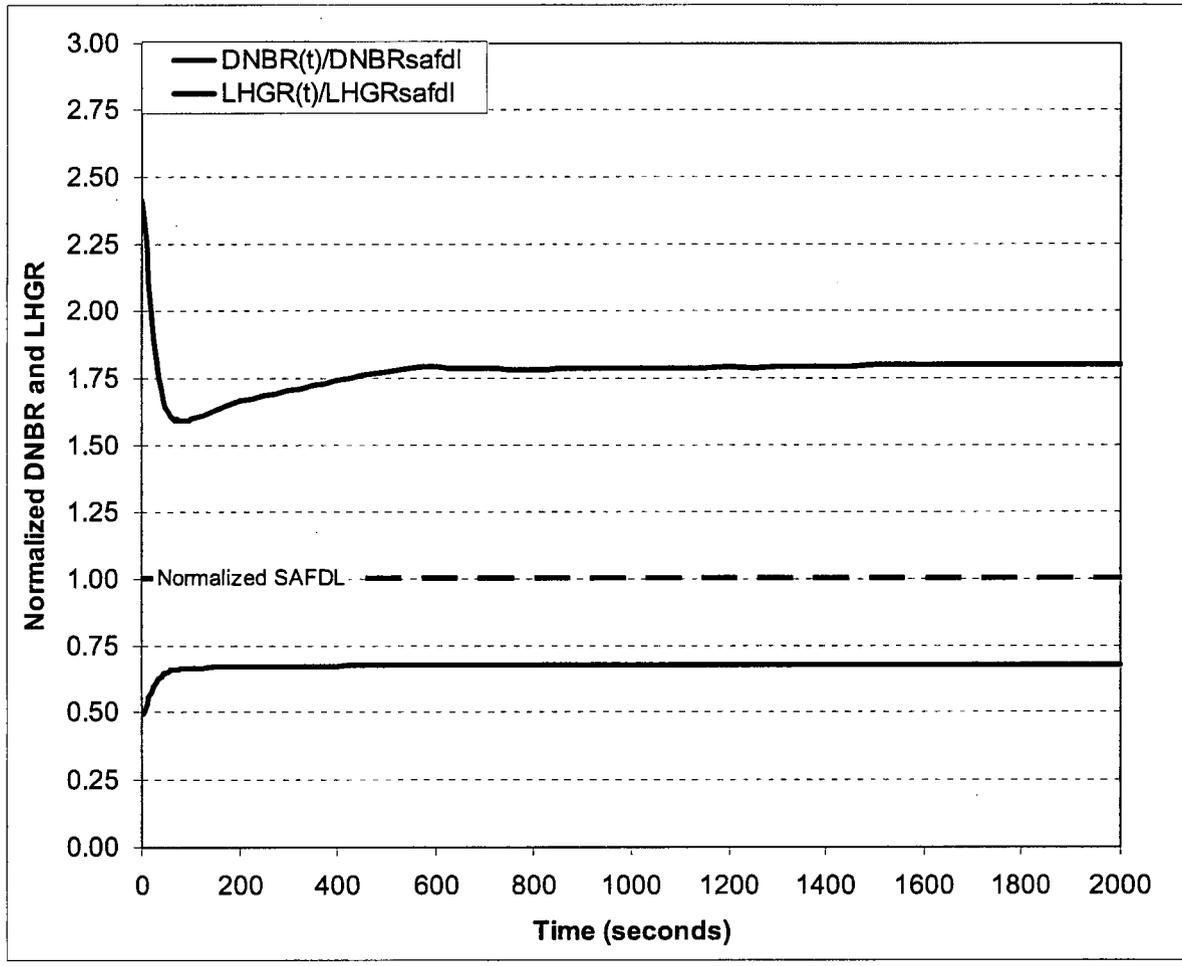
**Figure A.3.2-11—Increase in Steam Flow Event:  
Normalized DNBR and LHGR-PSRV Flow Rate**



**Figure A.3.2-12—Increase in Steam Flow Event: Power Response for Case Stabilizing under the High Neutron Flux Setpoint**



**Figure A.3.2-13—Increase in Steam Flow — Normalized DNBR and Linear Heat Generation Rate for Case Stabilizing under the High Neutron Flux Setpoint**



### **A.3.3 *Decrease in Heat Removal by Secondary System***

#### **A.3.3.1 Loss of External Load / Turbine Trip / Loss of Condenser Vacuum**

The Loss of External Load event is initiated by an electrical disturbance that causes a reduction or loss of electrical load on the turbine generator. It results in the fast closure of the turbine control valves. A turbine trip (TT) event causes the fast closure of the turbine stop valve. Because the turbine stop valve closes faster than the turbine control valves, the TT bounds the response of the LOEL event.

The main effect of this event is RCS overpressure consistent with the U.S. EPR FSAR analysis. Secondary side overpressure is bounded by the MSIV closure event of Section A.3.3.2. MDNBR limits are not challenged because RCS pressure increases during the event and there is little change in core power. In the U.S. EPR FSAR analysis, RT occurs on high pressurizer pressure. In the case of an SWCCF in the PS, DAS initiates RT on high pressurizer pressure, providing comparable protection. In addition, MFW is available to provide primary system heat removal. The TBS is available to limit the RCS and secondary pressure response to the TT event. Under this condition, if RCS pressure increases to the PSRV setpoint, the PSRVs limit RCS pressure to well below 120 percent of design pressure. (See Section A.2.4.) Therefore, the acceptance criteria are met and the U.S. EPR design is determined to be adequate in protecting against overpressure events with an SWCCF in the PS.

For the Loss of Condenser Vacuum event, the turbine, TBS and MFW are not available because of the loss of the condenser. Consequently, the secondary side pressure increases up to the MSSV setpoint after RT. The RCS pressure response is similar to that presented in the U.S. EPR FSAR. DAS initiates RT on high pressurizer pressure. Peak RCS pressure is limited by the PSRVs and remains below 120 percent of design pressure. In the long term, decay heat is removed through the MSSVs or manually through the MSRTs. DAS automatically actuates EFW on low SG level. SG level is maintained through manual control of the EFW system.

Therefore, the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS during the Loss of External Load, Turbine Trip, and Loss of Condenser Vacuum events.

### A.3.3.2 Inadvertent Closure of MSIV

The MSIV closure event is initiated by a control system or operator error that closes a single MSIV. The main effect of this event is secondary system overpressure. Although there is no specific secondary system pressure criteria specified in Reference A-1, this analysis applies a conservative limit of 120 percent of design pressure.

For the limiting case presented in the U.S. EPR FSAR analysis, the PS initiates RT on high SG pressure. DAS does not have a comparable RT function. Therefore, for the case with an SWCCF in the PS, an analysis is performed to assess whether DAS is adequate.

In the case of an SWCCF in the PS, the closure of a single MSIV results in isolation of steam flow to one SG. The net heat removal decrease leads to increasing pressure and temperature in the isolated SG and main steam line and a consequential rise in RCS loop temperature in the affected loop. The steam flow from the remaining SGs increases as a result, since the unaffected SGs attempt to supply the total turbine steam load demand, resulting in a concurrent cooldown of the unaffected SGs. Eventually, DAS initiates RT on low SG level in the affected loop, as a result of the affected SG pressure increase. The affected SG pressure increase significantly reduces the feedwater flow to that SG and also collapses the steam voids. The most limiting case occurs under EOC conditions, because of the large negative MTC and the cooldown in the unaffected loops.

~~Figure A.3.3-1~~~~Figure A.3.3-4~~ through ~~Figure A.3.3-7~~~~Figure A.3.3-7~~ show the responses of the key parameters for this event. The maximum pressure on the secondary side is found at the top of the affected ~~steam generator~~SG tubesheet below the cold-side downcomer. The peak pressure is 113 percent of its design pressure, at approximately 134 seconds. The pressure transient is controlled by the opening of the MSSVs in the affected steam line. Eventually, DAS initiates RT on low SG level. The peak RCS pressure (at the bottom of the reactor vessel) is 2364 psia, which is less than the RCS design pressure. DNB and PLPD limits are not challenged during this event. Thus, the acceptance criteria for D3 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS for the Inadvertent Close of MSIV event.

Long-term heat removal for this event is similar to the post-RT response described in Section A.3.2.1.

### A.3.3.3 Loss of Non-emergency AC Power to the Station Auxiliaries

Loss of non-emergency AC power to the station auxiliaries is initiated by a complete loss of either the external (offsite) grid or the onsite AC distribution system. Prior to RT, the event is similar to the Complete Loss of RCS Flow event (Section A.3.4.2) and, in the long-term after RT, the event is similar to the Loss of Normal Feedwater event (Section A.3.3.4). For the case with an SWCCF in the PS, the DAS initiates RT on low RCS flow, within a few seconds of the loss of ~~RPCs~~RCPs. Normally, the emergency diesel generators (EDG) automatically start and load the safety buses. However, with the loss of AC and the SWCCF failure of the PS, the EDGs must be manually started and loaded. The SBO DGs automatically start with a loss of AC in this scenario. However, in order to power the EFW pumps, it is necessary to manually load the EFW pumps to the SBO DGs.

For the loss of AC with an SWCCF in the PS, DAS initiates RT within a few seconds, on low RCS flow. At this point, all four SGs are still essentially at their normal full power water level. This amounts to approximately 170,000 lb<sub>m</sub> of liquid per ~~steam generator~~SG. If it is assumed this mass is at saturation and at a pressure corresponding to the low set MSSV (1460 psig), it requires 112.1 MW-hr of energy to boil the ~~steam generator~~SGs dry.

$$Q_{\text{boil dry}} = (\text{SG water mass per SG}) * (h_{fg}) * (\text{number of SGs})$$

$$Q_{\text{boil dry}} = 170,000 \text{ lb}_m * 563 \text{ Btu/lb}_m * 4$$

$$Q_{\text{boil dry}} = 382.8 \times 10^6 \text{ Btu} / 3.414 \times 10^6 \text{ Btu/MW-hr} = 112.1 \text{ MW-hr}$$

It takes approximately 1.5 hours for the cumulative decay heat to reach this value. Thus, it takes approximately 1.5 hours for the ~~steam generator~~SGs to boil dry, following a loss of AC. Therefore, sufficient time is available for the operator to start the EFW pumps by using either the EDGs or the SBO DGs, to prevent the ~~steam generator~~SGs from boiling dry and to maintain a heat sink throughout the event. The U.S. EPR design is therefore to be adequate in addressing SWCCF in the PS during a Loss of Non-emergency AC event.

If the SBO DGs are used to power the EFW pumps to provide liquid make up to the SGs, their capacity is such that only two EFW pumps can be loaded. Under the loss of AC conditions, two EFW pumps are sufficient to remove decay heat and recover level as illustrated below.

Decay heat (best estimate) is 75.6 MW, at 30 minutes after shutdown. Therefore, the flow required from the EFW system, to remove decay heat at 30 minutes after shutdown, is:

$$W = Q / (hg - hin) = \frac{75.6 \text{ MW} (3.414 \times 10^6 \text{ Btu/MW-hr}) (.01614 \text{ ft}^3/\text{lb}_m) (7.481 \text{ gal/ft}^3)}{(1171.5 \text{ Btu/ lb}_m - 93.6 \text{ Btu/ lb}_m) (60 \text{ min/hr})} = 482 \text{ gpm}$$

The flow from each EFW pump under best estimate conditions is approximately 400 gpm at 122°F and a pressure of 1460 psig. Therefore, two EFW pumps feeding two steam generator SGs are sufficient to remove heat and recover level.

~~At this time the U. S. EPR Emergency Procedure Guidelines/Emergency Operating Procedures are still under development. Symptom-based recovery instructions for all the secondary inventory loss scenarios are envisioned planned set to not require that a special D3 coping procedure will not be required.~~

~~There are alternative actions are available if EFW pumps cannot be started within the one and a half hours and the SGs boil dry, alternative actions are available. Once the SGs boil dry, the primary system will initiate a heat-up. If feedwater sources cannot be recovered, the operator initiates a primary system feed and bleed. The operator opens the pressurizer safety relief valves (PSRVs) to depressurize the primary system, activating the medium head safety injection (MHSI) and the low head safety injection (LHSI). Decay heat is removed by the vented steam and water through the PSRVs, and the safety injection (SI) pumps would provide make-up to keep the core covered. This process could continue indefinitely with recirculation from the in-containment refueling water storage tank (IRWST) or until secondary feedwater sources are recovered.~~

#### A.3.3.4 Loss of Normal Feedwater Flow

The Loss of Normal Feedwater event is an AOO initiated by the complete termination of MFV flow. This condition can be caused by a loss of power to the main feedwater pumps or a malfunction of the feedwater control system or equipment. The U.S. EPR FSAR criterion for this event is to confirm the ability of the EFW system to maintain SG inventories sufficient for decay heat removal. DNBR limits are not challenged, and, because the event progresses fairly slowly, peak RCS and secondary system pressures are bounded by the TT and MSIV closure events, respectively. In the U.S. EPR FSAR analysis, PS initiates RT on low SG liquid level. In the case of an SWCCF in the PS, best estimate assumptions are made for the setpoint for EFW

actuation (nominal) and EFW pump flow (nominal). The U.S. EPR FSAR analysis conservatively biases EFW actuation setpoints and flow rates low. In addition, a single failure of an EFW train and a train out for preventative maintenance are not assumed, such that the full flow from all four EFW trains are available. The response of the plant, with an SWCCF in the PS, is bounded by the U.S. EPR FSAR analysis response for this event.

Under the assumption of an SWCCF, MSRTs are not available for automatic actuation. However, the TBS is available to control secondary pressure and remove decay heat, after RT. Manual operation of the EFW flows is required for the operators to prevent SG overfill, during long-term control. It takes approximately one hour to fill the ~~steam generator~~SG with EFW from the low level EFW actuation setpoint to the PS EFW isolation setpoint. Therefore, there is sufficient time for the operator to manually control SG level with the EFW system. The operators can also manually open the MSRTs to control secondary pressure and decay heat removal. The BTP 7-19 acceptance criteria are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for the Loss of Normal Feedwater event.

#### **A.3.3.5 Feedwater System Piping Failures**

A feedwater line break (FWLB) results from a rupture in a feedwater line large enough that it is beyond what can be handled by the feedwater system. Smaller break sizes behave similar with a loss of feedwater event. Larger break sizes cause the complete blowdown of an SG, followed by a long term heatup. This event is more limiting than the loss of normal feedwater and presents the greatest challenge to the EFW system.

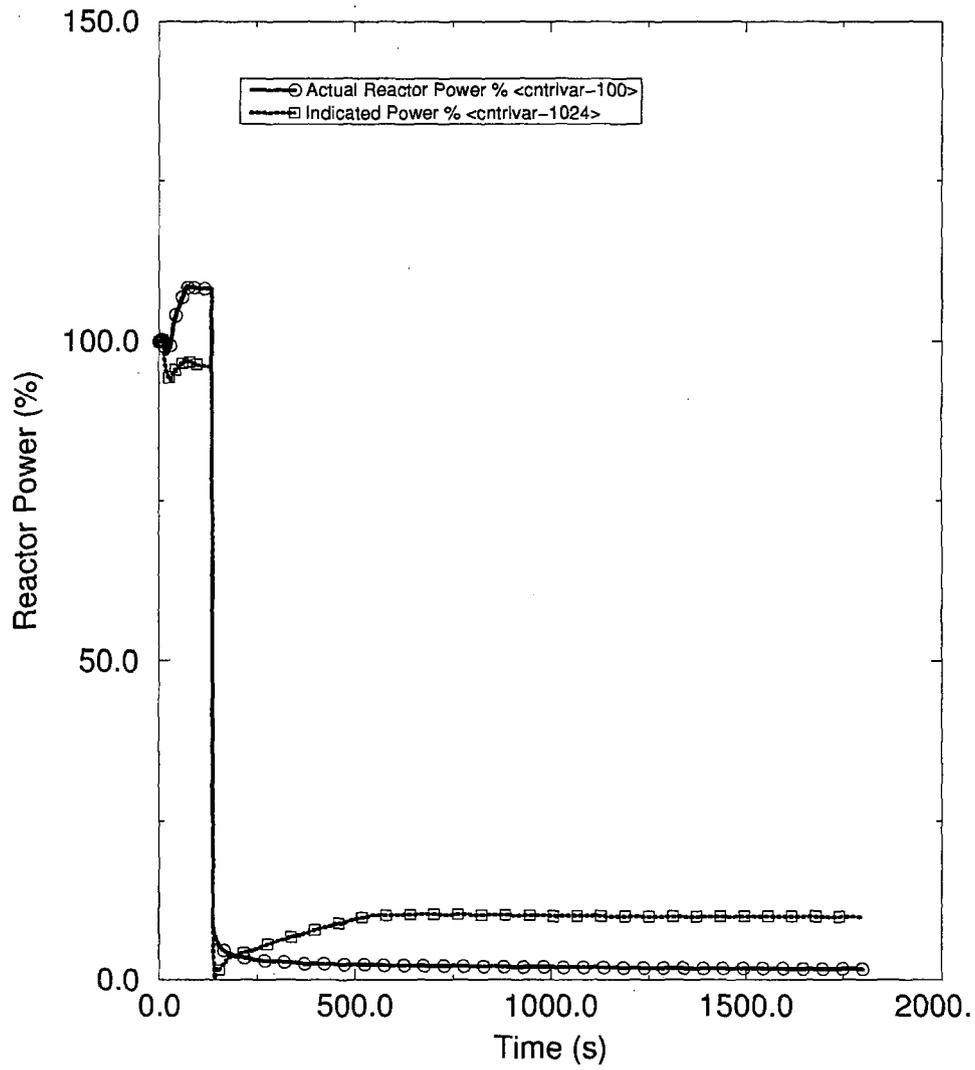
The U.S. EPR FSAR analysis covers a complete break spectrum, from very small breaks just beyond what can be handled by the feedwater system, to a complete severance of the main feedwater pipe. The smaller breaks trip the reactor on high pressurizer pressure. Intermediate breaks trip the reactor on low ~~steam generator~~SG level and the larger breaks trip on high ~~steam generator~~SG pressure drop or low ~~steam generator~~SG pressure. Except for very small breaks, the MSIVs close on high ~~steam generator~~SG pressure drop or low ~~steam generator~~SG pressure. EFW is actuated on low ~~steam generator~~SG level for the entire break spectrum. The MSRTs and MSSVs function to control secondary pressure. The PSRVs limit RCS pressure.

In the case of an SWCCF in the PS, DAS provides the same protection for the range of breaks. DAS has RT functions on high pressurizer pressure, low SG level, and low SG pressure. DAS

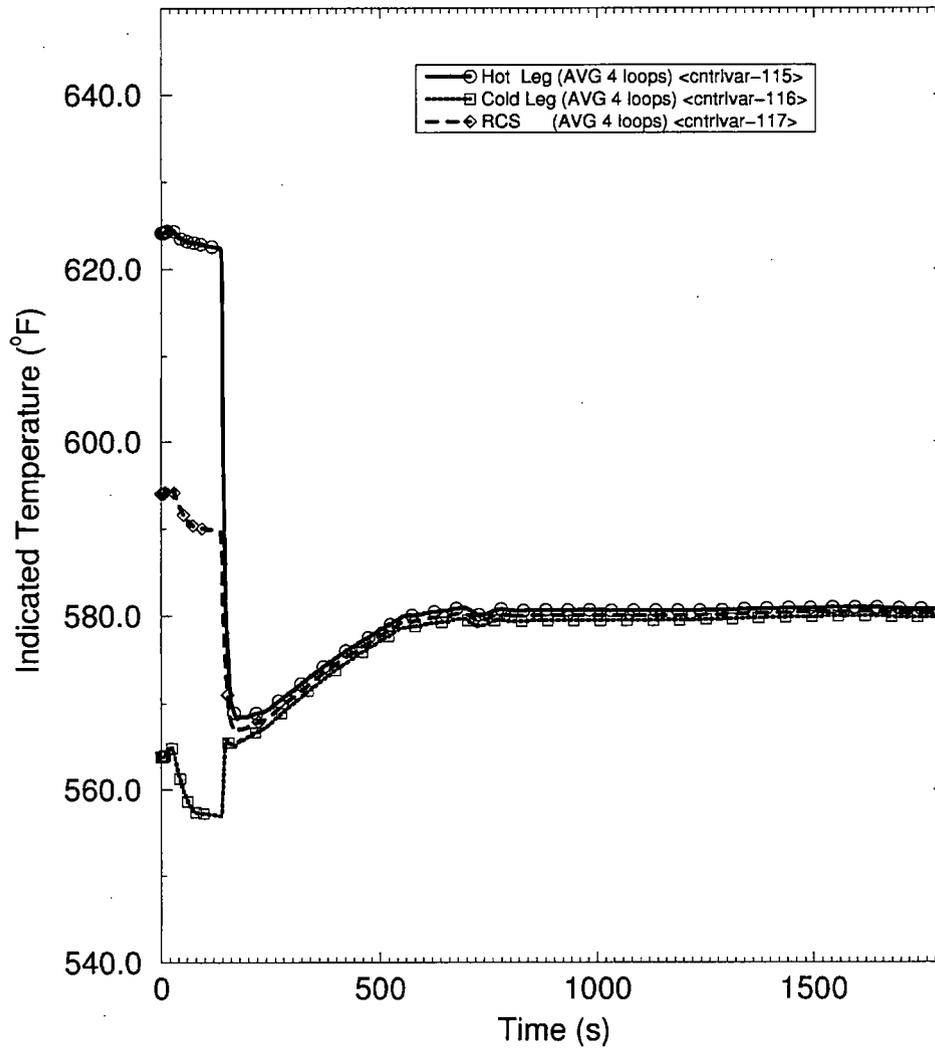
also has functions for MSIV closure on low SG pressure, MFW isolation in the affected SG on low SG pressure, and EFW actuation on low SG level. The PSRVs and MSSVs are not subject to SWCCF and are still available to limit RCS and secondary pressure. In the long term, decay heat would be removed through the intact MSSVs or through the MSRTs through manual operator action.

As noted in Table A.2-3~~Table A.2-3~~, the setpoints and time delays for the DAS functions are such that these functions are reached at a slightly later time in the transient. However, in the case of an SWCCF in the PS with best estimate assumptions, four EFW pumps are available to provide makeup to the SGs. The U.S. EPR FSAR analysis assumes only two EFW pumps are available, because of single failure and preventative maintenance, and that one of the two feed the break. Operator action is required in 30 minutes, to redirect EFW flow from the broken SG to an intact ~~steam generator~~SG. In the case of an SWCCF in the PS, three EFW pumps would feed intact SGs, while one feeds the break. Note also that, since three pumps are feeding intact SGs, as soon as EFW is actuated, sufficient cooling is available early in the transient to remove decay heat and recover levels. The operator terminates EFW flow to the affected SG at 30 minutes. In the U.S. EPR FSAR analysis, only one EFW pump is feeding an intact SG for 30 minutes, until the operator redirects flow from the EFW pump feeding the affected SG. Two EFW pumps feeding intact SGs are required to remove decay heat and recover levels. This added EFW flow more than offsets the delayed actuation of the DAS functions and the plant response is bounded by the U.S. EPR FSAR. Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for the spectrum of Feedwater Line Break events.

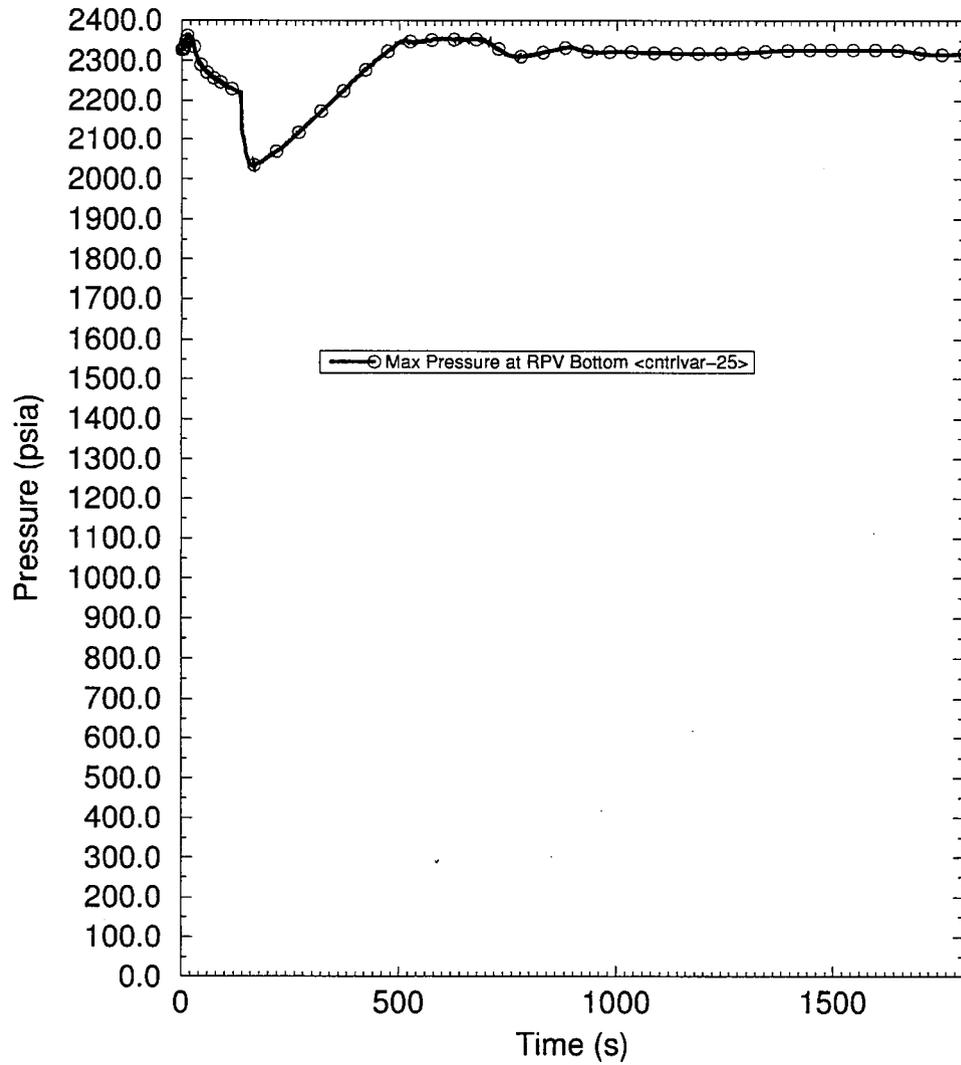
**Figure A.3.3-1—MSIVC Event:  
Indicated and Actual Reactor Power**



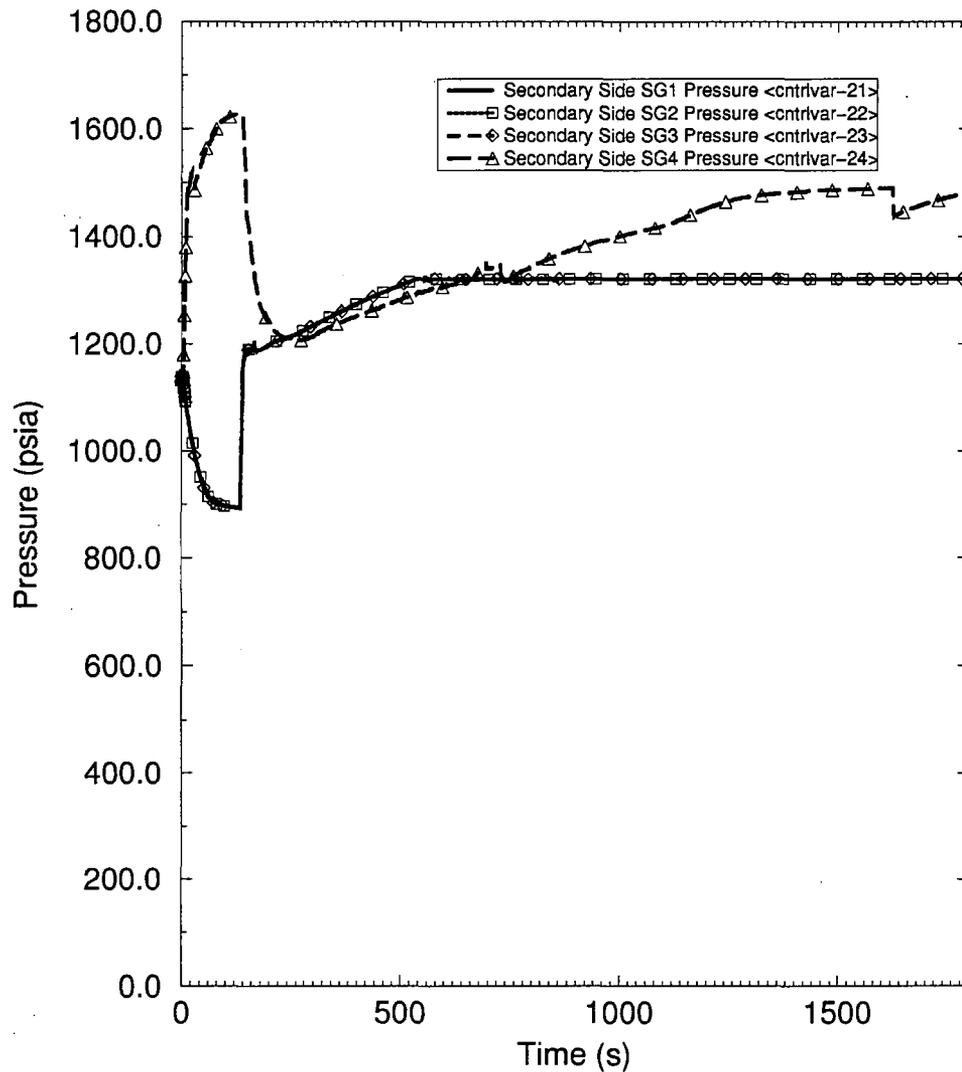
**Figure A.3.3-2—MSIVC Event:  
RCS Average Temperatures**



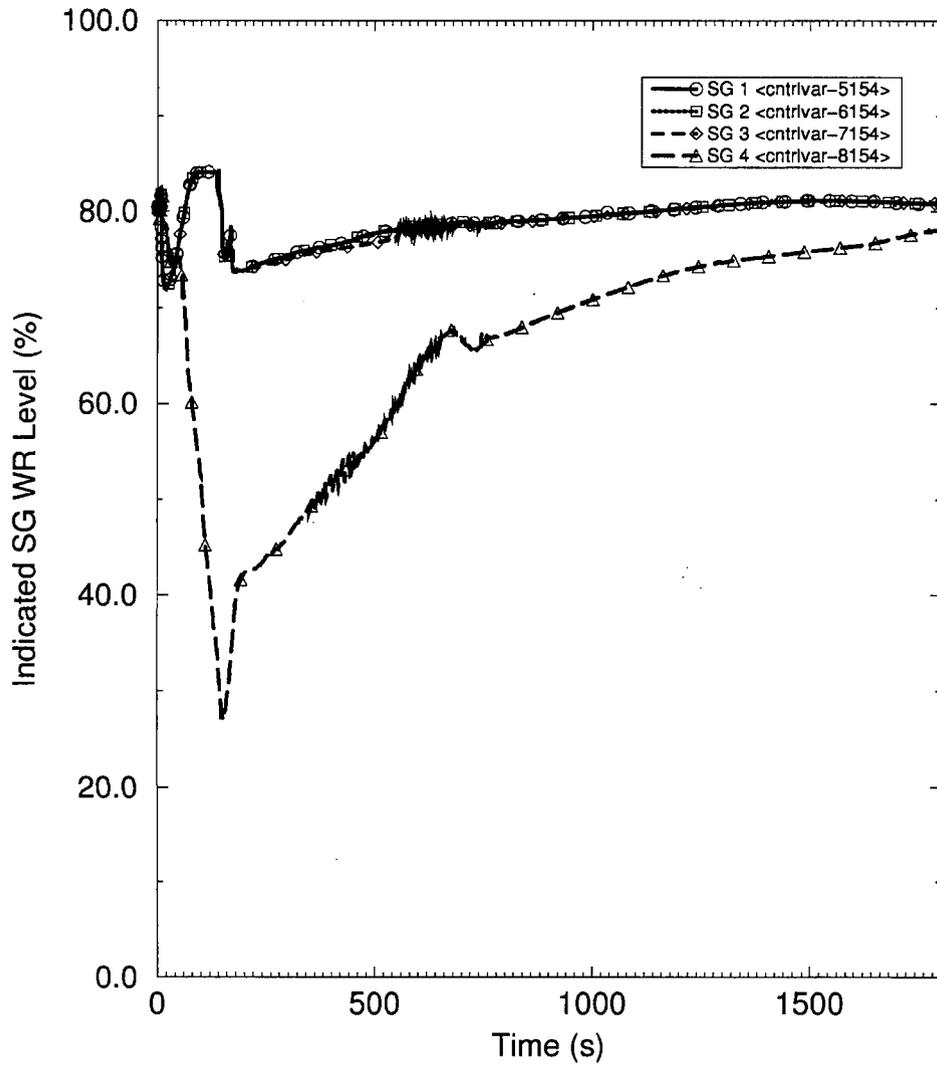
**Figure A.3.3-3—MSIVC Event:  
Maximum RCS Pressure (bottom of RPV)**



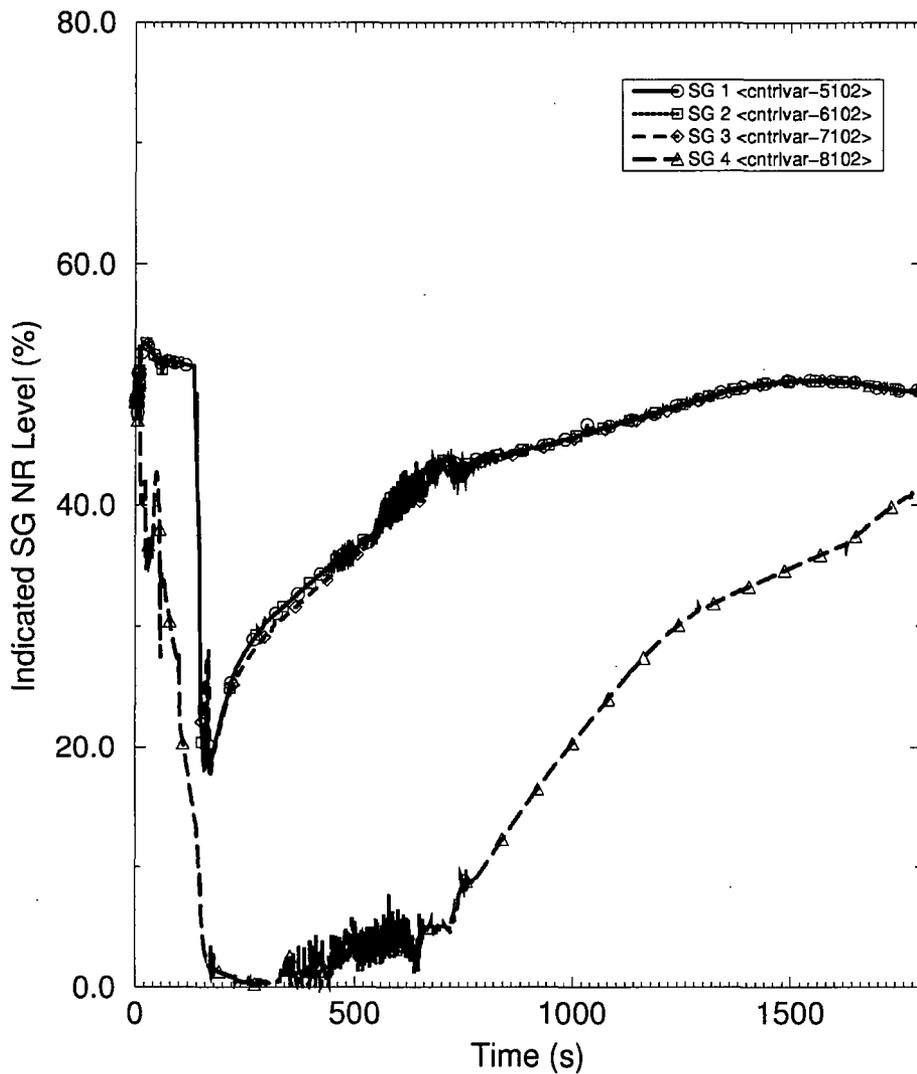
**Figure A.3.3-4—MSIVC Event:  
SG Pressure at Top of Tubesheet Below Cold-Side Downcomer**



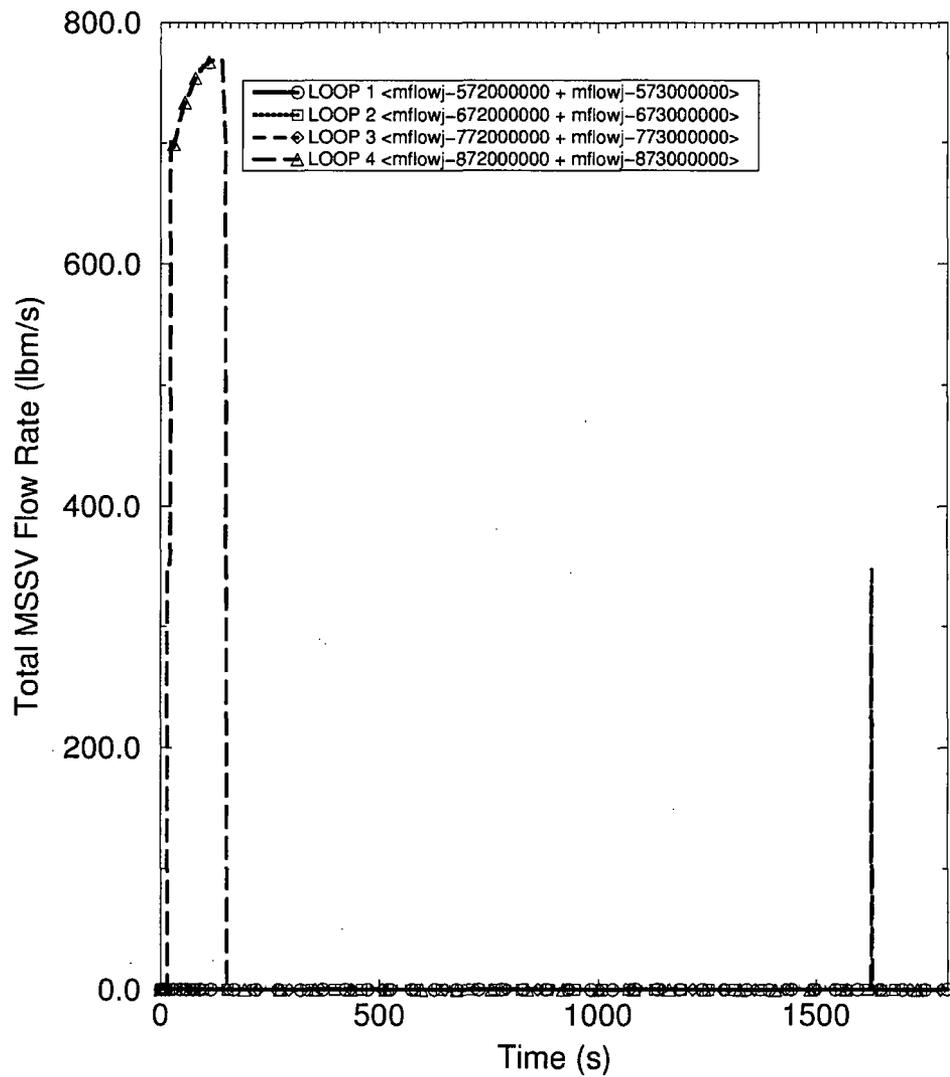
**Figure A.3.3-5—MSIVC Event:  
Steam Generator Wide Range Levels**



**Figure A.3.3-6—MSIVC Event:  
Steam Generator Narrow Range Levels**



**Figure A.3.3-7—MSIVC Event:  
MSSV Flow**



### **A.3.4     *Decrease in RCS Flow Rate***

#### **A.3.4.1    Partial Loss of Forced RCS Flow**

A partial loss of forced RCS flow is caused by an electrical or mechanical failure that causes the loss of one or more RCPs. For this event, the U.S. EPR FSAR analyzed the loss of one RCP. The results of losing two RCPs are bounded by losing a single RCP, because of the higher low-flow in two loops setpoint compared to the low-low flow in one loop setpoint. There is no single fault that could cause the loss of three RCPs.

In the U.S. EPR FSAR analysis of the loss of one RCP, PS initiates RT on low-low RCS flow in one loop. In the case of an SWCCF in the PS, the DAS RT on low-low RCS flow in one loop provides comparable protection. The setpoint for the DAS function is set slightly lower than the setpoint for the PS function, to prevent the DAS-initiated RT from occurring before the PS-initiated RT. However, for the case with an SWCCF in the PS, the nominal RT setpoints can be used as part of the best estimate assumptions. Best estimate assumptions also include more favorable power distributions. The gain in DNB margins from the use of these best estimate assumptions more than compensates for the small delay in RT due to the use of the DAS low-low flow RT setpoint, and DNB is precluded.

For the loss of two RCPs, DAS has an RT on low flow in two RCS loops that provides similar protection as PS. Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS during Partial Loss of Forced RCS Flow events.

#### **A.3.4.2    Complete Loss of Forced RCS Flow**

A complete loss of forced RCS flow is caused by a fault in the electrical power supply to the RCPs that cuts-off power to all four RCPs simultaneously.

In the U.S. EPR FSAR analysis, PS initiates RT on low RCS speed in two loops. In the case of an SWCCF in the PS, DAS initiates RT on low RCS flow in two loops, providing comparable protection. The DAS RT setpoint is set lower than the PS RT setpoint, to prevent the DAS RT from occurring before the PS RT. However, for the case with an SWCCF in the PS, the nominal setpoints for RT can be used as part of the best estimate assumptions. Best estimate

assumptions also include more favorable power distributions. Because this event is the limiting DNBR event, the complete loss of forced RCS flow event has been analyzed assuming an SWCCF in the PS, to demonstrate that adequate DNBR margin remains.

Two cases were analyzed from full power conditions; one for BOC conditions and one for EOC conditions. The results of the two calculations are nearly identical. Detailed results are presented below, for the BOC case. Figure A.3.4-1 through Figure A.3.4-10 present the response of key parameters for this event. Table A.3.4-1 presents the sequence of events. No fuel failures occur, for a complete loss of the PS functions. Any degradation in performance from a failure of the PS and reliance on the DAS is greatly offset by the best estimate conditions analyzed within the core. Long term heat removal for this event is similar to the post-RT response described in Section A.3.2.1.

The acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS for the Complete Loss of Forced RCS Flow Event.

#### **A.3.4.3 RCP Rotor Seizure or RCP Shaft Break**

The RCP Rotor Seizure and RCP Shaft Break events are PAs that result in a sudden decrease in flow in a single RCS loop. For the RCP rotor seizure event, flow in the affected loop decreases rapidly. For the RCP shaft break event, RCP inertia is reduced to that of the impeller and results in higher reverse flow in the affected loop than for rotor seizure. Because substantial reverse flow does not occur until beyond the minimum DNBR, the rotor seizure event is more limiting.

In the U.S. EPR FSAR analysis, PS initiates RT on low-low flow in one RCS loop. In the case of an SWCCF in the PS, DAS initiates RT on low-low flow in one RCS loop, providing comparable protection. The DAS RT setpoint is set slightly lower than the PS RT setpoint, to prevent the DAS trip from occurring before the PS trip. However, in the case of an SWCCF in the PS, the nominal setpoints for RT are used as part of best estimate assumptions. Best estimate assumptions also include more favorable power distributions and reactivity insertion characteristics following reactor trip. The gain in DNB margin from the use of best estimate assumptions more than offsets the delay in RT due to the use of the DAS low-low flow RT setpoint. In addition, with offsite power available, the three remaining RCPs continue to provide forced flow. Table A.3.4-2 provides a comparison between best estimate and U.

S. EPR FSAR assumptions for the Seized Rotor event. The U.S. EPR FSAR analysis is bounding for this event, and, therefore, the acceptance criteria of BTP 7-19 are met. Therefore, the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS during RCP Rotor Seizure and RCP Shaft Break events.

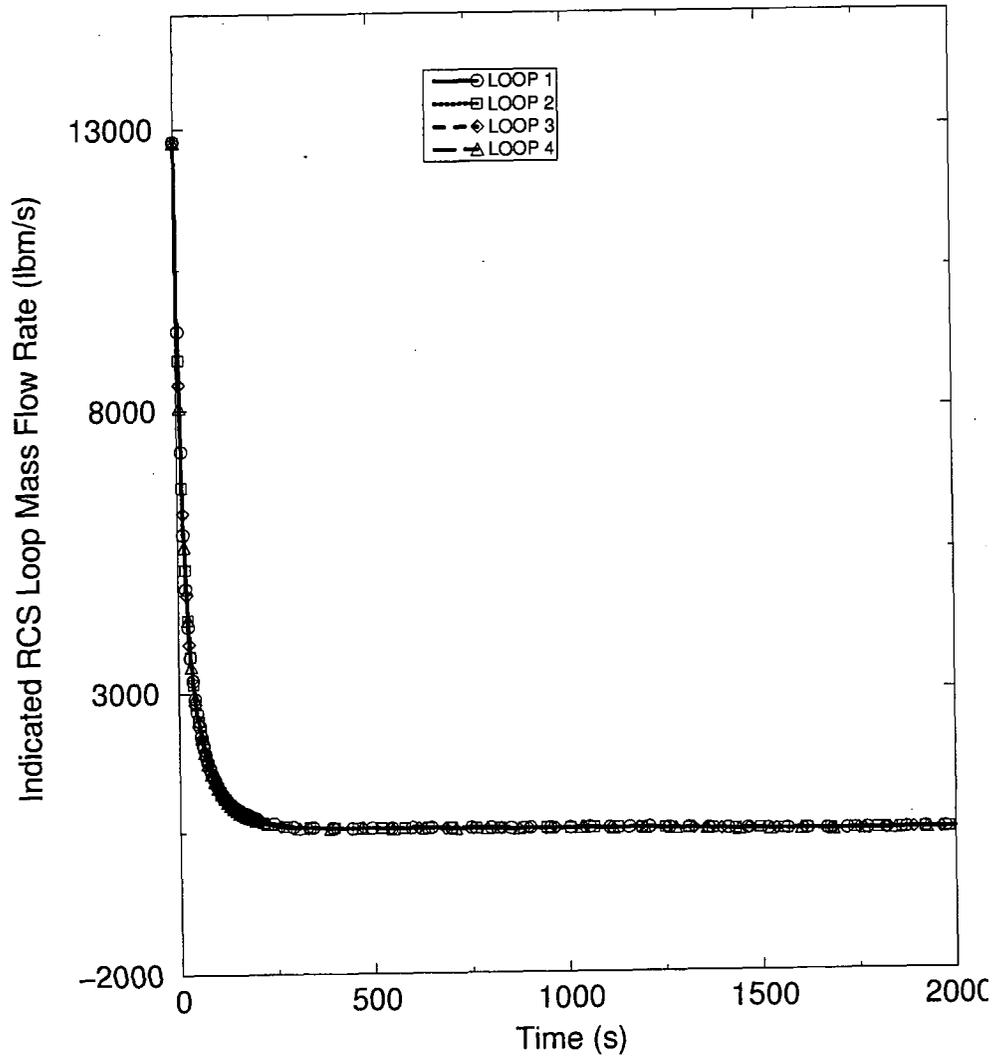
**Table A.3.4-1—Complete Loss of RCS FLOW – Sequence of Events**

<u>Event</u>	<u>Time (s)</u>
<u>Trip RCPs 1, 2, 3, 4</u>	<u>0.00</u>
<u>DAS Low RCS Loop Flow Setpoint reached</u>	<u>3.74</u>
<u>DAS Low RCS Loop Flow signal</u>	<u>4.24</u>
<u>Rods begin to drop</u>	<u>4.65</u>
<u>DNBR minimum</u>	<u>5.00</u>
<u>TT Trip</u>	<u>5.24</u>

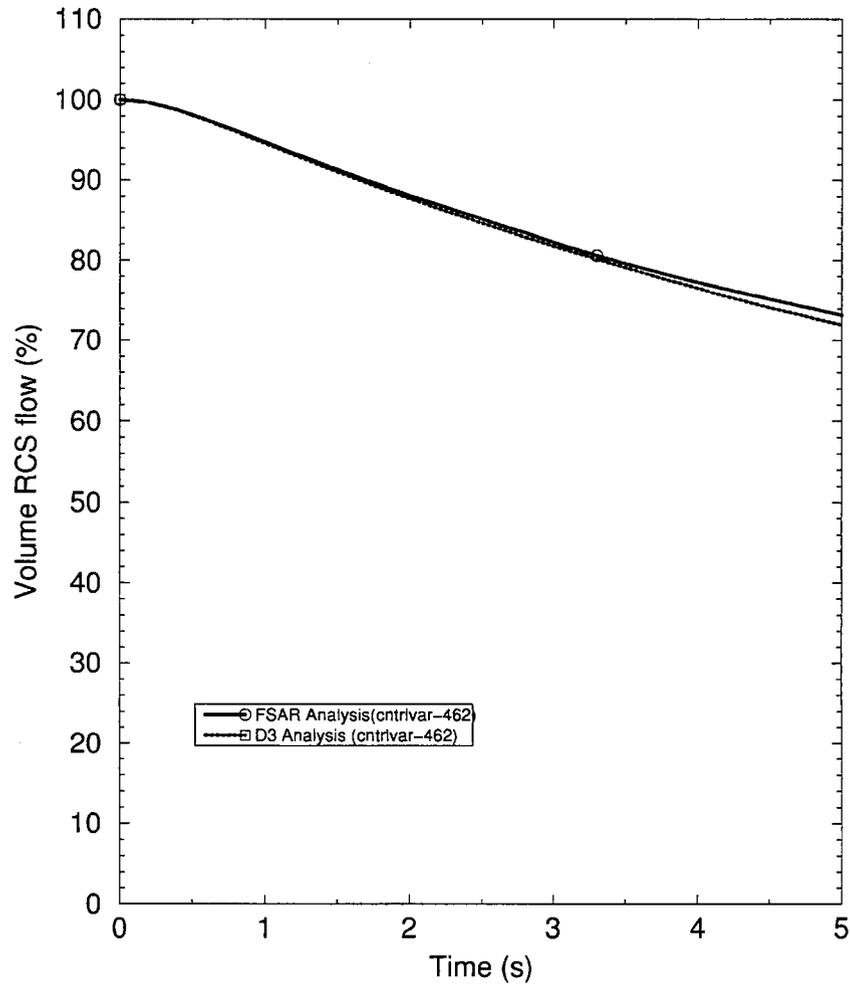
**Table A.3.4-2—D3 Rotor Seizure Event Parameters – Comparison FSAR  
Tier 2, Chapter 15 versus D3**

<u>Parameters</u>	<u>D3, DNBR Evaluation</u>	<u>FSAR Tier 2, Section 15.3.3 DNBR evaluation</u>
<u>Initial reactor power (MWt)</u>	<u>4590</u>	<u>4612</u>
<u>Average RCS temperature (°F)</u>	<u>594</u>	<u>594±4</u>
<u>Initial PZR pressure (psia)</u>	<u>2250</u>	<u>2250±50</u>
<u>Initial RCS loop flow rate (gpm)</u>	<u>124,741</u>	<u>119,692</u>
<u>Low-low flow trip setpoint (time delay)</u>	<u>44% (1.30 sec)</u>	<u>50% (1.05 sec)</u>
<u>Flow to core Inlet</u>	<u>RCPs in 3 unaffected loops continue</u>	<u>Impacted by LOOP (no RCPs available)</u>
<u>F<sub>q</sub></u>	<u>1.695 BOC 1.613 EOC</u>	<u>2.6</u>
<u>F<sub>ΔH</sub></u>	<u>1.476 BOC 1.425 EOC</u>	<u>1.70</u>
<u>Scram (pcm)</u>		
<u>BOC, HFP</u>	<u>9449 (\$14.87)</u>	<u>6161(\$10.35)</u>
<u>EOC, HFP</u>	<u>10349(\$19.63)</u>	<u>7353 (\$14.28)</u>
<u>core bypass fraction (%)</u>	<u>3.79</u>	<u>5.5</u>
<u>Initial DNBR (normalized to SAFDL)</u>	<u>2.41</u>	<u>1.30</u>

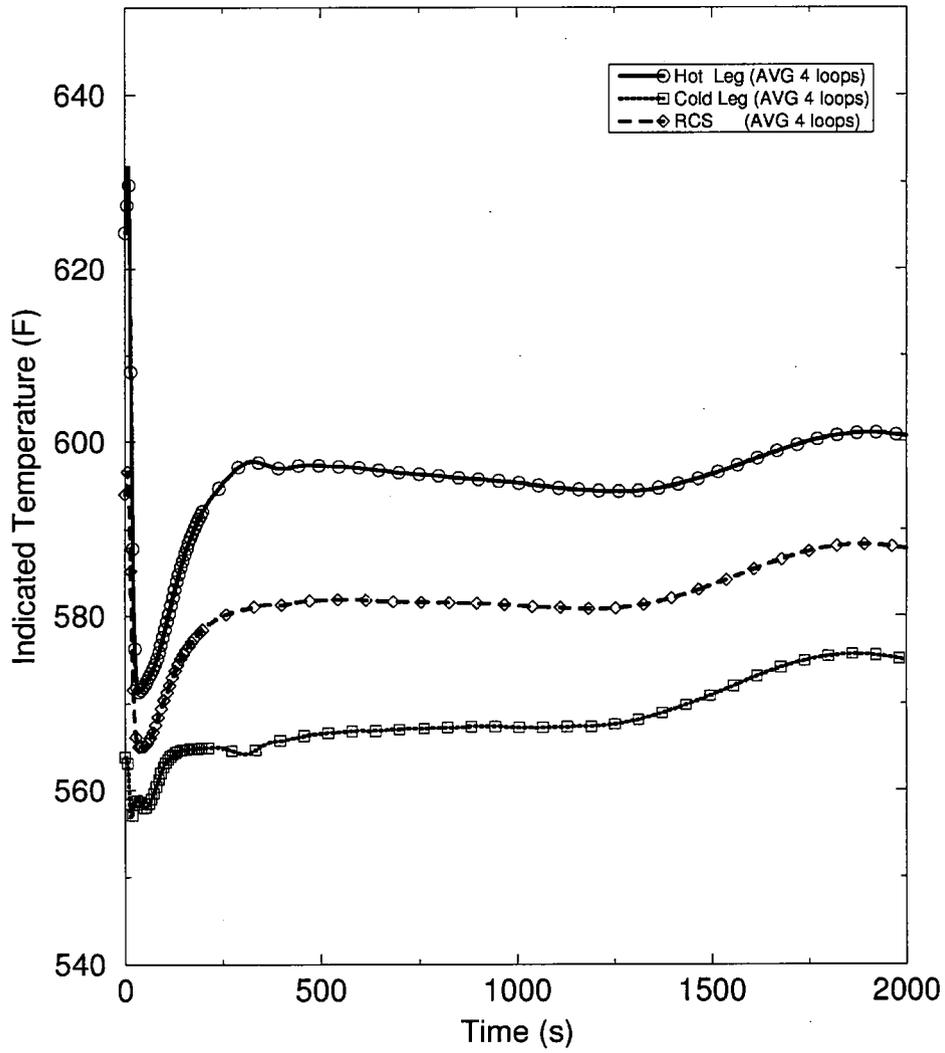
**Figure A.3.4-1—Complete Loss of Forced RCS Flow Event:  
Mass Flow Rates**



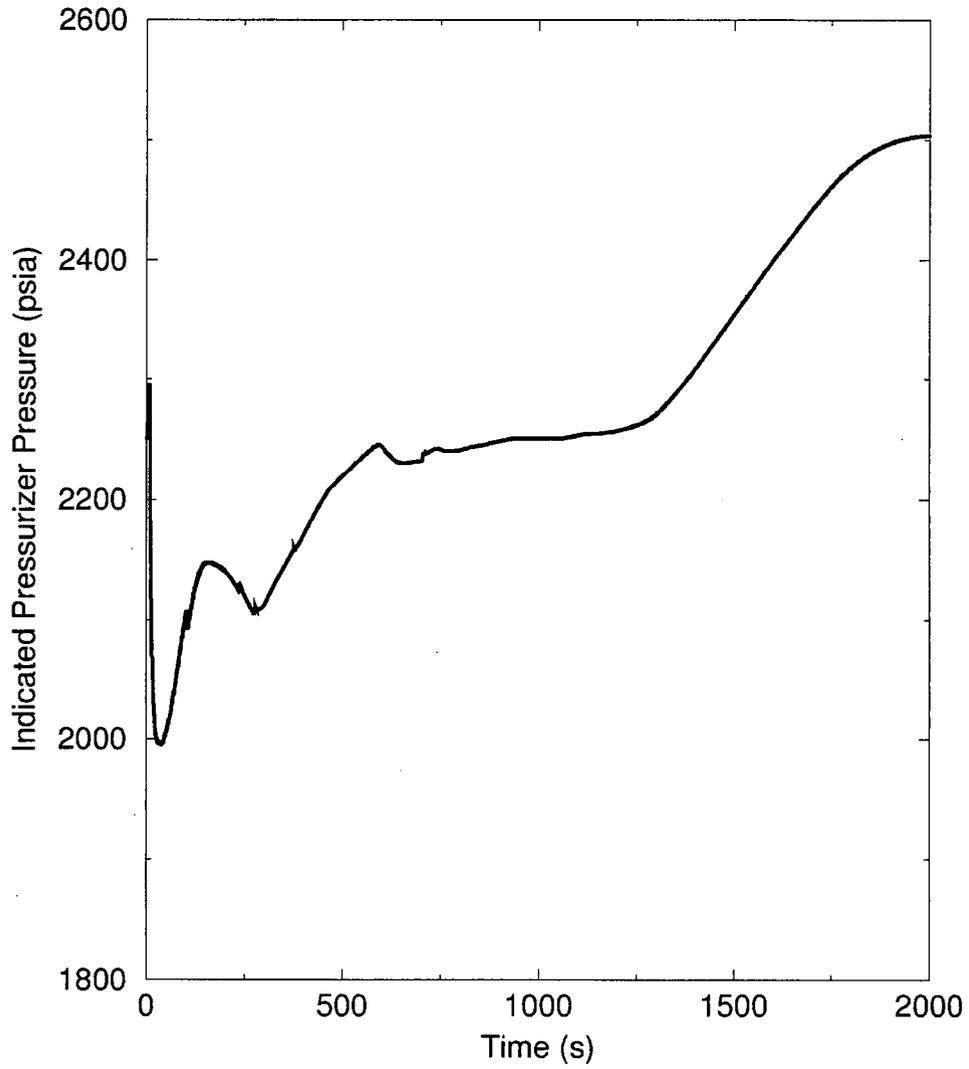
**Figure A.3.4-2—Complete Loss of RCS Flow – RCS Flow Coastdown Comparison**



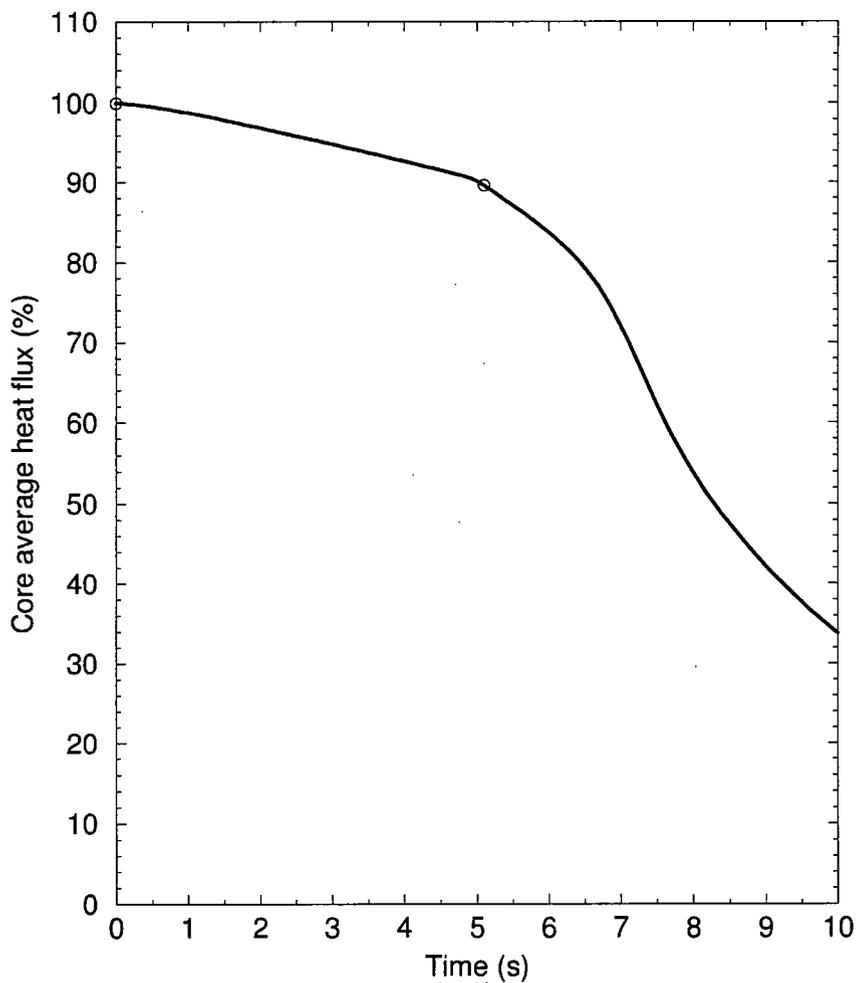
**Figure A.3.4-3—Complete Loss of Forced RCS Flow Event:  
RCS Temperatures**



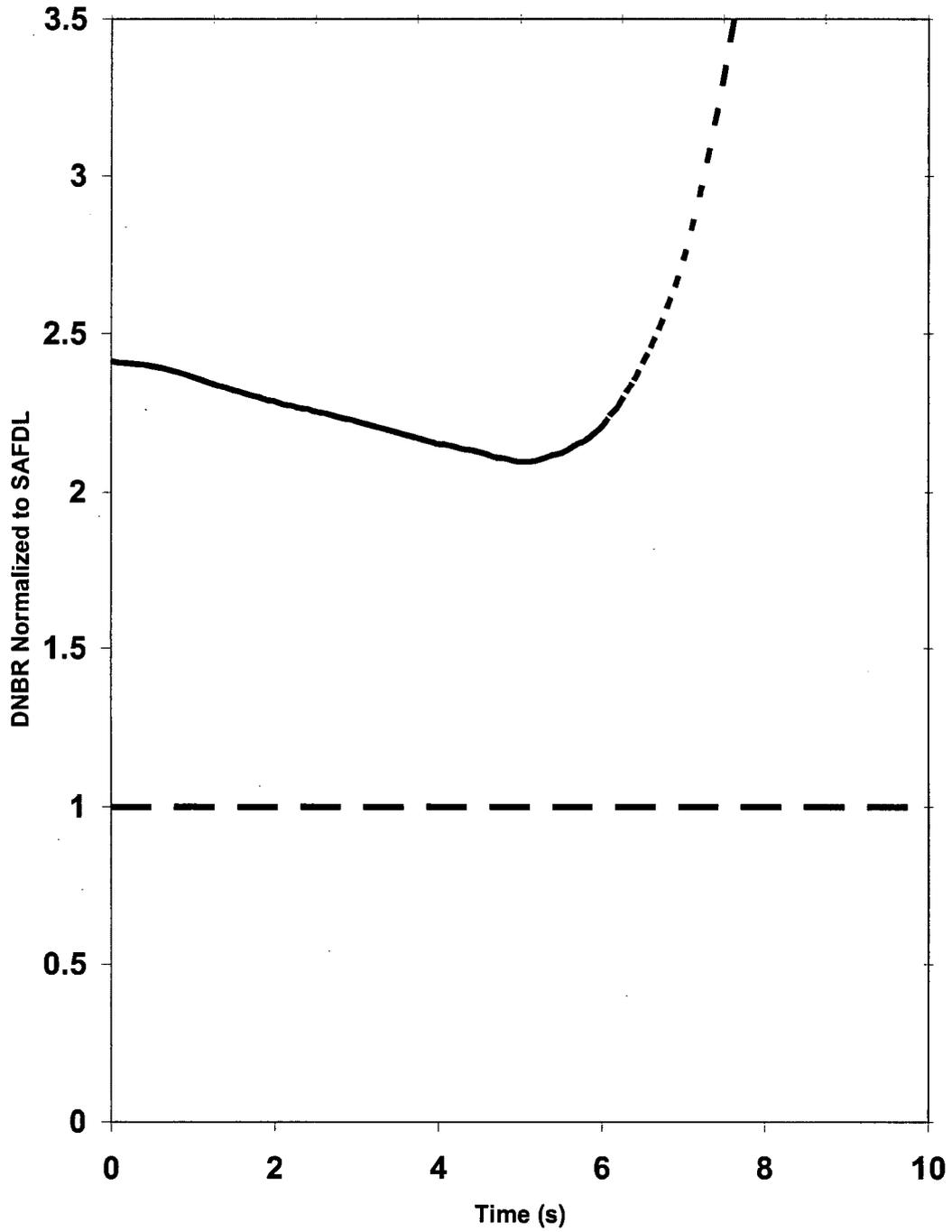
**Figure A.3.4-4—Complete Loss of Forced RCS Flow Event:  
Pressurizer Pressure**



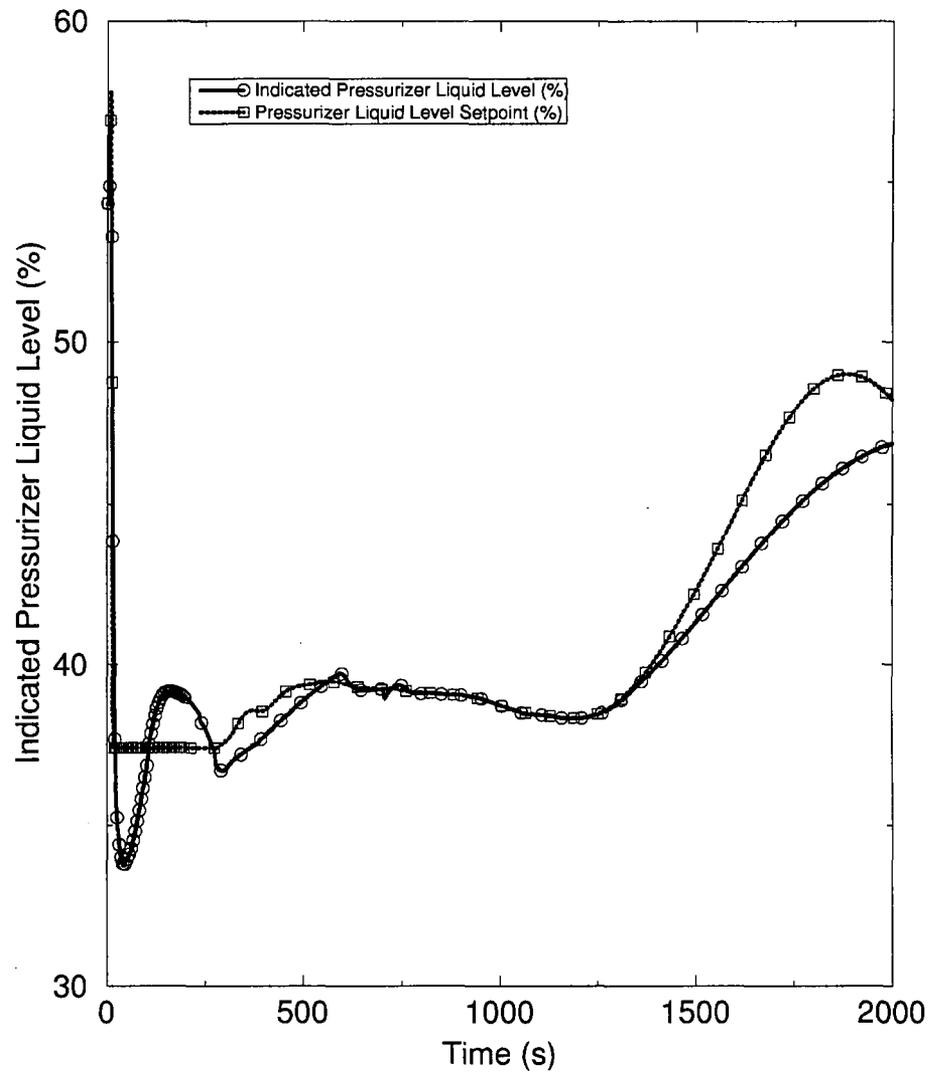
**Figure A.3.4-5—Complete Loss of Forced RCS Flow Event:  
Core Average Heat Flux**



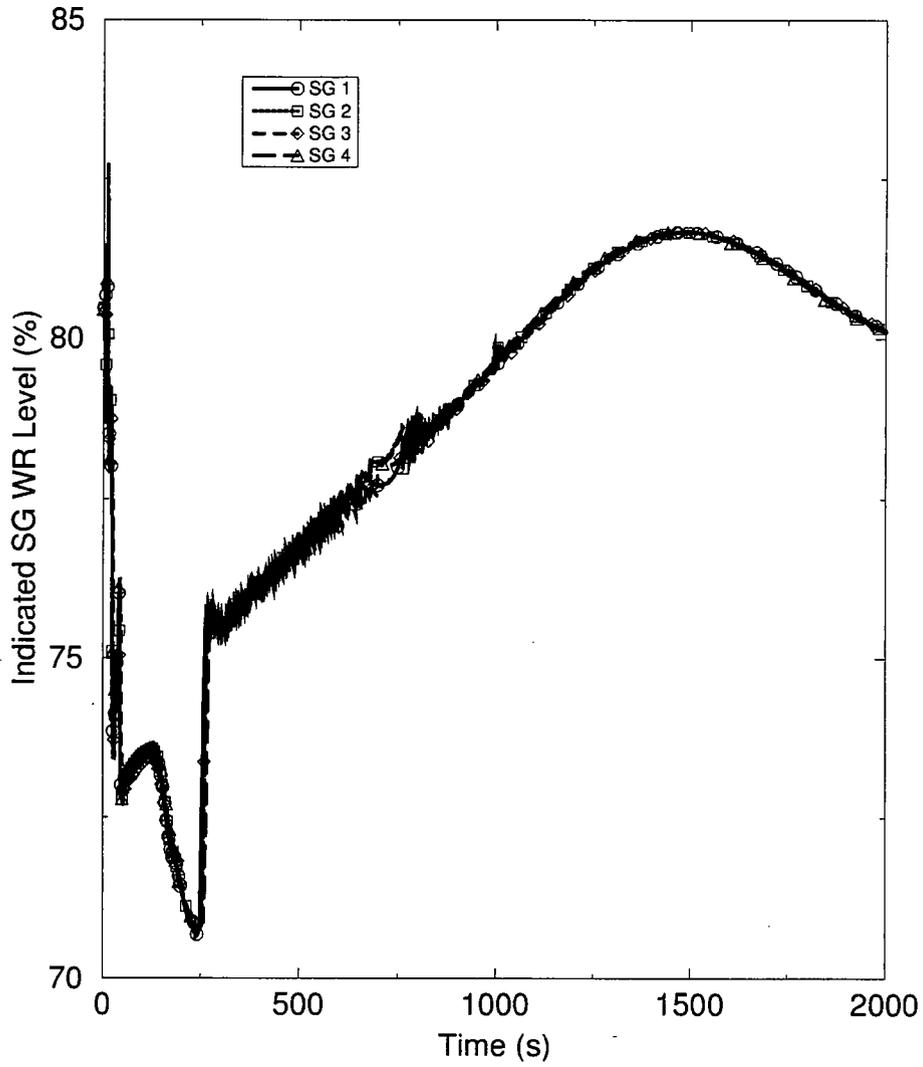
**Figure A.3.4-6—Complete Loss of RCS Flow – Plot of Minimum  
DNBR Normalized to SAFDL**



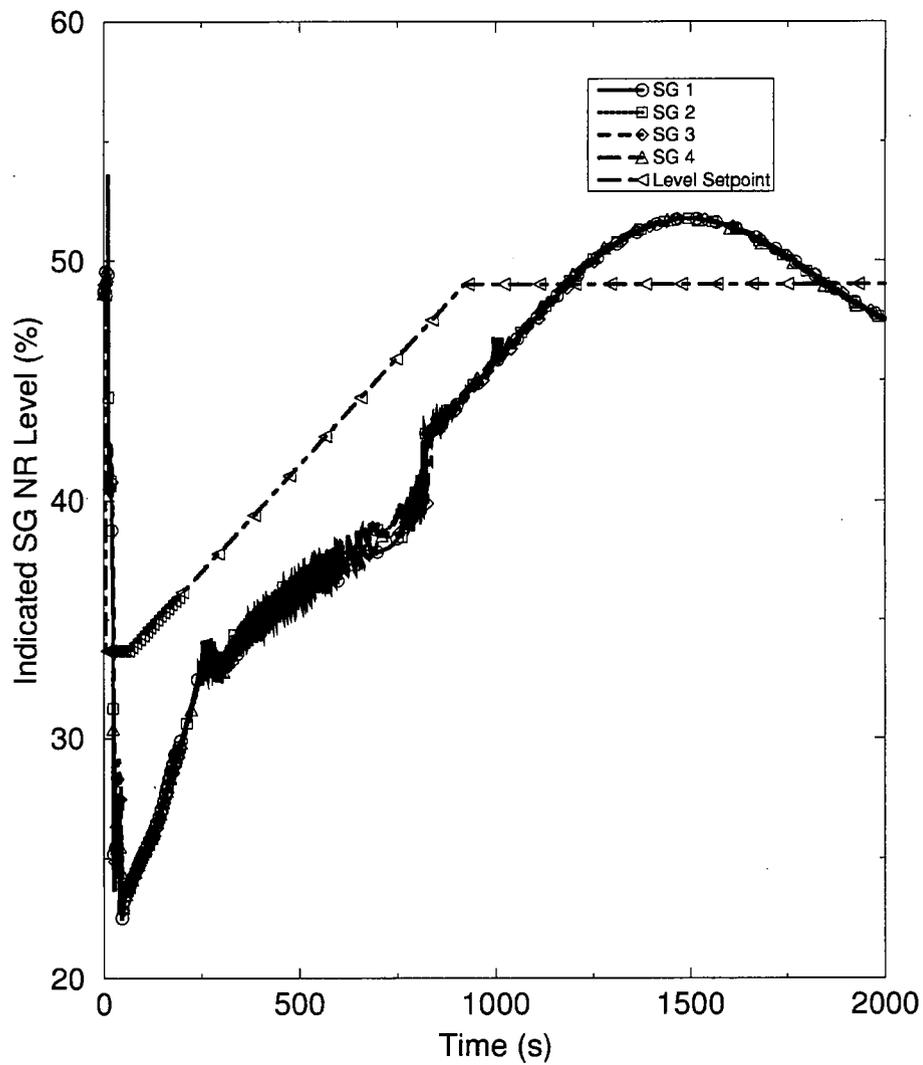
**Figure A.3.4-7—Complete Loss of Forced RCS Flow Event:  
Pressurizer Liquid Level**



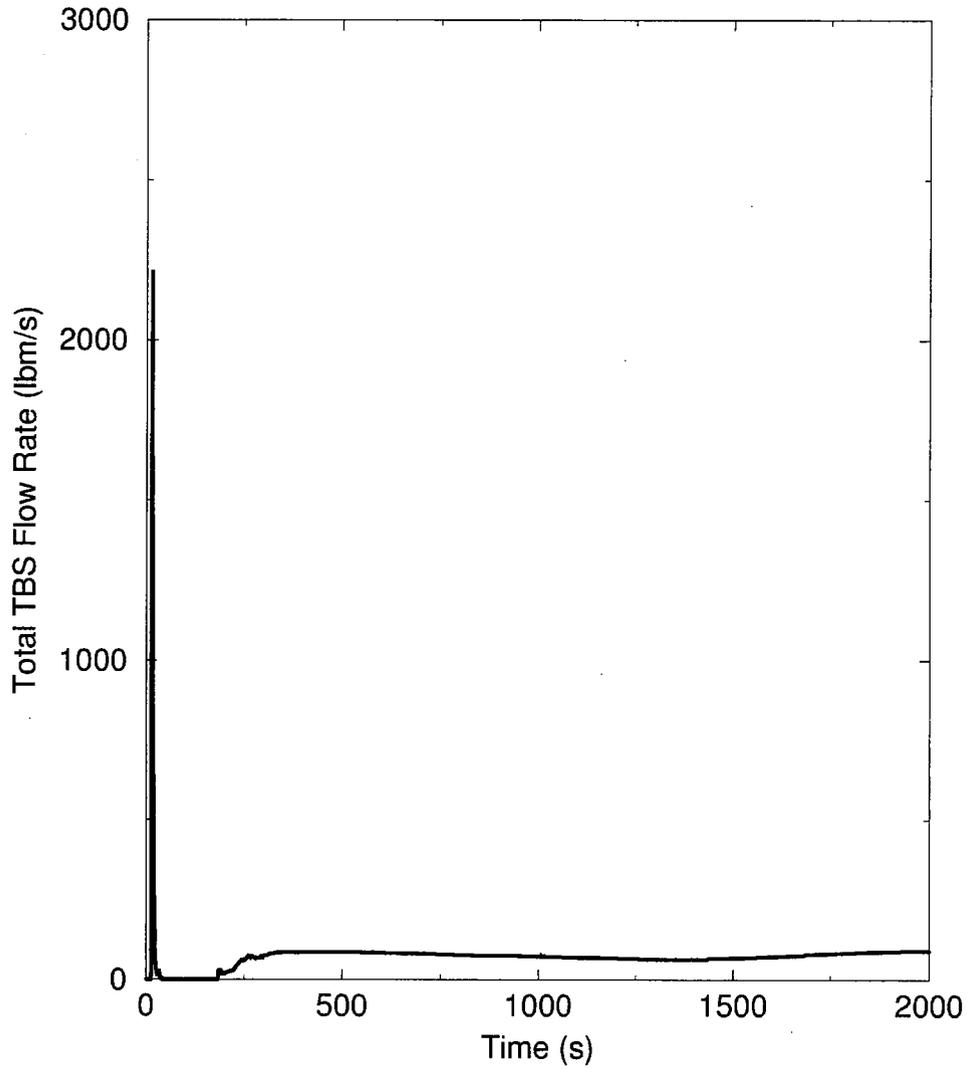
**Figure A.3.4-8—Complete Loss of Forced RCS Flow Event:  
Steam Generator Wide Range levels**



**Figure A.3.4-9—Complete Loss of Forced RCS Flow Event:  
Steam Generator Narrow Range Levels**



**Figure A.3.4-10—Complete Loss of Forced RCS Flow Event:  
Turbine Bypass Flows**



### **A.3.5     *Reactivity and Power Distribution Anomalies***

#### **A.3.5.1    Uncontrolled RCCA Withdrawal from a Subcritical or Low-Power Startup Condition**

The Uncontrolled RCCA Withdrawal from a Subcritical or Low-Power Startup Condition event is defined as the uncontrolled addition of reactivity due to the withdrawal of banks of RCCAs at hot shutdown or hot standby conditions. As discussed in Section A.2.1, in the analysis of an SWCCF in the PS, the initial condition is operation at full power with RCCAs withdrawn beyond the power-dependent insertion limit (PDIL). Therefore, this event is not relevant for SWCCF in the PS.

#### **A.3.5.2    Uncontrolled RCCA Withdrawal at Power**

The Uncontrolled RCCA Withdrawal at Power event is defined as the uncontrolled addition of reactivity due to the withdrawal of RCCAs during power operation, either due to a failure in an automatic control system or operator error.

In the U.S. EPR FSAR analysis, a spectrum of power levels is considered, including 25 percent, 60 percent, and 100 percent power. In the case of an SWCCF in the PS, only 100 percent power is considered. Furthermore, -for this event to be possible, RCCAs are conservatively assumed to be at the full power PDIL. Under normal conditions, all RCCAs are out, or the lead bank is barely inserted (i.e., at the bite position).

In the U.S. EPR FSAR analysis, PS initiates RT on high neutron flux rate of change, low DNBR, high thermal power, or high pressurizer level, depending on the initial power level, rate of reactivity insertion, and amount of reactivity feedback. In the case of an SWCCF in the PS, the only relevant DAS function is RT on excore high neutron flux. In the U.S. EPR FSAR analysis, BOC cases reached RT fairly quickly. EOC feedback cases reach RT much later, due to the greater negative reactivity feedback from the MTC, when RCS temperatures increase following the increase in core power. Slower reactivity insertion rate cases, with EOC feedbacks, stabilized at an increased core power below the RT on high thermal power setpoint, where the positive reactivity insertion of the withdrawn RCCA is balanced by the negative reactivity insertion from the MTC. In these cases, continued RCS heat-up causes pressurizer level to increase until the PS initiates RT on high pressurizer level.

Because this event has such a varied response and depends on a range of PS functions, a specific analysis is performed to demonstrate D3 adequacy in the case of an SWCCF in the PS. The analysis includes a BOC case (bank worth of 192 pcm) and an EOC case (bank worth of 363 pcm), initiated from full power from the PDIL, to test the adequacy of the DAS RT functions in limiting the power response and assess whether acceptance limits are met.

In the case of an SWCCF in the PS, the limiting RCCA withdrawal occurs from BOC conditions. At BOC, the reactivity feedback is the least negative, allowing the power and RCS temperatures to reach higher values. Figure A.3.5-1~~Figure A.3.5-1~~ through Figure A.3.5-4~~Figure A.3.5-4~~ show the response of the key parameters for this event. This transient causes an increase in core power, with a corresponding increase in RCS temperatures. The increases in RCS temperatures also lead to an increase in secondary pressure. Due to the increase in secondary side pressure, main feedwater flow decreases, eventually resulting in DAS initiating RT on low SG level followed by EFW actuation.

Reactor power peaks at 108.3 percent. No fuel failures occur during a complete loss of the PS functions. Any degradation in performance, from failure of the PS and reliance on the DAS functions, is greatly offset by the best estimate conditions analyzed within the core. The transient is simulated by an insertion of reactivity corresponding to the withdrawal of the Bank D from the PDIL to the all rods out position at the maximum RCCA extraction speed. The initial DNBR normalized to the specified acceptable fuel design limit (SAFDL) is 2.41 and the minimum DNBR normalized to the SAFDL value reached during the transient is 2.00 at 287.4 seconds. Table A.3.5-1~~Table A.3.5-1~~ provides a sequence of events for the RCCA withdrawal transient.

The acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS for the Uncontrolled RCCA Withdrawal at Power event.

### **A.3.5.3 RCCA Misoperation**

In this category, three events are analyzed in the U.S. EPR FSAR: Dropped RCCA, Statically Misaligned RCCA, and Single RCCA Withdrawal. For the Statically Misaligned RCCA event, the local peaking factors are significantly less under best estimate conditions such that fuel design limits are not challenged. In the U.S. EPR FSAR analysis, the transient analysis results

for the RCCA Bank Withdrawal event are used as the basis for the Single RCCA Withdrawal event DNBR calculations. In this D3 analysis, the Single RCCA Withdrawal event is addressed as part of the RCCA Ejection event (Section A.3.5.6). Therefore, the remainder of this section addresses only the Dropped RCCA event.

The Dropped RCCA event is initiated by de-energizing an RCCA drive mechanism or by a malfunction of a control bank. In the U.S. EPR FSAR analysis, the primary RT is the PS RT on low DNBR. In the case of an SWCCF in the PS, since DAS does not provide RT on low DNBR, RT may not occur.

Several cases are analyzed under best estimate conditions, to demonstrate that the BTP 7-19 criteria are met. These cases are selected, from among the limiting cases of the U.S. EPR FSAR analysis, for the characteristic of low worth coupled with severe radial power redistribution. Low worth limits the initial power and temperature reduction, while severe radial power redistribution maximizes local core power. High localized core power threatens core thermal limits.

The cases selected include three RCCA bank drops: (A bank of RCCAs is dropped, because the dropping of individual RCCAs under best estimate conditions has a limited perturbation on the core.)

- BOC, HFP, All RCCAs Out, dropping Bank A (435 pcm).
- EOC, HFP, PDIL, dropping Bank A (468 pcm).
- EOC, HFP, All RCCAs Out, dropping Bank C (1006 pcm).

In each of the dropped RCCA and dropped RCCA bank events, the core power distribution is perturbed leading to an increase in the magnitude of the radial power peak. Because each of these events have a similar return to full power, the DNBR performance is dominated by the increase in radial peaking that results from the drop of the RCCA or RCCAs. Table A.3.5-2 Table A.3.5-2 shows the calculated ratio of radial peaking factors for the largest single RCCA drop and for the drop of the RCCA Bank A for two times in life in two different fuel cycles. Comparing the ratio of radial ( $F_{\Delta H}$ ) augmentation factors shows that the peaking factors for the RCCA bank drop are consistently larger. While the larger magnitudes of negative reactivity insertion from the RCCA bank drop cases lead to larger decreases in core inlet temperature

than single RCCA drop cases, the impact on DNBR performance is small when compared to the increase in the radial power peak.

The limiting case involves returning to full power without a reactor trip. It corresponds to the drop of Bank A at EOC from the PDIL at full power. In this case, the analysis assumes RCSL is automatically controlling the RCCAs, which ~~worsens the results in a more severe power transient.~~ The rod cluster control assembly (RCCA) bank drop events are characterized by an initial decrease in reactor coolant system (RCS) temperature. The average coolant temperature (ACT) function in the reactor control, surveillance and limitation (RCSL) system will withdraw the controlling RCCA bank to restore nominal RCS temperature. For the limiting case, the drop of Bank A at end of cycle (EOC) conditions initialized with the controlling RCCA bank at the power-dependent insertion limit (PDIL), the RCSL system will automatically initiate a withdrawal of the controlling RCCA bank in order to restore RCS temperature. Following the initial decrease in core power, a return to power occurs, and the associated overshoot causes the maximum power level reached to be 102 percent.

~~Figure A.3.5-5~~Figure A.3.5-5 through Figure A.3.5-8~~Figure A.3.5-8~~ illustrate the response of key parameters for this event. No fuel failures occur, with a complete loss of the PS functions. Any degradation in performance from a failure of the PS is greatly offset by the best estimate conditions analyzed within the core. The limiting case of RCCA drop is the insertion of 468 pcm at EOC from PDIL without a reactor trip (RT). The initial departure from nucleate boiling ratio (DNBR) normalized to the specified acceptable fuel design limit (SAFDL) is 2.66, and the minimum DNBR normalized to SAFDL is 1.63. The improvement in the initial DNBR margin resulting from the use of best-estimate conditions is shown by comparing the 2.66 initial DNBR normalized to the SAFDL value for the D3 analysis to the 1.38 initial DNBR normalized to the SAFDL value for U.S. EPR FSAR Tier 2, Chapter 15.

The acceptance criteria for BTP 7-19 are met and the U.S. EPR is determined to be adequate in addressing an SWCCF in the PS during a Dropped RCCA event.

#### **A.3.5.4 Startup of an Inactive RCP at an Incorrect Temperature**

The Startup of an Inactive RCP at an Incorrect Temperature event was analyzed to cover the condition where the plant has undergone a partial scram due to the coastdown of one RCP.

This reduces reactor power to approximately 50 percent. The U.S. EPR technical specifications require idle RCP restart within a specified time.

In the U.S. EPR FSAR analysis of this event, RT conditions are not reached. Core power stabilizes at a level near the initial power level. In the case of an SWCCF in the PS, no DAS functions are required. Therefore, the U.S. EPR is determined to be adequate for this event.

#### **A.3.5.5 CVCS Malfunction Resulting in Decreased RCS Boron Concentration**

An Inadvertent Boron Dilution of the RCS event can result from an operator error or malfunction of the reactor boron and water make-up system (RBWMS). The U.S. EPR FSAR analyzes boron dilution events, in Modes 1 through 6, and credits the operation of the anti-dilution mitigation (ADM) system. The ADM system senses boron concentration in the CVCS charging line and isolates CVCS when a setpoint is reached. The predetermined setpoint is selected to prevent an inadvertent criticality in shutdown modes, and a loss of shutdown margin during power operation.

In the case of an SWCCF in the PS, the D3 analysis assumes the ADM system unavailable to isolate the dilution flow path. Under full power conditions, the reactivity insertion from the dilution and the minimum DNBR for this event are bounded by the Uncontrolled RCCA Withdrawal at Power event (Section A.3.5.2). In addition to the potential challenge to DNBR limits, continuous dilution of RCS boron can erode shutdown margin to the point that, upon RT, the inserted RCCAs fail to take the reactor subcritical.

If dilution occurs at power, the severity of the plant response depends on whether RCCA control is automatic (RCSL) or manual. To provide reasonable assurance that the limiting case is captured, both scenarios are examined.

If automatic (partial failure of PS), RCSL begins to insert RCCAs to maintain  $T_{avg}$  and core power. RCCA insertion alerts the operator that boron dilution is occurring.

If the RCCA control is manual, continuous boron dilution slowly increases reactor power and  $T_{avg}$ . These increases result in a slow increase in ~~steam generator~~SG pressure. The feedwater control system responds to increasing ~~steam generator~~SG pressure by opening feedwater control valves until they are fully open. Further increases in ~~steam generator~~SG pressure result

in a decrease in feedwater flow along the feedwater pump curve. Decreasing feedwater flow results in a decrease in SG level and, eventually, DAS initiates RT on low SG level (within about 5 minutes of the initiating event.) The action of the feedwater control system, and the eventual reactor trip, alert the operator that boron dilution is occurring. ~~Figure A.3.5-9~~ ~~Figure A.3.5-9~~ through ~~Figure A.3.5-13~~ ~~Figure A.3.5-13~~ provide the response of the key parameters to boron dilution at BOC and full power conditions, with manual RCCA control.

Under best estimate conditions, crediting the worth of inserted RCCAs post RT, it takes approximately four hours of continuous dilution at the maximum rate to erode the available shutdown margin. Therefore, from the above discussion, sufficient time is available for the operator to detect and terminate a dilution of the RCS and prevent a return to criticality. Manual CVCS isolation is through PAS and is not dependent on the PS. Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for an Inadvertent Boron Dilution of the RCS event.

#### **A.3.5.6 RCCA Ejection**

This event is defined as a rupture of an RCCA drive mechanism that results in the complete ejection of its RCCA from the core. In the U.S. EPR FSAR, the analysis is divided into RCS overpressurization and core protection (MDNBR and deposited enthalpy). The overpressurization part of the analysis is performed with the S-RELAP5 method used for the other U.S. EPR FSAR transient analyses. The core protection part of the analysis is performed with a newly developed RCCA ejection analysis methodology used in the U.S. EPR FSAR analysis.

The U.S. EPR FSAR analysis considers a spectrum of RCCA worths and initial reactor power levels. In the case of an SWCCF in the PS, only cases initiated from rated power conditions are considered (Section A.2.1). This event is analyzed to estimate the core response under best estimate assumptions and to determine the D3 adequacy of the DAS RT functions.

The limiting case occurs from BOC conditions, where Doppler feedback is the least. The analysis assumes an ejected RCCA worth of 65 pcm. Three cases are analyzed, to determine the response of the plant and core:

- No Rupture.

- Half Rupture (0.025 ft<sup>2</sup>).
- Full Rupture (0.048 ft<sup>2</sup>).

The No-Rupture case also serves to address the Single RCCA Withdrawal event (Section A.3.5.3). The three sizes provide a spectrum of possible coolant leakage path sizes if the control drive were to be ejected from the reactor by the pressure driving head from a flange break. This also allows consideration of the impact of the depressurization of the reactor coolant system (RCS) on the departure from nucleate boiling ratio (DNBR) performance.

Each of the events is initialized to the same operating conditions and each "ejects" a control rod with a worth of 65 pcm by adding the equivalent point kinetic worth in dollars (1\$ = 1 beta, or delayed neutron fraction) over a timeframe of 0.05 second to simulate the withdrawal from the hot full power (HFP) dependent insertion limit (~50 percent inserted)

The three-dimensional (3D) transient power shapes were determined for the fuel assembly of interest from a rod ejection calculation with the three-dimensional nodal kinetics code NEMO-K using constant inlet thermal hydraulic conditions. This captured the initial power shape redistribution in the assembly of interest, following the methods of U.S. EPR Control Rod Ejection Accident Methodology Topical Report, ANP-10286P. The total core power histories were determined from the point kinetics S-RELAP5 model. These accounted for the reactivity feedback effects from the depressurization and heatup of the RCS occurring after the addition of reactivity from the ejected control rod. The inputs to the LYNXT DNBR calculation were a combination of the transient 3D power shapes in the form of peaking factors and the total core power, mass flux, RCS pressure, and inlet temperature in the form of histories normalized to the initial conditions.

The core power response for the transient core thermal hydraulic boundary condition is determined from S-RELAP5 point kinetics model. The radial and axial power distributions are obtained from a 3-D transient neutronics calculation. Figure A.3.5-14~~Figure A.3.5-14~~ through Figure A.3.5-17~~Figure A.3.5-17~~ provide the response of key system parameters from S-RELAP for the zero break case. The minimum DNBR during the rod ejection does not violate the Specified Acceptable Fuel Design Limit (SAFDL). Simulations up to 1800 seconds do not produce a DAS RT. However, a RT is not required as the SAFDL is not violated.

For the break cases, a RT occurs from the DAS function low hot leg pressure after the MDNBR decreases below the SAFDL threshold. The post-trip response for the rupture cases behaves similarly to the small break LOCA (Section A.3.7.3.2). Fuel failures due to violation of the DNBR are predicted to be far lower than the 30 percent limit described in U.S. EPR FSAR Tier 2, Section 15.4. Table A.3.5-3~~Table A.3.5-3~~ provides a summary of results for the core performance for each case. All results are well within the U.S. EPR FSAR acceptance criteria. Therefore, the DAS functions adequately protect the core when the PS is lost during a HFP ejected rod accident. The results for the zero break case also show no fuel failures due to DNBR and, thus, means there are no fuel failures for the single rod withdrawal event. Table A.3.5-4~~Table A.3.5-4~~ through Table A.3.5-6~~Table A.3.5-6~~ provides sequence of events for each case.

The acceptance criteria for BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for an RCCA Ejection event and a Single RCCA Withdrawal event.

**Table A.3.5-1—RCCA Withdrawal at Power – Sequence of Events**

<u>Event</u>	<u>Time (sec)</u>
<u>Bank D Withdrawal from PDIL beginning</u>	<u>0.0</u>
<u>Bank D withdrawal from PDIL end</u>	<u>72.0</u>
<u>DAS low SG level delay (RT signal)</u>	<u>290.1</u>
<u>DAS RT with delay (rod release for scram)</u>	<u>290.5</u>
<u>Minimum DNBR</u>	<u>288.0</u>
<u>DAS turbine trip (TT) with delay</u>	<u>291.1</u>

**Table A.3.5-2—Radial Power Peaking Factors (FDH) for Single RCCA Drop and RCCA Bank A Drop**

<u>Condition</u>	<u>Ratio of Single RCCA Maximum F<math>\Delta</math>H Augmentation to RCCA Bank A F<math>\Delta</math>H Augmentation</u>
<u>Cycle 1 BOC PDIL</u>	<u>0.87</u>
<u>Cycle 1 EOC PDIL</u>	<u>0.88</u>
<u>Equilibrium Cycle BOC PDIL</u>	<u>0.91</u>
<u>Equilibrium Cycle EOC PDIL</u>	<u>0.94</u>

**Table A.3.5-3—RCCA Ejection Event: Core Performance Results**

Case	MDNBR/ SAFDL normalized	Max Fuel Temp (°F)	Max Cladding Temp (°F)	Peak RCCA Average Enthalpy (cal/gm)	Fuel Failures due to DNBR
U.S. EPR FSAR Failure/ Acceptance Criteria	1.00	< rim melt	< ballooning failure temperature	< 150	< 30%
No Break	1.198	2992.6	751.6	69.59	0%
Half Break	0.862	2976.8	1171.5	78.90	0.21%
Full Break	0.864	2944.0	1154.7	76.44	0.29%

Fuel rim melt temperature provided in Section 7.3 of Reference A-4.

Clad ballooning failure temperature provided in Section 2.2 of Reference A-4.

**Table A.3.5-4—Sequence of Events for Rod Ejection for Case with No Break**

<u>Event</u>	<u>Parameter</u>	<u>Time (sec)</u>
Peak core power reached	110.7%	0.066
High core power level delay (protection system (PS) reactor trip (RT) not active)	Trip 455	6.8
Minimum MDNBR/SAFDL reached	1.198	159
Transient terminated (without diverse actuation system (DAS) RT)		1800.0

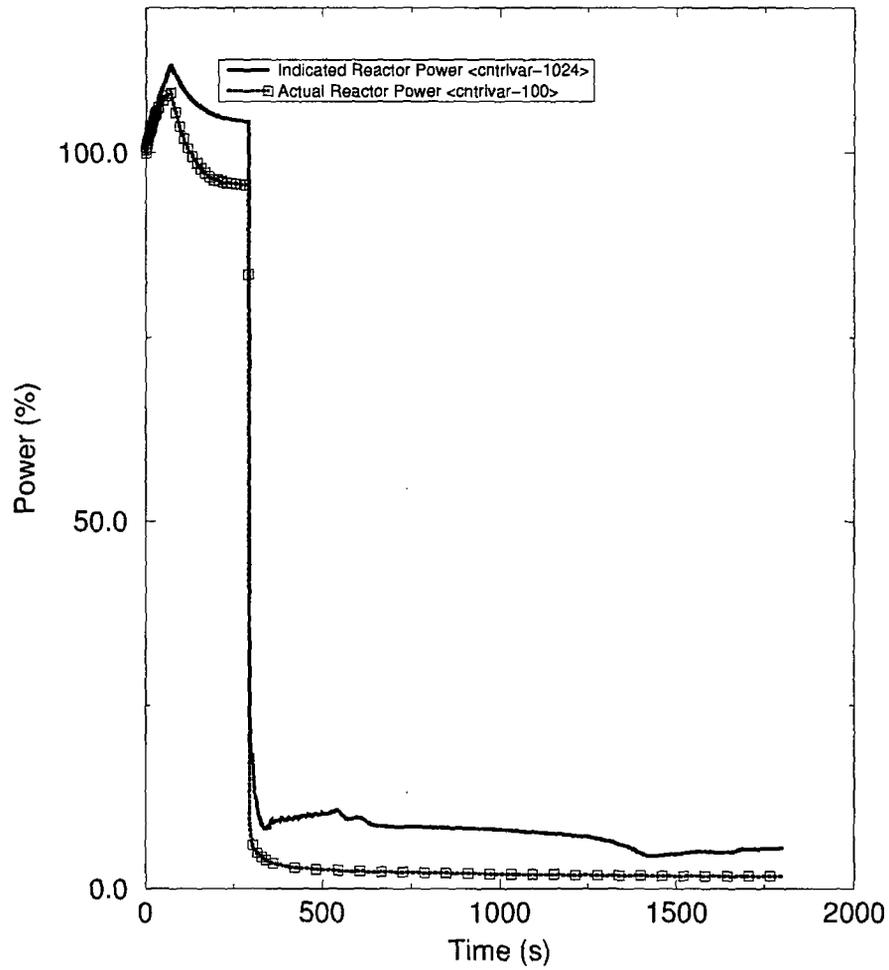
**Table A.3.5-5—Sequence of Events for Rod Ejection for Case with  
0.025 ft<sup>2</sup> Break**

<u>Event</u>	<u>Parameter</u>	<u>Time (sec)</u>
<u>Peak core power reached</u>	<u>110.7%</u>	<u>0.066</u>
<u>High core power level delay (PS RT not active)</u>	<u>Trip 455</u>	<u>7.2</u>
<u>MDNBR/SAFDL limit reached</u>	<u>1.000</u>	<u>29.0</u>
<u>Low hot leg saturation margin delay (PS RT not active)</u>	<u>Trip 460</u>	<u>29.5</u>
<u>Low PZR pressure delay (PS RT not active)</u>	<u>Trip 15</u>	<u>55.8</u>
<u>Low hot leg pressure delay (PS RT not active)</u>	<u>Trip 5</u>	<u>57.8</u>
<u>Minimum MDNBR/SAFDL reached</u>	<u>0.862</u>	<u>69.0</u>
<u>DAS low hot leg pressure delay</u>	<u>Trip 88</u>	<u>69.1</u>
<u>DAS RT with delay</u>	<u>Trip 900</u>	<u>69.5</u>
<u>DAS turbine trip (TT) with delay</u>	<u>Trip 899</u>	<u>70.1</u>
<u>Transient terminated</u>		<u>1281.6</u>

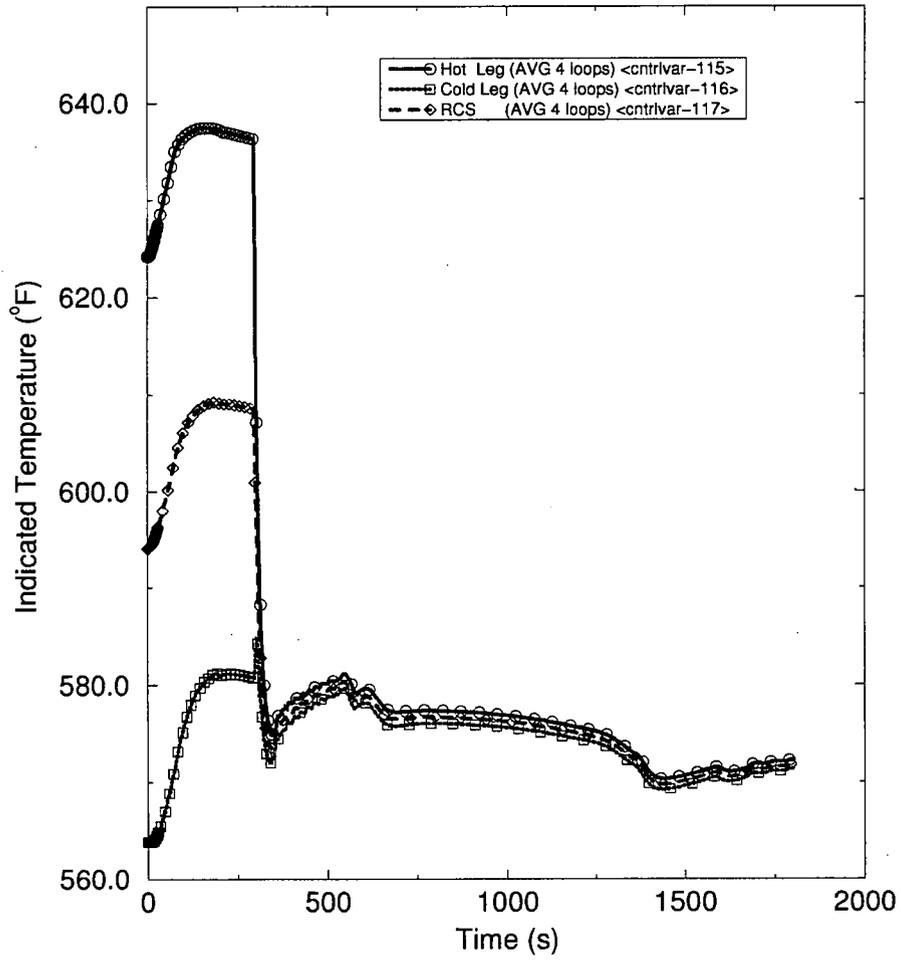
**Table A.3.5-6—Sequence of Events for Rod Ejection for Case with  
0.048 ft<sup>2</sup> Break**

<u>Event</u>	<u>Parameter</u>	<u>Time (sec)</u>
<u>Peak core power reached</u>	<u>110.7%</u>	<u>0.072</u>
<u>High core power level delay (PS RT not active)</u>	<u>Trip 455</u>	<u>8.8</u>
<u>MDNBR/SAFDL limit reached</u>	<u>1.000</u>	<u>14.5</u>
<u>Low hot leg saturation margin delay (PS RT not active)</u>	<u>Trip 460</u>	<u>15.1</u>
<u>Low PZR pressure delay (PS RT not active)</u>	<u>Trip 15</u>	<u>28.2</u>
<u>Low hot leg pressure delay (PS RT not active)</u>	<u>Trip 59</u>	<u>28.8</u>
<u>DAS low hot leg pressure delay</u>	<u>Trip 88</u>	<u>34.8</u>
<u>Minimum MDNBR/SAFDL reached</u>	<u>0.864</u>	<u>35.0</u>
<u>DAS RT with delay</u>	<u>Trip 900</u>	<u>35.2</u>
<u>DAS TT with delay</u>	<u>Trip 899</u>	<u>35.8</u>
<u>Safety injection system (SIS) by PS or by DAS</u>	<u>Trip 1058</u>	<u>58.1</u>
<u>Transient terminated</u>		<u>195.1</u>

**Figure A.3.5-1—Uncontrolled RCCA Withdrawal at Power Event:  
Indicated and Actual Reactor Power**

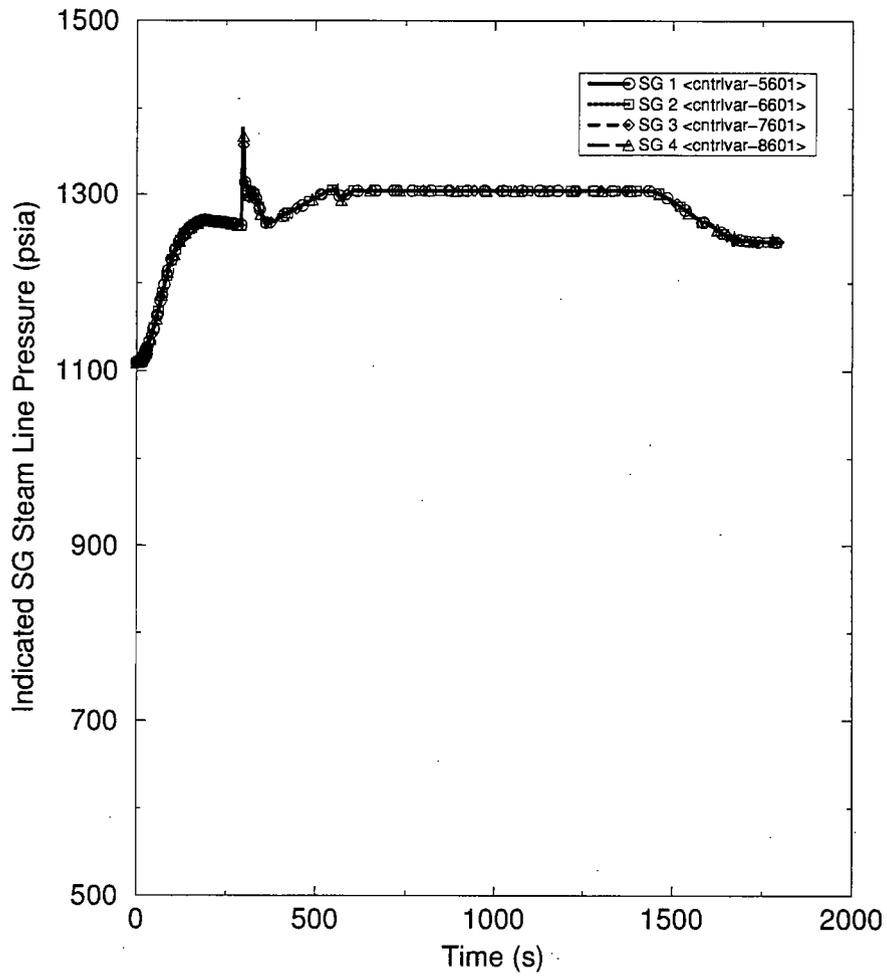


**Figure A.3.5-2—Uncontrolled RCCA Withdrawal at Power Event:  
RCS Temperatures**

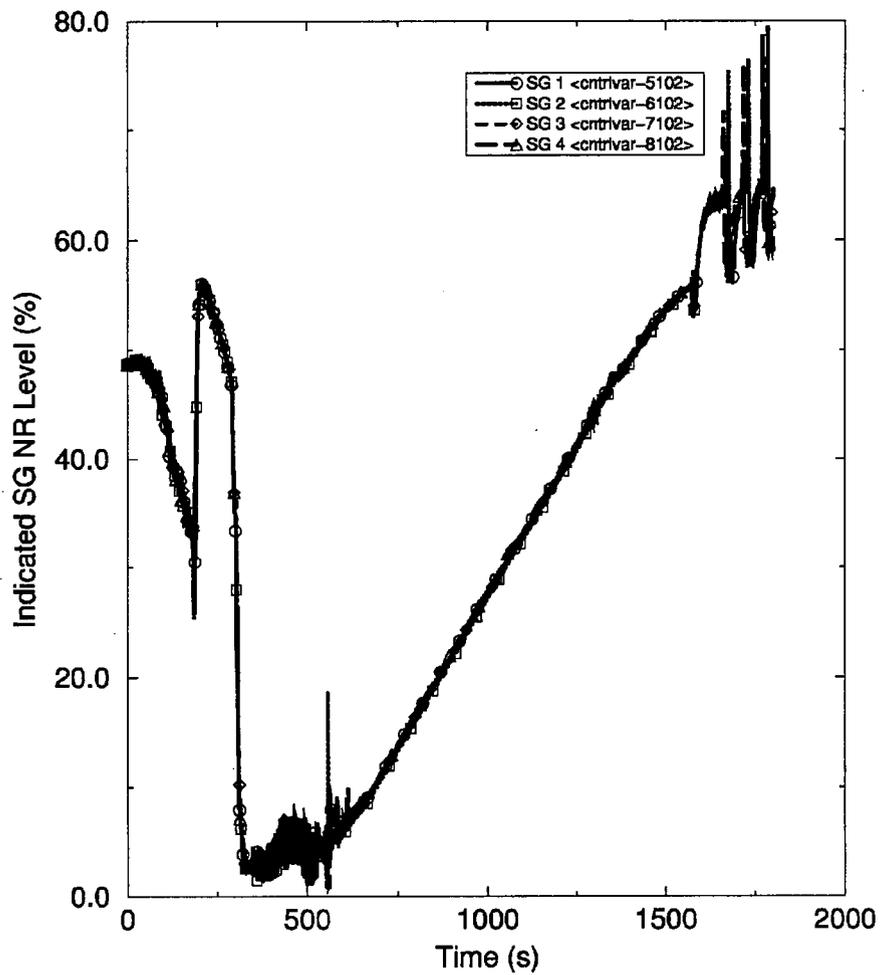


ID:06188 3Nov2009 13:20:03 UCBW\_hfp\_boc.dmx

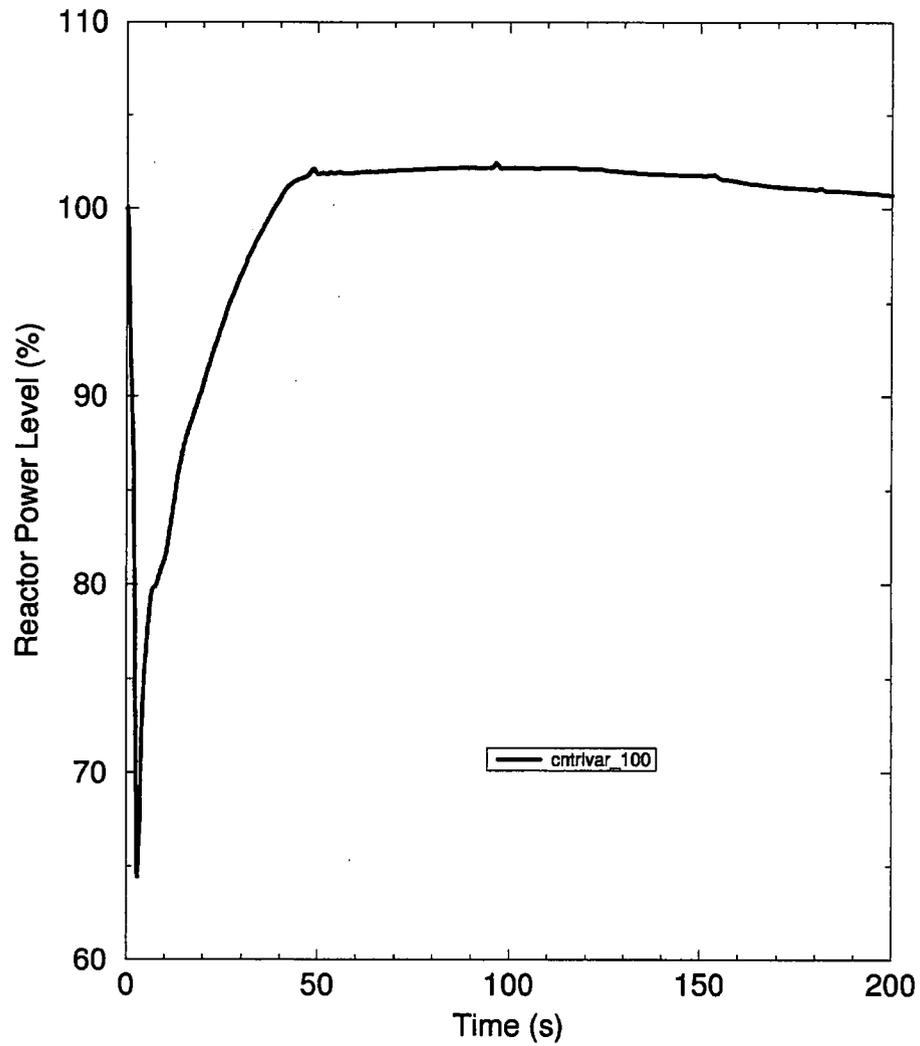
**Figure A.3.5-3—Uncontrolled RCCA Withdrawal at Power Event:  
Steam line Pressure**



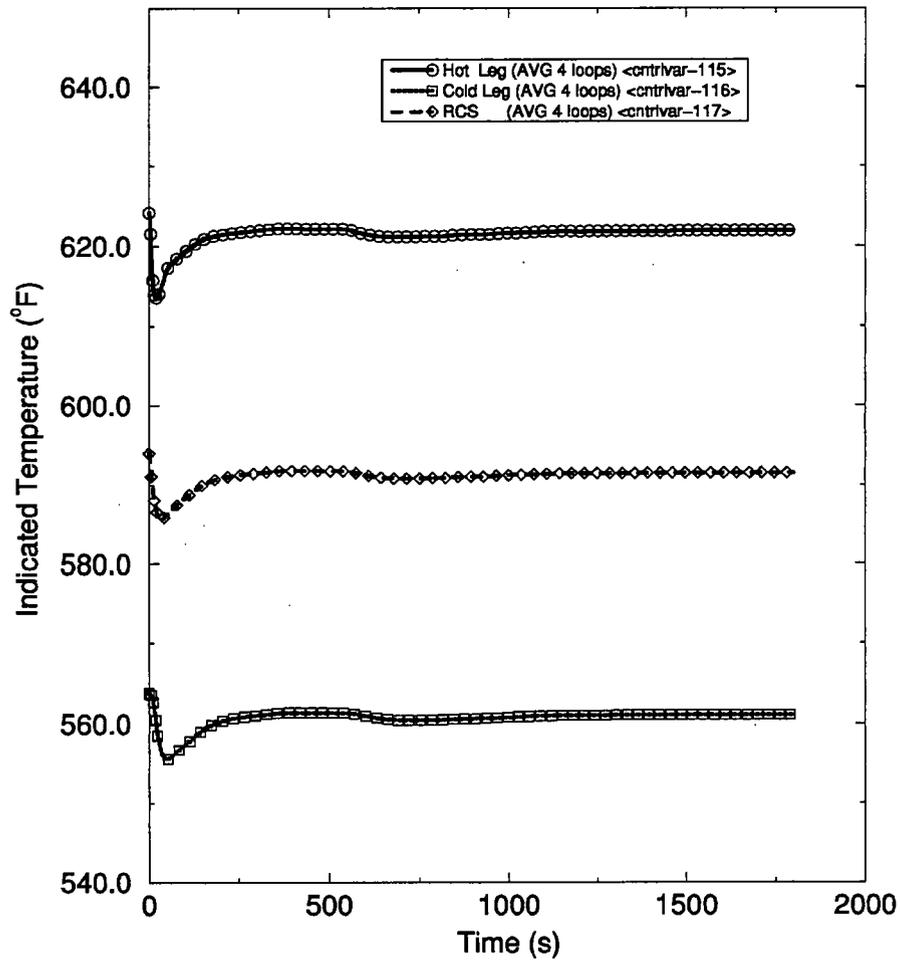
**Figure A.3.5-4—Uncontrolled RCCA Withdrawal at Power Event:  
Steam Generator Narrow range Level**



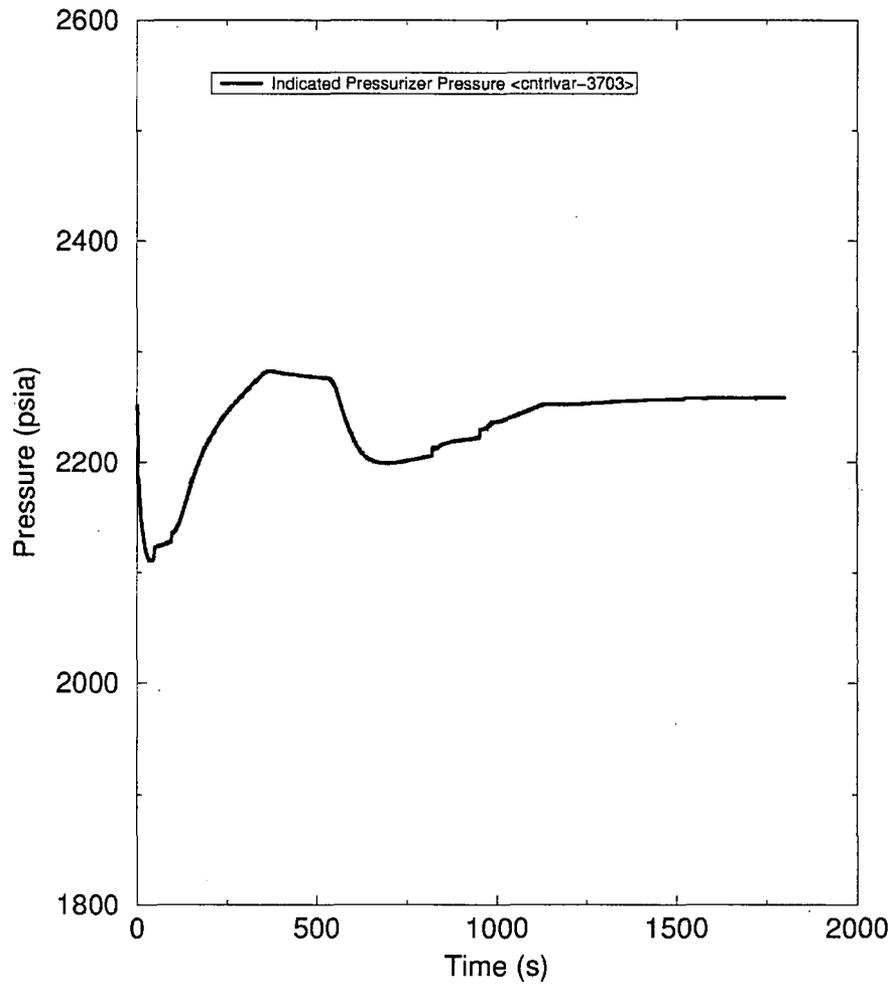
**Figure A.3.5-5—Bank A Drop at EOC Event:  
Indicated Reactor power**



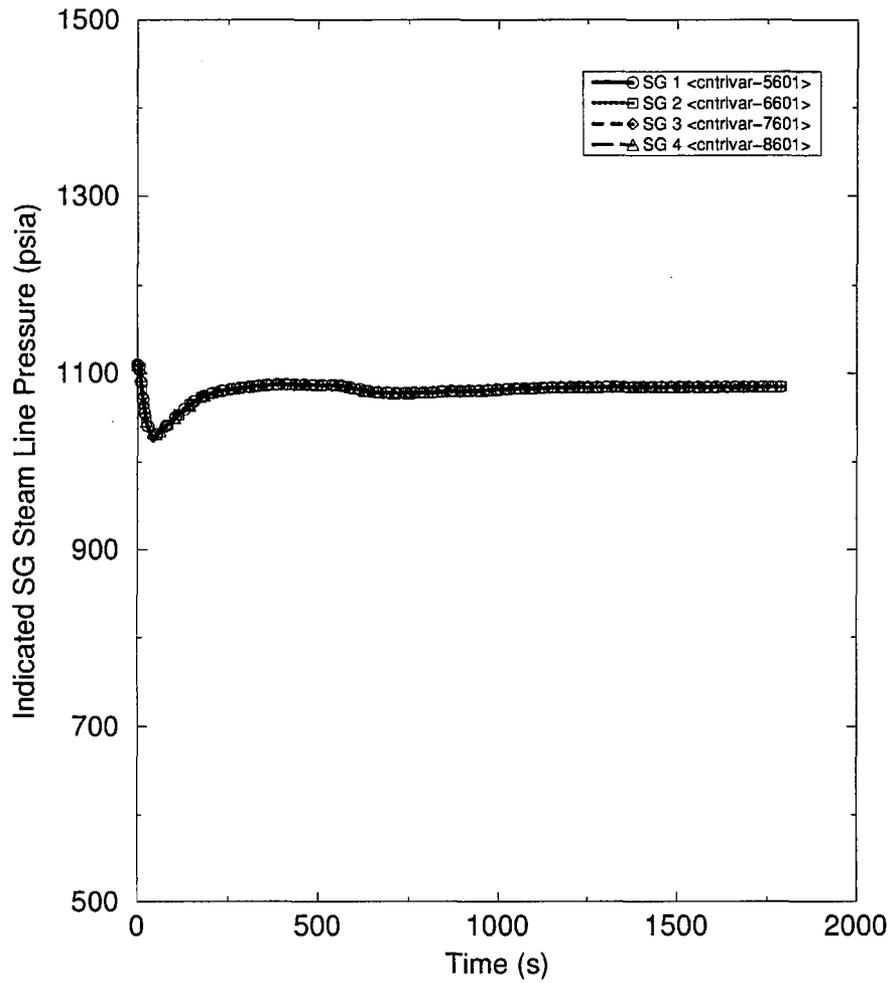
**Figure A.3.5-6—Bank A Drop at EOC Event:  
RCS Temperatures**



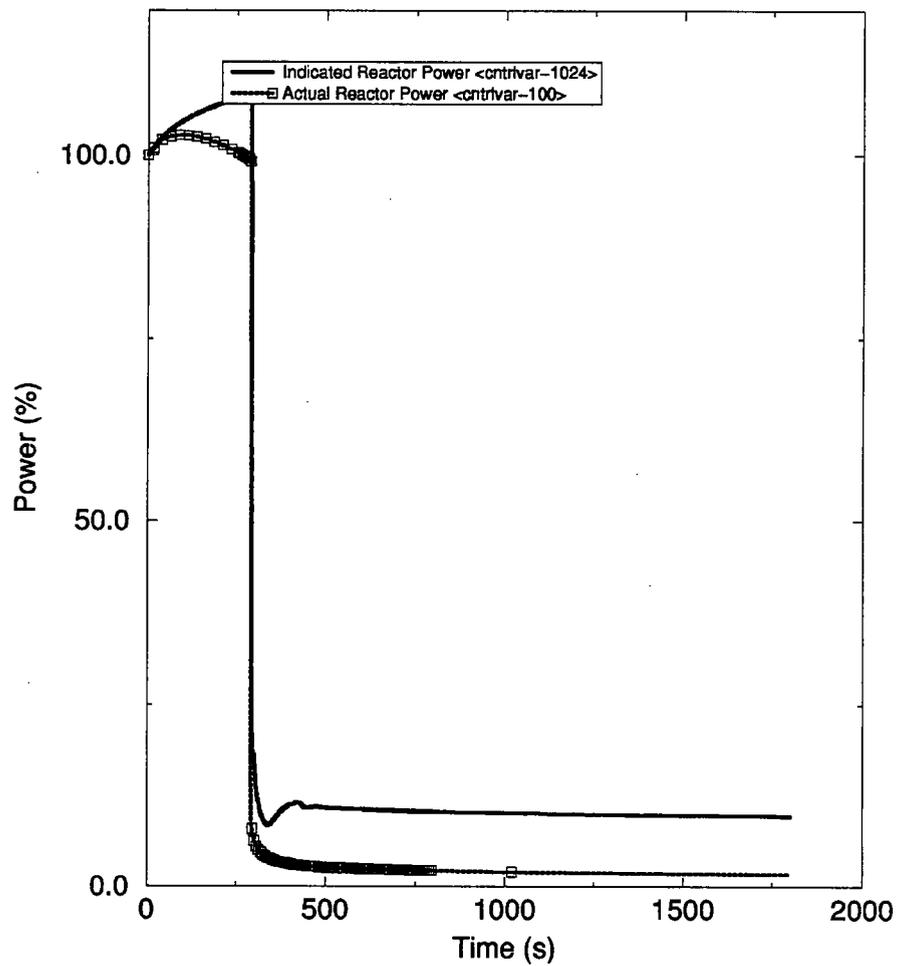
**Figure A.3.5-7—Bank A Drop at EOC Event:  
Pressurizer Pressure**



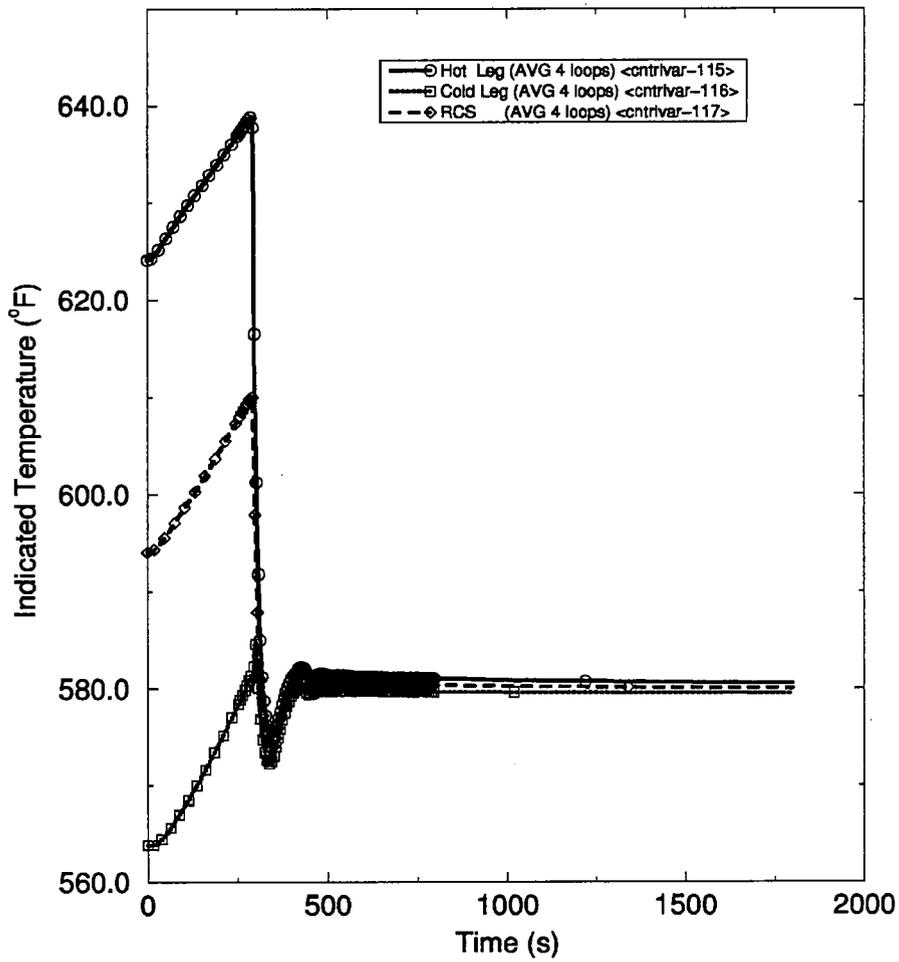
**Figure A.3.5-8—Bank A Drop at EOC Event:  
Steam Line Pressure**



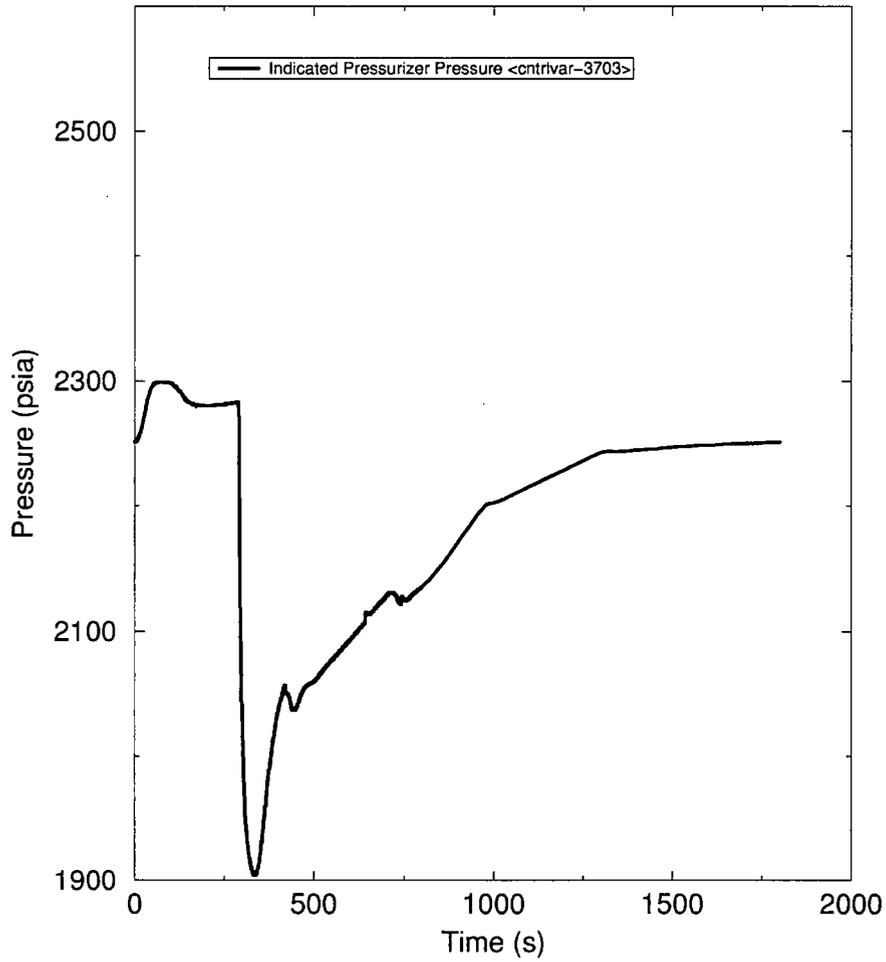
**Figure A.3.5-9—Boron Dilution at Power Event:  
Indicated and Actual Reactor Power**



**Figure A.3.5-10—Boron Dilution at Power Event:  
RCS Temperatures**

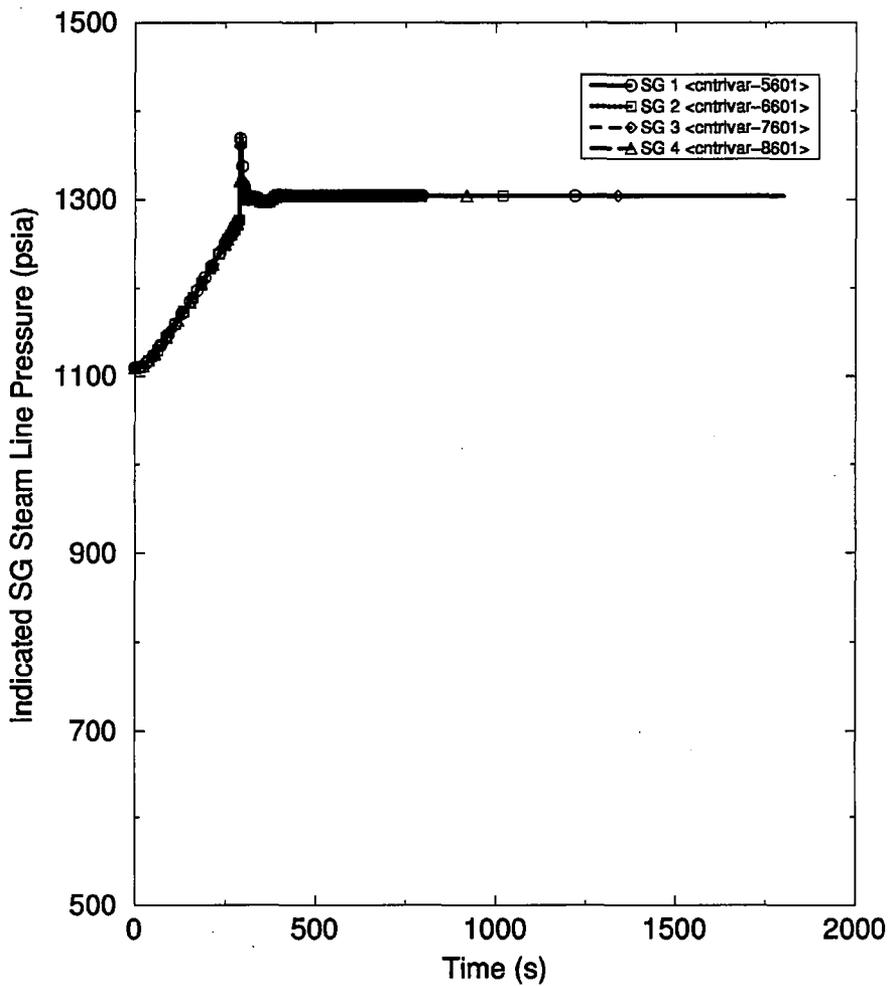


**Figure A.3.5-11—Boron Dilution at Power Event:  
Pressurizer Pressure**

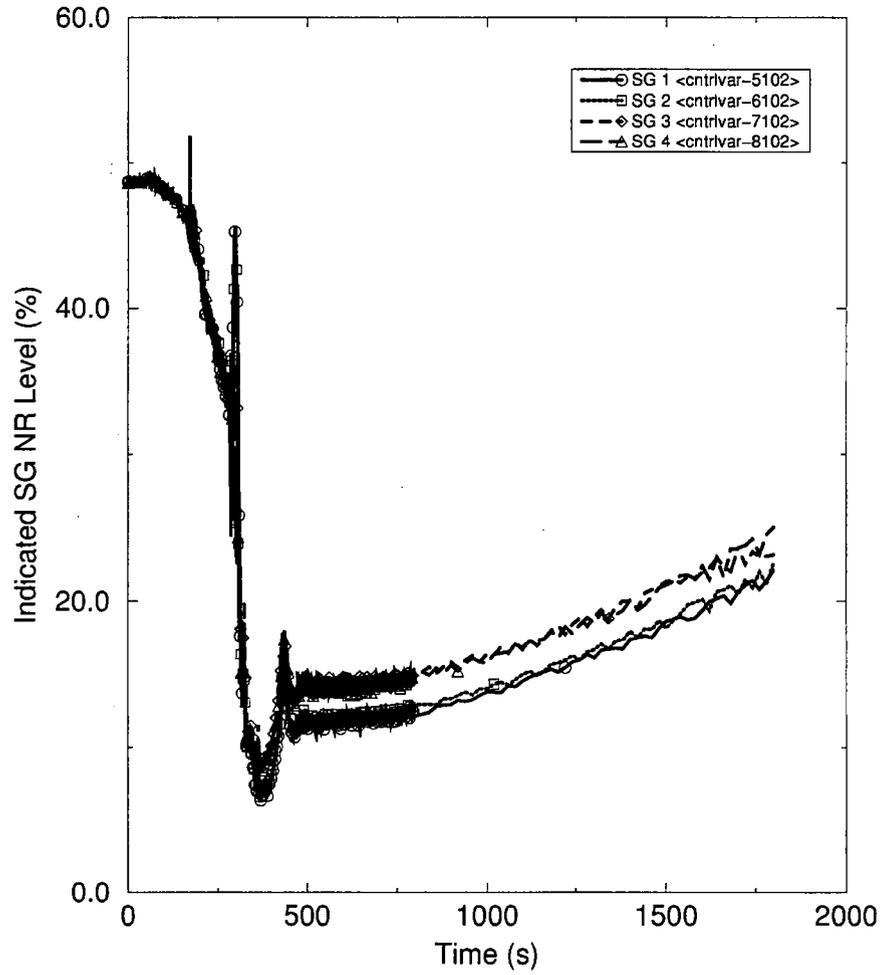


ID:13240 3Nov2009 14:13:11 boron\_dilution\_boc.dmx

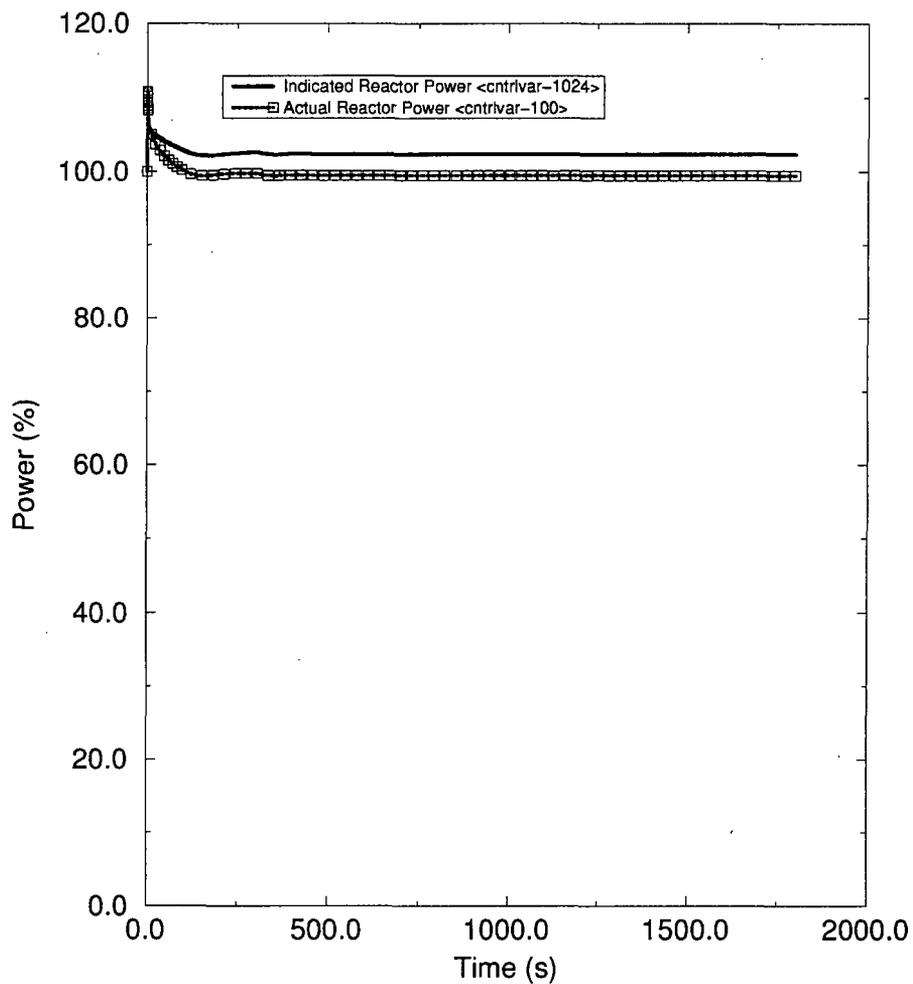
**Figure A.3.5-12—Boron Dilution at Power Event:  
Steam Line Pressure**



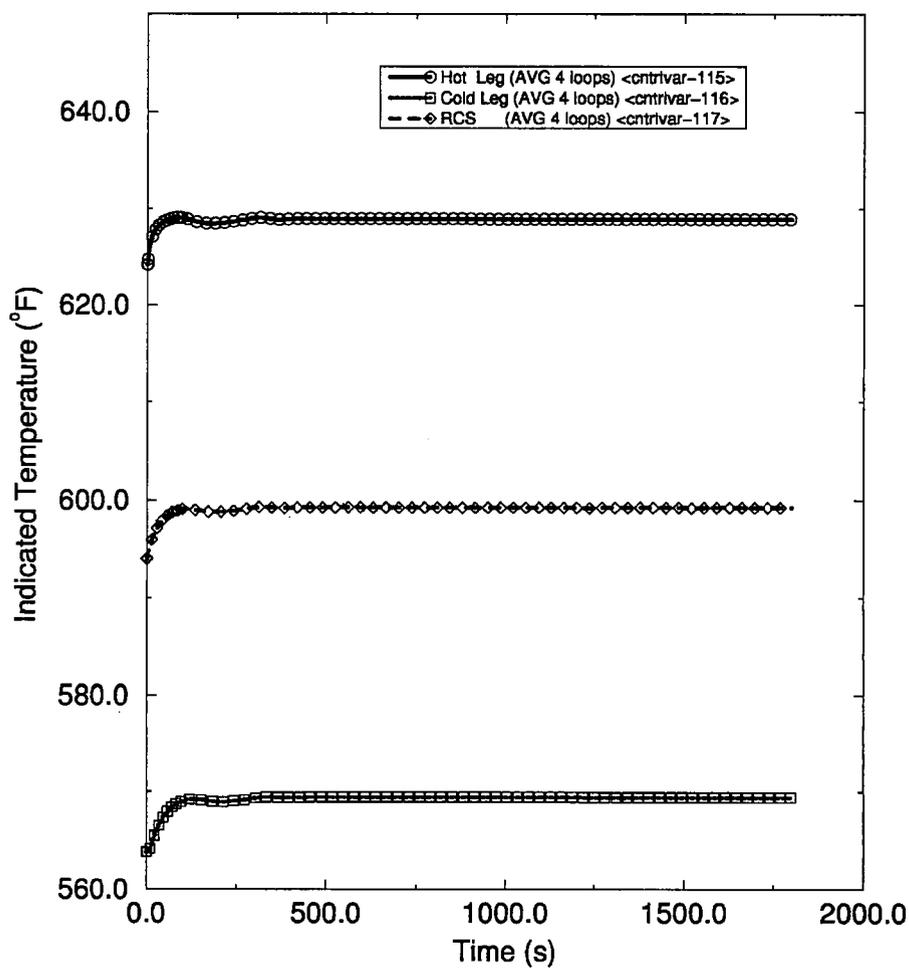
**Figure A.3.5-13—Boron Dilution at Power Event:  
Steam Generator Narrow Range Levels**



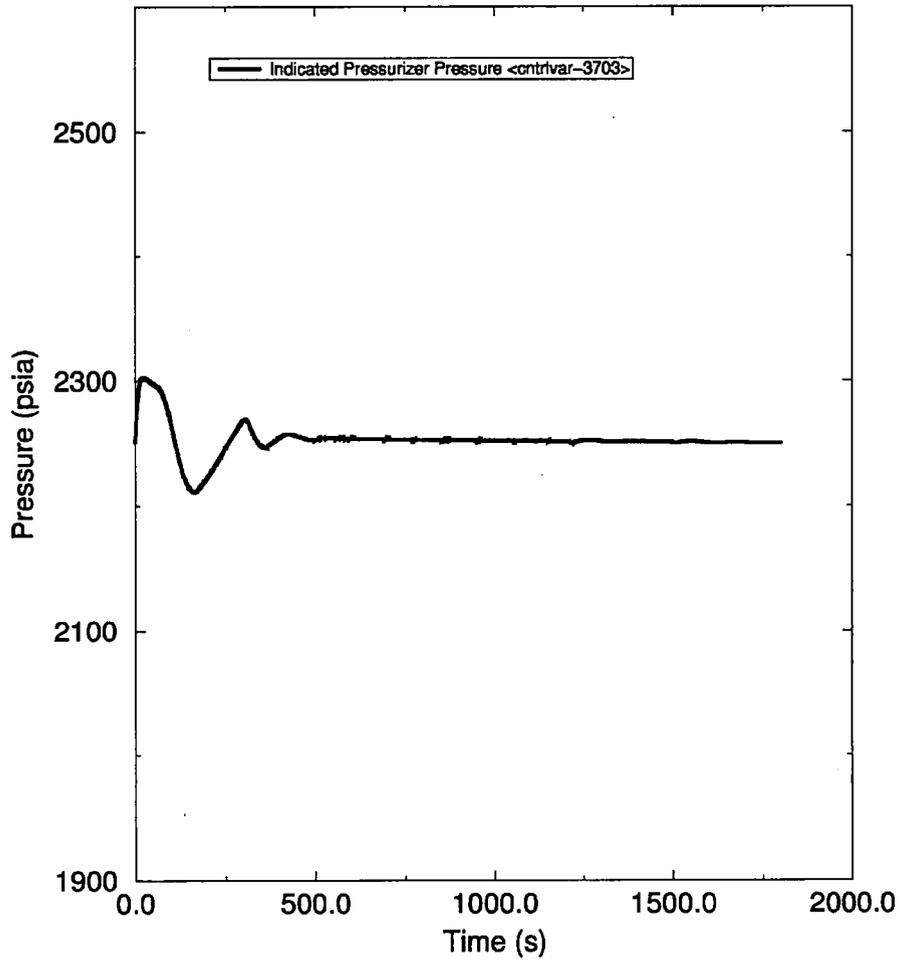
**Figure A.3.5-14—RCCA Ejection - No Rupture Event:  
Indicated and Actual Reactor Power**



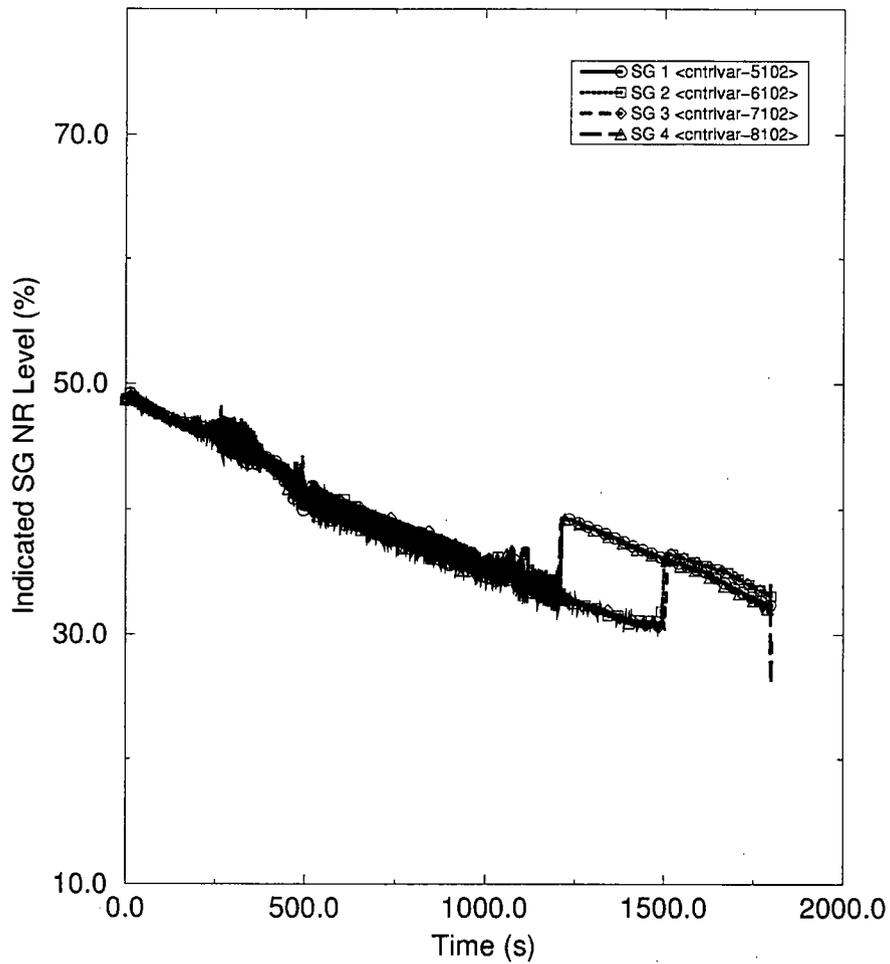
**Figure A.3.5-15—RCCA Ejection - No Rupture Event:  
RCS Temperatures**



**Figure A.3.5-16—RCCA Ejection - No Rupture Event:  
Pressurizer Pressure**



**Figure A.3.5-17—RCCA Ejection - No Rupture Event:  
Steam Generator NR Level**



### **A.3.6 Increase in RCS Inventory**

#### **A.3.6.1 Inadvertent Operation of SIS or EBS**

The Inadvertent Operation of SIS or EBS event results from a spurious actuation, either automatic or manual, of the SIS or EBS that adds fluid to the RCS, potentially overfilling the RCS. The actuation of SIS at power is not an issue for the U.S. EPR, because SIS consists only of low- and medium-head systems and lacks sufficient head to deliver flow to the RCS at power conditions.

As in the U.S. EPR FSAR, the Inadvertent Operation of EBS event is evaluated only as an RCS inventory increase event. No consideration is given to the reactivity aspects of the event. The EBS is a safety-related system designed to inject borated water into the RCS against RCS pressure, following DBEs. The EBS consists of two trains, each with a high pressure, positive displacement pump, and an EBS tank. During normal operation, the pumps are in standby and must be started manually. The pressurizer level control system maintains RCS inventory by regulating the CVCS letdown flow. The removal capacity of the letdown system is greater than the combined injection capacity of both EBS pumps. Therefore, as long as the letdown flow path is available, pressurizer level is maintained, even if both EBS pumps start inadvertently. In the case of an SWCCF in the PS, the PAS pressurizer level control function remains available and the inadvertent start of the EBS system would not result in filling the pressurizer. The U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for the Inadvertent Operation of EBS event.

#### **A.3.6.2 CVCS Malfunction that Increases RCS Inventory**

The CVCS Malfunction that Increases RCS Inventory event results from a spurious actuation, either by a control system or operator action, of the CVCS that adds fluid to the RCS without letdown, potentially overfilling the pressurizer. The U.S. EPR FSAR analysis considered cases with and without loss of offsite power (LOOP). The case with LOOP resulted in the highest pressurizer level, because of the greater RCS heat-up from the transition to natural circulation. Therefore, in the U.S. EPR FSAR analysis, the case with offsite power available is less severe. In the non-LOOP case, the PS initiates RT on high pressurizer level at 783 seconds and isolates the CVCS on high-high pressurizer level at 1052 seconds. A maximum pressurizer level of 88.6 percent is reached at 1672 seconds.

In the case of an SWCCF in the PS, DAS does not provide an RT on a high pressurizer level or a CVCS isolation on high pressurizer level. However, under best estimate conditions, the pressurizer pressure and level control systems would be available. The pressurizer level control system includes a limitation function that would isolate CVCS when the pressurizer level increases to 70 percent. The pressurizer level limitation function is separate from the PS and resides on PAS. This function is intended to improve plant availability by avoiding reactor trip RT and other safety function actuations for events that lead to increasing level in the pressurizer. Therefore, the pressurizer level limitation function would therefore terminate this event well before filling the pressurizer. This automatic feature would actuate approximately 8.5 minutes after event initiation.

~~When the pressurizer pressure control system is available, the pressurizer sprays actuate to maintain pressure. As level increases and the steam volume decreases, the spray flow becomes less effective in maintaining pressure in the pressurizer. Pressurizer pressure increases and DAS initiates RT on high pressurizer pressure, before the pressurizer overfills.~~

~~The pressurizer level response, in the case of an SWCCF in the PS, can be estimated from the non-LOOP case in the U.S. EPR FSAR analysis. From that analysis, pressurizer level is estimated to reach 100 percent in approximately 24 minutes without CVCS isolation. This is conservatively estimated by taking the level change in the U.S. EPR FSAR analysis, for the non-LOOP case between 641 and 783 seconds, and extrapolating from the 85.5 percent level at 1012 seconds. If the CVCS continues beyond 24 minutes, the pressurizer overfills, and liquid would be relieved through the PSRVs without a significant increase in RCS pressure. The PSRVs are designed to relieve water. Thus, RCS boundary integrity is maintained.~~

Automatic CVCS isolation is available on PAS to terminate this event without operator intervention. Pressurizer overfill is not challenged. Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS, for a CVCS Malfunction that Increases RCS Inventory event.

### **A.3.7 Decrease in RCS Inventory**

#### **A.3.7.1 Inadvertent Opening of a PSRV**

The Inadvertent Opening of a PSRV event is defined as the inadvertent opening of a pressurizer safety relief valve. Because the PSRVs serve as both relief and safety valves, there are no downstream block valves to isolate the relief line. The U.S. EPR FSAR analysis included cases beginning from both BOC and EOC conditions, with the BOC cases being limiting. In the U.S. EPR FSAR analysis, the PS initiates RT on low pressurizer pressure. In the case of an SWCCF in the PS, DAS initiates RT on low hot leg pressure. This is comparable to the PS function and provides adequate protection for this event.

The long-term progression of this event after RT is similar to that of a hot leg SBLOCA. The SBLOCA analysis covers all required system interaction (e.g., SI, EFW). Therefore, the long-term response for this event is bounded by the discussion for SBLOCA in Section A.3.7.3.

Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is ~~determined adequate~~determined to be adequate in addressing an SWCCF in the PS, for the Inadvertent Opening of a PSRV event.

#### **A.3.7.2 Steam Generator Tube Rupture**

The ~~Steam Generator Tube Rupture~~ SGTR event is defined as the double-ended rupture of a single SG tube. This event proceeds very slowly. The SGTR event is analyzed to evaluate offsite dose consequences and to demonstrate margin to SG overfill. In the U.S. EPR FSAR analysis of the SGTR event, multiple manual actions for event mitigation are credited. Those manual actions are listed below:

- Trip the reactor when CVCS is operating. Note: That this action results in a more severe response. Under normal conditions with CVCS in operation the break flow would be offset by the capacity of CVCS and no automatic reactor trip RT would occur. Under these conditions the operator would maneuver the plant through a controlled shutdown.
- Reset the MSRT setpoints on affected SG and, if necessary, initiate partial cooldown in the unaffected SGs.
- Close the MSIV on the affected SG.

- Isolate feedwater to the affected SG (MFW & EFW).
- Initiate and control MHSI.
- Extend partial cooldown of the unaffected SG and depressurize the RCS.
- Actuate EBS to add boron to the RCS during cooldown, to maintain subcriticality.

These actions are all performed beyond 30 minutes and control offsite dose consequences to within limits. Margin to SG overfill is also controlled by taking these actions.

In the case with an SWCCF in the PS, the above manual functions are available outside the PS. The main difference is that the MSRTs are not available to control the partial cooldown function automatically following SI, but are available for manual operation of the extended cooldown of the RCS. Under normal conditions CVCS would function to maintain RCS pressure and level (CVCS has the capacity to make-up for the rupture of a single steam generator SG tube). Under these conditions an RT or SI would not occur and therefore neither would the partial cooldown function. After 30 minutes the operator would perform the listed actions listed above to isolate the affected steam generator SG and terminate the leak. However, the turbine bypass system is available to perform the same function as the MSRTs and the event proceeds similarly as in the U.S. EPR FSAR analysis. MFW is remains available for primary system heat removal through the unaffected SGs, and DAS automatically actuates SI on low pressurizer pressure. The turbine bypass system would also remain available. Therefore, offsite dose consequences would be bounded by the FSAR analysis, are less, as a result of discharging through the condenser rather than directly to the atmosphere. The end state for this event considers a cooldown (manual use of MSRTs or turbine bypass) and depressurization to RHR entry to terminate any offsite releases. If the MSRTs are available (partial failure) the offsite dose consequences would be comparable to the results provided in the U. S. EPR FSAR analysis.

For steam generator SG overfill, DAS provides complete MFW isolation on SG high level for the affected SGs, but not on RT. In addition, the SG level control system closes the full load control valve (FLCV) and then the low load control valve (LLCV), in response to an increasing SG level. The FLCV begins to close upon reaching 52 percent narrow range (NR). At 58 percent (NR) level, both valves would be directed to close. Normal SG level is 49 percent (NR). Post-trip of the level control setpoint is reduced to 33.7 percent (NR). Therefore, in the absence of a full

load line isolation on RT, the SG level control system responds quickly to isolate MFW to the affected SG.

In the case of a SWCCF, the steam generator tube rupture SGTR event has been analyzed with S-RELAP5 to calculate the SG level response in the affected steam generator SG by crediting the response of the SG level control system to close on an increasing level. Figure A.3.7-1 through Figure A.3.7-8 shows the response of key parameters for the steam generator tube rupture SGTR event with a SWCCF. As illustrated in Figure A.3.7-5, Figure A.3.7-6, and Figure A.3.7-7, show that there is ample margin to overfill.

~~In the case of a SWCCF, an estimate of the SG level response has been made by crediting the response of the SG level control system to close on an increasing level. For this scenario, the affected generator fills rapidly following RT until the MFW FLCV and LLCV close. At that point, the level in the affected SG reaches approximately 90 percent (WR). The break flow continues until operator action to cool down and depressurize the RCS and bring the RCS pressure and the affected SG into equilibrium. The analysis estimates that the affected SG level exceeds 100 percent (WR) level and releases a small amount of liquid to the steam line. The steam line is designed to handle the loads associated with a steam line full of saturated water at hydrostatic test pressure of 1.25 design pressure. Thus, the steam piping integrity is maintained.~~

Therefore, the acceptance criteria of BTP 7-19 are met and the U.S. EPR design is determined to be adequate in addressing a SWCCF in the PS during SGTR events.

### **A.3.7.3 Loss of Coolant Accidents**

A LOCA event is initiated by the instantaneous rupture of an RCS pipe. Ruptures smaller than 10 percent of the cross-sectional area of the RCS loop piping are classified as SBLOCAs. Those larger are considered LBLOCAs.

#### **A.3.7.3.1 Large Break LOCA**

In the U.S. EPR FSAR analysis of an LBLOCA, RT is not credited. Therefore, although DAS provides RT on low hot leg pressure, no RT function is required from DAS for LBLOCA. The PS initiates an RCP trip on RCP low differential pressure. During an LBLOCA, the RCP trip occurs about 10 seconds from the initiation of the event. In the event of a SWCCF in the PS, because

DAS does not contain a RCP trip function, the RCPs would be expected to continue operation. ~~Continued operation of the RCPs does not have a significant impact on LBLOCA results. A sensitivity calculation is performed, with continued operation of the RCPs, and demonstrates this conclusion.~~

A sensitivity calculation was performed to assess the effect on peak cladding temperature (PCT) without an automatic reactor coolant pump (RCP) trip. This study removes the automatic RCP trip for selected cases from the U.S. EPR uncertainty analysis. These realistic large-break loss-of-coolant accident (RLBLOCA) cases are representative of an initial fuel cycle and are performed in accordance with ANP-10278, Revision 1 (Reference A-3). The results of the sensitivity study show that not actuating the automatic RCP trip has a minor impact of <less than 30-° F on the PCT (Figure A.3.7-9) and causes no discernible differences in break flow between the FSAR calculation cases with automatic RCP trip and the D3 sensitivity cases without an automatic RCP trip.

In the U.S. EPR FSAR ~~analysis~~ analyses, the PS actuates SI on low pressurizer pressure. DAS also actuates SI on low pressurizer pressure. The availability of all SI trains (no preventative maintenance or single failure) and the use of best estimate core parameters make the D3 analysis core response much less severe than in the U.S. EPR FSAR analysis.

The prevention of boron precipitation in the core during post-LOCA recovery requires the operators to switch to hot leg SI within 60 minutes of the LBLOCA. This action is also required to support the containment response to a LBLOCA. The ability to manually switch SI to the hot legs is available outside the PS and is available in the event of an SWCCF in the PS.

Therefore, the acceptance criteria of BTP 7-19 are met, and the U.S. EPR is determined to be adequate in addressing an SWCCF in the PS for LBLOCA events.

#### **A.3.7.3.2 Small Break LOCA**

A SBLOCA event is defined as a break in the RCS pressure boundary that has an area of 0.5 ft<sup>2</sup> or less (~10 percent of cold leg pipe area). The most limiting SBLOCA is in the cold leg pipe at the discharge side of the RCPs. This break results in the largest inventory loss and the largest fraction of SIS fluid being ejected through the break. In turn, this produces the greatest degree

of core uncover and the longest fuel rod heatup time. Consequently, it poses the greatest challenge to the 10 CFR 50.46 criteria.

In the U.S. EPR FSAR analysis, the PS initiates RT and actuates SI on low pressurizer pressure, for all cases. The U.S. EPR FSAR analysis evaluates cases with and without LOOP. In the LOOP case, it is assumed that LOOP occurs coincident with RT, which also initiates EFW flow, when the SI signal is reached. If LOOP does not occur, EFW is not initiated until a low SG level is reached.

The PS design for the U.S. EPR includes an automatic reactor coolant pump (RCP) trip on low differential pressure and a partial cooldown function on SI. An automatic RCP trip function is neither available, nor required, on DAS for the beyond design basis SWCCF event. The U.S. EPR design, therefore, conforms to the NUREG-0737 TMI Action Plan requirement II.K.3.5. assumes LOOP coincident with RT, which also initiates EFW flow, when the SI signal is reached. If LOOP does not occur, EFW is not initiated until a low SG level is reached.

In the case of an SWCCF in the PS, DAS initiates an RT on low hot leg pressure and actuates SI (i.e., MHSI) on low pressurizer pressure, providing protection equivalent similar to that described in the U.S. EPR FSAR scenario. With a SWCCF, the partial cooldown function may be lost with an SWCCF. MFW is available to provide decay heat removal. As discussed in Section A.2.1, under best estimate conditions, a single failure or preventative maintenance is not assumed. Thus, all EFW trains and SI trains are available.

For certain break sizes, the MSRTs are relied upon in the U.S. EPR FSAR analysis to perform a partial cooldown and depressurize the RCS to enable the injection of MHSI. In the case of an SWCCF in the PS, the MSRTs might not be available because actuation of the MSRT partial cooldown function is initiated in the PS. The TBS partial cooldown function is also dependent on a signal from the PS and is therefore not available. The PS includes an MSIV closure signal on high containment pressure. The MSIVs would remain open if this feature fails as part of the SWCCF. In the event of a partial SWCCF of the PS where the MSIVs still close on high containment pressure, the TBS would not be available to provide for any the cooldown function.

After 30 minutes and before 60 minutes, if the hot leg pressure indication is below 275 psig, the operators will manually realign LHSI to the hot legs to which will suppress steaming in the core

to prevent over-pressurization of the containment. This action also prevents boron precipitation. The ability to manually switch SI to the hot legs is available outside the PS and is available in the event of an SWCCF in the PS.

The PS provides an RCP trip on low RCP differential pressure to ensure provide reasonable assurance that, during an SBLOCA, the RCPs are tripped early in the event. During an SBLOCA with RCPs running, a greater amount of inventory could be lost out the break than with RCPs tripped. After sufficient inventory is lost and the RCPs are tripped, a deeper core uncover could result in a higher peak clad temperature (PCT). DAS does not include an RCP trip function. Thus, wWith an SWCCF in the PS, the RCPs continue operating, with the opportunity to be tripped (manually) at a later time. Manual RCP trip time sensitivity analyses are performed for a spectrum of break sizes, to determine the latest RCP trip time that gives provides acceptable PCT results (i.e., PCT less than 2200°F).

The SBLOCA RCP trip time sensitivity analysis is performed for a spectrum of break sizes ranging from a 1.0 inch inner diameter (ID) break to the maximum small break of 10 percent pipe cross-sectional area, the 9.71 inch ID break. RCP trip times of 10, 60, 900, and 1800 seconds were assumed. The analysis is performed using best estimate assumptions with an SWCCF in the PS. The key best estimate assumptions include the availability of four trains of SI (no single failure or preventative maintenance assumptions), offsite power available, and best estimate decay heat. A separate set of cases were included without a partial cooldown function.

The results of the sensitivity analysis, without a partial cooldown function, indicate that the maximum PCT remains below the 10 CFR 50.46 criteria for the entire break spectrum, whether or not the RCPs are operating or not. Therefore, †The timing of the RCP trip therefore has little impact and manually tripping the RCPs is not required. Except for the high end of the break spectrum, decay heat is first removed through the secondary steam generator SGs MSSVs until the loop seal clears. Upon loop seal clearing the break removes sufficient energy to depressurize the primary system actuating MHSI. Break sizes of 2.5 inches ID and larger clear the loops early and are able to depressurize the primary system to the MHSI injection setpoint. As the RCS continues to depressurizes further, the MHSI and LHSI flow overcome the break flow, establishing extended core cooling. The smaller the break, the longer it takes for the loop seal to clear. For breaks between 2.5 inches and 1.0 inch ID, decay heat is removed mostly through the steam generator SG MSSVs. The primary pressure remains above the MHSI

shutoff head until either EFW actuation or the loop seal clears. EFW actuation fills the secondary with cold water condensing steam and reducing secondary pressure. The reduction in secondary pressure then reduces primary pressure, leading to MHSI injection. In cases where the effectiveness of the EFW to condense steam was reduced to zero, recovery occurs when the loop seal clears. Once the loop seal clears, sufficient energy is removed through the break to depressurize the RCS to the MHSI actuation setpoint. For these breaks, injection from CVCS is sufficient to keep the core covered prior to MHSI injection. Actuation of MHSI recovers RCS inventory. For breaks around 1.0 inch ID the loop seal may take several hours to clear. In this case, the operator will need to take manual control and cooldown through the MSRTs to reduce RCS pressure and actuate MHSI. There is sufficient time to manually initiate the cooldown such so that the partial cooldown function is not required to be automated on DAS. Figure A.3.7-10 through Figure A.3.7-17 show the response of key parameters for representative breaks at both ends of the spectrum.

These analyses demonstrate that the U.S. EPR design is adequately in addressing an SWCCF in the PS during SBLOCA events, including partial failures. The analyses also demonstrate that an RCP trip during an SBLOCA event with an SWCCF in the PS is not needed to mitigate the event. Therefore, operator criteria or a D3 coping procedure for tripping the RCPs during this event are not necessary.

~~For certain break sizes, the MSRTs are relied upon in the U.S. EPR FSAR analysis to depressurize the RCS to enable the injection of MHSI. In the case of an SWCCF in the PS, the MSRTs might not be available because actuation of the MSRT partial cooldown function is handled in the PS. The TBS is a normal operation control system that also has the capability of implementing the partial cooldown function and reducing secondary system pressures. After RT, the TBS controls SG pressure to a fixed setpoint; after an SI signal is generated by DAS on low pressurizer pressure, a programmed cooldown begins, similar to the MSRT partial cooldown. This function is initiated by DAS and is available during an SBLOCA, as long as the MSIVs remain open.<sup>2</sup>~~

---

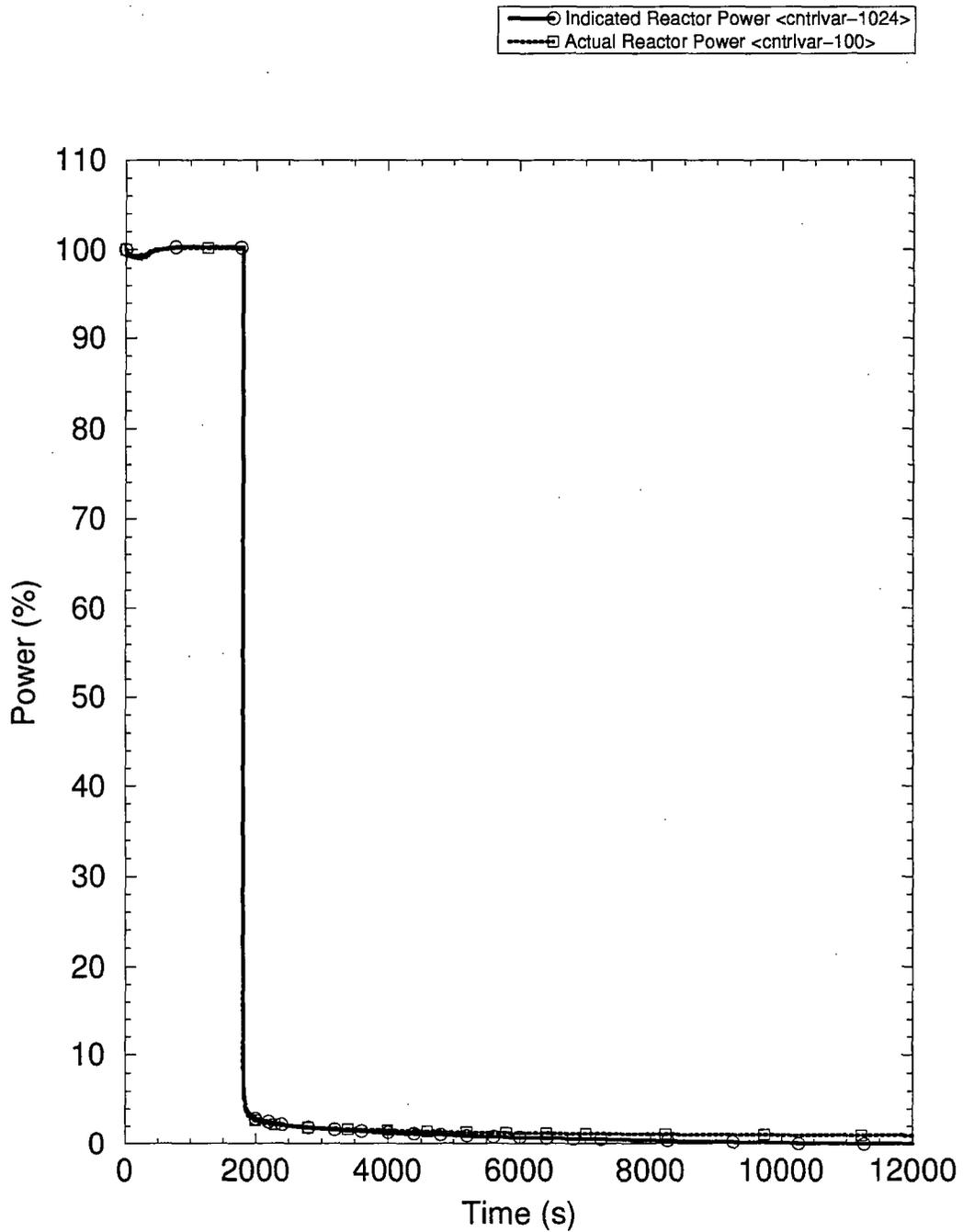
<sup>2</sup> A review is ongoing that could affect use of the turbine bypass system during a small break LOCA event. This may require an additional DAS function or justification for manual operator action to open the MSRTs.

After 30 minutes, if the hot leg pressure indication is below 275 psig, the operators will manually realign LHSI to the hot legs to suppress steaming in the core to prevent overpressurization of the containment. This action also prevents boron precipitation. The ability to manually switch SI to the hot legs is available outside the PS and is available in the event of an SWCCF in the PS.

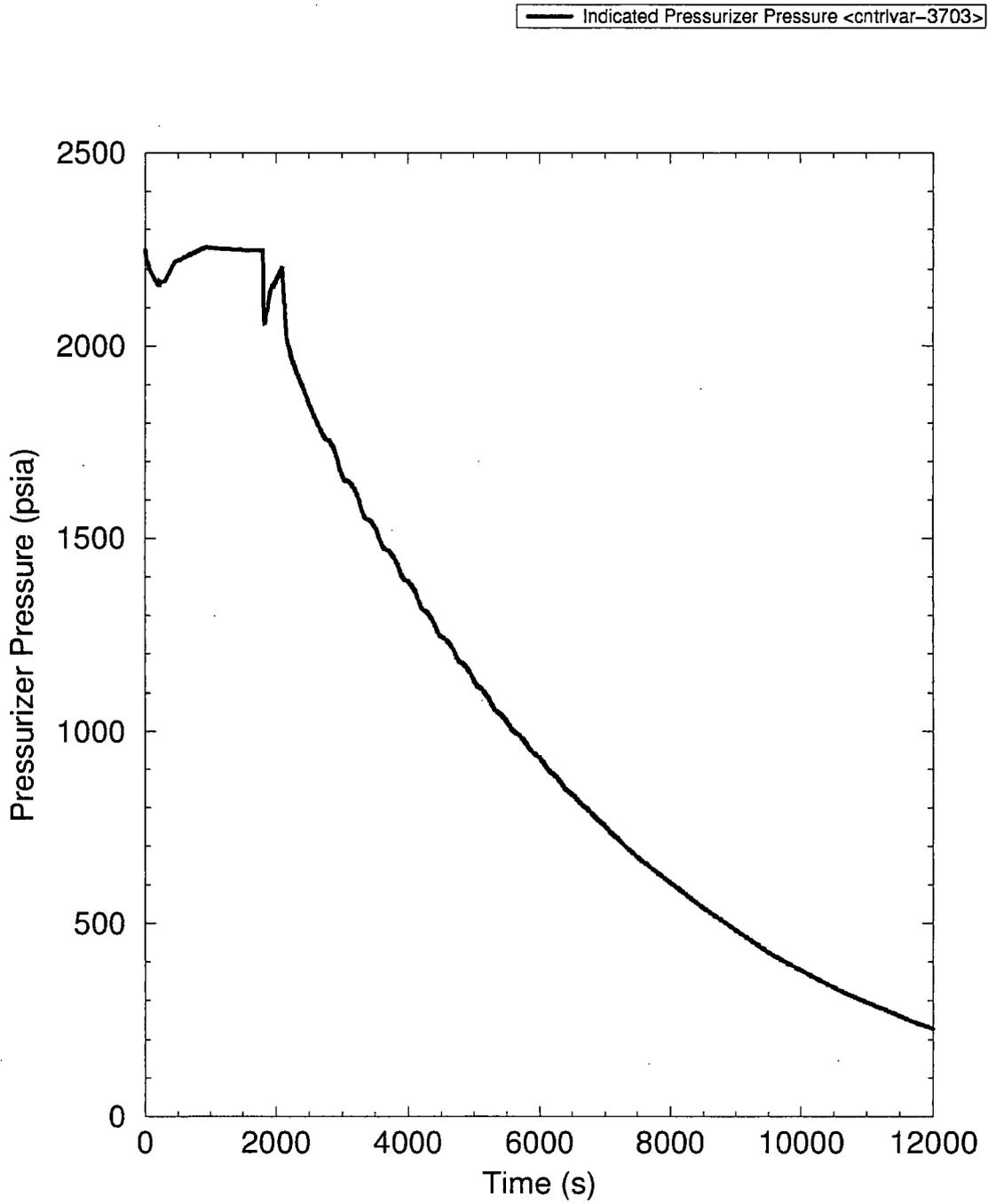
The PS provides an RCP trip on low RCP differential pressure to ensure that, during an SBLOCA, the RCPs are tripped early in the event. During an SBLOCA with RCPs running, a greater amount of inventory could be lost out the break than with RCPs tripped. After sufficient inventory is lost and the RCPs are tripped, a deeper core uncover could result in a higher peak clad temperature (PCT). DAS does not include an RCP trip function. Thus, with an SWCCF in the PS, the RCPs continue operating, with the opportunity to be tripped (manually) at a later time. Manual RCP trip time sensitivity analyses are performed for a spectrum of break sizes, to determine the latest RCP trip time that gives acceptable PCT results (i.e., PCT less than 2200°F).

The SBLOCA RCP trip time sensitivity analysis is performed for a spectrum of break sizes ranging from a 3.0 inch ID break to the maximum small break of 10 percent pipe cross-sectional area, the 9.71 inch ID break. RCP trip times of 10, 60, 900, and 1800 seconds were assumed. The analysis is performed using best estimate assumptions, with an SWCCF in the PS. The key best estimate assumptions include four trains of SI (no single failure or preventative maintenance), offsite power available, best estimate decay heat, and TBS available for partial cooldown. The results of the sensitivity analysis indicate that the maximum PCT remains below the 10 CFR 50.46 criteria for the entire break spectrum, whether or not the RCPs are operating. Therefore, the timing of the RCP trip has little impact and manually tripping the RCPs is not required. In fact, only breaks at the large end of the SBLOCA spectrum result in fuel heatup and only for cases where the RCPs are tripped at 60 seconds or less. This analysis demonstrates that the U.S. EPR design is adequate in addressing an SWCCF in the PS during SBLOCA events.

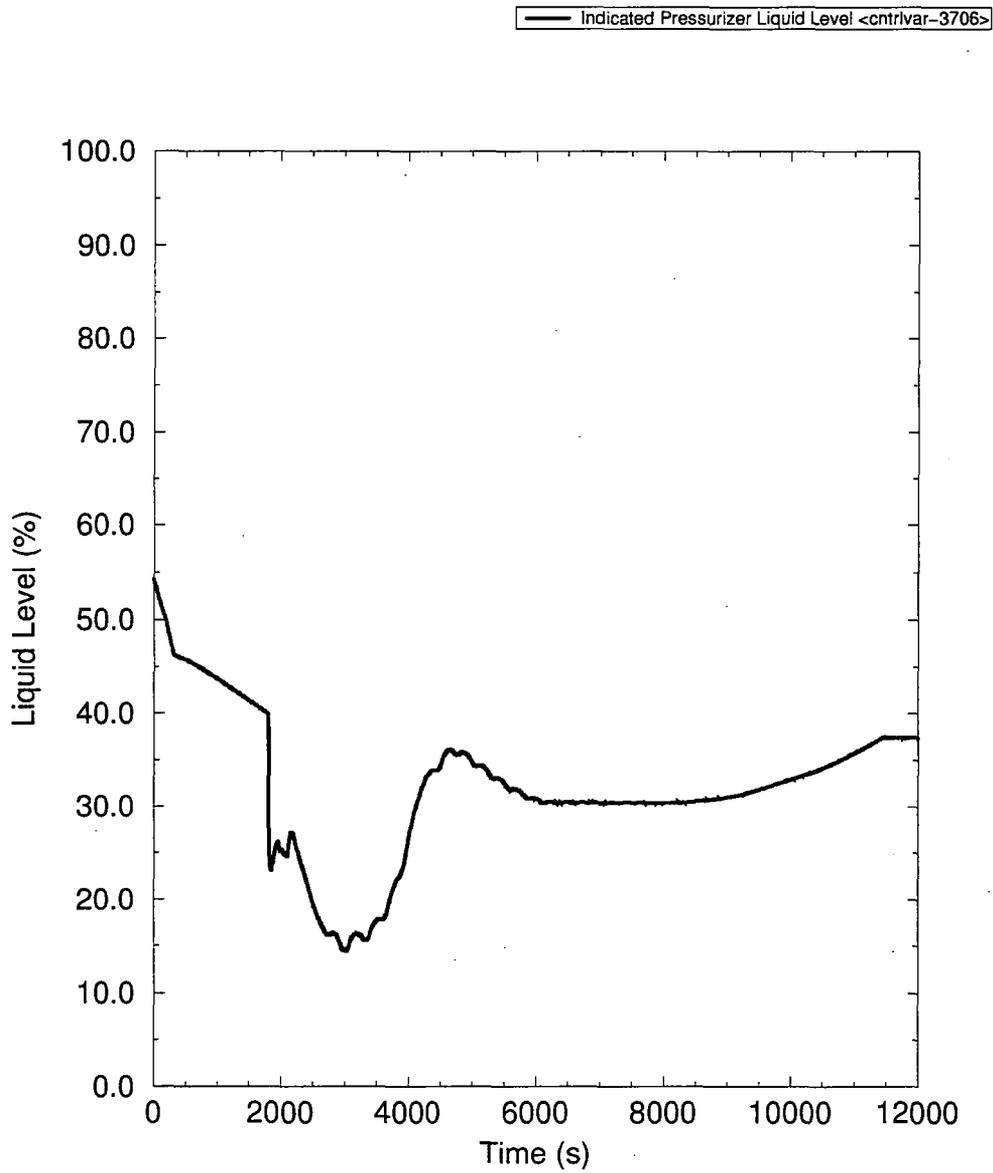
**Figure A.3.7-1—Steam Generator Tube Rupture – Reactor Power**



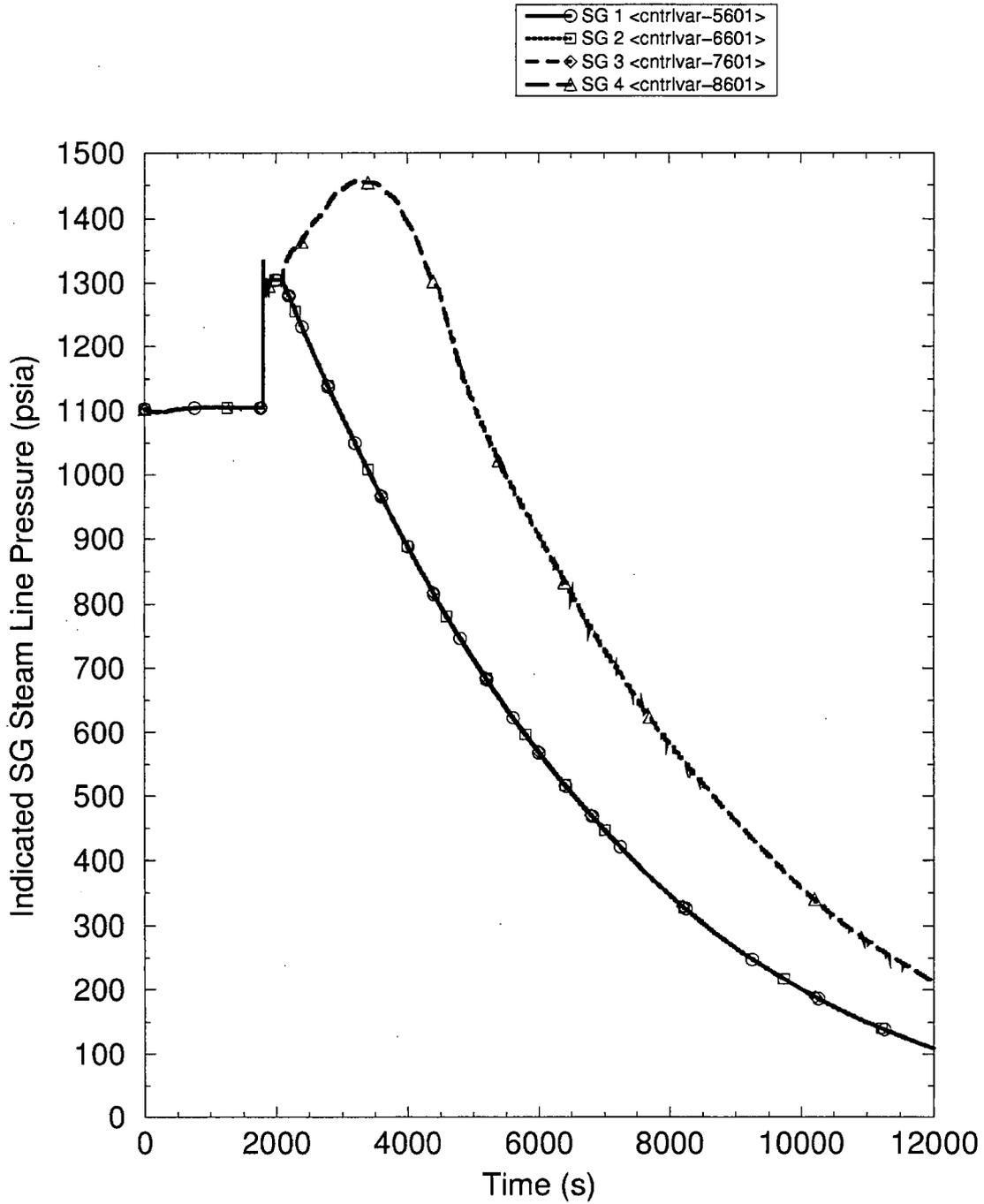
**Figure A.3.7-2—Steam Generator Tube Rupture – Pressurizer Pressure**



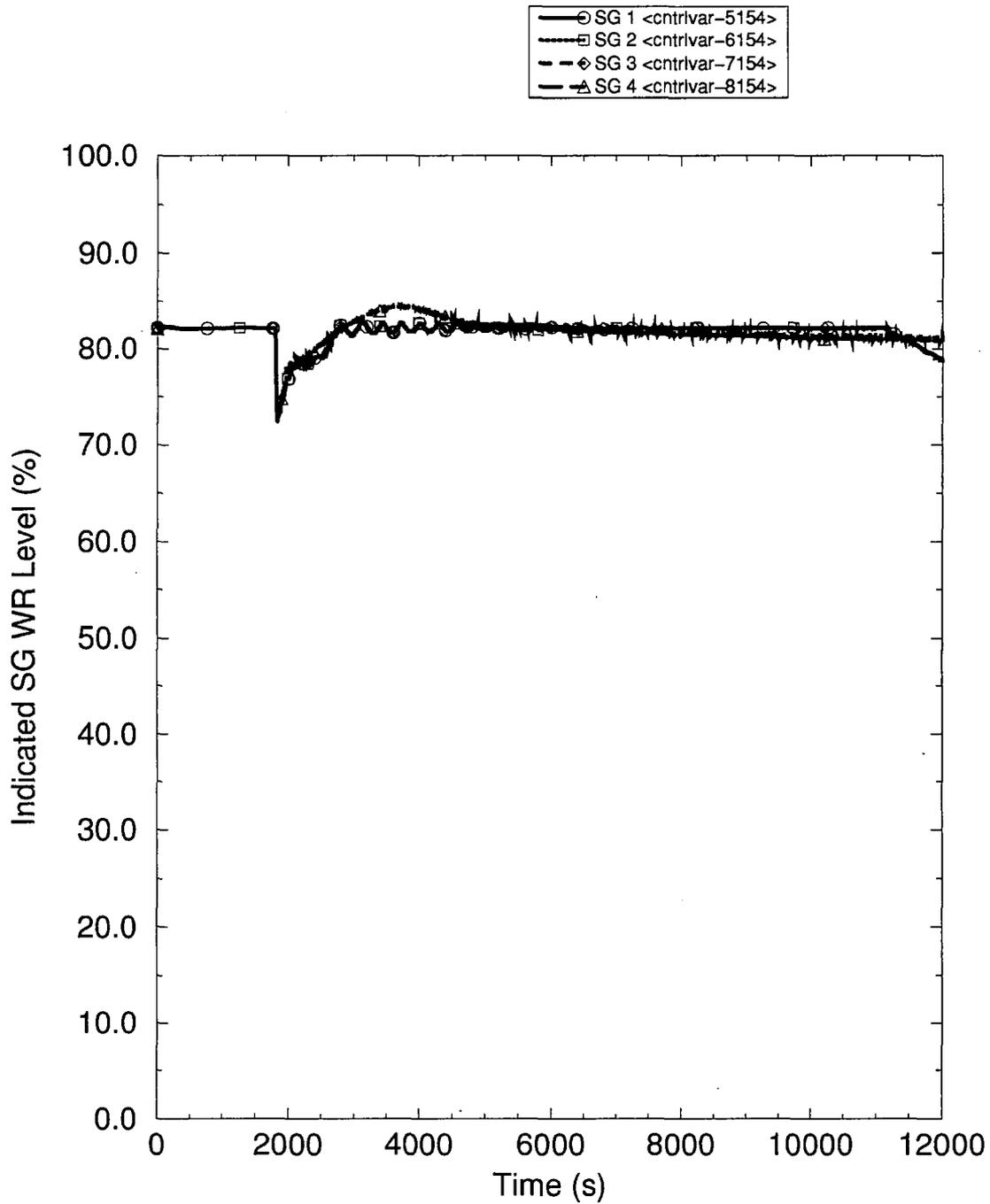
**Figure A.3.7-3—Steam Generator Tube Rupture – Pressurizer Level**



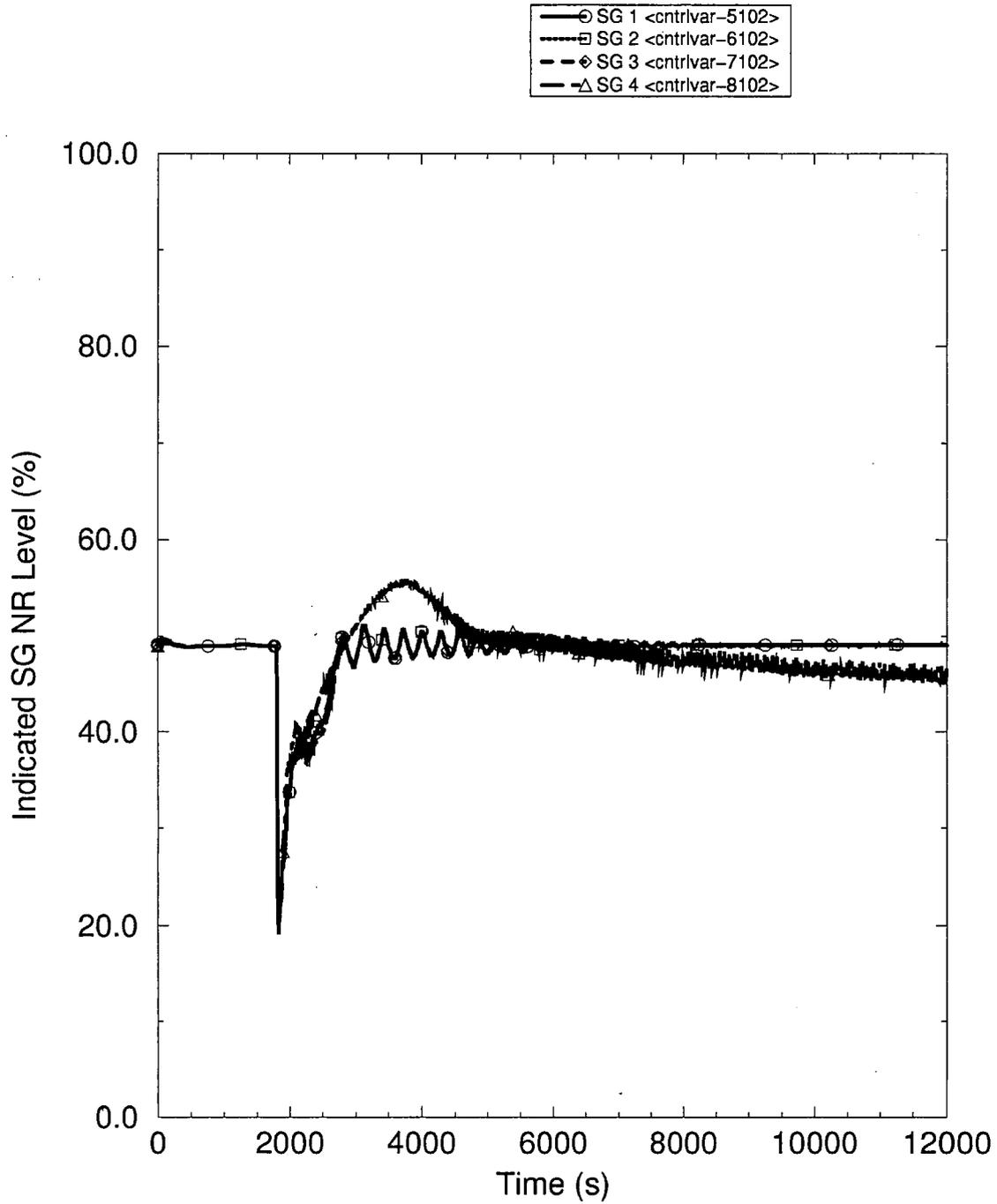
**Figure A.3.7-4—Steam Generator Tube Rupture – Steam Generator Pressure**



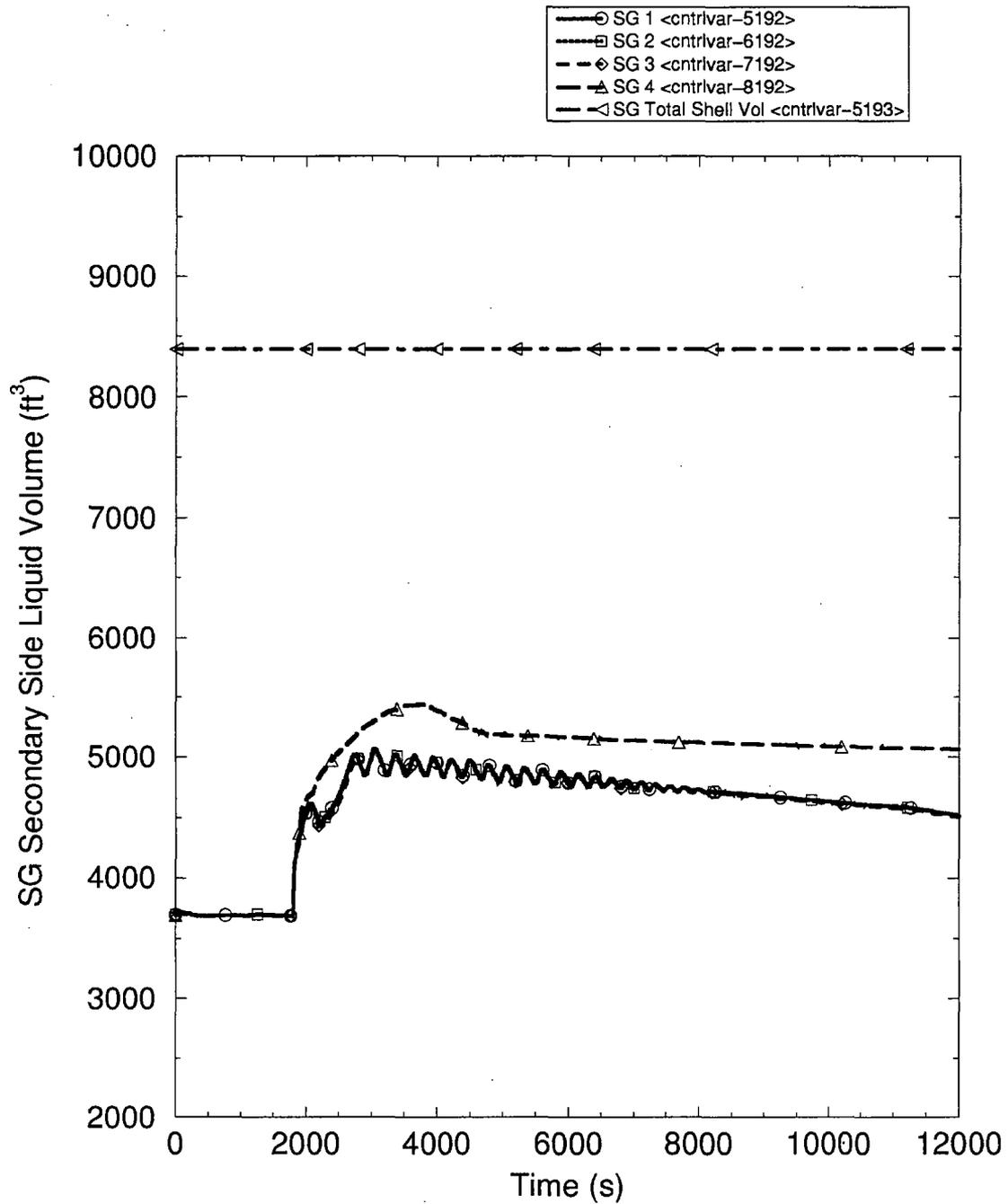
**Figure A.3.7-5—Steam Generator Tube Rupture – Steam Generator  
Wide Range Level**



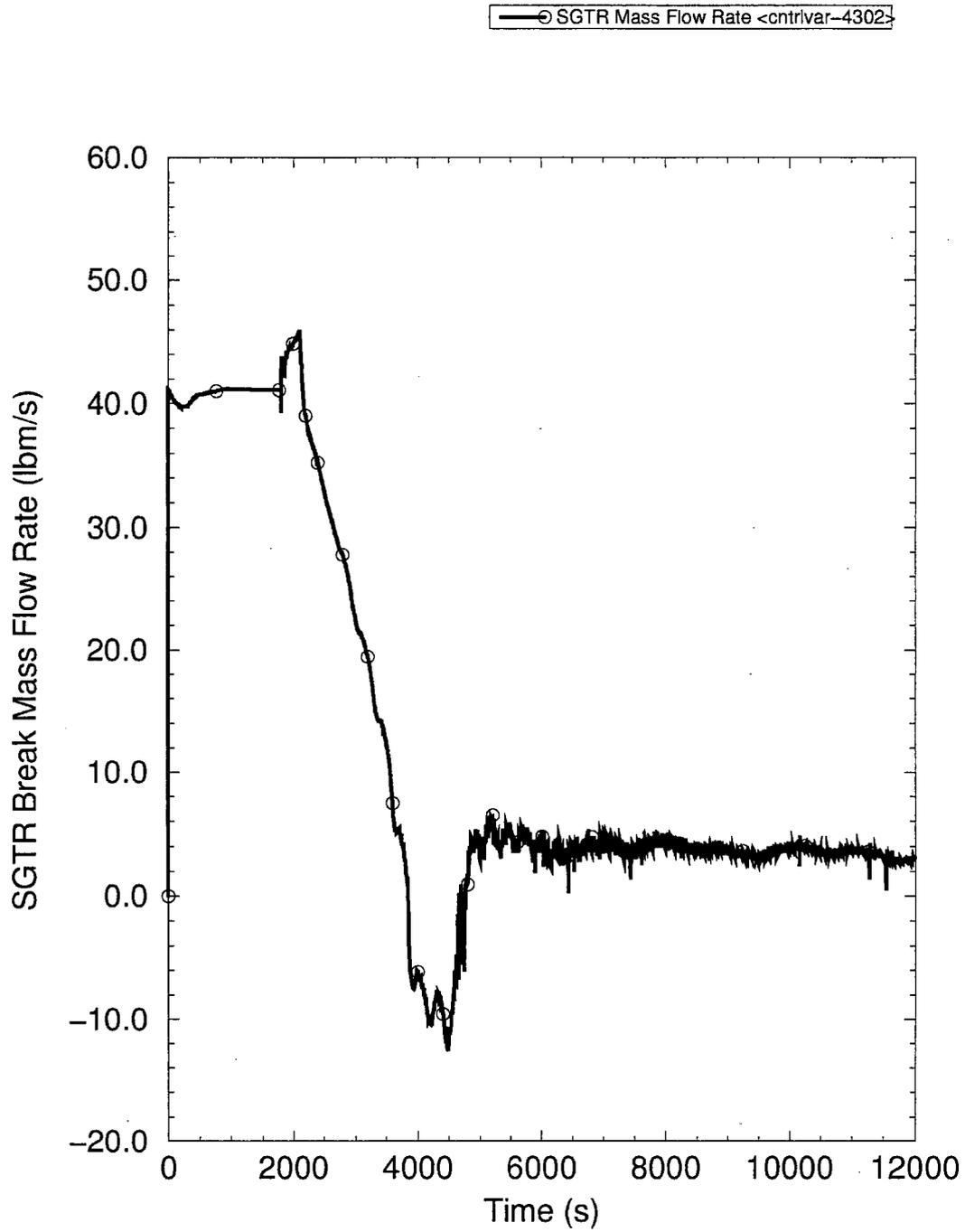
**Figure A.3.7-6—Steam Generator Tube Rupture – Steam Generator  
Narrow Range Level**



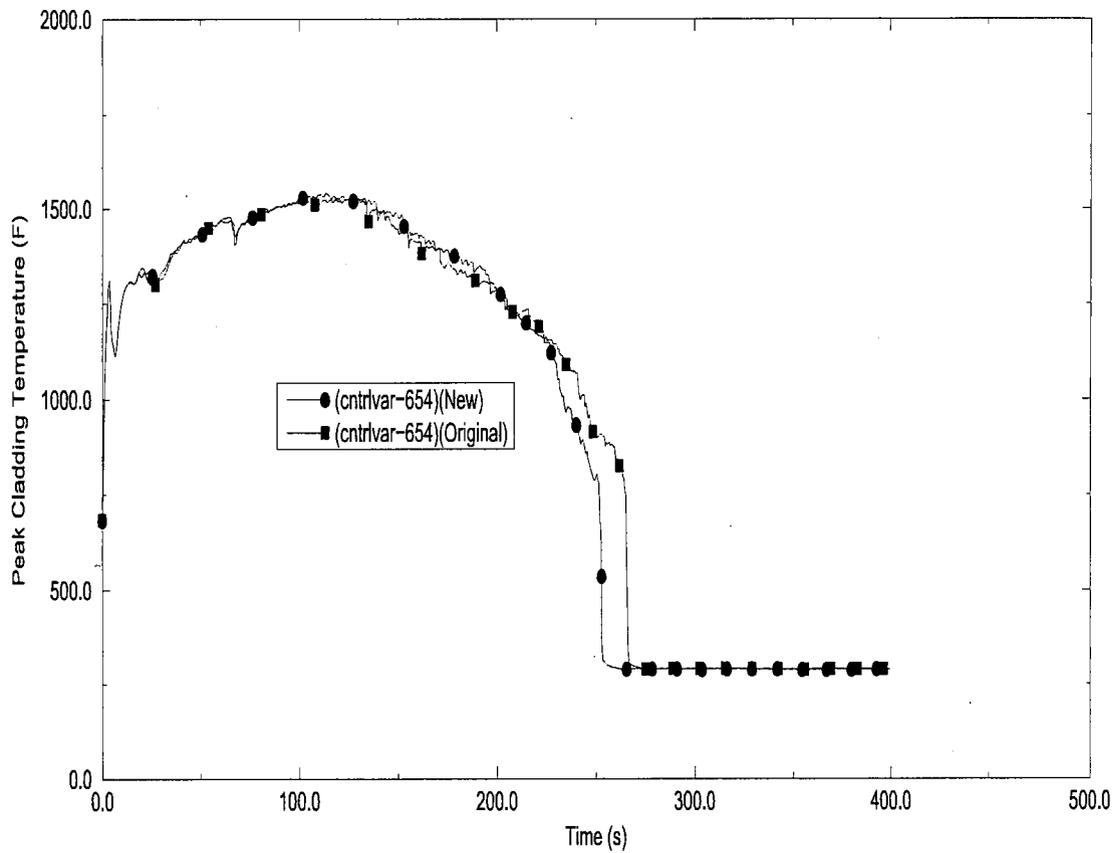
**Figure A.3.7-7—Steam Generator Tube Rupture —Affected- Steam  
Generator Liquid Volume**



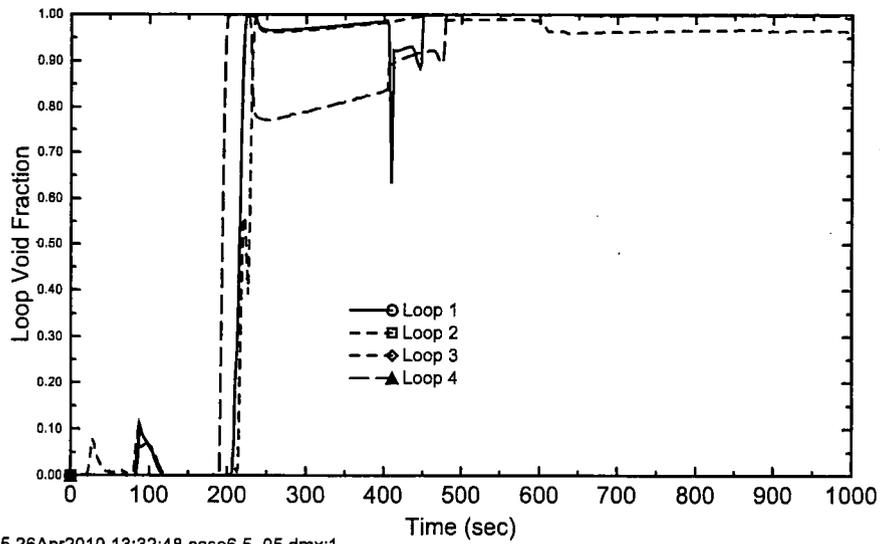
**Figure A.3.7-8—Steam Generator Tube Rupture – Break Mass Flow Rate**



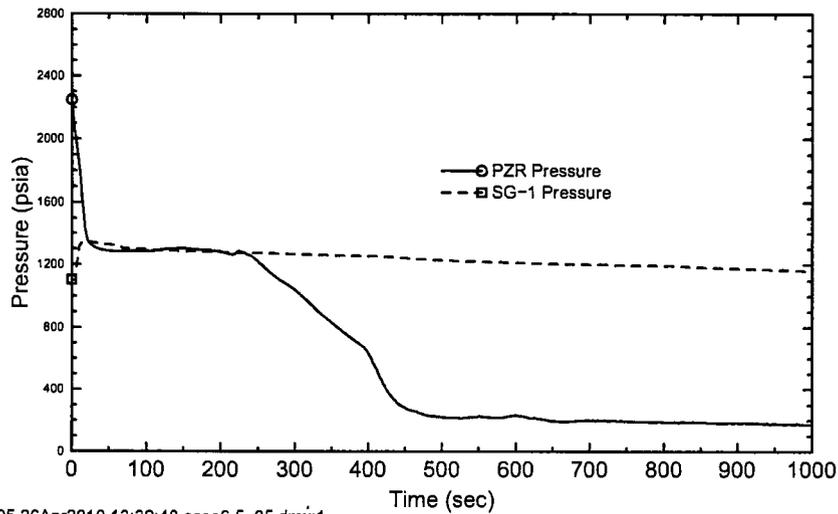
**Figure A.3.7-9—Comparison of PCT: RCP NO Trip (New) vs. RCP  
TRIP FSAR**



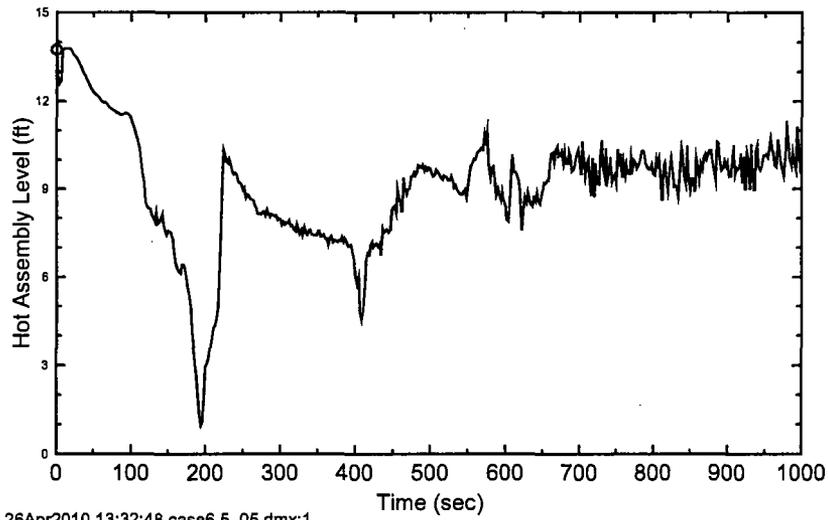
**Figure A.3.7-10—SBLOCA 6.5 inch diameter Break: Loop Seal Clearing Time**



**Figure A.3.7-11—SBLOCA 6.5 inch diameter Break: Primary/Secondary System Pressure**

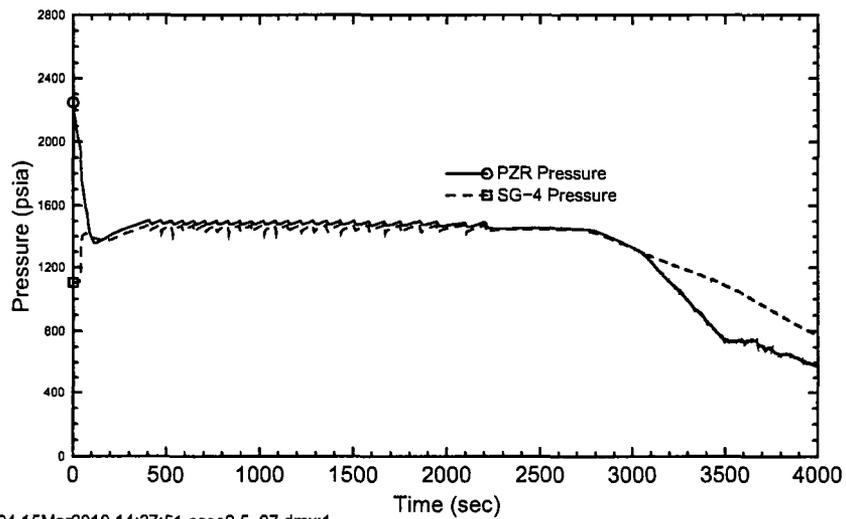


**Figure A.3.7-12—SBLOCA 6.5 inch diameter Break: Hot Assembly Collapsed Liquid Level**



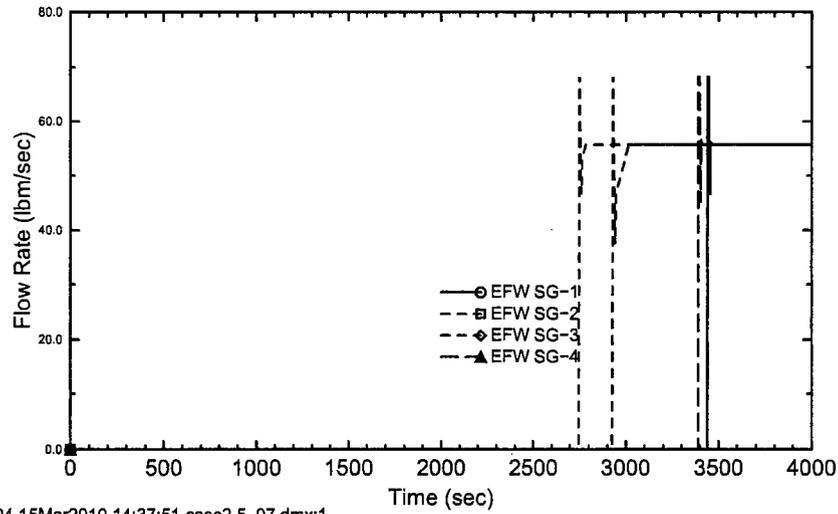
ID:06195 26Apr2010 13:32:48 case6.5\_05.dmx:1

**Figure A.3.7-13—SBLOCA 2.5 inch diameter Break: Primary/Secondary System Pressure**

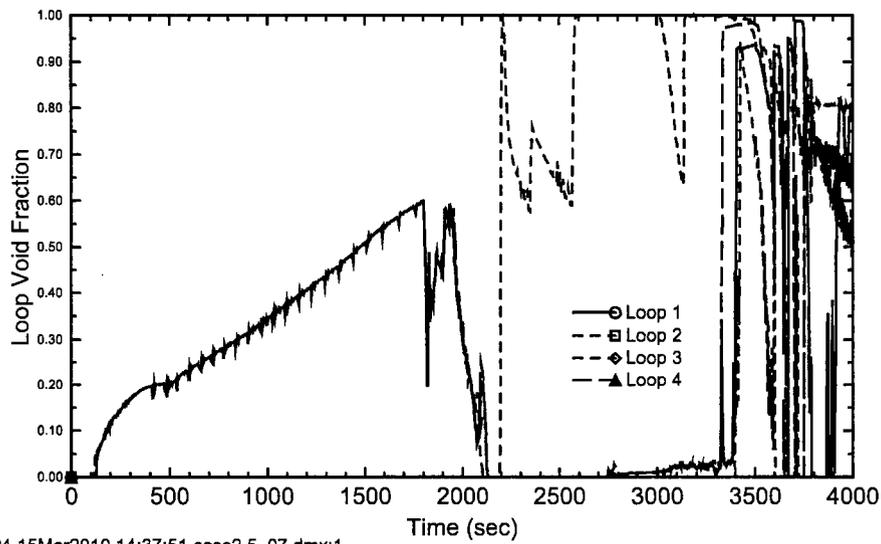


ID:22594 15Mar2010 14:37:51 case2.5\_07.dmx:1

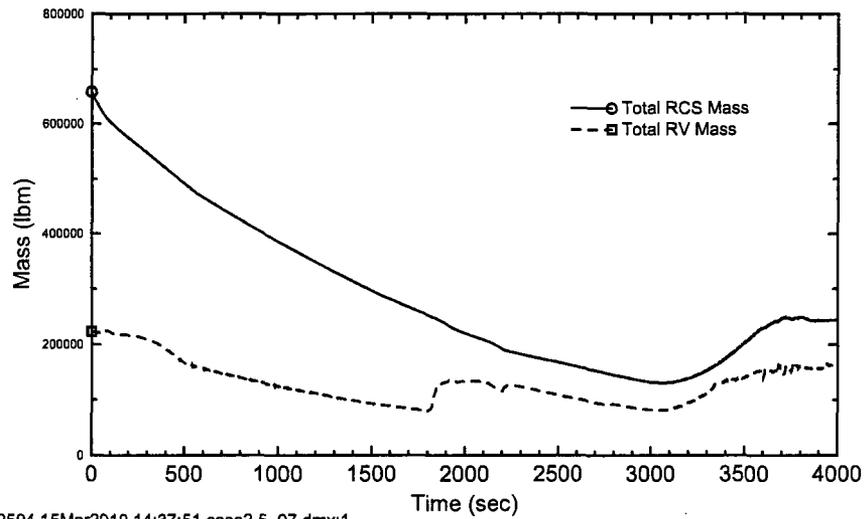
**Figure A.3.7-14—SBLOCA 2.5 inch diameter Break: EFW System  
Mass Flow Rate**



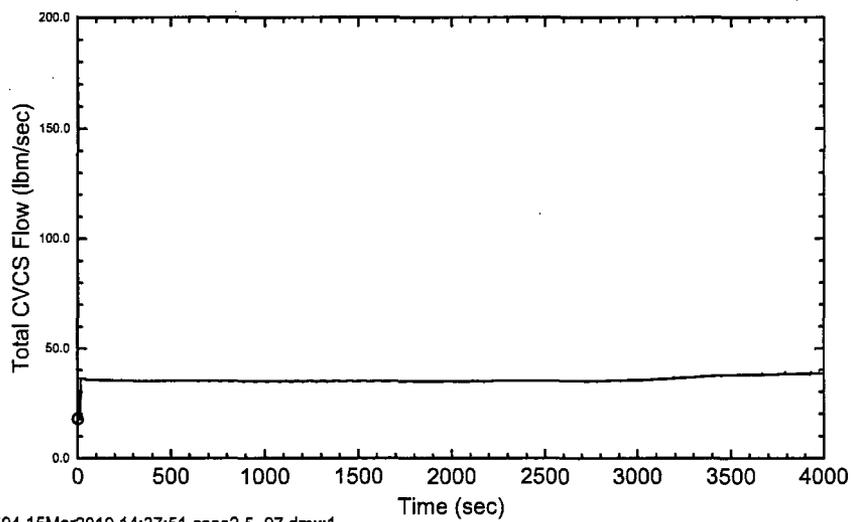
**Figure A.3.7-15—SBLOCA 2.5 inch diameter Break: Loop Seal Void Fraction**



**Figure A.3.7-16—SBLOCA 2.5 inch diameter Break: RCS/ RV Mass Inventory**



**Figure A.3.7-17—SBLOCA 2.5 inch diameter Break: Chemical and Volume Control System Flow Rate**



### **A.3.8 Containment Integrity**

The U.S. EPR FSAR analysis analyzes a spectrum of pipe breaks inside containment to demonstrate containment integrity is maintained. Criterion applied in the U.S. EPR FSAR analysis are that the design pressure and temperature of the containment structure (62 psig and 338°F) are not exceeded. As discussed in Section A.2.4, the ultimate strength of the containment structure exceeds the stated design pressure by a factor of 2.52. Therefore, in this D3 analysis, if containment pressure remains below 2.52 times design pressure, the conclusion is containment integrity is maintained. Pipe breaks in the RCS, main steam system, and main feedwater system are considered. Feedwater line breaks are bounded by ~~main steam line break~~MSLBs.

#### **A.3.8.1 LOCA Inside Containment**

To maximize the containment peak pressure and temperature response, the U.S. EPR FSAR LOCA containment analysis uses conservative assumptions that maximize the mass and energy released from the RCS to the containment atmosphere. These assumptions maximize the primary system inventory, the heat into the RCS, and transfer of mass and energy into containment. In the event of an SWCCF in the PS, the DAS includes comparable functions to trip the reactor and initiate safety injection. Therefore, the mass and energy released into containment during a LBLOCA event is not significantly different from the U.S. EPR FSAR analysis. In fact, under best estimate conditions, the mass and energy released into containment is less than assumed in the U.S. EPR FSAR analysis. DAS also includes opening of the hydrogen mixing dampers to assure that the containment atmosphere remains well mixed. As noted in Section A.3.7.3.1, manual SI hot leg switchover is a required action to support the containment response. The ability to manually switch SI to the hot legs is available outside the PS and is available in the event of an SWCCF in the PS.

Therefore, from the standpoint of the peak containment pressure and temperature response, the U.S. EPR FSAR analysis is bounding, and no further analysis is required. Therefore, the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS during LBLOCA Inside Containment events.

### A.3.8.2 MSLB inside containment

~~An main steam line break~~MSLB inside containment results in the release of high energy fluid to the containment atmosphere. The mass and energy release following an MSLB depends on the configuration of the main steam system, the containment design, the ~~protection system~~PS features, plant operating conditions, and the break size. The major factors that influence the mass and energy release following an MSLB include ~~steam generator~~SG fluid inventory, MFW isolation, main steam line isolation, and EFW operation.

It is important to isolate MFW to prevent extended energy loss into containment. It is also important to close the MSIVs to prevent the extended blowdown of the intact SGs through the break. The U.S. EPR FSAR analysis isolates MFW and main steam on high SG pressure drop. In the case of an SWCCF in the PS, DAS isolates the MFW and main steam on low SG pressure. These isolation functions are comparable to the PS function, but they may result in delayed isolation, for some break sizes. In those cases, the peak containment pressure may slightly exceed the design pressure. However, containment integrity is maintained, because the ultimate strength of the containment structure far exceeds the design pressure and, therefore, the peak pressure for this event.

Therefore, the U.S. EPR design is determined to be adequate in addressing an SWCCF in the PS during an MSLB Inside Containment event.

### A.3.9 Radiological consequences

The analysis of radiological consequences from ~~design basis event~~DBEs is presented in the U.S. EPR FSAR Chapter 15. The specific DBEs evaluated are given in Table A.2-1~~Table A.2-1~~ and are listed below.

- Small line break outside containment.
- LOCA.
- SGTR.
- MSLB.
- FWLB.
- RCP rotor seizure / RCP shaft break.

- RCCA ejection.
- Fuel handling accident (FHA).

The radiological consequence analysis credits certain functions, to limit offsite and control room dose. For events that result in radiological releases inside containment (loss of coolant accident, MSLB, FWLB, and RCCA Ejection), the containment isolation function and associated system activations are credited. The containment isolation function limits offsite dose consequences. For events that result in direct radiological releases outside containment (small line break outside containment, SGTR, MSLB, FWLB, FHA, and RCP rotor seizure / shaft break), isolation of the pathway and the failed fuel fraction are important. Control room dose is also evaluated, for those events where radiological releases occur outside containment. Control room isolation is credited in these DBEs. Conservative bounding assumptions are made in the DBE evaluations to maximize the radiological consequences (e.g., the activity level of the reactor coolant is assumed to be at technical specification limits, bounding failed fuel fractions are applied, a coincident iodine spike is assumed).

In the case of an SWCCF in the PS, the DAS function available (from Table A.2-2) to limit radiological consequences is containment isolation on high activity.

This DAS function provides comparable protection for those events that result in pipe breaks inside containment, and, therefore, the containment is isolated in a timely manner.

For events where the radiological release is outside containment, the required function that limits dose consequences is event-dependent. As long as the failed fuel fractions are not significantly different and the releases are roughly the same duration as the design basis evaluation, the radiological consequences are bounded. Under best estimate assumptions, the radiological consequences are expected to be less than in the U.S. EPR FSAR analysis. A review of the specific events in Section A.3.2 through A.3.7 demonstrates DAS is adequate in maintaining overall plant response within the bounds of the U.S. EPR FSAR analysis, for these events.

Isolation of the main control room (MCR) is required following events with radiological consequences. The events of interest include loss of coolant accident (LOCA), steam generator tube rupture SGTR, main steam line break MSLB, reactor coolant pump RCP locked

rotor, rod ejection, and fuel handling accident. Under normal conditions, the protection system (PS) would automatically actuate the MCR emergency filtration system upon receipt of a high radiation signal in the MCR air intakes or a primary containment isolation signal. In the event of an software common cause failure (SWCCF), automatic isolation of the MCR is assumed to not be available, but the radiation signal and alarms are still present. In each of these scenarios with a SWCCF in the PS, the MCR high radiation air intake alarms would alert the operator that MCR isolation is required. Since the air intakes to the MCR are close to the release point in each scenario, the alarm is expected to occur relatively early in the event (within approximately five minutes). A specific radiological analysis was performed that relies on this alarm function to alert the operator so that the MCR is manually isolated within 30 minutes. Radiological limits are maintained in each of these above events.

In regard to control room dose, the U.S. EPR FSAR analysis credits the isolation and reconfiguration of the MCR HVAC system on high air intake activity. Because DAS does not provide automatic control room isolation, a specific radiological evaluation of postulated events has been performed to determine whether an automatic function to isolate the MCR is required. The evaluation determined that manual isolation of the control room within 30 minutes is sufficient, because the following PS functions are also provided by DAS:

- Containment isolation on high activity.
- Annulus ventilation system actuation on containment isolation.
- Safeguards building HVAC reconfiguration on containment isolation.

Therefore, the radiological consequence criteria of BTP 7-19 are met and the U.S. EPR design is determined adequate determined to be adequate in addressing an SWCCF in the PS during design basis event DBEs.

Emergency response procedures for the U.S. EPR are not developed as a part of Design Certification. It is, however, anticipated that either abnormal operating procedures or emergency operating procedures will include instructions in response to high radiation at the MCR intakes. These instructions will either direct the operator to confirm MCR filtration system actuation or provide for manual isolation. A special D3 coping procedure is not anticipated.

## A.4 CONCLUSION

This appendix summarizes the safety analysis assessment performed to demonstrate the U.S. EPR design's conformance with BTP 7-19 for an SWCCF in the PS. The scope of the assessment covers the U.S. EPR FSAR safety analysis (U.S. EPR FSAR Tier 2, Chapter 15), radiological consequence analysis (U.S. EPR FSAR Tier 2, Chapter 15) and containment analysis (U.S. EPR FSAR Tier 2, Chapter 6). DAS functions are available where needed to replace functionality lost due to the SWCCF in the PS.

The U.S. EPR design, including DAS functions, available plant control systems and manual operator actions are sufficient to satisfy the acceptance criteria of BTP 7-19 for an SWCCF in the PS for design basis event DBEs, which includes AOOs and PAs.

## A.5 REFERENCES

- A-1. U.S. NRC, NUREG-800, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," March 2007.
- A-2. AREVA NP Topical Report, ANP-10263PA, Revision 0, "Codes and Methods Applicability Report for U.S. EPR", AREVA NP, August 2007.
- A-3. AREVA NP Topical Report, ANP10278P, Revision 0<sub>1</sub>, "U.S. EPR Realistic Large Break Loss of Coolant Accident", AREVA NP, ~~March 2007~~ January 2010.
- A-4. AREVA NP Topical Report, ANP-10286P, Revision 0, "U.S. EPR Rod Ejection Accident Methodology Topical Report", November 2007.