CCF Coping Analysis

Revision 3

Non-Proprietary

July 2018

REVISION HISTORY

Revision	Date	Page (Sections)	Description
0	November 2014	All	First Issue
1	February 2017	v (List of Tables)	Editorial correction (match the title)
		iv (Acronyms)	Editorial correction (“PAMI” deleted)
		x (Acronyms)	Editorial correction (“QIAS-PAMI” changed to “QIAS-P”)
		3 (3.3)	Description for the manual operator action modified (315-8091)
		4 (4.1)	Editorial correction (“post accident monitoring instrumentation (PAMI)” changed to “P”)
		5 (Figure 4-1)	Figure 4-1 modified to reflect the revised I&C system overview architecture (8281-17)
		8 (Section 4.2.2)	Editorial correction (“with three (3) seconds delay” added)
		10 (4.3)	Description for the manual operator action modified (315-8091)
		10, 21, 40, 43, 44, 45, 51, 52 (4.3, 5.2, 5.3.6.5, 5.4.1.2, 5.4.2.1.2, 5.4.2.2.2, 5.4.2.7.2, 5.4.2.8.2)	Reference number changed due to the deletion of Reference related operator action (Reference 5 changed to 3, 6 changed to 2, 7 changed to 4, 8 changed to 5, 9 changed to 6, 10 changed to 7, 11 changed to 8, 12 changed to 9, 13 changed to 10, 14 changed to 11)
		47 thru 48 (5.4.2.4.2)	Description for the MDNBR point modified based on RAI response (379-8476)
		84 (Figure 5-23)	Editorial correction (“Long term” added)

Revision	Date	Page (Sections)	Description
		85 (Figure 5-24) 107 (7.0)	Editorial correction (“Short term” added) Reference related manual operator action deleted and modified with latest version (November 2009 changed to April 2014) (315-8091)
2	January 2018	10 (4.3) 107 (7.0)	Editorial correction (“immediately” deleted) (315-8091) Reference related D3 TeR modified with latest version (Rev.0 changed to Rev.2)
3	July 2018	5 (Figure 4-1) 107	Figure 4.1-1 modified to reflect the revised I&C System Overview Architecture (RAI 45-7883, Question 07.09-2) TR and TeR issue date revised.

ABSTRACT

This document provides the methodology and results of common-cause failure (CCF) coping analysis for the Advanced Power Reactor 1400 (APR1400).

CCF coping analysis is performed based on Nuclear Regulatory Commission (NRC) requirements stated in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19 for all anticipated operational occurrences (AOOs) and postulated accidents (PAs) in the design controlled document (DCD) chapter 15 safety analyses. The CCF in the digital safety instrumentation and control (I&C) systems is assumed to exist before each initiating event occurs and, the safety systems affected by the CCF are assumed to be unable to actuate their safety functions during the event. But the systems which are diverse from the safety I&C systems or not affected by the CCF are credited in the CCF coping analysis.

The evaluation is performed in two steps. In the first step, the evaluation is qualitatively performed based on the characteristics and the sequence of events, available and unavailable design features. Some events can be identified in this step for the further quantitative analysis in detail. In the second step, the events selected in the previous step are quantitatively analyzed using computer codes to evaluate the conformance of the acceptance criteria.

In summary, the realistic evaluations of the plant response to the initiating events analyzed in the APR1400 DCD chapter 15 with a CCF in the digital safety I&C systems demonstrate that the integrities of the reactor coolant system pressure boundary and the containment pressure boundary are maintained, and the resulting radiological releases do not exceed the applicable acceptance criteria.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

AC	alternating current
ADV	atmospheric dump valve
AFAS	auxiliary feedwater actuation signal
AFWS	auxiliary feedwater system
AOO	anticipated operational occurrence
AOPM	available over power margin
APR1400	Advanced Power Reactor 1400
ARP	alarm response procedure
ATWS	anticipated transients without scram
BTP	Branch Technical Position
CCF	common-cause failure
CEA	control element assembly
CEDM	control element drive mechanisms
CHF	critical heat flux
CIAS	containment isolation actuation signal
CIM	component interface module
COLSS	core operating limit supervisory system
CPC	core protection calculator
CPCS	core protection calculator system
CPIAS	containment purge isolation actuation signal
CREVAS	control room emergency ventilation actuation signal
CSAS	containment spray actuation signal
CVCS	chemical and volume control system
D3	diversity and defense-in-depth
DAS	diverse actuation system
DBE	design basis event
DC	design certification
DCD	design control document
DCS	distributed control system
DIS	diverse indication system
DMA	diverse manual engineered safety feature actuation
DNBR	departure from nucleate boiling ratio
DPS	diverse protection system
DRCS	digital rod control system
EAB	exclusion area boundary

ECCS	emergency core cooling system
EOP	emergency operating procedure
ESF	engineered safety feature
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety feature - component control system
FPD	flat panel display
FHEVAS	fuel handling area emergency ventilation actuation signal
FLB	feedwater line break
FWCS	feedwater control system
HFE	human factor engineering
HPPT	high pressurizer pressure trip
HSI	human-system interface
HVAC	heating, ventilating and air conditioning
I&C	instrumentation and control
IFWF	increase in feedwater flow
IOSGADV	inadvertent opening of an atmospheric dump valve
IPS	information processing system
KEPCO	Korea Electric Power Corporation
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
LBLOCA	large break loss of coolant accident
LDP	large display panel
LOCA	loss of coolant accident
LOCV	loss of condenser vacuum
LPZ	low population zone
MCR	main control room
MFIV	main feedwater isolation valve
MG	motor-generator
MSIV	main steam isolation valve
MSIS	main steam isolation signal
MSSV	main steam safety valve
NPCS	nuclear steam supply system process control system
NR	narrow range
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
PA	postulated accident
P-CCS	process - component control system

PCS	power control system
PLC	programmable logic controller
PLCS	pressurizer level control system
POSRV	pilot operated safety and relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
PZR	pressurizer
QIAS-N	qualified indication and alarm system - non-safety
QIAS-P	qualified indication and alarm system - P
RCGVS	reactor coolant gas vent system
RCP	reactor coolant pump
RCS	reactor coolant system
ROPM	required over power margin
RPCS	reactor power cutback system
RPS	reactor protection system
RRS	reactor regulating system
RSR	remote shutdown room
SAR	safety analysis report
SAFDL	specified acceptable fuel design limit
SBCS	steam bypass control system
SBLOCA	small break loss of coolant accident
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SIS	safety injection system
SIAS	safety injection actuation signal
SIT	safety injection tank
SLB	steam line break
SRP	Standard Review Plan
SRM	staff requirements memorandum
TBV	turbine bypass valve
TLRCF	total loss of reactor coolant flow
WR	wide range

Page intentionally blank

1. PURPOSE

The purpose of this document is to provide the results of the analysis performed using realistic methods for all initiating events analyzed in the Advanced Power Reactor 1400 (APR1400) design control documents (DCD) chapter 15 with a postulated common-cause failure (CCF) in the digital safety instrumentation and control (I&C) systems. The results demonstrate that adequate diversity exists within the plant I&C system such that the applicable acceptance criteria are met.

2. SCOPE

This document describes the methods and results of the CCF coping analysis for the initiating events in the DCD Chapters 15 with a postulated CCF in the digital safety I&C systems. It is conservatively assumed in the analysis that all safety functions implemented on the common safety platform fail due to a postulated CCF, while the automatic actuations, controls and indications implemented on diverse platform(s) operate as designed.

The detailed description of diverse I&C systems, diversity and defense-in-depth (D3) analysis are not the scope of this document and provided in separate reports (Reference 1).

3. APPLICABLE CODES AND REGULATIONS

This section describes the compliance of the CCF coping analysis with the applicable codes and regulations.

3.1 Code of Federal Regulations

- 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients Without Scram”.

  The diverse protection system (DPS) and its related equipment are provided to mitigate the effects of an anticipated operational occurrence (AOO) followed by the failure of the reactor trip portion of the protection system.

- 10 CFR 52.47(a)(2)(iv) provides guideline values of radiation dose for design certification (DC) applicants.

  The offsite radiological consequences evaluated in Section 5 are within the acceptance criteria specified in this code.

3.2 Staff Requirements Memorandum (SRM)

- SRM on SECY-93-087, Item II.Q, “Defense against Common-Mode Failures in Digital Instrumentation and Control Systems”.

  Each postulated CCF for each event is evaluated in the accident analysis section of the safety analysis report (SAR) using realistic assumptions and methods. Adequate diversity within the APR1400 design for each of these events is demonstrated.

3.3 Standard Review Plan (SRP)

- SRP Branch Technical Position (BTP) 7-19, “Guideline for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems”.

  The events in SAR Chapter 15 are evaluated and analyzed with realistic assumptions and methods. The acceptance criteria provided in this guide are used when performing the evaluation. Diverse actuation system (DAS) and control systems are credited in the evaluation since they are independent from the CCF in the safety I&C system.

- SRP Appendix 18-A, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses”.

- After the occurrence of a DBE concurrent with a postulated CCF in the safety I&C systems, the operator will take appropriate actions to mitigate the CCF event. These operator actions are evaluated according to NUREG-0800, Appendix 18-A (Reference 2). However, the licensing analysis for a DBE with a postulated CCF in the safety I&C systems does not credit any operator action conservatively until 30 minutes after event initiation.

4. BASES FOR THE EVALUATION

4.1 Overall I&C System

As shown in Figure 4-1, the APR1400 I&C system consists of the protection & safety monitoring systems, control & non-safety monitoring systems, diverse systems and human-system interfaces (HSI) in the main control room (MCR) and remote shutdown room (RSR).

The I&C system uses full digital technology, and limited number of hardware switches are installed to meet the safety I&C system design criteria in IEEE standard 603-1991. The safety systems are based on a common programmable logic controller (PLC) platform which has been dedicated for nuclear applications. The safety systems implemented on the common PLC platform consist of the plant protection system (PPS), engineered safety feature-component control system (ESF-CCS), core protection calculator system (CPCS) and qualified indication and alarm system-P (QIAS-P). The qualified indication and alarm system–non-safety (QIAS–N) is also implemented on the common PLC platform even though it is a non-safety system.

Most of the non-safety I&C systems are implemented in a distributed control system (DCS) based common platform. The non-safety systems implemented in the DCS are the power control system (PCS), nuclear steam supply system (NSSS) process control system (NPCS), process–component control system (P-CCS). The DPS is independent from the protection systems such as PPS and ESF-CCS in aspects of trip mechanism, hardware and software. In addition to the DPS, the hardwired diverse manual engineered safety feature (ESF) actuation (DMA) switches, manual reactor trip switches and diverse indication system (DIS) are provided to cope with CCFs of the safety I&C systems. Further specific descriptions of diversity and defense-in-depth of the APR1400 I&C systems are provided in Reference 1.

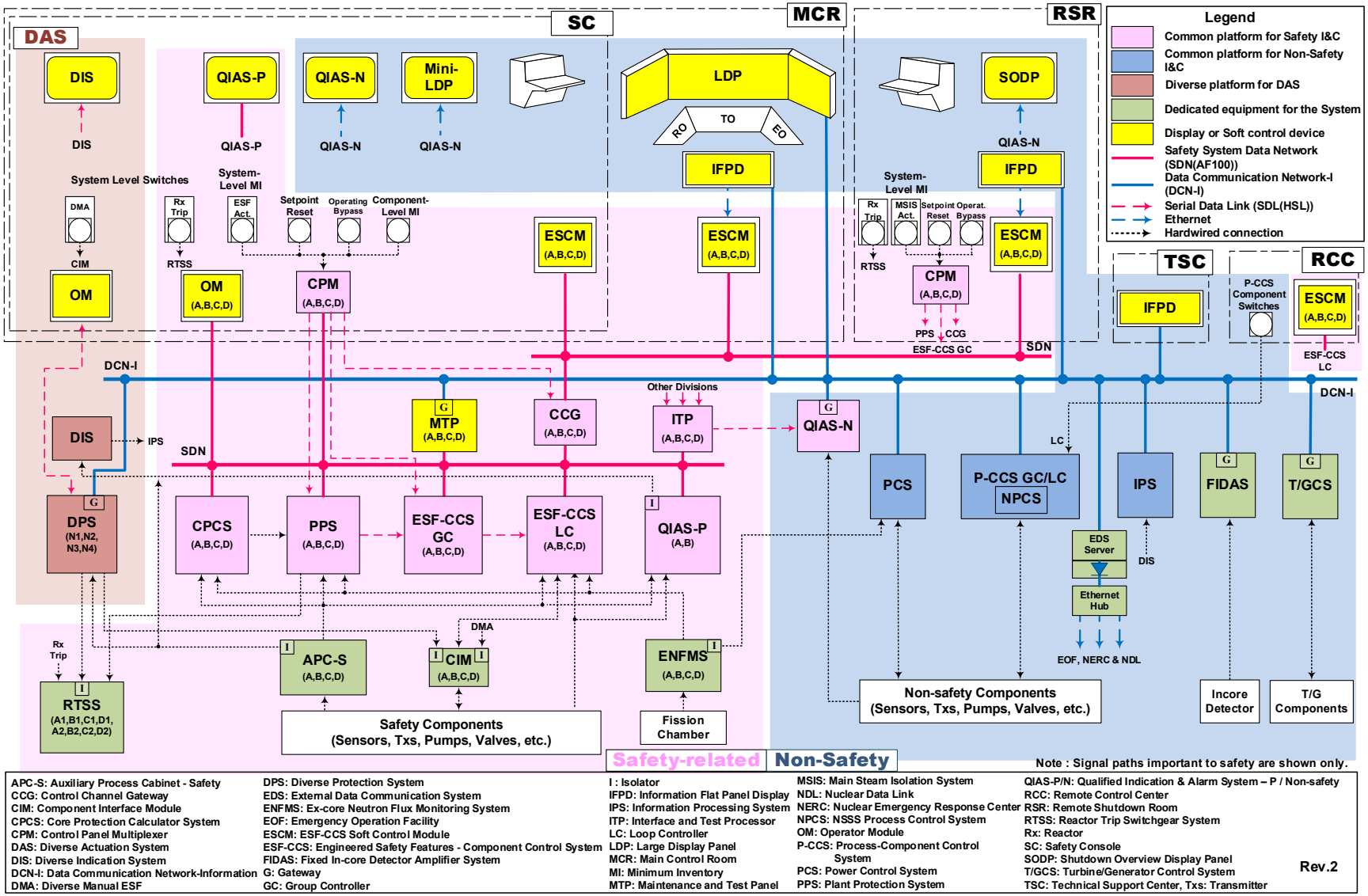

Figure 4-1 Overview of APR1400 I&C System Architecture

4.2 I&C Information for CCF Coping Analysis

It is assumed that a CCF in the common PLC safety I&C platform causes a complete failure of all safety functions of the digital safety I&C systems. This bounding approach provides adequate conservatism in the CCF coping analysis.

4.2.1 Unavailable I&C Functions

The postulated CCF prevents the digital safety I&C systems from providing any actuation or control of their associated safety equipment. Digital safety I&C systems include PPS, ESF-CCS, CPCS, and QIAS-P. The following automatic PPS and ESF-CCS safety functions are assumed to be unavailable.

- Reactor trip
- Safety injection (SI) actuation
- Containment isolation actuation
- Containment spray actuation
- Main steam isolation actuation
- Auxiliary feedwater actuation

Also, the following systems which are not diverse from the digital safety I&C systems are assumed to be affected by the CCF, and therefore they fail to receive signals through the ESF-CCS as a result of the postulated CCF.

- Atmospheric dump valves
- Shutdown cooling system (safety-grade portions)
- Component cooling water (safety-grade portions)
- Service water (safety-grade portions)
- Heating, ventilating and air conditioning (HVAC) (safety-grade portions)
- Emergency diesel generators
- Fuel handling area emergency ventilation actuation signal (FHEVAS)
- Containment purge isolation actuation signal (CPIAS)
- Control room emergency ventilation actuation signal (CREVAS)

The data from the systems other than safety systems remain valid and are processed for information processing system (IPS) display and alarm which are still available to the operators. However, since QIAS-N is also implemented on the common PLC platform even though it is a non-safety system, the postulated CCF causes the data passed to the QIAS-N to be invalid; and therefore not valid for use by the operators.

4.2.2 Available I&C Functions

A number of plant I&C systems have hardware and software diversity from the systems affected by the CCF, and their plant operation functions are thus available to mitigate the effects of an event with CCF. The followings are diverse plant functions and systems that remain available after the CCF in the safety I&C systems:

- Diverse protection system
- Diverse indication system
- Auxiliary process cabinet (both safety and non-safety)
- Process-component control system (both automatic and manual functions)
    - Component cooling water system (non-safety portions only)
    - Heating, ventilation and air conditioning (non-safety portions only)
    - Turbine generator auxiliaries
    - Electrical distribution system
    - Gas turbine generators
    - Steam bypass control system (SBCS)
    - Feedwater control system (FWCS)
    - Chemical and volume control system (CVCS)
    - Pressurizer level control system (PLCS)
    - Pressurizer pressure control system (PPCS)
    - Reactor power cutback system (RPCS)
    - Reactor regulating system (RRS)
    - Digital rod control system (DRCS)
    - Main steam system (non-safety portions)
- Manual reactor trip (in the MCR/RSR)
- Diverse manual ESF actuation switch
- Local manual actions (at the local equipment)
- Indications, displays and alarms provided in the IPS

The non-safety control systems such as PCS, NPCS and P-CCS are implemented on the common non-safety platform which is based on a DCS. The PCS consists of RRS, DRCS and RPCS while NPCS

includes FWCS, SBCS, PPCS and PLCS. Since the DCS based common non-safety platform is independent from the common PLC safety I&C platform, the non-safety control systems are available for the mitigation of the DBEs with a postulated CCF of the safety I&C systems.

The DPS augments the PPS for reduction of risk from the anticipated transient without scram (ATWS) events. The DPS design includes a reactor trip, auxiliary feedwater actuation and safety injection. In addition, a turbine trip is automatically initiated with three (3) seconds delay under conditions of reactor trip from either the PPS or DPS. These diverse functions of the DPS provide not only a significant decrease of the risk due to the ATWS events but also the mitigation of the effects of DBEs with a postulated CCF of the safety I&C systems.

The DMA switches are provided to permit the operator to actuate ESF systems from the MCR after a postulated CCF of the safety I&C system. To achieve system-level actuation independently and diversely from the ESF-CCS, the DMA switches are connected to the lowest level in the ESF-CCS architecture.

The DMA switches provide protection against CCF of PPS and ESF-CCS implemented in accordance with BTP 7-19 requirement of SRP. These DMA switches are implemented by manual, system level hardwired switches to manage the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity, addressed in SRP BTP 7-19.

The DMA switches consist of following switches for system level actuation:

- Safety injection (2 trains)
- Containment spray
- Auxiliary feedwater (each steam generator (SG))
- Main steam isolation (each SG)
- Containment isolation
- Letdown isolation

To achieve system-level actuation at the lowest level in ESF-CCS architecture, the switches are hardwired to the lowest level. In addition, to ensure the system-level actuation, the split devices are provided for receiving the actuation signal from DMA switches and performing fan-out control to the lowest level in ESF-CCS. To implement adequate diversity for digital I&C system application, the DMA switches are hardwired to component interface module (CIM) which is downstream of the ESF-CCS loop controller outputs. The CIM is designed with independent and diverse hardware from the ESF-CCS. The CIM is a non-software-based qualified nuclear safety grade module. Therefore the CIM is not subjected to the same CCF with ESF-CCS which is implemented by qualified PLC platform. The CIM provides the priority logic function between ESF-CCS actuation signals and DMA switch signals and also provides the interface function from the ESF-CCS to the plant component.

Command inputs to open or close a valve, or to open or close a switchgear for rotating devices (e.g., pumps and fans), are received from three sources to the CIM; two I&C subsystem (ESF-CCS and DPS) commands and DMA switches. The ESF-CCS commands to Port X in the CIM are terminated, and diverse actuation commands from the DPS to Port Y in the CIM are terminated. Commands from the DMA switches are received at Port Z in the CIM by a hardwired connection.

For normal or accident condition except CCF, each command is generated by a logical OR of the demand from the ESF-CCS with the demand from the DPS. When the resulting signals conflict (e.g., open vs. close), the outputs are driven to the safe state which is selectable on a component basis. The DMA switch

signal blocks the command from ESF-CCS and DPS.

For the CIM priority the Port Z input for the DMA switch command is not intended to be the “normal” manual control for ESF components. Such normal control should be done through the ESF-CCS or DPS where the appropriate relationship to automatic control, operational modes, interlocks, etc. can be established. The DMA switch is required principally for the purpose of diversity and defense in depth following a postulated software CCF in the ESF-CCS and PPS. This establishes the basis for its high priority. However, there is nothing that will prevent the operators or maintenance personnel from using Port Z for some other function, manual or automatic, that is suited to its design.

The DMA switches located on safety console in MCR, and the display and control means are independent and diverse from the digital equipment such as PPS and ESF-CCS.

The DMA switch is designed to achieve the required plant equipment state for mitigation of the postulated accident conditions. No design provision has been made to give the operator ability to return the plant equipment to the original state the equipment was in prior to the accident. If the operator has to perform this task, it has to be done using local controls including the CIMs. This is again to make the DMA control design to be most direct and as simple and minimal as possible.

- Manual closure of affected main steam isolation valve (MSIV) (SG isolation)

  Manual closure of the MSIV is required after 30 minutes of the accident coupled with a complete loss of PPS/ESF-CCS due to the postulated software CCF for the main steam line break accident outside the containment. Since the break could occur on any of the four main steam lines (steam line 1A, 1B, 2A and 2B), DMA-main steam isolation signal (MSIS) switch has the capability to close all four MSIVs.

  MSIV bypass valves (MS-V011, 012, 013, 014) are normally closed valves with a fail safe mode of fail closed. Since it is assumed that the software failure would manifest itself as fail-as-is, these normally closed valves will remain closed at the onset of the software CCF. Therefore these valves would not require to be closed with a manual DMA switch.

- Manual closure of containment and letdown isolation

  DMA-containment isolation actuation signal (CIAS) switch has capability to close isolation valves for containment and letdown isolation at system level.

- Primary pressure reduction using pilot operated safety and relief valve (POSRV) and reactor coolant gas vent system (RCGVS)

  Recovery equipment is for the normal hot shutdown after the initial design basis accident mitigation and will be commonly applicable for all the design basis accidents. However, all may not be required for each DBE.

  The manual control switches for POSRV and RCGVS are not listed on DMA switches. To manipulate these equipment are required to operate at the CIM in the I&C equipment room. There are local control switches in the CIM.

- Manual open/closure of atmospheric dump valve (ADV)

  The operation procedure of ADV is the same as that of POSRV and RCGVS. The ADV is required to operate at the CIM in the I&C equipment room. There are local control switches in the CIM.

- Manual actuation of auxiliary feedwater system (AFWS)

The DPS is outside of PPS and ESF-CCS and will not be affected by the postulated software CCF. Therefore, manual actuation of the AFWS equipment is not required. However, capability of manual actuation of the required AFWS equipment is provided as part of the DMA design. The motor-driven auxiliary feedwater (AFW) pumps are assumed to be available for manual actuation during the postulated software CCF because the steam supply to the turbine-driven AFW pump might not be assured depending on the break location. Each motor-driven pump is sized to supply full rated flow required by each steam generator.

Manual modulating control of the AFW control valve requires a hardwired manual station. One hardwired manual station is currently planned for each modulating control valve and this controller is used for the DPS operation if needed. This manual station is to be shared for the DMA control. The manual station output signal will be provided directly to the valve operator, thus bypassing ESF-CCS.

- Manual operation of safety injection system pumps and valves

  DMA-safety injection actuation signal (SIAS) switch has capability to start safety injection pumps at system level during the loss of coolant accident (LOCA). Also SI valves are opened to initiate SI flow by DMA-SIAS switch at system level. Reactor coolant pump (RCP) which is non-safety equipment is stopped by IPS flat panel display (FPD) and P-CCS. These devices are assumed available according to realistic method approach.

  In addition, selected safety injection system valves are to be closed with DMA actuation. The valves are not directly involved in the mitigation of accidents that require safety injection, but provide minor peripheral support functions during a normal plant operation such as fill, drain, leakage isolation, etc. Included valves are safety injection tank (SIT) fill and drain valves, hot leg check valve leakage line isolation valve and SIT injection line check valve leakage line isolation valves. All these valves are normally closed valves with a fail-safe mode of fail closed. It is assumed that the software failure would cause the system to fail-as-is and the normally closed valves will remain closed at the onset of the software CCF. Therefore these valves would not require to be closed manually.

The DIS is designed to provide the information necessary to monitor the critical safety functions under the CCF of the safety I&C systems. For this purpose, the DIS receives field input signals through signal splitters/isolators before they get into safety I&C systems. Hardwired signal communication provided by the DIS displays would not be affected by the CCF. The DIS displays the information required for operators to maintain the plant in a safe shutdown condition, under the CCF of the safety I&C system with an initiating event.

4.3 Operator Actions

Manual operator actions can be credited as a diverse means to cope with AOOs and postulated accidents (PAs) with a CCF in the safety I&C systems as mentioned in Reference 3. If the operator actions are credited as a diverse means, the required and available operator action time should be evaluated and justified based on the HFE methodology described in Reference 2.

After the occurrence of a DBE concurrent with a postulated CCF in the safety I&C systems, the operator will take appropriate actions to mitigate the CCF event. These operator actions are evaluated according to NUREG-0800, Appendix 18-A (Reference 2).

In the CCF coping analysis for the APR1400 design, the operator actions to mitigate a DBE with a postulated CCF in the safety I&C systems have been delayed until 30 minutes after event initiation, which is considered to be conservative since the IPS or large display panel (LDP) will provide several alarms much earlier than 30 minutes after an event occurs, and the operators will take appropriate actions based

on the relevant alarm response procedures (ARPs). At about 30 minutes after an event initiation, the major operating parameters are generally expected to be on a mildly changing condition or a nearly quasi-steady state condition without any abrupt transients. Therefore, it would be reasonable that the operators can take decision-making process and operator action steps based on the emergency operating procedures (EOPs) and the available indications and controls as mentioned in section 4.2.2. The operators will keep controlling and cooling down the plant until a safe shutdown condition (i.e., hot shutdown condition) is reached.

The long term manual operation to reach a cold shutdown condition is beyond the scope of this report. For the selected events which are considered to be limiting among all of the DBEs, the available information to the operators are provided in Table 4-1. It should be noted that all of the available information to the operators are not included in the table.

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (1 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
1. Increase in Feedwater flow	·Reactivity control -Alarms High core power rate DNBR[1)] -Indication Core power RCS[2)] inlet temperature Control rod bottom contact	 IPS IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR[3)]) IPS	Safety injection
	·RCS heat removal -Alarm High core power rate High SG level -Indication Core power SG level SG pressure Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature	 IPS IPS, LDP IPS, LDP, DIS IPS,LDP, DIS LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR)	Auxiliary feedwater
	·RCS pressure control -Alarm Low PZR pressure -Indication PZR[4)] pressure	 IPS, LDP IPS(NR[5)]), LDP(NR), DIS(WR)	-

1) departure from nucleate boiling ratio (DNBR)

2) reactor coolant system (RCS)

3) wide range (WR)

4) pressurizer (PZR)

5) narrow range (NR)

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (2 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
2. Main Steam Line Break Outside Containment	·Reactivity control -Alarms High core power rate DNBR -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm High core power rate -Indication Core power SG level SG pressure Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature	 IPS IPS, LDP, DIS IPS, LDP, DIS LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR)	Auxiliary feedwater
	·RCS pressure control -Alarm Low PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (3 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
3. Total loss of Flow	·Reactivity control -Alarm DNBR -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm High RCS outlet temperature -Indication Core power SG level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature RCP status	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR) IPS	Auxiliary feedwater
	·RCS pressure control -Alarm High PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (4 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
4a. RCP Shaft Seizure	·Reactivity control -Alarm DNBR -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm High RCS outlet temperature -Indication Core power SG level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature RCP status	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR) IPS	Auxiliary feedwater
	·RCS pressure control -Alarm High PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-
4b. RCP Shaft Break	Same as the RCP Shaft Seizure		

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (5 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
5a. CEA Ejection without Primary System Rupture	·Reactivity control -Alarms High core power rate DNBR -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm High RCS outlet temperature -Indication Core power SG level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR)	Auxiliary feedwater
	·RCS pressure control -Alarm High PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-
5b. CEA Ejection With Primary System Rupture	Same as the Loss of Coolant Accident		

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (6 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
6. Steam Generator Tube Rupture	·Reactivity control -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm Low PZR level High SG level -Indication Core power SG level SG pressure PZR level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature Subcooling margin	 IPS, LDP IPS, LDP IPS, LDP, DIS IPS, LDP, DIS LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR) LDP, DIS	Auxiliary feedwater
	·RCS pressure control -Alarm Low PZR pressure High SG level -Indication PZR pressure SG level	 IPS, LDP IPS, LDP IPS(NR), LDP(NR), DIS(WR) IPS, LDP, DIS	-
	. Radioactivity Control -Alarms Main steam line(N-16) Radiation -Indication Main steam line(N-16) Radiation	 IPS IPS	Main steam isolation Containment isolation

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (7 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
7. Loss of Coolant Accident	·Reactivity control -Alarm DNBR -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm Low PZR level -Indication Core power SG level SG pressure PZR level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature Subcooling margin	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR) DIS	Auxiliary feedwater
	·RCS pressure control -Alarm Low PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-
	. Containment pressure control -Alarms High containment pressure -Indication Containment pressure Containment temperature	 IPS, LDP IPS, LDP, DIS DIS	Containment spray Containment isolation

Table 4-1 Key Available Information for Operators for DBEs with a CCF in Digital Safety I&C Systems (8 of 8)

Event	Alarms and Indications Available	Available Systems in Non-Safety Platforms	Available DMA Switches
8. Steam Line Break Inside Containment	·Reactivity control -Alarm High core power rate -Indication Core power RCS inlet temperature Control rod bottom contact	 IPS IPS, LDP, DIS IPS, LDP, DIS(WR) IPS	Safety injection
	·RCS heat removal -Alarm Low PZR level -Indication Core power SG level SG pressure PZR level Feedwater flow RCS flow RCS outlet temperature RCS inlet temperature Subcooling margin	 IPS, LDP IPS, LDP, DIS IPS, LDP, DIS LDP, DIS IPS, LDP, DIS IPS, LDP, DIS IPS, LDP IPS, LDP, DIS(WR) IPS, LDP, DIS(WR) DIS	Auxiliary feedwater
	·RCS pressure control -Alarm Low PZR pressure -Indication PZR pressure	 IPS, LDP IPS(NR), LDP(NR), DIS(WR)	-
	. Containment pressure control -Alarms High containment pressure -Indication Containment pressure Containment temperature	 IPS, LDP IPS, LDP, DIS DIS	Containment spray Containment isolation

5. CCF COPING ANALYSIS

This section describes the propriety of D3 capability of the APR1400 design by showing that the acceptance criteria required by SRP BTP 7-19 are well met for all AOOs and PAs with a CCF in the safety I&C systems. The CCF is conservatively postulated to exist before the events occur and to prevent the safety I&C systems from providing any mitigating actuation and control of their associated safety equipment.

5.1 Major Assumptions and Initial Conditions

As a first step, a qualitative evaluation is performed for all DBEs based on the unavailable and the available I&C systems and information identified in Section 4.2. If it is concluded that the qualitative evaluation results for a DBE reasonably demonstrate the applicable acceptance criteria are met, no further analysis is required for the DBE. However, if it is judged that the sequence of events for a DBE with a CCF in the safety I&C systems is quite different from that of DCD Chapter 15 and hence the results are unpredictable, an in-depth analysis is needed for the event. The following are the evaluation bases which are different from those applied to the analysis in DCD Chapter 15.

a. A CCF in the digital safety I&C systems is postulated, such that reactor trip from the reactor protection system (RPS) and the engineered safety feature functions from ESF-CCS are not actuated. The failure includes both automatic and manual actuation (except for the hardwired DMA and the hardwired manual reactor trip).

b. Additional independent single failure is not assumed in the evaluation. According to the SRP BTP 7-19, all safety and non-safety systems or components independent from the CCF are assumed to function correctly.

c. Control systems are in the automatic mode to respond as designed, unless the initiating event is the malfunction of the control system or a controlled component within the plant system.

d. Initial conditions for an event are at their nominal values. The nominal or average capacities are assumed when some systems or components are actuated during the event.

e. A CCF in the safety I&C system does not prevent the diverse reactor trip on high pressurizer pressure or high containment pressure and the diverse turbine trip triggered by DPS. The DPS are diverse from the safety I&C system. A proper time delay is assumed from when the monitored parameter exceeds the trip setpoint until the output of the DPS changes state.

f. A CCF in the digital PPS/ESF-CCS does not prevent the auxiliary feedwater and safety injection system actuation functions of the DPS.

g. Hardwired DMA switches at the system level are provided for:

- Safety injection
- Containment isolation, with letdown isolation
- Containment spray
- Auxiliary feedwater
- Main steam and feedwater line isolation

h. Reactor coolant pumps (RCPs) are assumed to be normally operating if offsite power is available.

i. Offsite power is assumed to be available during the event if loss of offsite power is not an initiating event.

j. It is assumed that no operator action is taken during 30 minutes after an event initiation. At 30 minutes after the event, the operators begin to perform manual controls of the plant under the appropriate recovery procedures to achieve a safe shutdown condition. Alarms and indications will be provided via equipment not affected by the CCF in the digital safety I&C systems to support operators to perform a controlled cooldown of the plant. Long term manual operation to reach a safe shutdown condition is beyond the scope of this report.

k. External hazards such as fires, earthquakes, floods and other natural phenomena are not considered in the CCF coping analysis.

5.2 Acceptance Criteria

Acceptance criteria for the CCF evaluation are as given in Reference 3:

- For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding 10% of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.

- For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation releases exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.

5.3 Qualitative Evaluation

The qualitative evaluations are based on the expected safety and control systems functions, each system's capability and the experiences of DBE analysis of DCD Chapter 15 events. From the results of these evaluations, some DBEs with a CCF in the digital safety I&C systems are identified to need further quantitative analyses for confirming their acceptability.

5.3.1 Increase in Heat Removal by the Secondary System

At this category of events, one or more of the following symptoms may be present:

- Abnormal decrease of one or both steam generator pressure.
- Decreasing RCS average temperature caused by the increased RCS heat removal.
- Increased steam generator steam flow and decreased electrical power output prior to the trip.
- Increase in containment temperature, pressure, humidity, and sump level for a steam line break (SLB) inside containment.
- Loud noise or visible steam plume, indicative of a high-energy SLB or the inadvertent opening of an atmospheric dump valve.

5.3.1.1. Decrease in Feedwater Temperature

A feedwater temperature decrease can result from the loss of one of the two high pressure feedwater heater trains. If the feedwater enthalpy decreases, it will cause the reactor coolant temperature, RCS pressure, and the generator pressure to drop while raising the core power due to the negative moderator temperature feedback effect. NSSS control systems such as PPCS, PLCS, and RRS would act to restore changes in major plant parameters in a programmed manner as implemented in those NSSS control systems. If perturbation is large enough to exceed normal controllable range of these NSSS control systems, it will initiate alarms for low pressurizer pressure, low steam generator pressure, and high core power.

The core power increase expected due to the feedwater enthalpy decrease can be calculated by a simple hand calculation using the feedwater system design data.

TS

The hand calculation estimates that the core power would increase up to a stabilized quasi-steady-state value of approximately [ ]^{TS} %. The APR1400 plant is operating with a certain amount of thermal margin which is preset enough to protect fuel damages from AOOs. This means that if the increased reactor power is below the preset required overpower value, fuel failure will not occur. The preset required overpower margin (ROPM) for the APR1400 design is set to [ ]^{TS} %, and determined from the worst event among the DBEs. Since the ROPM is sufficiently higher than the increased power owing to the feedwater temperature decrease, the fuel integrity cannot be affected by this event. Since the RCS temperature becomes lower during the event, the RCS pressure will decrease; and hence the RCS pressure boundary is maintained.

Therefore, it is concluded that no detailed quantitative analysis using computer programs is required for the feedwater temperature decrease event with a CCF in the digital safety I&C systems.

5.3.1.2. Increase in Feedwater Flow

A feedwater flow increase is caused by a spurious SG low level signal, excessive opening of the feedwater control valves, or the increase in feedwater pump speed. The maximum increase of feedwater flow at full power is less than approximately [ ]^{TS} % above nominal flow for the main feedwater system, which is an interface design requirement. A feedwater flow increase results in a feedwater enthalpy decrease.

The decrease in the feedwater enthalpy caused by the increase in feedwater flow can be estimated by a simple hand calculation using a heat balance equation on the high pressure feedwater heaters.

TS

From the results of the hand calculation, it is roughly estimated that the cooldown effect of this event is about [ ]^{TS} % which is higher than that of the decrease in feedwater temperature event because the heat removal effect for this event is the combined effects of feedwater flow increase and feedwater temperature decrease.

It is concluded that a detailed quantitative analysis using computer programs is required for the increase in feedwater flow event with a CCF in the digital safety I&C systems, since the ROPM is not clearly sufficient to cover the estimated increased power due to the combination effects mentioned above.

5.3.1.3. Increased Main Steam Flow

An inadvertently increased opening of the turbine control valves causes an increase in main steam flow. This may be caused by operator error or by turbine load limit malfunctions, and will result in no more than an [ ]^{TS} % increase over the nominal hot full power steam flow rate. Events caused by opening of a turbine bypass valve or atmospheric dump valve are discussed separately in the next section.

The maximum increase of steam flow is identical to that of the inadvertent opening of an atmospheric dump valve (IOSGADV) event. The core power increase in response to the increased main steam flow event is therefore the same as that of the IOSGADV event. Since the preset ROPM is sufficient enough to compensate the increased power due to the increased main steam flow, the fuel integrity cannot be affected by this event. Since the RCS temperature becomes lower during the event, the RCS pressure tends to decrease, and hence the RCS pressure boundary is maintained.

Therefore, it is concluded that no detailed quantitative analysis using computer programs is required for the increased main steam flow event with a CCF in the digital safety I&C systems.

5.3.1.4. Inadvertent Opening of a Steam Generator Relief or Safety Valve

An atmospheric dump valve or a turbine bypass valve may be inadvertently opened by the operator, or may open due to a failure of the control systems that control the valves. A main steam safety valve will remain open only as a result of a mechanical valve failure. The consequences of opening of any of these valves will be similar, relieving steam at the same maximum flow rate which is less than or equal to [ ]^{TS} % of full power steam flow rate. IOSGADV event is evaluated in this section.

The plant parameter inputs for the RRS come from reactor coolant temperature, turbine power, and the core power. If the reactor coolant temperature changes, then the signal of control element assembly (CEA) withdrawal demand, CEA insertion demand, or CEA rate demand is generated by the RRS and delivered to the DRCS. This RRS action is designed to maintain average core coolant temperature at the programmed reference temperature, which is a function of turbine power. Reactor coolant temperature decreases due to an inadvertent opening of a SG ADV even though turbine power does not change. The CEA withdrawal demand signal corresponding to the difference between decreased reactor coolant temperature and the programmed reference temperature will be generated by the RRS. Core power would reach an elevated quasi-steady state level in response to the moderator and fuel temperature feedback effect and the RRS control action. The maximum steam flow through an ADV is restricted to about [ ]^{TS} % of the steam flow at the hot full power condition. Therefore, it is expected that the core power increase due to an inadvertent opening of one ADV would be about [ ]^{TS} %. Since the preset ROPM is sufficient enough to compensate the increased power due to IOSGADV, the fuel integrity cannot be affected by this event. Since the RCS temperature becomes lower during the event, the RCS pressure tends to decrease, and hence the RCS pressure boundary is maintained.

Based on the above evaluation, it is concluded that a detailed quantitative analysis using computer programs is not required for the IOSGADV event with a CCF in the digital safety I&C systems.

5.3.1.5. Steam System Piping Failures Inside and Outside Containment

The steam system piping failure is defined as a pipe break in the main steam system. The steam line break is characterized as a cooldown event due to increased steam flow rate, which causes excessive energy removal from the steam generators and the RCS. This results in a decrease in reactor coolant temperature as well as a decrease in the RCS and steam generator pressure. The cooldown inserts positive reactivity into the core due to negative moderator and Doppler reactivity feedback coefficients. Excessive cooldown can be detected by the following alarms:

- Low pressurizer pressure alarm
- Low steam generator pressure alarm
- High core power rate alarm
- Low steam generator water level alarm

In the SLB analysis presented in the DCD Chapter 15.1.5, reactor trip can be triggered by one of several

reactor trip signals including low steam generator pressure, low pressurizer pressure, low steam generator water level, variable overpower, low departure from nucleate boiling ratio (DNBR) initiated by the CPC, and high containment pressure (for SLBs inside containment only). The ESF functions credited in the SLB analysis in the DCD Chapter 15.1.5 are as follows:

- MSIS on low steam generator pressure (both main steam isolation valves and main feedwater isolation valves are closed on MSIS)
- SIAS on low pressurizer pressure
- Auxiliary feedwater actuation signal (AFAS) on low steam generator water level
- CIAS and containment spray actuation signal (CSAS) on high containment pressure (for SLBs inside containment only).

Should an SLB occur concurrently with a CCF in the digital safety I&C systems, the reactor trip and ESF functions are not actuated except the functions incorporated in the DPS. When the loss of reactor trip functions is caused by the CCF, the core power will rapidly increase due to the moderator temperature feedback effect. The fuel temperature will increase due to the increase in core power. This results in negative reactivity insertion into the core because of negative characteristics of fuel temperature feedback effect. Core power will be stabilized at an elevated value, which is determined by the balance of the reactivity insertion due to moderator and fuel temperature feedback effects.

The SLB inside containment will cause a rapid increase in temperature and pressure within the containment due to the steam released from the ruptured steam generator. In the SLB analysis with respect to mass and energy release described in the DCD Section 6.2, an automatic actuation of the containment spray and main steam isolation prevent containment pressure from rapidly increasing to design limit. However, should the SLB inside containment occur with a CCF in the digital safety I&C systems, the resultant containment pressure increases up to the reactor trip setpoint on DPS. After the trip, operators will then manually close the MSIV, main feedwater isolation valve (MFIV) and actuate the containment spray. These functions are available in the hardwired reactor trip and ESF-CCS backup actuations which are not affected by CCF. Even with these design characteristics, it is determined that detailed quantitative analysis with respect to containment integrity is required for the SLB inside containment.

Based on the above evaluations, it is expected that the consequences for the SLB with a CCF can be worse than that for the case presented in the DCD Sections 6.2 and 15.1.5. Therefore, it is concluded that a detailed quantitative analysis using computer programs is required for the SLB inside and outside containment with a CCF in the digital safety I&C systems.

5.3.2 Decrease in Heat Removal by the Secondary System

At this class of events, any one or more of the following symptoms may be present:

- Decreasing steam generator water level
- Increasing steam generator pressure
- Increasing RCS pressure and temperature
- Low main feedwater flow or loss of main feedwater supply

5.3.2.1. Loss of External Load

The most severe loss of external load event is caused by the disconnection of the turbine-generator from the electrical distribution grid resulting in a turbine trip. It is assumed in the loss of external load analysis for the DCD Chapter 15.2 that the NSSS control systems such as SBCS, RPCS, RRS, PPCS, and PLCS are in manual mode when the event occurs. The decrease in heat removal capability of the secondary system caused by turbine trip will trigger the reactor trip on high pressurizer pressure.

Even though a CCF in the digital safety I&C systems occurs, the NSSS control systems mentioned above will be operated normally. The normal actuation of these NSSS control systems will accommodate the load rejection without necessitating reactor trip and opening of primary and secondary safety valves. The sequence of events for the loss of full external load is very similar to the turbine trip event analyzed with respect to the plant performance, in which nominal initial conditions are assumed, and normal operation of all the NSSS control systems are credited. Moreover, even if the NSSS control systems were conservatively assumed to be in the manual mode, the acceptance criteria for the integrity of the RCS would be met by the DPS reactor trip function on high pressurizer pressure.

Based on the above evaluation, it is concluded that no detailed quantitative analysis using computer programs is required for the loss of load event with a CCF in the digital safety I&C systems.

5.3.2.2. Turbine Trip

A turbine trip may result from a number of conditions which cause the turbine-generator trip system to initiate a turbine trip signal, causing closure of the turbine stop valves and control valves. This event is the same in effect as the loss of full load event described in the above section.

Therefore, it is concluded that no detailed quantitative analysis is required for the turbine trip event with a CCF in the digital safety I&C systems.

5.3.2.3. Loss of Condenser Vacuum

A loss of condenser vacuum (LOCV) may occur due to the failure of the water circulation system to supply cooling water, failure of the main condenser evacuation system to remove noncondensible gases, or excessive air in-leakage. The turbine is assumed to trip immediately on low condenser vacuum.

If condenser vacuum is lost, all turbine bypass valves (TBVs) connected to condenser are unavailable. The RPCS would receive a signal from the SBCS to reduce reactor power by simultaneous drop of one or more selected full strength CEA groups into the reactor core.

The rate of increase in the RCS pressure in the LOCV with a CCF in the digital safety I&C systems is slower than that of the LOCV presented in the DCD Chapter 15.2 due to the normal operation of various NSSS control systems. The normal operation of PPCS and PLCS would reduce the increasing rate of the RCS pressure. When the steam generator level is lowered to the actuation setpoint, an auxiliary

feedwater actuation signal would be generated by the DPS, which is not affected by the CCF in the digital safety I&C systems. The core power would be a lowered value due to the RPCS control action, which will alleviate the increasing RCS pressure.

If the RCS pressure increases to high pressurizer pressure trip setpoint despite the various mitigating design features mentioned above, the trip signal on high pressurizer pressure would be generated by the DPS. This ensures that the acceptance criteria with respect to RCS integrity can be met for the LOCV event with a CCF in the digital safety I&C systems.

Therefore, it is concluded that no detailed quantitative analysis is required for the loss of condenser vacuum with a CCF in the digital safety I&C systems.

5.3.2.4. Main Steam Isolation Valve Closure

The MSIV closure event is initiated by the closure of all MSIV's due to a spurious closure signal. Due to the termination of steam supply to the turbine driven main feedwater pumps, the main feedwater pumps would trip immediately after all the MSIVs are closed. The sequence of this event is very similar to the LOCV event described in the previous section.

Therefore, it is concluded that no detailed quantitative analysis is required for the MSIV closure event with a CCF in the digital safety I&C systems.

5.3.2.5. Steam Pressure Regulator Failure

This event does not apply to the APR1400 design.

5.3.2.6. Loss of Non-Emergency Alternating Current (AC) Power to the Station Auxiliaries

The loss of non-emergency AC power to the station auxiliaries may result from either a complete loss of the external grid or a loss of the on-site AC distribution system. A diverse reactor trip function from DPS on high pressurizer pressure and POSRV opening will mitigate the increase in the RCS pressure. In addition, the loss of non-emergency AC power to the motor-generator (MG) set results in the drop of the CEA's by gravity which can prevent the fuel failure.

Therefore, it is concluded that no detailed quantitative analysis is required for the event of loss of non-emergency AC power to the station auxiliaries with a CCF in the digital safety I&C systems.

5.3.2.7. Loss of Normal Feedwater Flow

The loss of normal feedwater flow may be initiated by losing more than one main feedwater pump, or by a spurious signal being generated by the feedwater control system, resulting in a closure of the feedwater control valves. This causes the decrease in the steam generator water level and the increase in the steam generator pressure and temperature, and hence the increase in the RCS temperature and pressure.

There are three turbine-driven main feedwater pumps in the APR1400 design. When only one main feedwater pump is lost, the core power level would be maintained at 100% core power without a reactor trip, due to the backup capacity of the two remaining feedwater pumps. When all three main feedwater pumps are lost, the pressurizer pressure and steam generator level might reach their trip setpoints even though the NSSS control systems act to mitigate the transient.

Although a postulated CCF in the digital safety I&C systems disables a reactor trip on high pressurizer pressure and auxiliary feedwater actuation on low steam generator level, DPS should initiate reactor trip and auxiliary feedwater. Therefore, it is expected that the acceptance criteria with respect to the RCS and fuel integrity would be met for the loss of main feedwater flow event with a CCF in the digital safety I&C systems.

Therefore, it is concluded that no detailed quantitative analysis is required for the loss of main feedwater flow event with a CCF in the digital safety I&C systems.

5.3.2.8. Feedwater System Pipe Breaks

The feedwater line break (FLB) is initiated by a breach of the main feedwater system piping. For the purpose of this evaluation, it is assumed that the break occurs in the downstream of the feedwater line reverse flow check valves that are located between the steam generator feedwater nozzles and the containment penetration. This results in the blowdown of the affected steam generator, while the intact steam generator continues to release steam until the MSIV closure (for the design basis event analysis presented in the DCD Chapter 15.2).

The FLB causing a steam generator blowdown may include either an RCS heatup or cooldown, depending upon the affected steam generator heat transfer characteristics and the enthalpy of the blowdown flow. For the purpose of this evaluation, like the DCD Chapter 15.2, only the case with respect to RCS heat-up is considered. The results of an RCS cooldown due to a steam generator piping rupture are covered by the main steam system piping rupture.

Should the FLB occur with a CCF in the digital safety I&C systems, the reactor trip functions and engineered safety features functions are not actuated (for example, reactor trip on high pressurizer pressure or on low steam generator level and main steam isolation on low steam generator pressure or on high containment pressure). However, because of the DPS reactor trip on high pressurizer pressure and DPS auxiliary feedwater actuation on low steam generator water level, the acceptance criteria for RCS integrity can be met for this accident. Operators would recognize the abnormal condition in the secondary system piping by various displays and alarms available under the condition of a CCF in the digital safety I&C systems. Based on this information, operators would recognize the need to isolate the steam generators by using ESF-CCS hardwired backup controls which are not subject to the CCF. Once the isolation of the steam generators is completed, a ruptured steam generator can be identified by comparing the pressures and water levels of both steam generators. After identification of the ruptured steam generator, operators would bring the plant to shutdown cooling entry condition by using the intact steam generator.

Based on the above evaluation, it is concluded that no detailed quantitative analysis with respect to RCS integrity is required for the FLB with a CCF in the digital safety I&C systems.

The containment pressure for FLB is bounded by that for the main SLB which discharges higher energy flow than the FLB. Therefore, no quantitative analysis with respect to containment integrity is required for FLB.

5.3.3 Decrease in Reactor Coolant Flow Rate

At this class of events, one or more of the following symptoms may be present:

- Decreasing reactor coolant flow
- Increasing reactor coolant temperature
- Increasing RCS pressure
- Increasing pressurizer level.

5.3.3.1. Loss of Forced Reactor Coolant Flow

The total loss of reactor coolant flow (TLRCF) event is caused by the simultaneous loss of power to the 13.8 kV electrical buses connected to the RCPs while a partial loss of reactor coolant flow may be caused by mechanical or electrical failure in a pump motor. The only credible failure that can result in the simultaneous loss of power to these buses is a complete loss of offsite power, which would also result in a turbine-generator trip and loss of normal electrical power to the station equipment.

For the total loss of reactor coolant flow event analyzed in the DCD Chapter 15.3, more limiting than the partial loss of reactor coolant flow event, a reactor trip on low RCP shaft speed is triggered by the CPC within one (1) second after event initiation. A CCF in the digital safety I&C systems prevents the reactor trip from being generated by the CPC. However, loss of power to the 4.16 kV non-safety buses would cause a power loss in the motor-generator sets that provide power to the control element drive mechanisms (CEDM). Consequently, the CEA's would fall into the reactor core by gravity after coil decay in the CEDM. The drop of the CEA's by gravity would require several seconds because of the setting value of the under voltage time delay relay and CEDM coil decay time. Once the total loss of reactor coolant flow occurs, thermal margin is rapidly reduced. Degraded thermal margin is ultimately recovered by the insertion of the CEA's into the core. Due to the extended period of time for CEA's to be inserted into the core caused by the CCF in the digital safety I&C systems (compared with the case for the DCD Chapter 15.3), an adverse effect on the fuel performance is expected, even though the best estimate analysis methodology can be applied.

To quantify the severity of the total loss of reactor coolant flow with a CCF in the digital safety I&C systems, it is concluded that a detailed quantitative analysis using computer programs is required for this event.

5.3.3.2. Flow Controller Malfunction Causing Flow Coastdown

This event does not apply to the APR1400 design.

5.3.3.3. RCP Rotor Seizure

A single reactor coolant pump rotor seizure can be caused by the seizure of the upper or lower thrust-journal bearings. For this event analyzed in the DCD Chapter 15.3, a reactor trip on low reactor coolant flow is triggered by the PPS within 2 seconds after event initiation. Low reactor coolant flow trip setpoint for the APR1400 design is [ ]^{TS} % of full power steady state hot leg flow. In addition, remaining three RCPs are assumed to be tripped according to the loss of offsite power concurrent with reactor trip. Thermal margin degradation in the early stage results from a single RCP rotor seizure, followed by larger degradation due to the coastdown of the remaining RCPs (caused by the assumed loss of offsite power concurrent with reactor trip). Finally, degraded thermal margin is recovered by the insertion of the CEA's into the core.

Should the single RCP rotor seizure occur with a CCF in the digital safety I&C systems, the reactor trip on low reactor coolant flow is not actuated and the reactor coolant flow would be maintained about at [ ]^{TS} % of rated flow. The RCS pressure will increase due to partial loss of reactor coolant flow in the early stage of the transient. The PPCS would prevent the RCS pressure from exceeding the DPS high pressurizer pressure reactor trip setpoint. If the reactor trip by the DPS is triggered, degraded thermal margin due to the single RCP rotor seizure would be rapidly recovered.

Reactor coolant temperature increases due to the loss of reactor coolant flow. If the reactor coolant temperature changes, the RRS will transmit the signals such as CEA withdrawal demand, CEA insertion demand, or CEA rate demand to the DRCS to maintain a programmed (i.e., a function of turbine power) reactor coolant temperature. The inputs for RRS come from reactor coolant temperature, turbine power, and core power. Since the core power would be maintained at full power and the reactor coolant temperature would increase, the RRS would generate a CEA insertion signal to restore the reactor coolant temperature to the programmed temperature corresponding to full power.

Sufficient indications would be available via the normal control systems for the operator to determine the need to take manual actions. These include RCPs and RCS flow indication, revealing the failure of one RCP, and lack of indication that CEAs had reached bottom positions (revealing the lack of a reactor trip, and therefore a malfunction in the PPS). With such indications, it is reasonable that the operator would manually initiate a reactor trip in a timely manner.

In spite of various beneficial echelon such as NSSS control systems and indication systems, it is concluded that a detailed quantitative analysis using computer programs is required for the single RCP rotor seizure with a CCF in the digital safety I&C systems to determine the impact of no reactor trip due to the CCF in the digital safety I&C systems compared with the case for the DCD Chapter 15.3.

5.3.3.4. RCP Shaft Break

A single reactor coolant pump sheared shaft could be caused by the mechanical failure of the RCP shaft. This is assumed to result from a manufacturing defect in the shaft. The characteristics of the RCP shaft break are very similar to those of the shaft seizure event.

The flow coastdown for a rotor seizure event is faster than the coastdown for a shaft break event. For a shaft break, the rotor is still capable of rotating, thereby offering less resistance to flow during the rapid flow decrease. This results in a less severe coastdown for the shaft break event than for the rotor seizure event.

Therefore, it is concluded that no detailed quantitative analysis is required for the single RCP shaft break with a CCF in the digital safety I&C systems.

5.3.4 Reactivity and Power Distribution Anomalies

Any one or more of the following symptoms may be present at this class of events:

- Change in core power
- Change in pressurizer pressure
- Change in pressurizer level.
- Change in reactor coolant temperature
- Decreasing core operating limit supervisory system (COLSS) core power limit
- Increasing COLSS azimuthal tilt

5.3.4.1. Uncontrolled CEA Withdrawal from Subcritical or Low Power Conditions

An uncontrolled withdrawal of CEA's is assumed to occur as a result of a single failure in the CEDM, DRCS, or RRS, or as a result of operator error. The withdrawal of CEA's from subcritical or low power conditions adds positive reactivity to the reactor core, causing both the core power level and the core heat flux to increase, with corresponding increase in reactor coolant temperature and RCS pressure. The withdrawal motion of CEA's also produces a time-dependent redistribution of core power. For the case presented in the DCD Chapter 15.4, these transient variations in core thermal parameters result in an approach to the specified acceptable fuel design limit (SAFDL), thereby requiring the protective action of the RPS.

The reactivity insertion rate accompanying the uncontrolled CEA withdrawal is dependent upon the CEA withdrawal rate and the CEA worth. At subcritical and low power conditions normal reactor feedback mechanisms do not occur until power generation in the core is large enough to cause changes in the fuel and moderator temperatures. The reactivity insertion rate determines the rate of approach to the fuel design limits. For the DCD Chapter 15.4 case, the uncontrolled withdrawal transient is terminated by any of a variable overpower trip, high pressurizer pressure trip, a low DNBR trip or high local power density depending on the initial conditions and reactivity insertion rate.

Should this event occur with a CCF in the digital safety I&C systems, the reactor trip on high pressurizer pressure in the DPS is available to mitigate the event, even though the trip functions from PPS are not available. For the case presented in the DCD Chapter 15.4, the minimum pressurizer pressure of [ ]^{TS} was selected as an initial condition to delay the high pressurizer pressure trip. Since the CCF coping analysis can utilize the realistic methods, a nominal pressurizer pressure of 158.19 kg/cm^2 (2,250 psia) can be chosen as an initial condition, which would trigger reactor trip on high pressurizer pressure much earlier than the case for the DCD Chapter 15.4. The most important factor for this event with a CCF in the digital safety I&C systems is the amount of thermal margin degradation before the CEA's is inserted into the core by the DPS high pressurizer pressure trip. According to the results of this event in the DCD Chapter 15.4, it is expected that the high pressurizer pressure trip would occur before the minimum DNBR approaches the DNB SAFDL of 1.29.

Based on the above evaluation, it is concluded that no detailed quantitative analysis using computer programs is required for the uncontrolled CEA withdrawal from subcritical or low power conditions with CCF in the digital safety I&C systems.

5.3.4.2. Uncontrolled CEA Withdrawal at Power

The cause of this event is identical to the event described in uncontrolled CEA Withdrawal from subcritical

or low power conditions. The evaluation of this event is essentially similar to that event.

Therefore, it is concluded that no detailed quantitative analysis is required for the uncontrolled CEA withdrawal at power with CCF in the digital safety I&C systems.

5.3.4.3. Single CEA Drop

A single full-length CEA drop results from an interruption in the electrical power to the CEDM holding coil of a single CEA. This interruption can be caused by a holding coil failure, or by a loss of power to the holding coil. The drop of a single full length CEA into the core reduces the fission power in the vicinity of the dropped CEA, and adds negative reactivity throughout the core. The radial and axial power distributions would shift in response to the reactivity feedback effects and neutron flux redistribution caused by the dropped CEA. If an asymmetry in the radial power distribution occurs, a new "tilted" asymptotic state is gradually reached with higher radial peaks. Xenon redistribution accompanies this process. The negative reactivity addition causes a prompt drop in core power and heat flux.

The result of the limiting case in the DCD Chapter 15.4 shows that the minimum DNBR does not exceed the DNB SAFDL of 1.29. The power mismatch between the primary and secondary systems leads to a cooldown of the RCS. The amount of power mismatch is not usually large enough to initiate turbine runback, or a setback to reduce the turbine power. The core power will be restored to its initial value due to the normal response of the RRS to the single CEA drop, and due to the moderator and fuel temperature feedback. No engineered safety features actuation system (ESFAS) is expected to be actuated in response to the single CEA drop with a CCF in the digital safety I&C systems. Based on changes in the major NSSS parameters, COLSS alarms, and DRCS CEA position indication, a reactor operator may choose to manually trip the reactor or manually insert CEA banks.

Due to the event characteristics discussed above, no reactor trip function and/or engineered safety features function is required to mitigate the single CEA drop with a CCF in the digital safety I&C systems. No violation against the acceptance criterion with respect to fuel performance is anticipated by the radial distortion factor and Xenon redistribution throughout the event with CCF. Therefore, it is concluded that a detailed quantitative analysis is not required for this event with CCF in the digital safety I&C systems.

5.3.4.4. A Single CEA Withdrawal

The postulated incident is the accidental withdrawal of a single CEA from an inserted control bank when operating at power. No single electrical or mechanical failure or operator error in the CEA control system could cause the accident. The event analyzed must result from multiple wiring failures, multiple serious operator errors, and subsequent and repeated operator disregard of event indication. The probability of such a combination of conditions is so low that the limiting consequences may include slight fuel damage.

The characteristics of this event are essentially similar to the single CEA drop except for a prompt increase in core power and heat flux. There are no reactor trip functions or engineered safety features actuation functions required for the mitigation of the single CEA withdrawal with a CCF in the digital safety I&C systems. Comparing to the DCD Ch.15.4 analysis, therefore, it is concluded that no additional detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.3.4.5. Startup of an Inactive Reactor Coolant Pump

This event is evaluated during Modes 3 through 6 since plant operation with fewer than all four reactor coolant pumps is permitted only during those modes. Therefore, this event is not necessarily considered for the CCF coping analysis since the best estimate method is adapted. Nevertheless, the startup of an inactive reactor coolant pump is evaluated with respect to RCS integrity and fuel performance degradation. The cases considered are no more than one reactor coolant pump operating, or two reactor coolant pumps operating in one loop (the other loop idle) to maximize the pressure increase.

The RCP startup causes a sudden surge of relatively cooler or hotter water to enter the core, which may cause a core power or RCS pressure increase. With no more than one reactor coolant pump operating or two reactor coolant pumps operating in one loop (the other loop idle), the RCP startup may lead to an increase in RCS pressure. For Modes 3 and 4, the primary safety valves, main steam safety valves will maintain the RCS pressure below 110% of design pressure during the worst pressure transients. During Modes 4, 5 and 6, when the shutdown cooling system is aligned, overpressure protection is provided by the shutdown cooling system relief valves.

The maximum RCS pressure for the startup of an inactive reactor coolant pump event with a CCF in the digital safety I&C systems will not exceed 110% of design pressure. For Modes 3 and 4, the heat imbalance due to the RCP startup is less limiting than that caused by the CEA withdrawal event. In Modes 5 and 6, the capacity of the shutdown cooling relief valves prevents the RCS pressure from exceeding the pressure and temperature limits for these modes. Fuel damage would not be expected, as DNBR increases during the event.

Therefore, it is concluded that a detailed quantitative analysis is not required for this event with a CCF in the digital safety I&C systems.

5.3.4.6. Flow Controller Malfunction

This event does not apply to the APR1400 design.

5.3.4.7. Inadvertent Deboration

Inadvertent deboration may be caused by the improper operator action or by a failure in the boric acid makeup flow path that reduces the flow of borated water to the charging pump suction. Either cause can produce a boron concentration that is below the concentration of the reactor coolant. The resulting decrease in RCS boron concentration adds positive reactivity in the core.

For Modes 1 and 2, the inadvertent deboration with a CCF in the digital safety I&C systems will cause an DPS reactor trip on high pressurizer pressure, and the subsequent reactor scram will bring the core to subcritical conditions. For the remaining modes, the core is initially subcritical with the shutdown margin at the minimum value consistent with the Technical Specification limit for cold shutdown.

The operator is alerted to a decrease in the RCS boron concentration either through a high neutron flux alarm on the startup flux channel, the reactor makeup water flow alarm, the sampling, boronometer indications, or boric acid flow rate. The operator turns off the charging pump and closes the letdown orifice isolation valves in order to stop further dilution. At the maximum dilution rate, the operator has more than 30 minutes to terminate dilution before the reactor core becomes critical. Next, the operator increases the RCS boron concentration by implementing the emergency boration procedure for achieving cold shutdown boron concentration. This can be done using the CVCS.

The DPS reactor trip on high pressurizer pressure will ensure primary system integrity for Modes 1 and 2. No engineered safety feature actuation function is required for the mitigation of the inadvertent deboration with a CCF in the digital safety I&C systems.

Therefore, it is concluded that no detailed quantitative analysis is needed for this event with a CCF in the digital safety I&C systems.

5.3.4.8. Inadvertent Loading of a Fuel Assembly into the Improper Position

This event results from inadvertently interchanging two fuel assemblies, in violation of core loading procedures. The anomaly would be expected to be revealed during low-power physics tests, or early in the fuel cycle checks of ex-core and in-core detector readings. There are no reactor trip functions or

engineered safety features actuation functions required for the mitigation of the inadvertent loading of a fuel assembly into the improper position with a CCF in the digital safety I&C systems.

Therefore, it is concluded that no detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.3.4.9. Control Element Assembly Ejection

This event results from a rupture in the circumference of the CEDM housing of the CEDM nozzle. Ejection of a CEA causes the core power to rapidly increase because of the almost instantaneous addition of positive reactivity. However, the rapid increase in core power is terminated by the moderator and Doppler feedback effects.

Should the CEA ejection occur concurrently with a CCF in the digital safety I&C systems, the reactor trip functions and ESF functions are not available while DPS diverse functions remain available. The amount of core power increase mainly depends on the magnitude of the ejected CEA worth. Even though the core power increase is large enough to trigger the variable overpower trip, no reactor trip signal would be generated due to the CCF in the digital safety I&C systems. Accompanying rapid increase in core power, the RCS pressure will increase dramatically. An appropriate response of the PPCS to the pressure excursion would retard the increasing rate of the RCS pressure. If the amount of the RCS pressure increase is large enough to trigger the DPS reactor trip on high pressurizer pressure despite the programmed PPCS action, CEAs would be inserted into the core followed by termination of the thermal margin degradation.

The CEA ejection causes a small-break LOCA. The evaluation in terms of LOCA is included in Section 5.3.6.5 of this report. Also the effects on containment integrity and the means for event mitigation are bounded by LOCA described in Section 5.3.6.5 of this report.

Based on the above evaluation, it is concluded that a detailed quantitative analysis using computer programs is required for the CEA ejection with a CCF in the digital safety I&C systems. If the core power increase is large enough to threaten the fuel rods to melt, a detailed quantitative analysis should be performed to verify the maintenance of coolable geometry. At the same time, an analysis with respect to fuel failure caused by the violation of the DNB SAFDL should be done separately.

5.3.5 Increase in Reactor Coolant System Inventory

For the events in this category, one or more of the following symptoms will be present:

- Increasing pressurizer level
- Increasing pressurizer pressure
- Valve configuration corresponding to minimum letdown flow
- Increased charging flow (one of the initiating event)
- Safety injection flow (one of the initiating event)
- Safety injection pumps running (one of the initiating event)
- Safety injection valves position - open (one of the initiating event)

5.3.5.1. Inadvertent Operation of the ECCS

The inadvertent operation of the safety injection system (SIS) is assumed to actuate four SI pumps and open the corresponding discharge valves. This operation occurs as a result of a spurious signal to the system or an operator error.

Inadvertent operation of the SIS is important to examine when it occurs with RCS pressure below the SI pump shutoff head pressure. Above that pressure, there will be no injection of fluid into the RCS. If the RCS pressure is below the SI pump shutoff head pressure, the SI flow will increase the RCS inventory and pressure until the pressure reaches the pump shutoff head pressure (when the shutdown cooling system is isolated). Should the SIS inadvertently actuate during shutdown cooling operation, the shutdown cooling relief valves will mitigate the pressure transient.

Due to the pressure increase caused by this transient at low RCS temperatures, there is an approach to the brittle fracture limits of the RCS. However, the APR1400 DCD Chapter 15 concludes that brittle fracture limits will not be violated for this transient.

There are no reactor trip functions or engineered safety features actuation functions required for the mitigation of the inadvertent operation of the emergency core cooling system (ECCS) with a CCF in the digital safety I&C systems. Therefore, it is concluded that no detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.3.5.2. CVCS Malfunction - Pressurizer Level Control System Malfunction

This event results from an assumed failure in the PLCS, which increases charging flow to its maximum rate and reduces the letdown system to its minimum flow. If the pressurizer level controller fails low, a low pressurizer level signal can be transmitted to the controller. The resulting increase in reactor coolant system inventory causes an increased pressurizer level and pressure. The increased pressure is mitigated by the PPCS, which would use pressurizer spray to condense steam in the pressurizer steam space that is being compressed by the rising water level. The increased charging flow would not have a significant effect on reactor power, RCS temperatures, or steam generator conditions.

With the normal pressurizer steam space of about [ ]^{TS}, and the net RCS inventory increase rate of [ ]^{TS}, the time available for an operator to terminate the spurious increased charging flow before the pressurizer fills with water can be simply calculated by:

[ ]TS

The value of [ ]TS is based on cold water at [ ]TS. This water would be heated once it gets to the RCS and heated further as it enters the pressurizer. The second term of the equation accounts for this volume expansion effect. This calculation result shows that an operator will have about [ ]TS minutes to prevent the pressurizer from being filled with water (or reaching solid condition). This can be accomplished by manual local action to open the charging pump electrical power breakers.

Therefore, sufficient time exists for manual local operation by operator to terminate the spurious increased charging flow. If the pressure increase due to the increased reactor coolant inventory is large enough to trigger the DPS high pressurizer pressure trip, the primary system integrity will be protected due to the shutdown CEA insertion. The primary system integrity is maintained by the actuation of the primary safety valves to open, when needed, and limit the pressure increase.

There are no engineered safety features actuation functions required for the mitigation of the CVCS malfunction with a CCF in the digital safety I&C systems. It is concluded that no detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.3.6 Decrease in Reactor Coolant System Inventory

For the events in this category, one or more of the following symptoms may be present:

- Decreasing pressurizer pressure
- Decreasing pressurizer level
- Increasing auxiliary building sump level (letdown line break only)
- Increasing auxiliary building temperature (letdown line break only)
- Increasing auxiliary building humidity (letdown line break only)
- Increasing auxiliary building radiation (letdown line break only)
- Decreasing Letdown Line Pressure (letdown line break only)
- Decreasing volume control tank level
- Increased main steam line activity (steam generator tube rupture only)
- Air ejector high activity (steam generator tube rupture only)
- Steam generator blowdown high activity (steam generator tube rupture only)

5.3.6.1. Inadvertent Opening of a Pressurizer Safety/Relief Valve

This event is covered by LOCA, Section 5.3.6.5.

5.3.6.2. Double-ended Break of a Letdown Line Outside Containment

Reactor coolant could be released to outside of the containment if a break or leak occurs in a letdown line, sample line, or instrument line in a location outside of the containment. Since the letdown line is the largest of these, a double-ended break of the letdown line, outside the containment and upstream of the letdown isolation valve, has the largest potential for release of reactor coolant outside the containment.

The leak flow is limited to approximately [ ]^{TS} by the letdown line orifices located inside containment downstream of the letdown heat exchanger. Due to the continuing release of the reactor coolant through the letdown line break, the pressurizer level decreases continually. Several alarms provide indication of the letdown line break. The letdown line low pressure and high radiation alarms would immediately alert the operator after the initiation of the event. In addition, low pressurizer pressure and level alarms, and volume control tank low level alarms are also expected to occur. In response to the alarms, the operator will take actions to close the letdown isolation valves which are located serially along the letdown line in order to terminate the leak flow.

Notwithstanding a postulated CCF in the digital safety I&C systems, the alarms which are not influenced by the CCF in the digital safety I&C systems are still be available for operators to close he letdown isolation valve within much earlier than 30 minutes.

The postulated CCF in the digital safety I&C systems prevents the actuation to manually close the letdown isolation valves. However, hardwired backup actuation of letdown isolation and monitoring of parameters is available to the operator to terminate the event. According to the results of this event in the

DCD, it is conservatively assumed that operator action is delayed until thirty minutes after event initiation.

There are no reactor trip functions or engineered safety features actuation functions required for the mitigation of double-ended break of a letdown line outside containment with a CCF in the digital safety I&C systems.

Based on the above evaluations, it is concluded that no detailed quantitative analysis using a computer program is required for the double-ended break of the letdown line outside the containment with a CCF in the digital safety I&C systems.

5.3.6.3. Steam Generator Tube Rupture

Reactor coolant leakage into the secondary system through the steam generator tube rupture can result in radiological release to the environment via the condenser air ejectors or via the steam relief to the atmosphere. The depletion of the reactor coolant inventory through the double-ended steam generator tube rupture cannot be restored by the charging flow. This is because the amount of flow rate through the ruptured steam generator tube is greater than that of the maximum charging flow rate for the APR1400 design.

The principle objectives of mitigating actions in responding to a steam generator tube rupture are to limit radiological release to the environment, to maintain the RCS inventory, and to provide continued heat removal via the remaining intact steam generator.

The postulated CCF in the digital safety I&C systems precludes an automatic reactor trip. Since the leak would deplete the RCS inventory, the pressurizer level and pressure would decrease. The loss of reactor coolant through the leak would be mitigated by the automatic control of the PLCS and PPCS.

The operator would be able to observe the decrease of pressurizer level and initiate a manual trip based on various alarms and displays alerting the operators that a LOCA is occurring. For smaller leaks, the loss of inventory would be more gradual, effectively allowing a longer period of time for the operator to observe the plant condition and take appropriate actions to mitigate the transient. For a leak for which the CVCS can make up the leak flow, a controlled reactor shutdown would be performed. For such leaks, the postulated CCF in the digital safety I&C systems would not affect plant recovery during the event. A steam generator tube rupture which causes a leak flow in excess of the makeup capacity of the CVCS may decrease the RCS inventory. Continued decrease in the pressurizer level would turn off the pressurizer heaters to protect the heaters. After pressurizer heaters are turned off, the only means to retard the decrease in RCS pressure is the charging flow, of which the flow rate is expected to be the maximum value. Eventually, the pressurizer will be empty.

It is concluded that a detailed quantitative analysis using computer programs is required for confirming the safety of the steam generator tube rupture with CCF in the digital safety I&C systems.

5.3.6.4. Radiological Consequences of Steam Line Break outside Containment (BWR)

This evaluation is not necessary for the APR1400 design, a Pressurized Water Reactor (PWR) design.

5.3.6.5. Loss of Coolant Accident

A reactor trip needs to be initiated to limit the temperature excursion of the fuel rods and to limit the containment pressure peak promptly after a LOCA occurs. The postulated CCF of the digital safety I&C systems, however, would preclude PPS initiation of the reactor trip. Since the pressurizer pressure would decrease during the LOCA, initiation of a reactor trip on high pressurizer pressure by the DPS would not occur. However, the manual reactor trip and the high containment pressure trip by the DPS remain available and unaffected by the postulated CCF of the digital safety I&C systems. Further quantitative

analysis with operator actions would be necessary to determine if the manual reactor trip needs to be conducted by the operator within the required time for adequate control of the excursion of fuel rods and containment peak pressure. If not, diverse means should be considered for automatic DPS initiation of reactor trip on low pressurizer pressure, if needed to meet Reference 3 criteria.

There are two different heat removal mechanisms available following a LOCA: 1) heat removal accomplished by heating the SI flow, which is injected from the in-containment refueling water storage tank then escapes through the break into the containment, and 2) heat removal by natural circulation through the steam generators, which is implemented by providing feed flow and steam dump. Injection from at least two SI trains needs to be initiated between 20 and 500 seconds, mainly depending on the break size, for the RCS heat removal and RCS inventory control.

The generation of SIAS on low pressurizer pressure or high containment pressure from the PPS would be prevented by the postulated CCF of the digital safety I&C systems. However, the SI actuation from DPS remains available, since it is not affected by the postulated CCF of the digital safety I&C systems. Closure of the containment isolation valves limits the radiological release to the environment following a LOCA. Initiation of a CIAS on low pressurizer pressure or high containment pressure would be prevented by the postulated CCF of the digital safety I&C systems.

Initiation of containment spray flow adequately limits the containment pressure excursion following a LOCA. The postulated CCF of the digital safety I&C systems would preclude initiation of the CSAS signal on high containment pressure to automatically start the containment spray pumps and open the containment spray header valves.

It is concluded that a detailed quantitative analysis using computer programs is required for confirming the core safety and the extent of offsite dose of the LOCA with CCF in the digital safety I&C systems.

5.3.7 Radioactive Material Release form a Subsystem or Component

5.3.7.1. Radioactive Gas Waste System Failure

Regulatory position on this event is not specified in the SRP but described in the BTP 11-5. The evaluation methods and the results for this event are addressed in DCD section 11.3.7. No specific diversity and defense-in-depth evaluation of the digital safety I&C systems is necessary for this event because this event does not require any reactor trip and engineered safety features action.

5.3.7.2. Radioactive Liquid Waste System Leak or Failure

Regulatory position on this event is not specified in the SRP. The evaluation methods and the results for this event are addressed in DCD sections 9 and 11. No specific diversity and defense-in-depth evaluation of the digital safety I&C systems is necessary for this event because this event does not require any reactor trip and engineered safety features action.

5.3.7.3. Postulated Radioactive Release Due to Liquid Containing Tank Failures

The most limiting radioactive tank failure is the uncontrolled release of liquid from the holdup tank, which is part of the CVCS. This event as described in the APR1400 DCD Chapter 15 does not require any reactor trip and engineered safety features actuation functions to mitigate the consequences of the event. Therefore, it is concluded that no detailed quantitative analysis is required for this event with CCF in the digital safety I&C systems.

5.3.7.4. Fuel Handling Accident

The fuel handling accident results from the dropping of a single fuel assembly during fuel handling. This event as described in the APR1400 DCD Chapter 15 does not require any reactor trip and engineered safety features functions to mitigate the consequences of the event. Therefore, it is concluded that no detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.3.7.5. Spent Fuel Cask Drop Accidents

This event is evaluated in the APR1400 DCD Chapter 15 with respect to the possibility of a drop from a height exceeding 30 feet, or drop/tip onto irradiated fuel. This event as described in the APR1400 DCD Chapter 15 does not require any reactor trip and engineered safety features functions to mitigate the consequences of the event. Therefore, it is concluded that no detailed quantitative analysis is required for this event with a CCF in the digital safety I&C systems.

5.4 Quantitative Evaluation

As a result of the qualitative evaluation, eight events are identified to be quantitatively analyzed and their results are presented in this section. The selected subjects of analysis of the eight events are as follows:

a. Increase in feedwater flow

b. Steam line break outside containment (Offsite Dose)

c. Total loss of reactor coolant flow

d. Single RCP shaft seizure/break

e. CEA ejection

f. Steam generator tube rupture

g. Loss of coolant accident (LOCA)

h. Steam line break inside containment (Containment Integrity)

The evaluation uses the realistic assumptions such as nominal initial operating conditions, continuous operation of the RCPs (except in case of the loss of offsite power event). NSSS control systems function normally in automatic mode since they are not affected by the CCF of the PPS and ESF-CCS. The DPS provides automatic reactor trips on high pressurizer pressure and high containment pressure while performing an automatic actuation of the auxiliary feedwater and safety injection on low steam generator level and low pressurizer pressure, respectively. For each event, this section describes the causes of the event, sequence and physical phenomena of the event, analytical methodology, systems availability, operator actions evaluation and their justification when they are credited, and the conformance of the acceptance criteria required from SRP BTP 7-19.

The major assumptions used in analyzing each event are the same as the description provided in Section 5.1. The initial conditions for major operating parameters for each event are shown in Tables 5-1 through 5-8. The mathematical models are summarized as follows.

5.4.1 Mathematical Models

Each event uses one and/or more computer codes for its mathematical models. The computer codes used are summarized as follows.

5.4.1.1. CESEC-III Computer Program

The CESEC-III computer program is used to simulate the nuclear steam supply system. CESEC-III is a version of CESEC which incorporates the ATWS model modifications. This program was approved by Nuclear Regulatory Commission (NRC) in 1984. CESEC-III explicitly models the steam void formation and collapse in the upper head region of the reactor vessel. CESEC-III computes key system parameters during a transient including core heat flux, pressures, temperatures, and valve actions. A partial list of the dynamic functions included in this NSSS simulation includes the following: point kinetics neutron behavior, Doppler and moderator reactivity feedback, boron and CEA reactivity effects, multi-node average thermal hydraulics, reactor coolant pressurization and mass transport, reactor coolant system safety valve behavior, steam generation, steam generator water level, turbine bypass, main steam safety and turbine admission valve behavior, as well as alarm, control, protection, and engineered safety feature systems. The steam turbines, condensers and their associated controls are not included in the simulation. Steam generator feedwater enthalpy and flow rate are provided as input to CESEC-III.

5.4.1.2. TORC and CETOP Computer Programs

The TORC computer program is used to simulate the three-dimensional fluid conditions within the reactor core. The program was approved by NRC in 1981. Results from the TORC program include the core radial distribution of the relative channel axial flow rate that is used to calibrate CETOP, and approved in 1981. Transient core heat flux and thermal-hydraulic conditions from CESEC are input to CETOP which employs the KCE-1 critical heat flux (CHF) correlation described in Reference 4.

5.4.1.3. STRIKIN-II Computer Program

The STRIKIN-II computer program is used to simulate the heat conduction within reactor fuel rods and its associated surface heat transfer. The STRIKIN-II program was approved by NRC in 1976. The STRIKIN-II computer program provides a single, or dual, closed channel model of a core flow channel to calculate the clad and fuel temperatures for an average or hot fuel rod, and the extent of the zirconium water reaction for a cylindrical geometry fuel rod. STRIKIN-II includes the following:

- Incorporation of all major reactivity feedback mechanisms,
- A maximum of six delayed neutron groups,
- Both axial (maximum of 20) and radial (maximum of 20) segmentation of the fuel element, and
- Control rod scram initiation on high neutron power.

5.4.1.4. RELAP5/MOD3 Program

The RELAP5/MOD3 computer program has been developed for best-estimate transient simulation of light water reactor coolant systems during postulated accidents. The code models the coupled behavior of the reactor coolant system and the core for loss-of-coolant accidents and operational transients such as anticipated transient without scram, loss of offsite power, loss of feedwater, and loss of flow. A generic modeling approach is used that permits simulating a variety of thermal hydraulic systems. Control system and secondary system components are included to permit modeling of plant controls, turbines, condensers, and secondary feedwater systems.

5.4.2 Analysis Results

The results of 8 events quantitatively analyzed using computer codes are provided in this section. In summary, the integrities of the RCS and the containment are well maintained and the offsite doses resulted from each event also meet the acceptance criteria required in SRP BTP 7-19.

5.4.2.1. Increase in Feedwater Flow

5.4.2.1.1. Events Overview

Increase in feedwater flow (IFWF) is classified as an AOO and caused by a further opening of a feedwater control valve or an increase in the feedwater pump speed. The maximum increase at full power shall not exceed [ ]^{TS} % of above nominal value for the main feedwater system.

A postulated pre-existing CCF in the digital PPS/ESF-CCS will preclude the initiation of reactor trip on variable over power or high steam generator level and main steam and feedwater isolation on high steam generator level which are considered to be probably actuated during increase in feedwater event. NSSS control systems, which are independent and diverse from PPS/ESF-CCS, are assumed to operate normally to respond to the increase in feedwater with a CCF in the PPS/ESF-CCS.

5.4.2.1.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS thermal hydraulic response to the increase in feedwater flow event with the CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program (Reference 5). The minimum DNBR was calculated using the CETOP computer program (Reference 6) which uses the KCE-1 CHF correlation.

b. Initial Conditions and assumptions

The initial conditions and assumptions used to analyze the NSSS and core thermal hydraulic response to an increase in feedwater flow event with the CCF in the PPS/ESF-CCS are presented in Table 5-1. It is assumed that turbine and secondary systems are normally operating and removing heat transferred from the primary system throughout the event.

c. Results

The dynamic behaviors of important NSSS parameters following an increase in feedwater flow with the CCF in the PPS/ESF-CCS are provided in Figures 5-1 through 5-5. The increase in main feedwater flow shall bring a core power increase due to the negative moderator and fuel temperature feedback effect caused by the decrease in the primary coolant temperature.

If the reactor trip functions are not properly work by the postulated CCF in the PPS, the core power will increase to a certain level because of the overcooling due to the increased feedwater. Pressurizer proportional heaters fully turn on at 6.0 seconds and pressurizer backup heaters turn on 9.8 seconds due to the decrease in RCS pressure. The thermal margin degradation is mainly caused by the core power increase. The minimum DNBR is [ ]^{TS} and occurs at 125.0 seconds. Subsequent to this time, the DNBR gradually increases due to the recovery of the RCS pressure (refer to Figure 5-2 and Figure 5-5). When the pressurizer pressure reaches to 156.43 kg/cm^2 (2,225 psia), backup heaters are turned off. After 30 minutes from the event initiation, the operator is assumed to take manual control of the plant according to appropriate recovery procedures. Alarms and indications will be provided via equipments not affected by the postulated CCF in the PPS/ESF-CCS to support operator action to trip the reactor. Alarms due to high core power rate, high SG level or low pressurizer pressure and lots of indications would help operators perform manual reactor trip in a short time after the event, but the manual reactor trip is conservatively delayed until 30 minutes.

5.4.2.1.3. Conclusions

The minimum DNBR remained well above the SAFDL ensuring that no fuel failures occur. The RCS pressure integrity is well maintained.

5.4.2.2. Steam Line Break outside Containment

5.4.2.2.1. Events Overview

This analysis covers double-ended steam line break outside containment. Core coolability could be threatened due to the assumption that automatic reactor trip is not operated by RPS and the isolation of main steam and feedwater is not automatically operated by ESF. However, due to Doppler reactivity feedback effect and available over power margin (AOPM) which intrinsically exist in the core, it limits power excursion and also helps to ease the effect of the postulated CCF in the PPS/ESF-CCS.

5.4.2.2.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS thermal hydraulic response to the steam line break outside containment with a postulated CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program. The CESEC-III results were used as input to the STRIKIN-II computer program (Reference 7) to calculate fuel centerline and cladding temperatures and into the CETOP computer program to calculate the minimum DNBR and fuel failure percentage.

b. Initial Conditions and Assumptions

Table 5-2 presents the initial conditions and assumptions used to analyze the NSSS and core thermal hydraulic responses and those used to calculate offsite dose for the double-ended break of a steam line outside containment with a postulated CCF in the PPS/ESF-CCS.

c. Results

The time dependent behaviors of the important NSSS parameters following a double-ended break of a steam line outside containment with a postulated CCF in the PPS/ESF-CCS are shown in Figures 5-6 through 5-13.

Due to the release of excessive energy through steam line break, steam generator pressure is dramatically reduced resulting in turbine-generator trip. Cooling water supply to feedwater system is recirculated by condensing the steam that went through turbine, and due to the turbine-generator trip, resupply of condensation water to feedwater system is also suspended. The feedwater control system shall increase main feedwater flow to the steam generators due to the decrease in the steam generator level and high steam flow. It is conservatively assumed that an initiation of the steam line break results in an immediate loss of all feedwater heating such that the enthalpy of feedwater equals to that of condenser hotwells. It is also conservatively assumed that the feedwater system and feedwater control system are able to maintain the mass of liquid in the steam generators essentially constant until the entire source of main feedwater supply is exhausted. The resulting primary system subcooling causes a rapid increase in core power which is calculated to peak at approximately [ ]^{TS} % power at around 400 seconds of event initiation, and thereafter, has hardly changed. The minimum DNBR of [ ]^{TS} occurs at 746 seconds. The maximum cladding and fuel centerline temperature changes follow the same trend as the core power, reaching peak values of less than [ ]^{TS} and [ ]^{TS}, respectively, at about 13 minutes after the event.

Feedwater mass in the deaerator storage tanks at the beginning of the event is sufficient to supply feedwater to the steam generators at a rate equal to the steam flow through the break for about [ ]^{TS} minutes. Thereafter, it is assumed that the feedwater flow is drawn from the condenser hotwells. It is at a lower enthalpy than that of the deaerator storage tanks due to the loss of feedwater heating, and that source is also exhausted within about [ ]^{TS} minutes. When the feedwater in the condenser hotwells is completely exhausted, the condensate storage tank becomes the source of feedwater. The feedwater in the storage tank is at the lowest enthalpy and is supplied for [ ]^{TS} minutes. Eventually, the steam generator level begins to decrease as all the source of feedwater is exhausted. On the other hand, the core power increases according to the change of the enthalpy of the feedwater source, and as described above it reaches about [ ]^{TS} % of the design power, after that, it has hardly changed. Auxiliary feedwater actuation signal is generated at [ ]^{TS} minutes after the event by the DPS. Depletion of the steam generators causes primary pressure spike, which results in a reactor trip on high pressurizer pressure by the DPS at about [ ]^{TS} minutes after the event initiation. The calculated peak RCS pressure is less than [ ]^{TS} within 2 seconds after generation of the high pressurizer pressure trip signal. The steam generators are completely depleted at about [ ]^{TS} minutes. Auxiliary feedwater begins to reach the steam generators at about [ ]^{TS} minutes. The operator

manually closes the main steam isolation valves 30 minutes after event initiation and initiates a controlled plant cooldown in accordance with appropriate recovery procedures.

The calculated maximum fuel cladding and fuel centerline temperatures demonstrate that the core shall maintain its coolability for this event. From the predicted minimum DNBR, it is predicted less than [ ]^{TS} % of the fuel experience DNB. The resulting two-hour exclusion area boundary (EAB) and eight-hour low population zone (LPZ) doses are [ ]^{TS} mSv and [ ]^{TS} mSv, respectively. These values are within 10CFR50.34 guidelines.

5.4.2.2.3. Conclusions

The calculated maximum cladding and fuel centerline temperatures demonstrate that the core maintains coolable geometry for a steam line break with a postulated CCF in the PPS/ESF-CCS. Less than [ ]^{TS} % of the fuel was predicted to fail. The calculated offsite radiological doses are within 10CFR50.34 guidelines. The peak RCS pressure remains below the service level C limit of 226 kg/cm^{2}A (3,215 psia) and the primary system integrity is maintained.

5.4.2.3. Loss of Forced Reactor Coolant Flow

5.4.2.3.1. Events Overview

The total loss of forced reactor coolant flow event is caused by the simultaneous power loss of 13.8kV buses that supply power to RCPs. The only credible failure that can result in the simultaneous power loss to these buses is a complete loss of offsite power to the unit main and auxiliary transformers. And if the offsite power is lost, turbine-generator will trip and then normal electrical power supply is also lost. For total loss of forced reactor coolant flow with a postulated CCF in the PPS/ESF-CCS, no reactor trip occurs by low RCP shaft speed from the PPS. The loss of the normal electric power to station equipment will include the loss of 4.16kV non-class 1E buses. The buses supply power to the motor-generator sets that provide power to the CEDMs. With the loss of the normal electric power to station equipment CEDMs, an under voltage relay of motor-generator sets would open an output breaker. This would cut power to the CEDMs, allowing the control rods to drop into the core by gravity. Even quicker action would be taken by an output contactor on each motor-generator set, which will open at about 4 seconds after power is lost on the bus, cutting power to the CEDMs and causing the CEAs to drop into the core at that point.

5.4.2.3.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS thermal hydraulic response to a total loss of forced reactor coolant flow with a CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program. The minimum DNBR was calculated using the CETOP computer program which uses the KCE-1 CHF correlation.

b. Initial Conditions and Assumptions

The initial conditions and assumptions used to analyze the NSSS and core thermal hydraulic responses to the total loss of forced reactor coolant flow with a CCF in the PPS/ESF-CCS are presented in Table 5-3.

c. Results

The time-dependent behavior of important NSSS parameters following a total loss of forced reactor coolant flow with the CCF in the PPS/ESF-CCS is provided in Figures 5-14 through 5-19.

The loss of offsite power assumed to occur at [ ]^{TS} second causes the plant to experience a simultaneous turbine trip, loss of main feedwater, condenser in-operability, and a coast down of all four

reactor coolant pumps. Due to the loss of offsite power, power supply to CEDM is shut off. Then reactor trip breakers open at 5.55 seconds and a CEA is inserted. High pressurizer pressure trip (HPPT) signal by the DPS occurs at 5.65 seconds. The core maintains its full power before CEA drop; however, the DNBR is reduced by the reduction in reactor coolant flow. The DNBR degradation is terminated by the insertion of CEA and then increased suddenly. The minimum DNBR is [ ]^{TS} and occurs at 7.23 seconds. Subsequent to this minimum value, the DNBR continuously increases and, after 30 minutes, the operator is assumed to take manual control of the plant under appropriate recovery procedures. Alarms and indications support the operators to trip the reactor.

5.4.2.3.3. Conclusions

The minimum DNBR was shown to remain well above the specified acceptable fuel design limit ensuring that no fuel failures occur. Also, the plant was shown to remain in a stable condition for at least 30 minutes ensuring that the operator has sufficient time to take manual control of the plant in order to execute a controlled cooldown.

5.4.2.4. RCP Rotor Seizure/Shaft Break

5.4.2.4.1. Events Overview

A single reactor coolant pump rotor seizure (rocked rotor) can be caused by seizure of the upper or lower thrust-journal bearings. A single reactor coolant pump shaft break (sheared shaft) could be caused by mechanical failure of the pump shaft. Since the sheared shaft event related flow coastdown is determined to be less adverse than that related to the rotor seizure event, it is judged that the sheared shaft event is less challenging to the event acceptance limits. Therefore, only single reactor coolant pump rotor seizure event is analyzed.

5.4.2.4.2. Analysis of Effects and Consequences

a. Mathematical Model

The NSSS thermal hydraulic response to a reactor coolant pump locked rotor with a postulated CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program. The minimum DNBR was calculated using the CETOP computer program which uses the KCE-1 CHF correlation.

b. Initial Conditions and Assumptions

Table 5-4 presents the input parameters and initial conditions used to analyze the NSSS and core thermal hydraulic responses to the reactor coolant pump locked rotor with a postulated CCF in the PPS/ESF-CCS.

c. Results

The time-dependent behavior of the important NSSS parameters following a reactor coolant pump locked rotor with a postulated CCF in the PPS/ESF-CCS is provided in Figures 5-20 through 5-26. If the one rotor locked out of 4 reactor coolant pumps, it will bring a rapid decrease in reactor coolant flow. The flow reduction terminates within a few seconds and stabilizes at a flow of approximately [ ]^{TS} % of the rated flow. Low reactor coolant flow trip signal is assumed not to be generated due to the CCF in the PPS/ESF-CCS. The flow reduction results in degradation of DNBR in the early stage of the transient. Core power decreases due to the fuel temperature feedback effect within several seconds after event initiation and then restores to the initial core power due to the moderator temperature feedback effect. When the fuel and moderator temperature feedback effects lead to another balanced reactivity condition, a quasi-steady state is reached. The minimum DNBR of [ ]^{TS} occurs at 0.6 seconds. Subsequence to this minimum, the DNBR rapidly increases and then slowly decreases until an essentially constant value is reached.

After 30 minutes into the event, the operator is assumed to trip the reactor at which time the DNBR will again increase. The operator will then perform a controlled cooldown of the plant under appropriate recovery procedures. Alarms and indications will be provided via equipment not affected by the CCF in the PPS/ESF-CCS to support operator action to trip the reactor. Figures demonstrate that the plant remains in a stable condition for at least 30 minutes into the event.

5.4.2.4.3. Conclusions

The minimum DNBR was shown to remain well above the specified acceptable fuel design limit ensuring that no fuel failures occur. Also, the plant was shown to remain in a stable condition for at least 30 minutes into the event ensuring that the operator has sufficient time to trip the reactor and take manual control of the plant in order to execute a controlled cooldown.

5.4.2.5. CEA Ejection

5.4.2.5.1. Events Overview

A CEA ejection occurs when a circumferential rupture happened in the hosing of control element drive mechanism (CEDM) nozzle. The CEA ejection event resulting in primary system rupture is considered as an LOCA discussed in Section 5.4.2.7 of this report. This section only deals with CEA ejection without any rupture in the primary system.

5.4.2.5.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS thermal hydraulic response to the CEA ejection with a CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program. The CESEC-III results were used as input to the STRIKIN-II computer program to calculate fuel centerline and cladding temperatures and into the CETOP computer program to calculate the transient DNBR profile and minimum DNBR.

b. Initial Conditions and Assumptions

The initial conditions and assumptions used to analyze the NSSS and core response to the CEA ejection with a CCF in the PPS/ESF-CCS are presented in Table 5-5.

c. Results

The time-dependent behavior of important NSSS parameters following a CEA ejection with CCF in the PPS/ESF-CCS is provided in Figures 5-27 through 5-33. The CEA ejection causes the core power to increase rapidly to approximately [ ]^{TS} % in less than 1 second. The RCS pressure increases due to the increase in the reactor coolant temperature caused by this power spike. The peak RCS pressure [ ]^{TS} occurs at approximately 29 seconds and then decreases gradually to its nominal operating value by the normal response of PPCS to the system parameter excursions followed by CEA ejection. The Doppler and moderator reactivity feedback due to the heat-up caused by the power spike, coupled with the constant turbine power demand, result in core power falling back to re stabilize at 100 % power within 100 seconds following event initiation. The DNBR decreases rapidly following the power spike caused by the ejected CEA. The minimum DNBR of [ ]^{TS} occurs at approximately 5 seconds, ensuring no fuel failures occur. Subsequent to the minimum, the DNBR increases due to the reduction in core power. The peak clad temperature obtained during the transient was less than [ ]^{TS}, well below the 1,204.5 °C (2,200 °F) limit. Also the peak centerline temperature was less than [ ]^{TS} which is well below 2,704.5 °C (4,900 °F), the temperature at which fuel melting could occur. The peak radial averaged fuel enthalpy was below the 230 cal/gm, which is normally used for acceptance criteria for the CEA ejection. At 30 minutes, the operator is assumed to take manual control of

the plant in order to trip the reactor and execute a controlled cooldown. Alarms and indications would be provided via equipment which is not affected by the CCF in the PPS/ESF-CCS to support operator action to trip the reactor.

5.4.2.5.3. Conclusions

Even though a CEA ejection with postulated CCF in the PPS/ESF-CCS occurs, the minimum DNBR was shown to remain well above the specified acceptable fuel design limit ensuring that no fuel failures occur. Also, the peak cladding temperature was well below the limit of 1,204.5 °C (2,200 °F). No fuel melting occurred and the peak radial averaged fuel enthalpy was below the limit of 230 cal/gm. The maximum RCS pressure remained well below the limit of 226 kg/cm^{2}A (3,215 psia); therefore the primary system integrity is maintained.

5.4.2.6. Steam Generator Tube Rupture

5.4.2.6.1. Events Overview

The steam generator tube rupture (SGTR) accident is a penetration of the barrier between the RCS and the main steam system caused by a damage of U-tube in the steam generator. The accident is likely caused by the etch pits or small cracks in the U tubes or by cracks in the welds joining the tubes to the tube sheet. The most critical SGTR event with a CCF in the PPS/ESF-CCS is a double-ended rupture of a U-tube at full power condition. The postulated CCF in the PPS/ESF-CCS would disturb the reactor trip on hot leg saturation, low DNBR or high SG level from PPS.

5.4.2.6.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS thermal hydraulic response to a steam generator tube rupture with the CCF in the PPS/ESF-CCS was simulated using the CESEC-III computer program. The minimum DNBR was calculated using the CETOP computer program which uses the KCE-1 CHF correlation.

b. Initial Conditions and Assumptions

The initial conditions used to analyze the NSSS and core thermal hydraulic responses to a steam generator tube rupture with a CCF in the PPS/ESF-CCS are presented in Table 5-6.

c. Results

The time-dependent behavior of important NSSS parameters following a steam generator tube rupture with a CCF in the PPS/ESF-CCS is provided in Figures 5-34 and 5-36. Because of a CCF in the digital PPS/ESF-CCS, a reactor trip and corresponding turbine trip will not occur until operator actions begin at 30 minutes after event initiation. This can give a positive effect with regard to the radiological dose release because the possibility of radiation release to the environment through main steam safety valves will reduce. From the perspective of radiation effects by the steam generator tube rupture, the evaluation will focus on the calculation of the DNBR since the radiological consequences from the DBA of the APR1400 DCD Chapter 15 would be more restrictive than this case if no fuel failure occurs.

If a steam generator tube rupture occurs, the RCS pressure decreases due to the decrease in the reactor coolant inventory. The DNBR decreases as the RCS pressure decreases. This degradation continues until the assumed operator action to trip the reactor and isolate the affected steam generator. Operators would trigger the reactor trip by the following indications:

- Radiation monitors not affected by the CCF in the digital safety I&C systems indicate an increase

in radioactivity levels at the condenser vacuum vent, at the main steam line, at the steam generator blowdown lines, and at the turbine or auxiliary building ventilation monitors.

- Decreasing level in the volume control tank.
- An unaccounted increase in the charging and/or a decrease in the letdown system flow rates.
- Decreasing pressurizer pressure and level.

After diagnosing a probable steam generator tube leak and manually tripping the reactor, operators will take actions to minimize the primary to secondary leakage by minimizing the pressure differential between the reactor coolant system and the steam generators. The optimum response to control the RCS inventory and radiological releases is to minimize the RCS and steam generator pressure differential as soon as possible. Also, the response would be to lower the RCS pressure and to control the RCS temperature (to prevent the main steam safety valves (MSSVs) from lifting) by heat transfer to the steam generators. Operators will perform these actions according to the EOP after a manual reactor trip.

Radiation monitors unaffected by the CCF in the digital safety I&C systems are crucial factors for operators to identify the affected (leaking) steam generator and to isolate it. The isolation of the affected steam generator can be made by controlling the MSIVs, which are available by hardwired ESF-CCS backup actuation in the MCR.

Continued heat removal through the intact steam generator allows the RCS heat removal to be achieved with the RCS and secondary pressure below the MSSV opening setpoint, preventing release of steam through the MSSVs of the affected steam generator. Also, the EOP may require tripping one or more RCPs to control heat removal.

The normal operation of the feedwater system and the SBCS and the RCPs can be used for the RCS heat removal and are not affected by the CCF in the digital safety I&C systems. Appropriate monitoring information will also remain available via the IPS.

For offsite dose calculation, the manual actions are assumed to begin step by step according to appropriate operating procedures using available functions from 30 minutes after the event initiation. Given the fact that the N-16 monitors and alarms give immediate indication of a SGTR in either SG, the assumption of the start of manual action at 30 minutes into the event mitigative action is very conservative.

According to calculation, just before the operator intervention, the minimum DNBR is [ ]^{TS}. Thus, the DNBR remains above the specified acceptable fuel design limit, and no fuel failure occurs. Steam generator overfilling for this event prior to operator action will be prevented by normal response of feedwater control system as shown in the Figure 5-36. Subsequent operator actions, observing the event mitigation procedures presented in the EOPs will prevent overfilling.

The resulting EAB and LPZ doses are [ ]^{TS} mSv and [ ]^{TS} mSv, respectively. It satisfies the limit presented in SRP BTP 7-19.

5.4.2.6.3. Conclusions

The minimum DNBR was shown to remain well above the specified acceptable fuel design limit ensuring that no fuel failures occur. Also, overfilling of the affected steam generator will be prevented. As the radiological consequences are bounded by the analysis of APR1400 DCD Chapter 15, the offsite doses meet the limit presented in SRP BTP 7-19.

5.4.2.7. Loss of Coolant Accident

5.4.2.7.1. Events Overview

The NRC no longer allows the use of probability or leak before break to exclude analysis of the large break LOCA concurrent with a postulated software CCF. Therefore, an additional DPS function of SIAS initiation has been designed to mitigate the CCF effects within the safety grade protection systems during the large break LOCA (LBLOCA) or small break LOCA (SBLOCA) event. The reactor trip that occurs due to the DPS operation caused by the high containment pressure signal is not credited during the LBLOCA, while it is credited during the SBLOCA. The total discharged mass during the SBLOCA event is less than that during the LBLOCA. Therefore, in the point of view of consequential dose the result of the SBLOCA analysis is bounded by LBLOCA analysis. The evaluation with a CCF in the PPS/ESF-CCS is performed to show the integrity of the RCS during LBLOCA event.

5.4.2.7.2. Analysis of Effects and Consequences

a. Mathematical Models

The NSSS response to LBLOCAs with a postulated CCF in the PPS/ESF-CCS was simulated using the RELAP5/MOD3 code (Reference 8).

b. Initial Conditions and Assumptions

Table 5-7 presents the initial conditions and assumptions used to analyze the NSSS response for LBLOCAs with a postulated CCF in the PPS/ESF-CCS.

c. Results

Refer to the following Figures 5-37 through 5-43 for the explanation of the DPS - SIAS function during the LBLOCA on the double ended discharge leg. As the LBLOCA occurs, the RCS inventory flows out through the break. The discharge of RCS inventory rapidly reduces the RCS pressure as shown in Figure 5-37. Because of the passive safety features, the RCS pressure drop triggers the coolant injection from the SIT as shown in Figure 5-38. During the SIT coolant injection the reactor core can be maintained without damage. But as the SIT inventory is limited, the SIT injection is soon finished, and the RCS inventory falls again, and also exposes fuel rods. After the coolant depletion in the SIT, the coolant leaks through the break lowers the reactor collapsed water level as shown in Figure 5-39, and the core can be damaged within 5 minutes because of the temperature rise in the core which contains 20 fuel nodes by axial as shown in Figure 5-41 if the plant has no other automatic coolant recovery function of the coolant injection.

If the PPS does not actuate the SIAS because of any possible CCF, and also the DPS does not have function of SIAS initiation, the reactor water level cannot be recovered as shown in Figure 5-39 and the cladding temperature rises rapidly as shown in Figure 5-41. The soaring of cladding temperature results in core melt down which is not desirable.

The automatic DPS-SIAS function is implemented to have function of SIAS initiation. With the DPS - SIAS initiation with [ ]^{TS} on low pressurizer pressure, the four safety injection pumps and the four safety injection tanks work automatically without single failure as indicated in Figure 5-38. The reactor water level can be recovered as shown in Figure 5-40. The liquid fraction is maintained at average 0.4 on the hot channel top as shown in Figure 5-42. Since two-phase mixture level is generally 0.3 of liquid fraction for vertical flow (Reference 9), it can be shown that core mixture level would be maintained above the core. Therefore the peak cladding temperature is limited to 1,204.4 °C (2,200 °F) as shown in Figure 5-43. After 1,800 seconds of the initiation of LBLOCA with a CCF, the operator would take action to ensure that plant is placed in stable and safe condition.

5.4.2.7.3. Conclusions

The evaluation of the response to breaks in branch lines connected to the RCS shows that the peak cladding temperature does not challenge the limit of LBLOCAs with reactor coolant pump operating and a postulated CCF in the PPS/ESF-CCS. Consequently no cladding rupture or high temperature oxidation are predicted. LBLOCA event assuming a CCF does not result in significant consequence to the core coolability. Therefore, the dose associated with this event does not exceed the dose guidelines of SRP BTP 7-19.

5.4.2.8. Steam Line Break Inside Containment

5.4.2.8.1. Events Overview

This evaluation considers double-ended steam line break inside containment. The break is assumed to occur between the steam nozzle and main steam isolation valve. If the PPS functions of automatic reactor trip, automatic main steam and feedwater line isolation are lost by a CCF in the PPS/ESF-CCS, containment integrity shall be threatened. However, the high containment pressure reactor trip of DPS helps to prevent rapid increase in containment pressure. This analysis focuses on the containment response as the primary system responses are discussed in Section 5.4.2.2.

5.4.2.8.2. Analysis of Effects and Consequences

a. Mathematical Models

The containment response to the steam line break event was simulated using the SGN-III computer program (Reference 10). In SGN-III, subroutine CONTRANS has a capability to calculate containment pressure and temperature using containment model, which was approved by NRC for containment design (Reference 11).

b. Initial Conditions and Assumptions

The initial conditions and assumptions used to analyze the containment response to a steam line break event are presented in Table 5-8.

c. Results

The containment pressure is presented in Figure 5-44. If steam line break occurred inside the containment, the steam generator mass and energy will be released to the containment, so the containment pressure shall rapidly increase. In this analysis a reactor trip on high containment pressure via DPS occurs at 3.15 seconds. The feedwater flow before reactor trip is injected to both steam generators at the pump run out rate. However, after reactor trip, feedwater control system reduces feedwater flow to less than [ ]^{TS} % of normal feedwater flow. As shown in Figure 5-44, the peak containment pressure occurs at 262 seconds. After that, the pressure decreases slightly and begins to increase at 1,290 seconds. It is assumed that no operator action occurs during the first 30 minutes of the event. At 30 minutes, the operator is assumed to actuate two containment sprays and shut down the main steam isolation valve of the affected steam generator. Containment pressure, steam generator pressure and level alarms will provide indication of the need for operator action. The actuation of containment spray system will prevent the increase in the containment pressure and decrease pressure. The peak containment pressure is [ ]^{TS} and it is less than the ASME factored load category limit of 8.70 kg/cm^{2}A (123.70 psia).

5.4.2.8.3. Conclusions

The peak containment pressure following the steam line break event remains less than the containment

factored load category of [ ]^{TS}. Based on this analysis, it is concluded that the containment integrity is maintained even for steam line break inside containment with a postulated CCF in the PPS/ESF-CCS.

Table 5-1 Initial Conditions and Assumptions for Increase in Feedwater Flow

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, m^3 (ft^3)	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Table 5-2 Initial Conditions and Assumptions for Steam Line Break Outside Containment

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^2A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, $m^3(ft^3)$	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Assumptions Applied to Offsite Dose Evaluation

[ ] TS

Table 5-3 Initial Conditions and Assumptions for Total Loss of Reactor Coolant Flow

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, m^3 (ft^3)	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Table 5-4 Initial Conditions and Assumptions for RCP Shaft Seizure/Shaft Break

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, m^3 (ft^3)	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Table 5-5 Initial Conditions and Assumptions for CEA Ejection w/o Primary System Rupture

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, m^3 (ft^3)	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Table 5-6 Initial Conditions and Assumptions for Steam Generator Tube Rupture

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)
Pressurizer Water Volume, m^3 (ft^3)	33.16 (1,171.2)
Steam Generator Inventory, kg/SG (lbm/SG)	97,046 (213,950)
Axial Shape Index (ASI)	- 0.07
Radial Peaking Factor	1.4138

Assumptions Applied to Offsite Dose Evaluation

[ ] TS

Table 5-7 Initial Conditions and Assumptions for Loss of Coolant Accident

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^2A (psia)	158.19 (2,250)
RCS Mass Flow Rate, 10^6 kg/hr (lbm/hr)	75.57 (166.6)

Assumptions Applied to Offsite Dose Evaluation

[ ] TS

Table 5-8 Initial Conditions and Assumptions for Steam Line Break Inside Containment

Parameter	Value
Core Power Level, MWt	3,983
Cold Leg Temperature, °C (°F)	290.56 (555)
Pressurizer Pressure, kg/cm^{2}A (psia)	158.19 (2,250)
Containment Pressure, kg/cm^{2}A (psia)	1.10 (15.7)
Containment Temperature, °C (°F)	48.89 (120)
Containment Relative Humidity, %	5

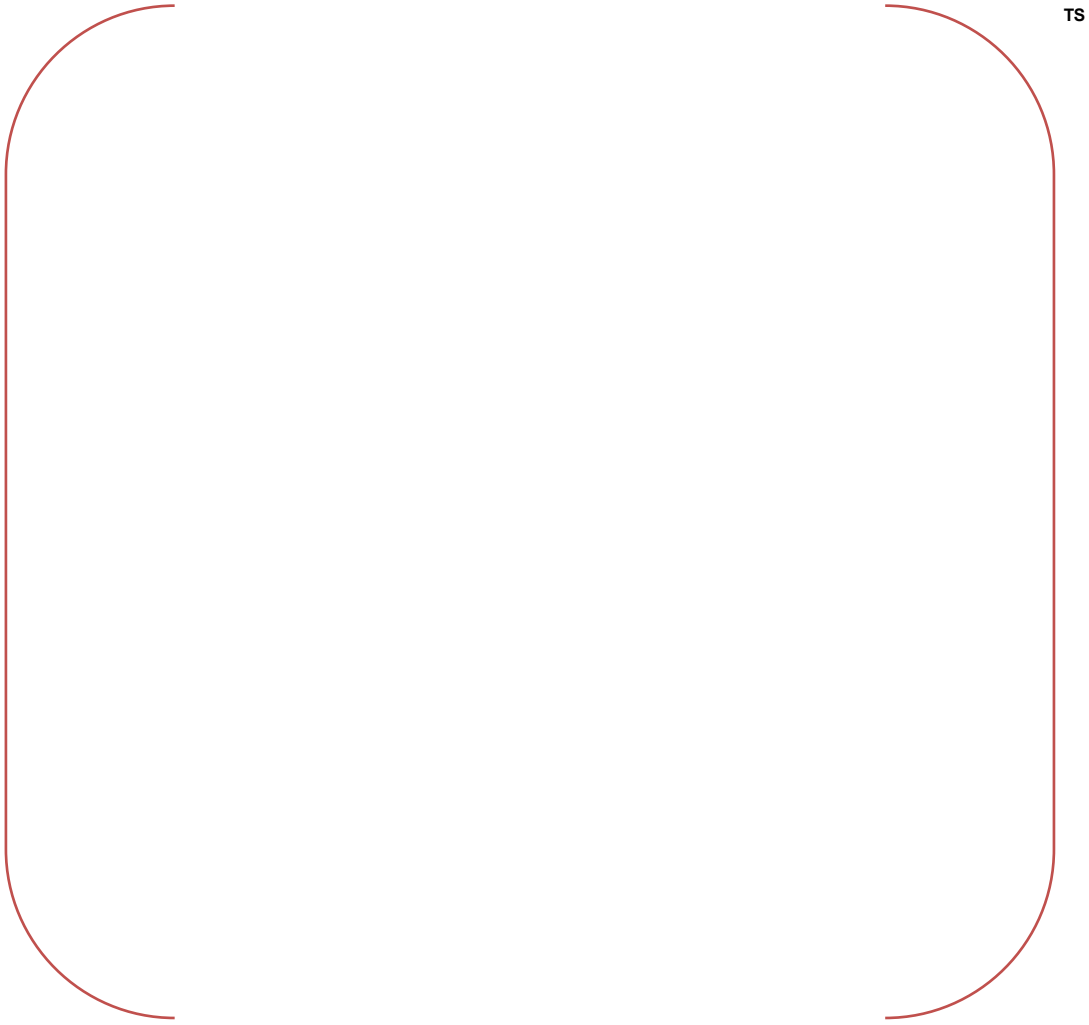

Figure 5-1 IFWF with a CCF in the PPS/ESF-CCS; Core Power vs. Time

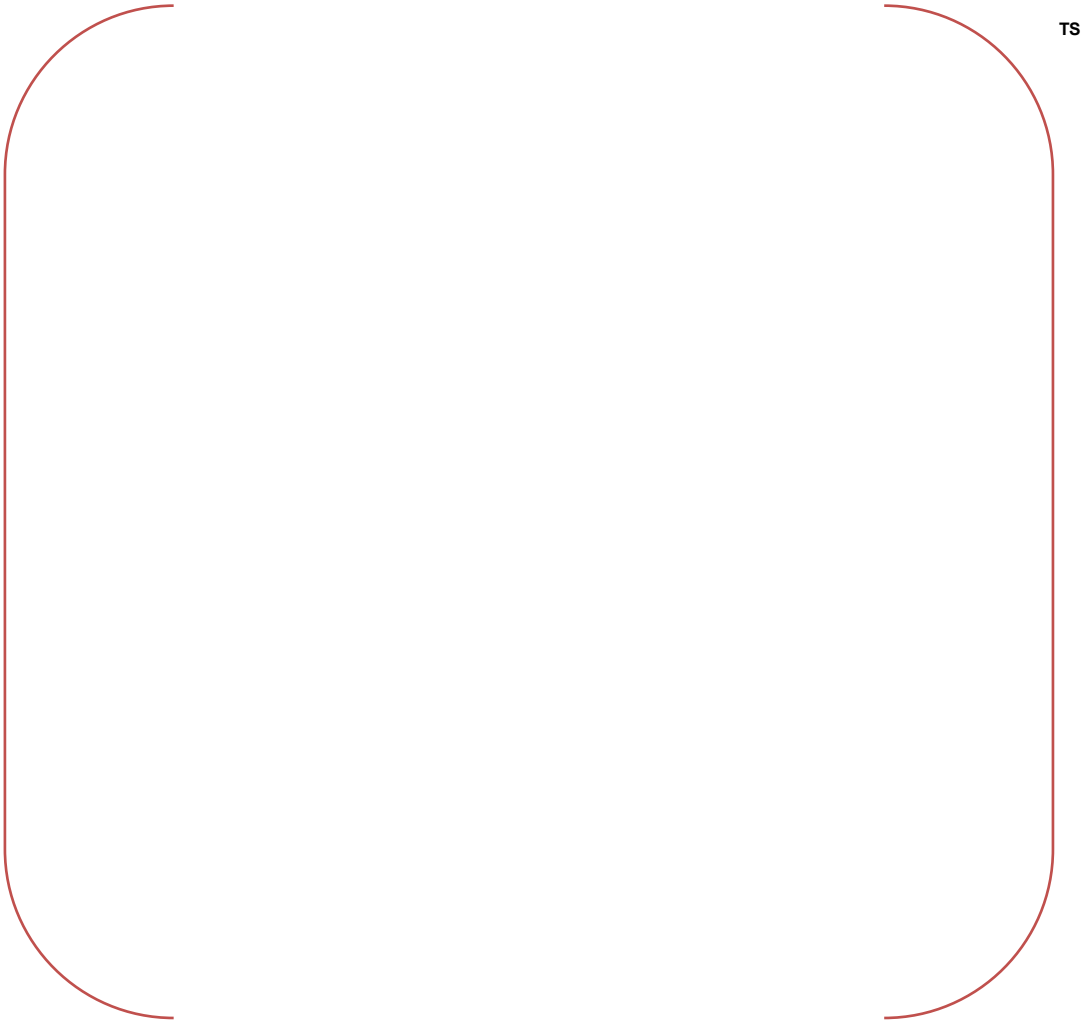

Figure 5-2 IFWF with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

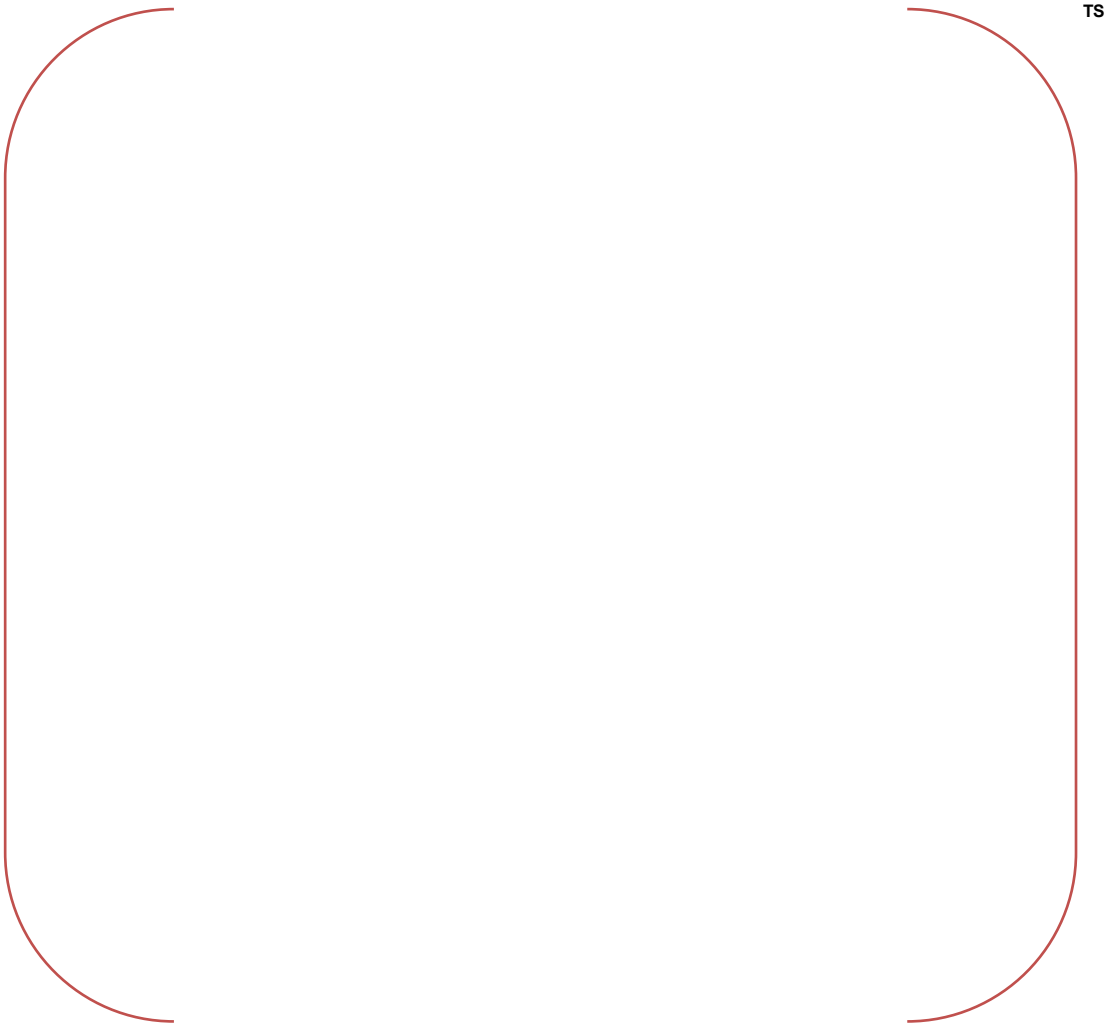

Figure 5-3 IFWF with a CCF in the PPS/ESF-CCS; Reactor Coolant Temperature vs. Time

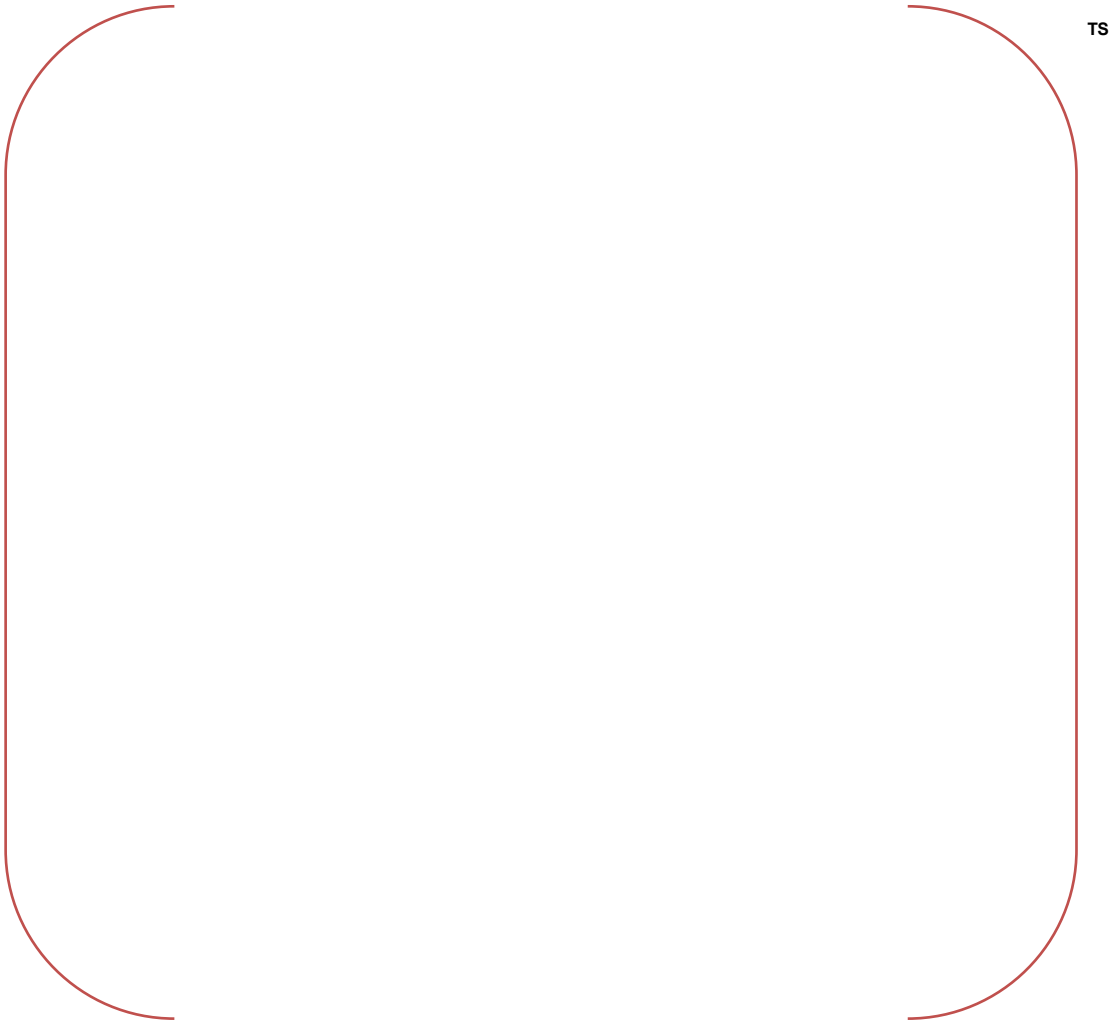

Figure 5-4 IFWF with a CCF in the PPS/ESF-CCS; Core Flow Rate vs. Time

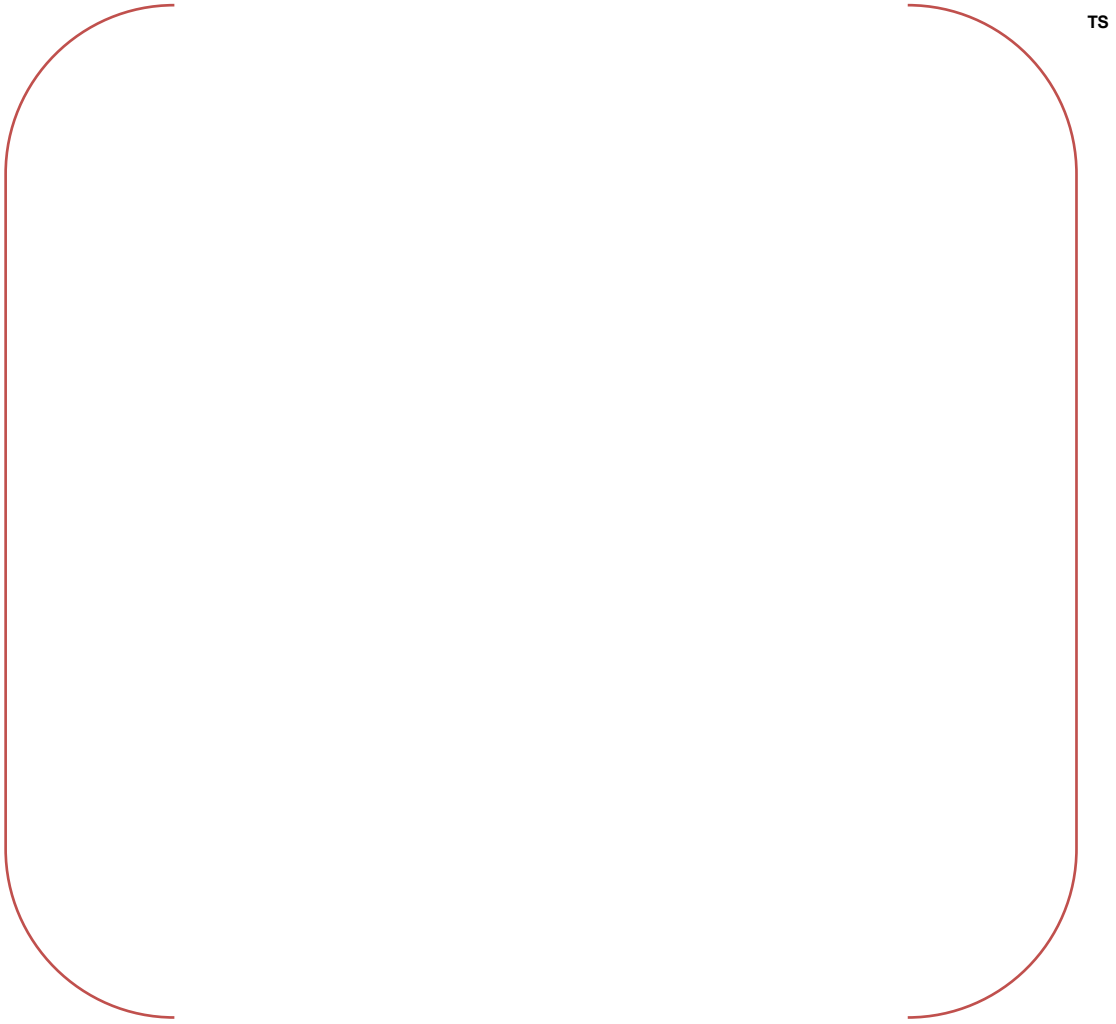

Figure 5-5 IFWF with a CCF in the PPS/ESF-CCS; DNBR vs. Time

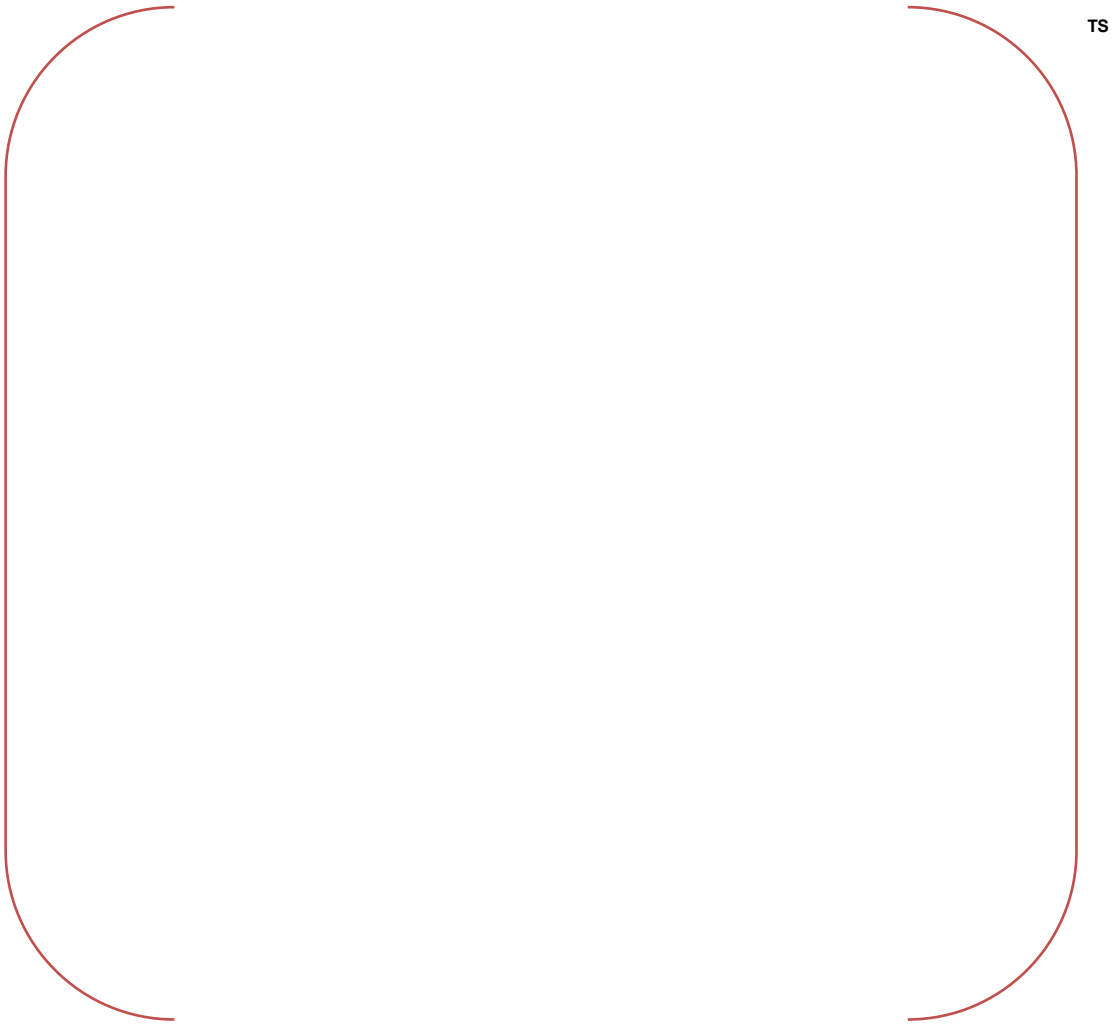

Figure 5-6 SLB with a CCF in the PPS/ESF-CCS; Core Power vs. Time

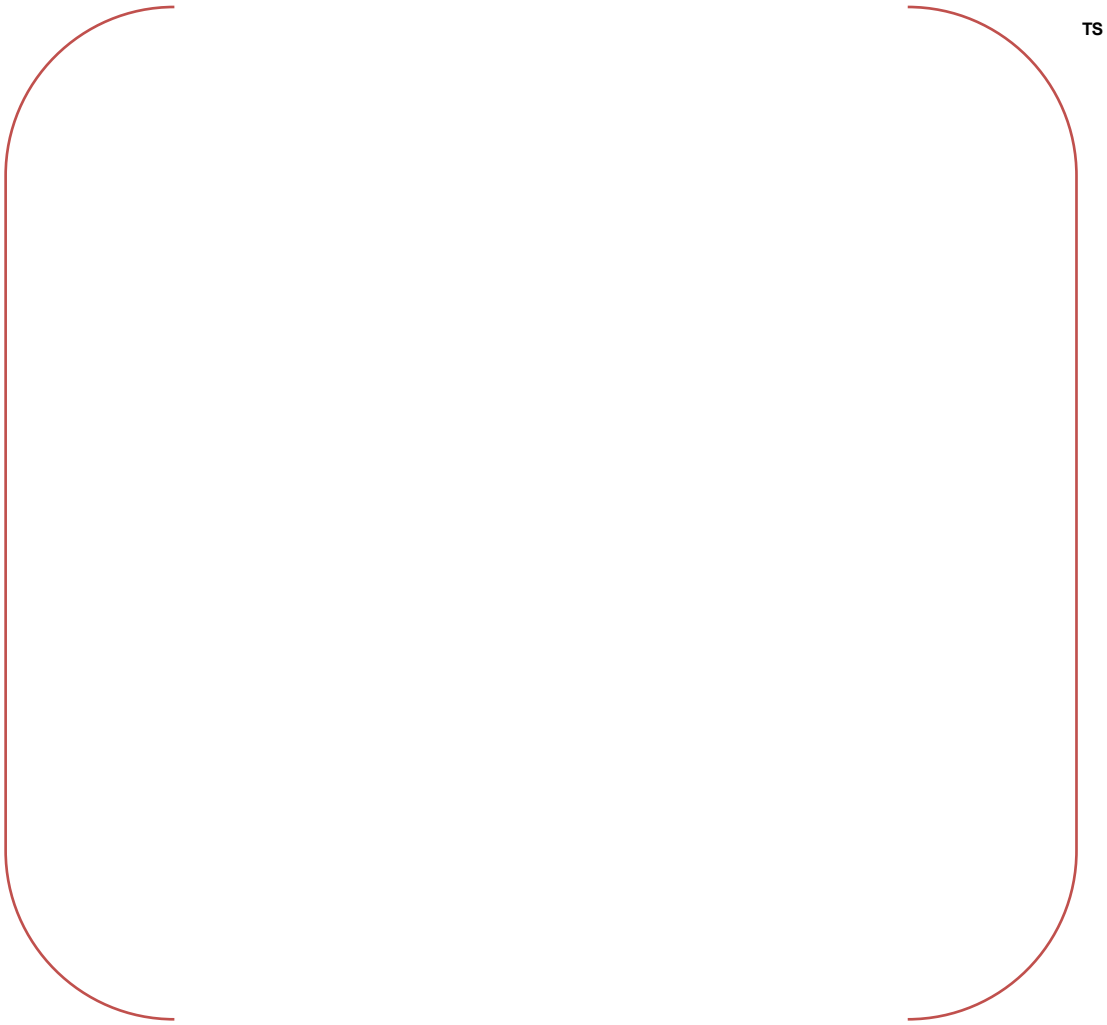

Figure 5-7 SLB with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

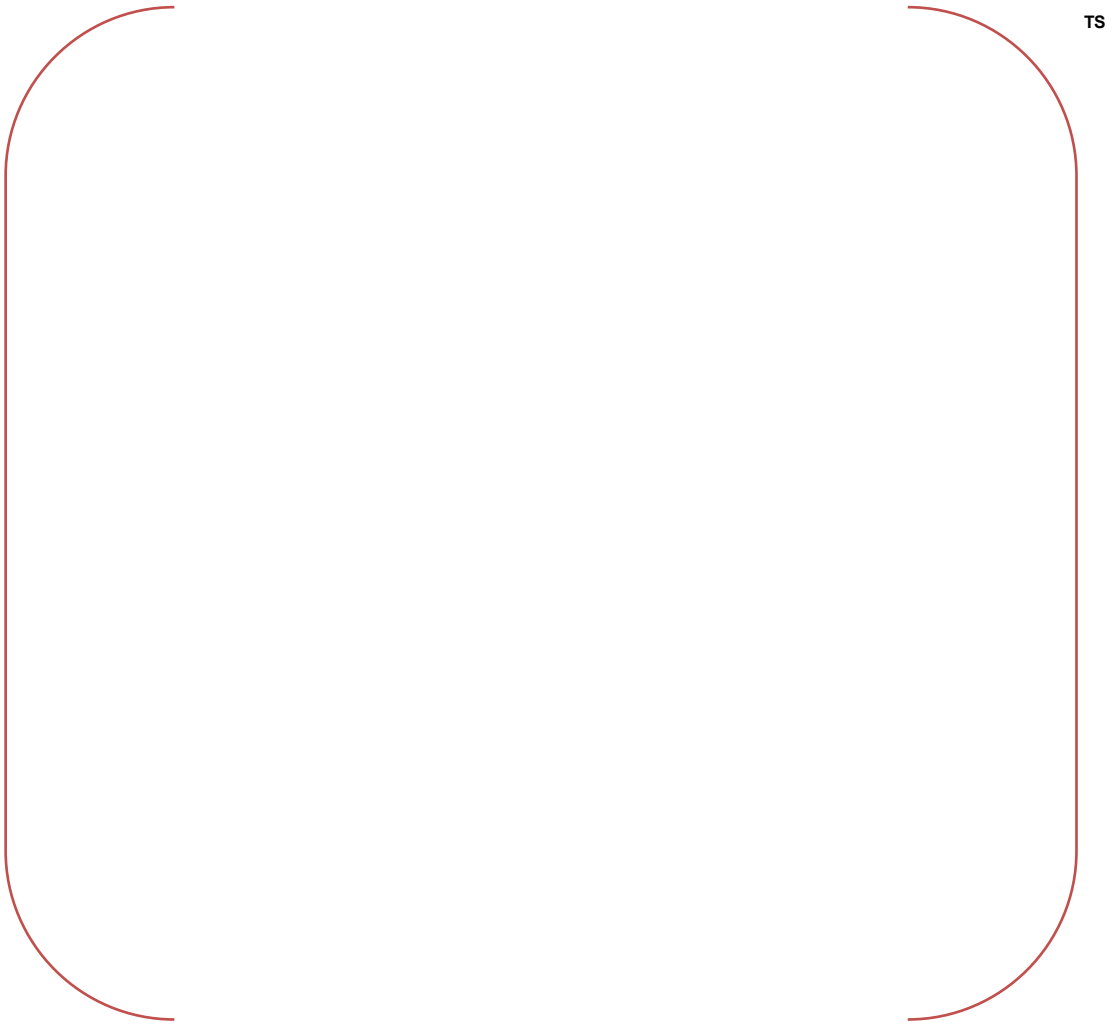

Figure 5-8 SLB with a CCF in the PPS/ESF-CCS; Reactivities vs. Time

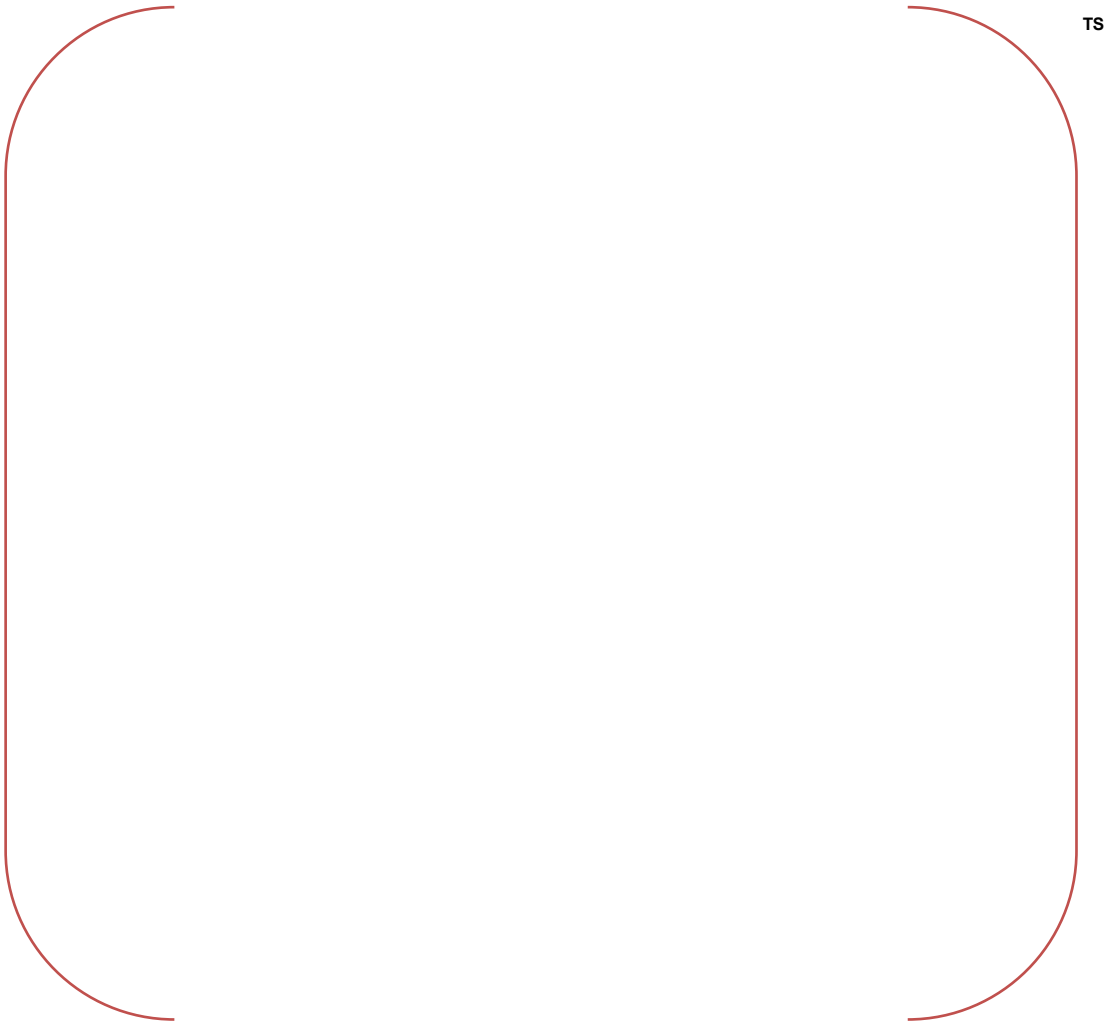

Figure 5-9 SLB with a CCF in the PPS/ESF-CCS; SG Inventory vs. Time

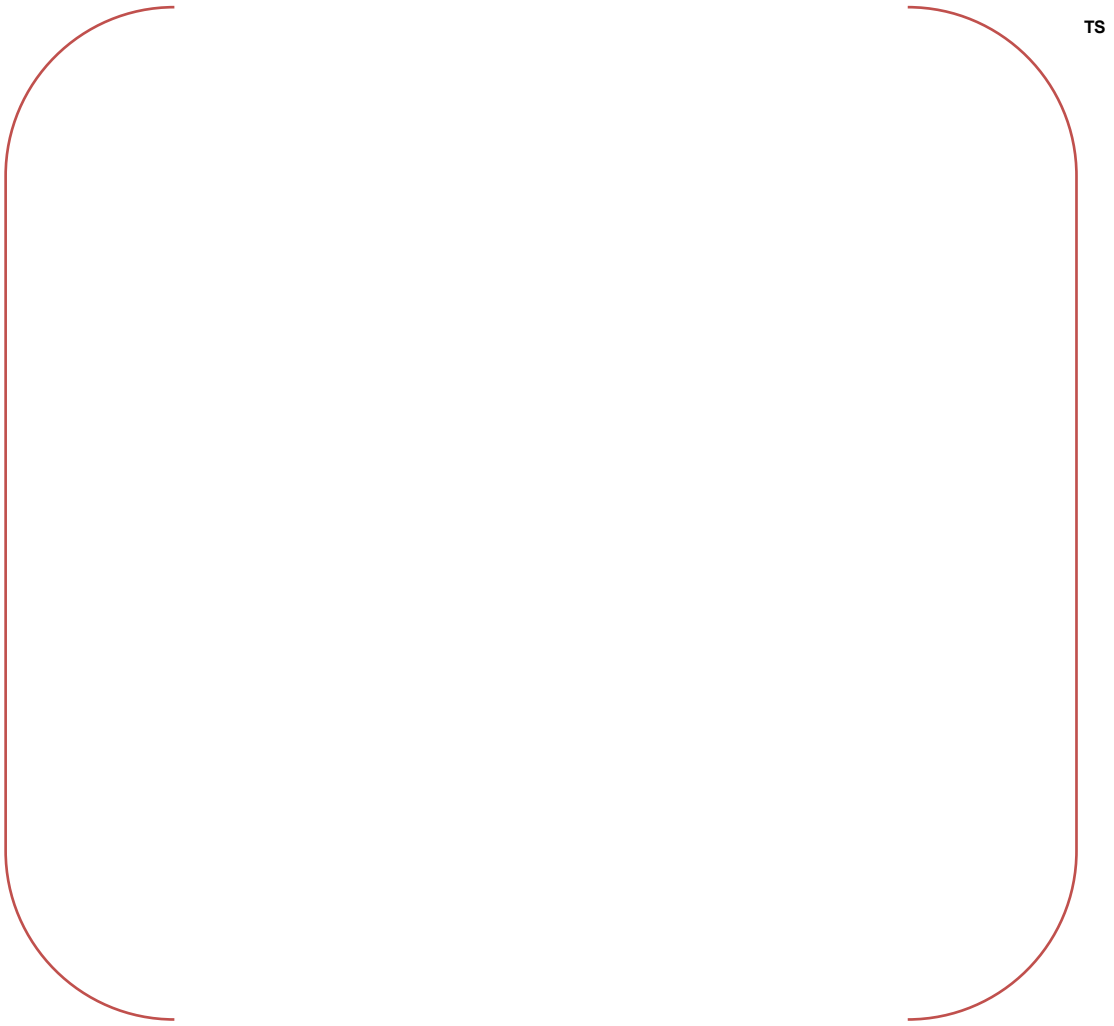

Figure 5-10 SLB with a CCF in the PPS/ESF-CCS; Reactor Coolant Temperature vs. Time

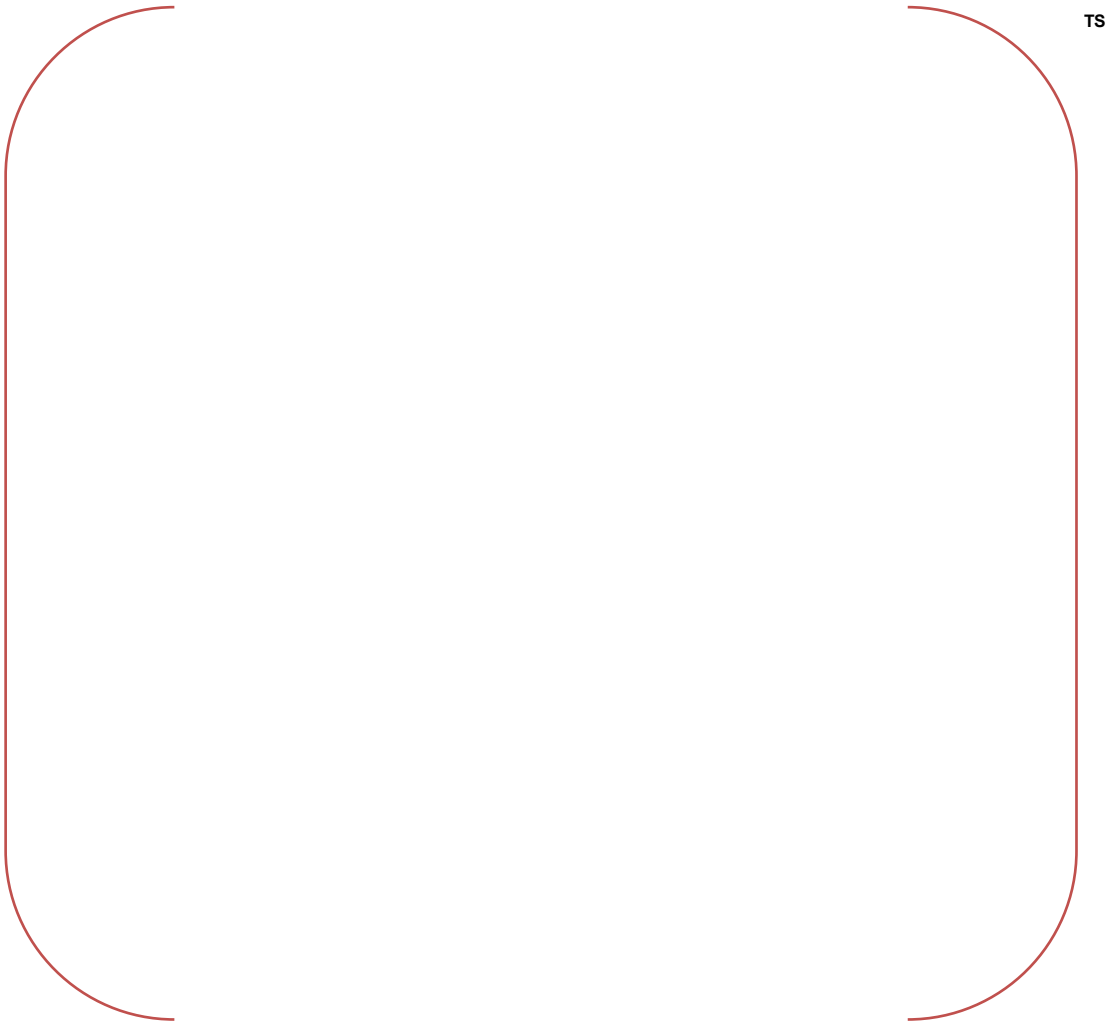

Figure 5-11 SLB with a CCF in the PPS/ESF-CCS; DNBR vs. Time

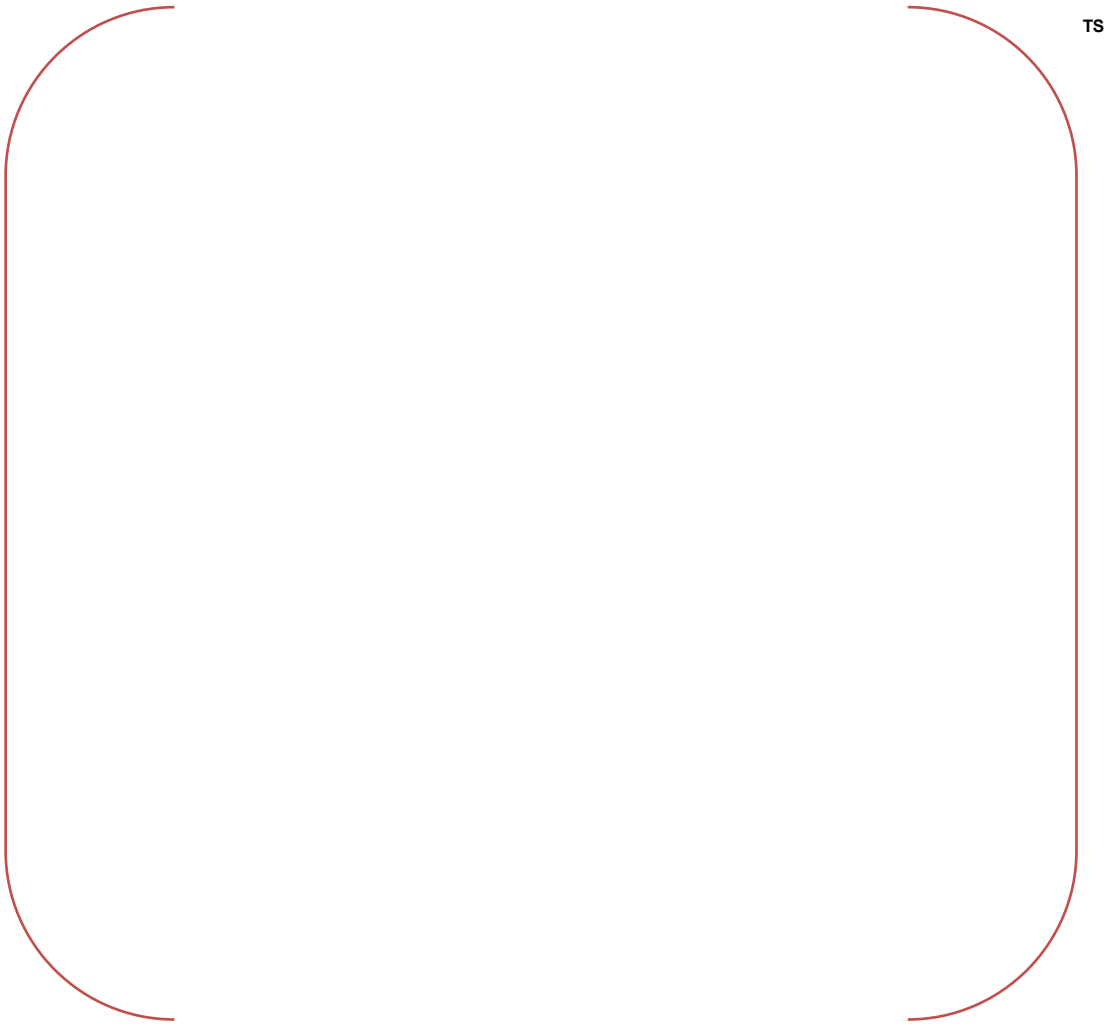

Figure 5-12 SLB with a CCF in the PPS/ESF-CCS; Fuel Centerline Temperature vs. Time

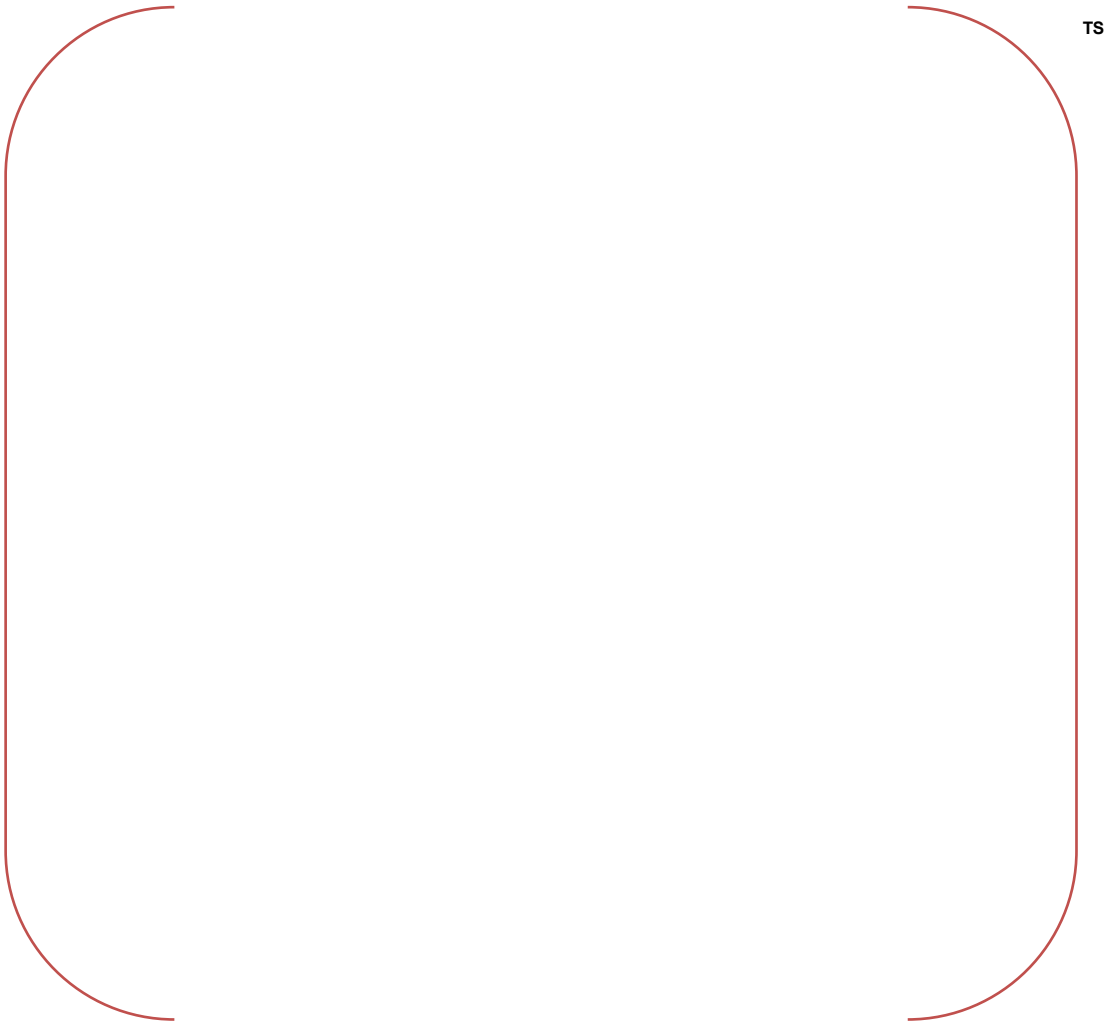

Figure 5-13 SLB with a CCF in the PPS/ESF-CCS; Fuel Cladding Temperature vs. Time

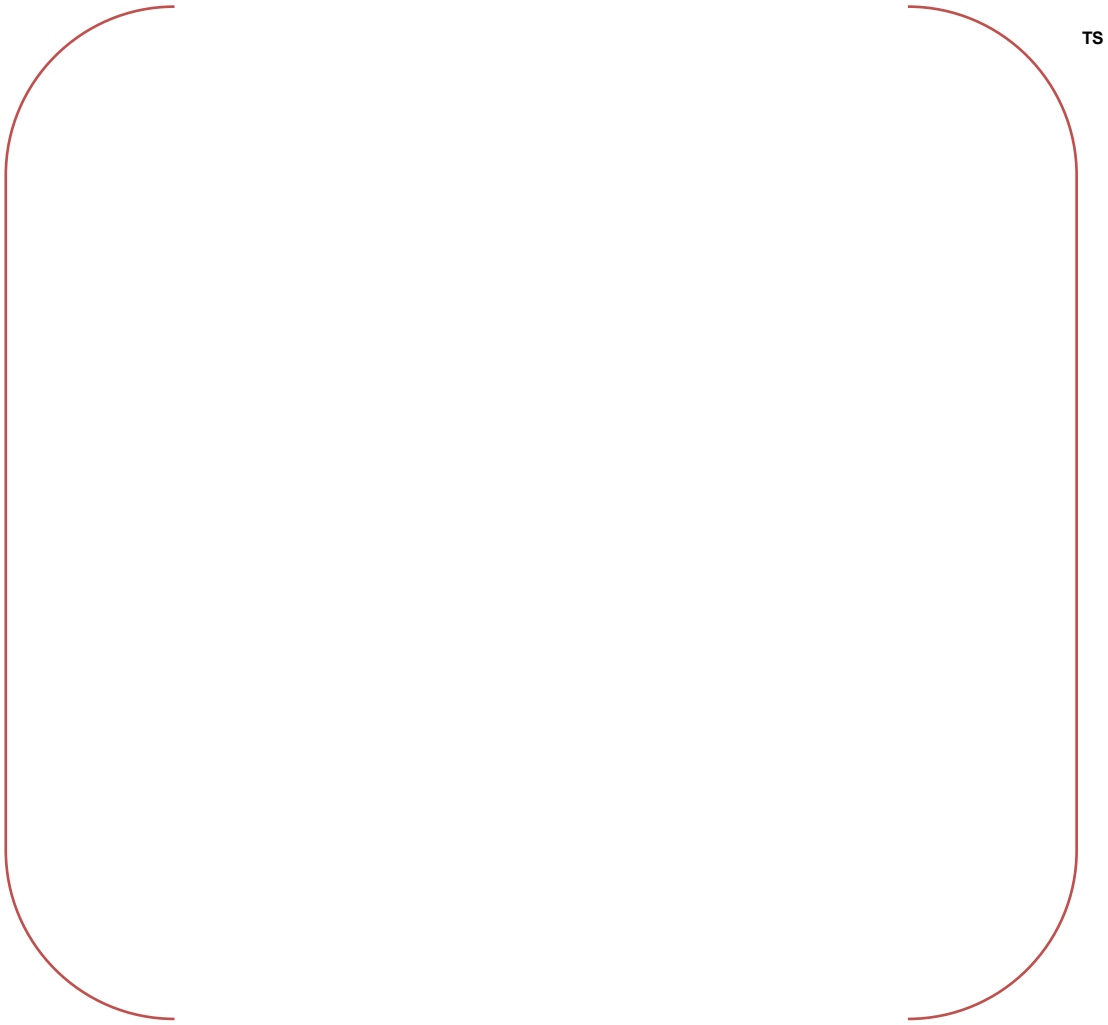

Figure 5-14 TLRCF with a CCF in the PPS/ESF-CCS; Core Power vs. Time (Long Term)

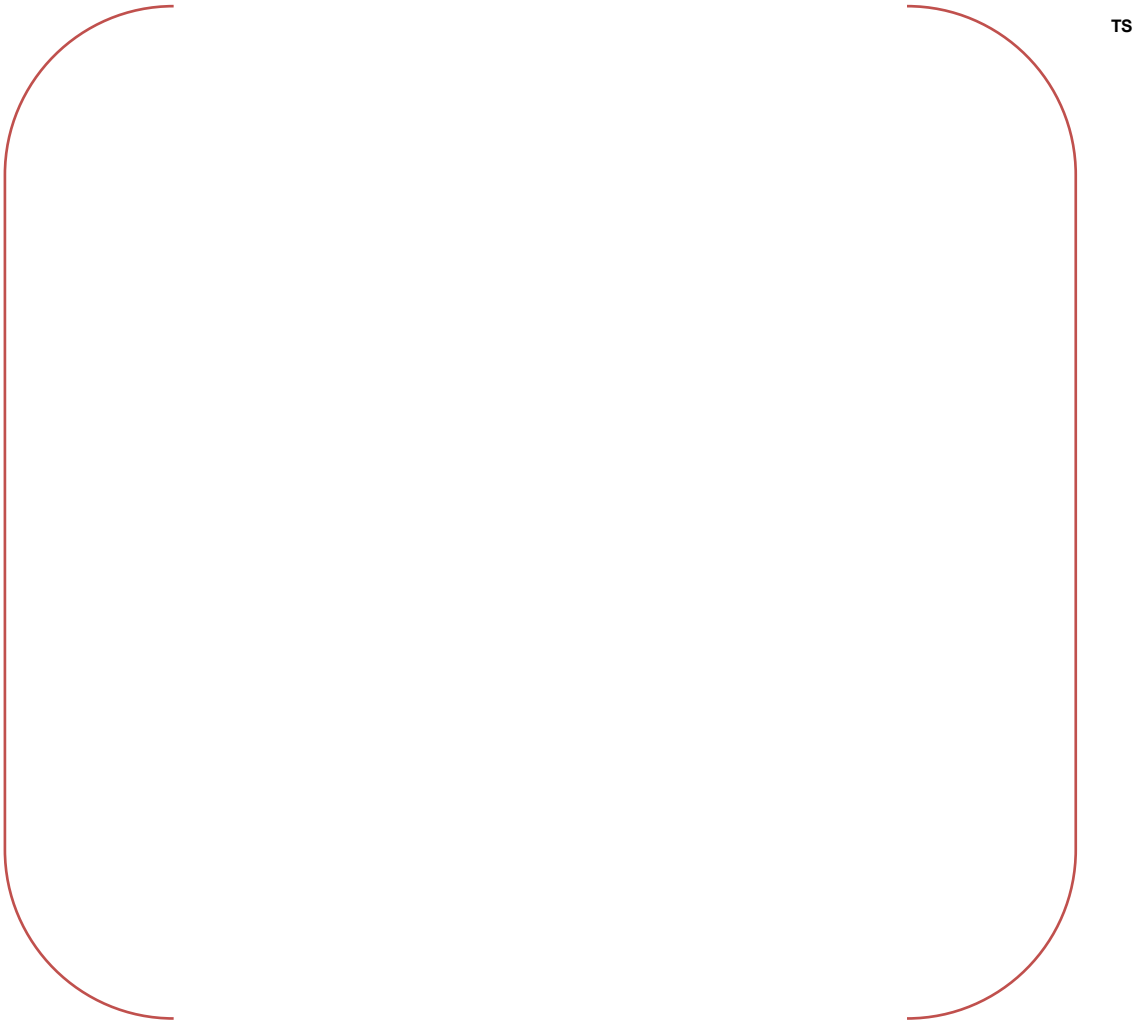

Figure 5-15 TLRCF with a CCF in the PPS/ESF-CCS; Core Power vs. Time (Short Term)

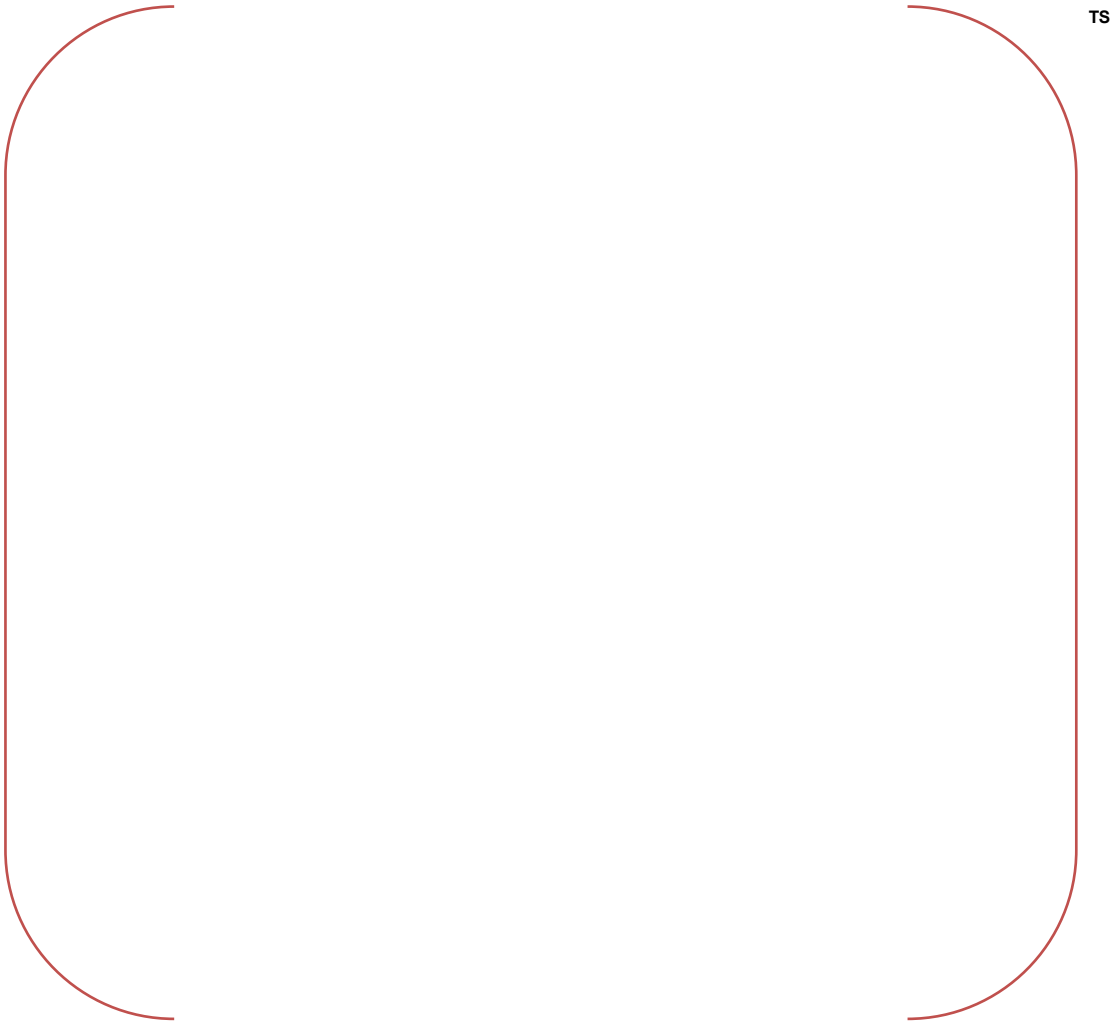

Figure 5-16 TLRCF with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

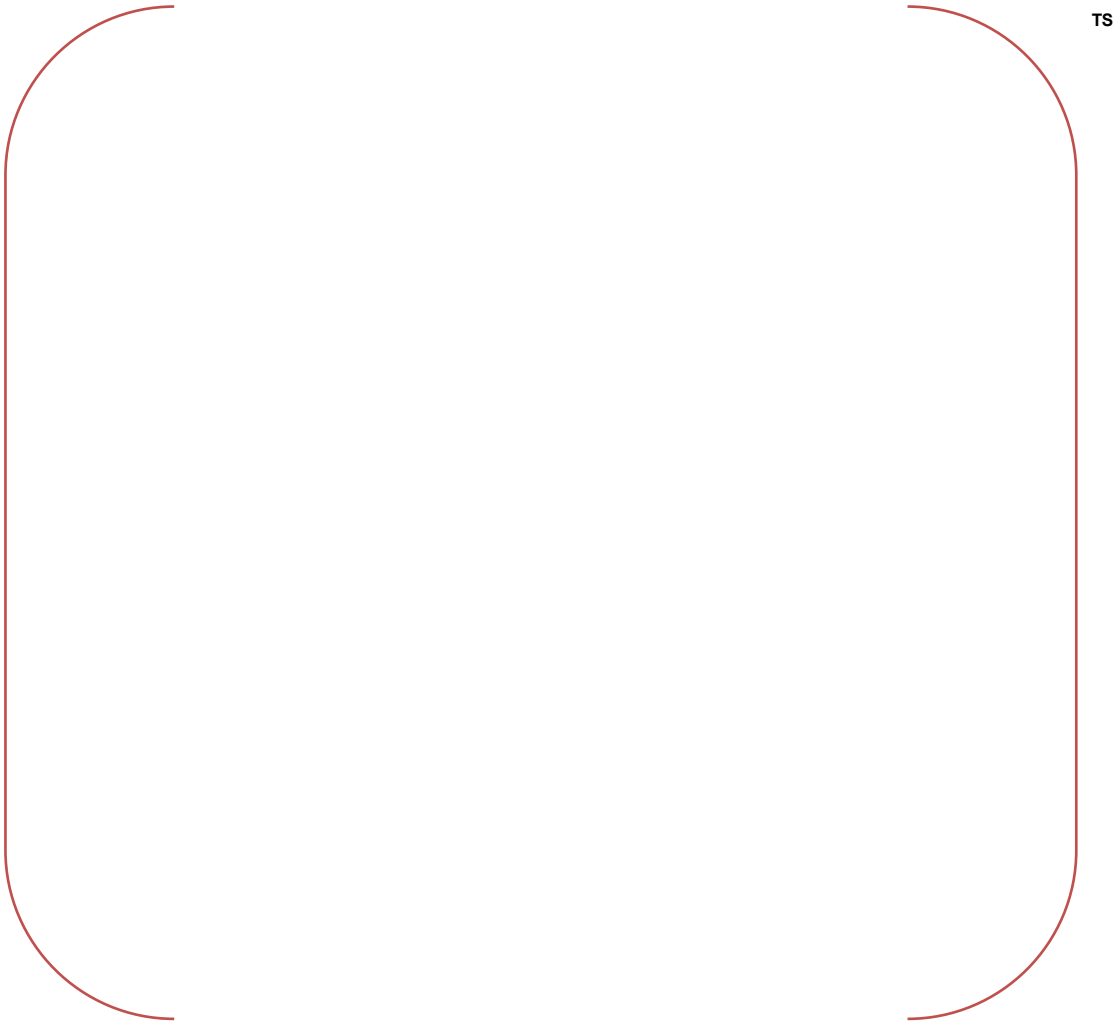

Figure 5-17 TLRCF with a CCF in the PPS/ESF-CCS; Reactor Coolant Temperature vs. Time

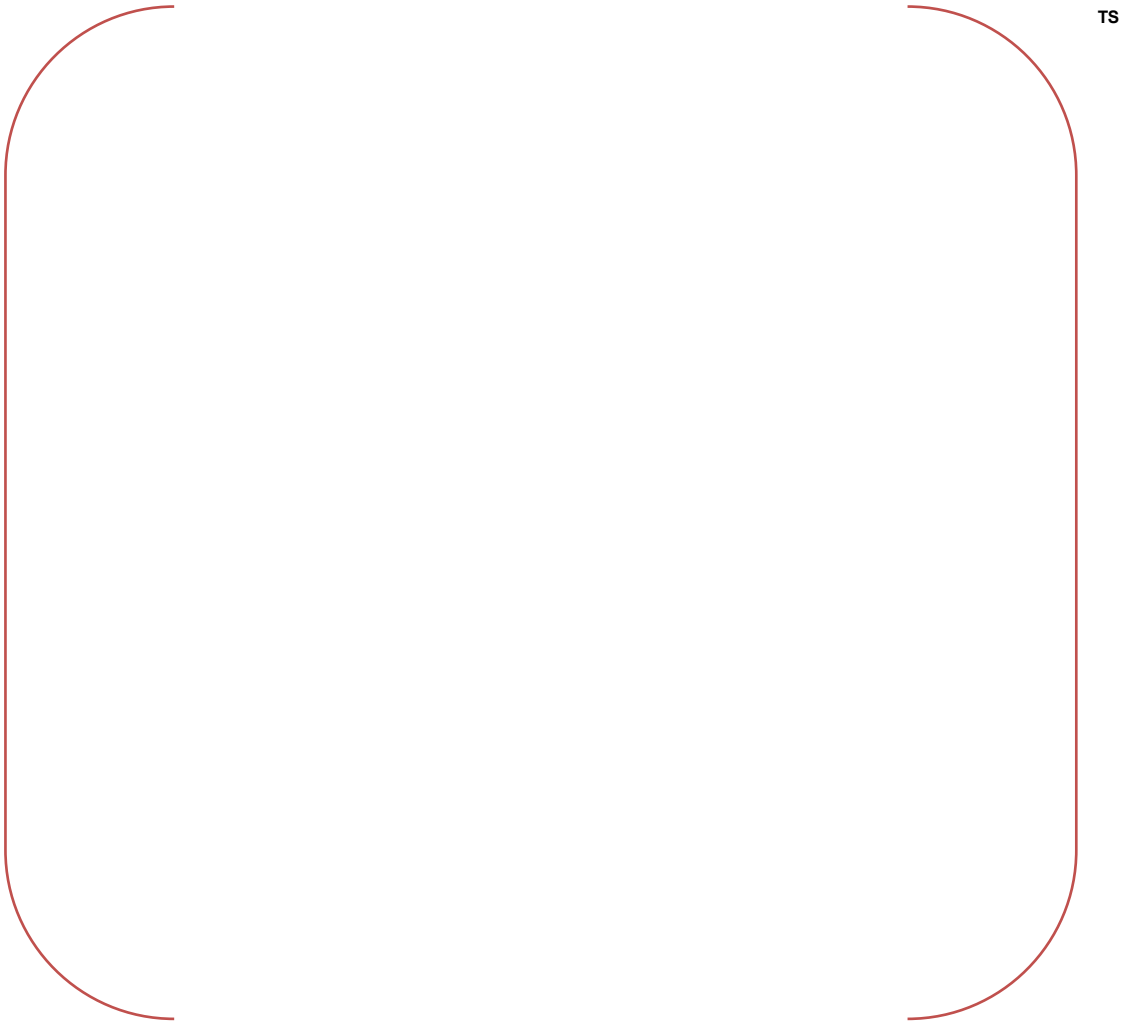

Figure 5-18 TLRCF with a CCF in the PPS/ESF-CCS; Core Flow Rate vs. Time

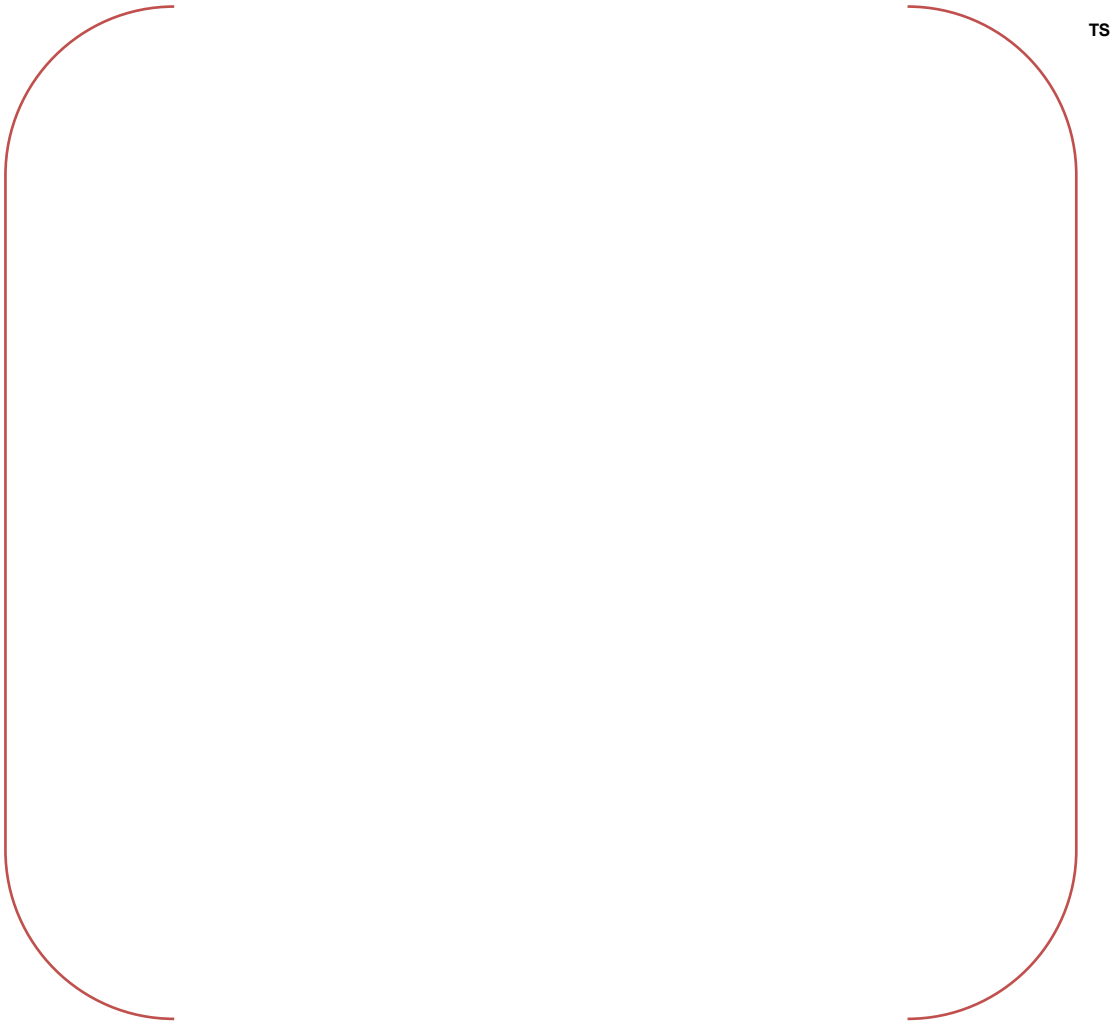

Figure 5-19 TLRCF with a CCF in the PPS/ESF-CCS; DNBR vs. Time

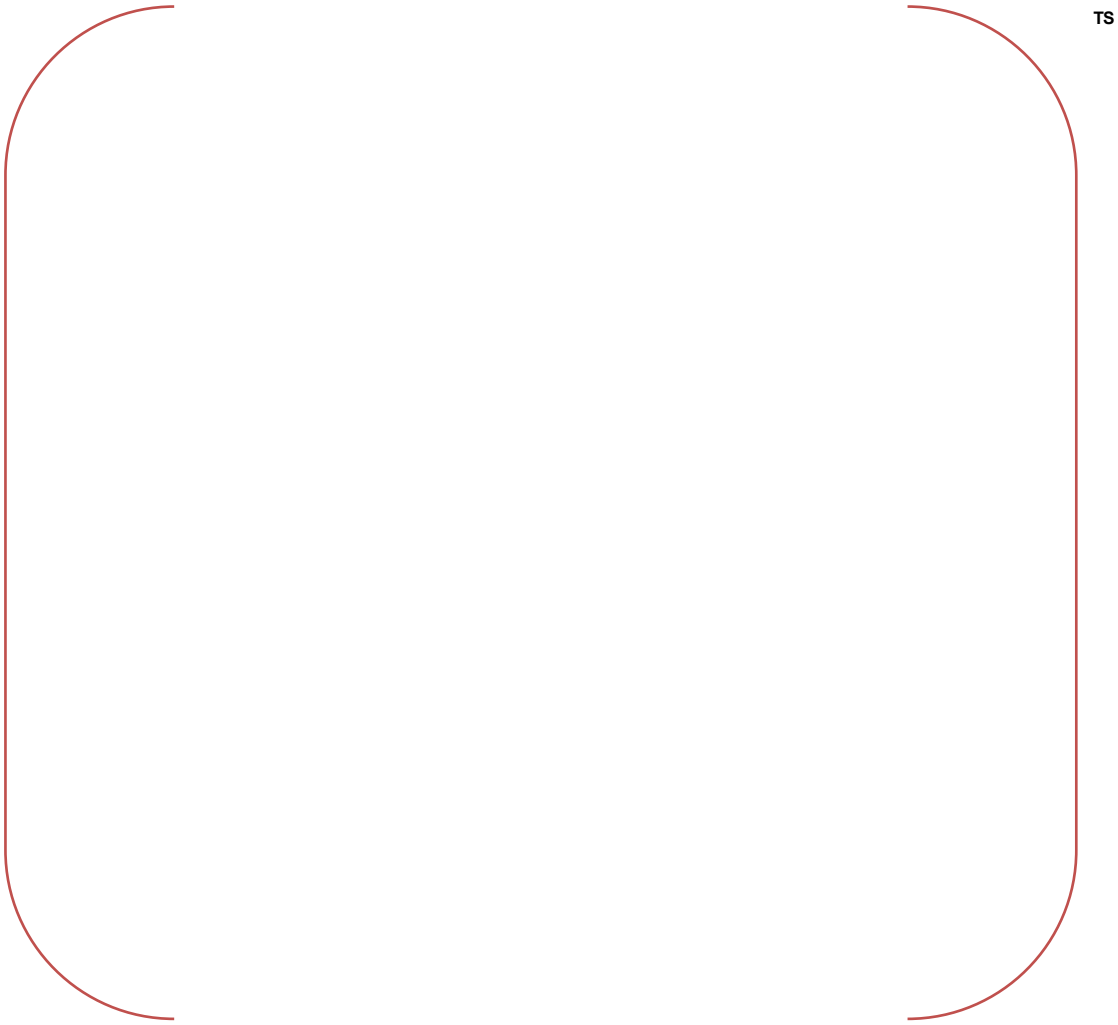

Figure 5-20 RCP SS/SB with a CCF in the PPS/ESF-CCS; Core Power vs. Time

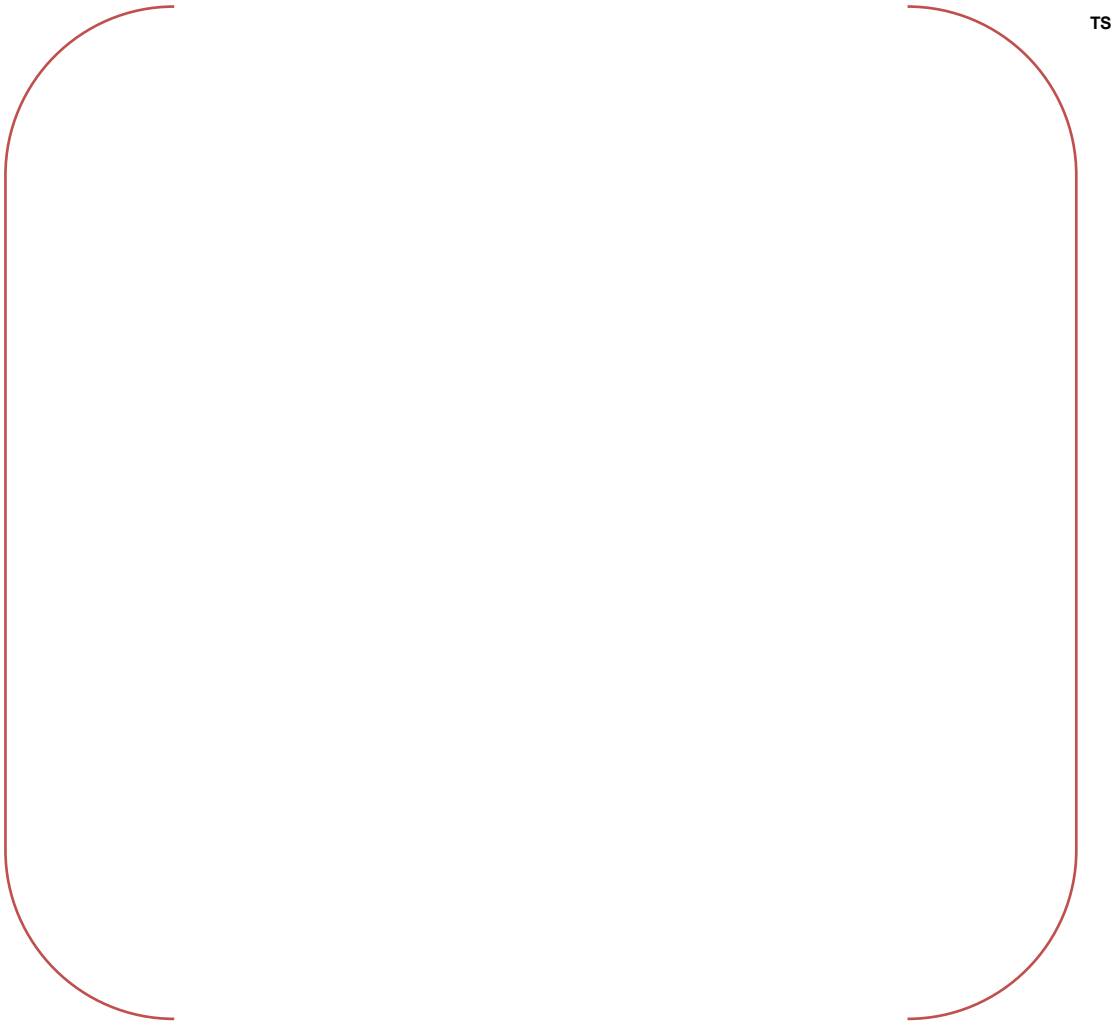

Figure 5-21 RCP SS/SB with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

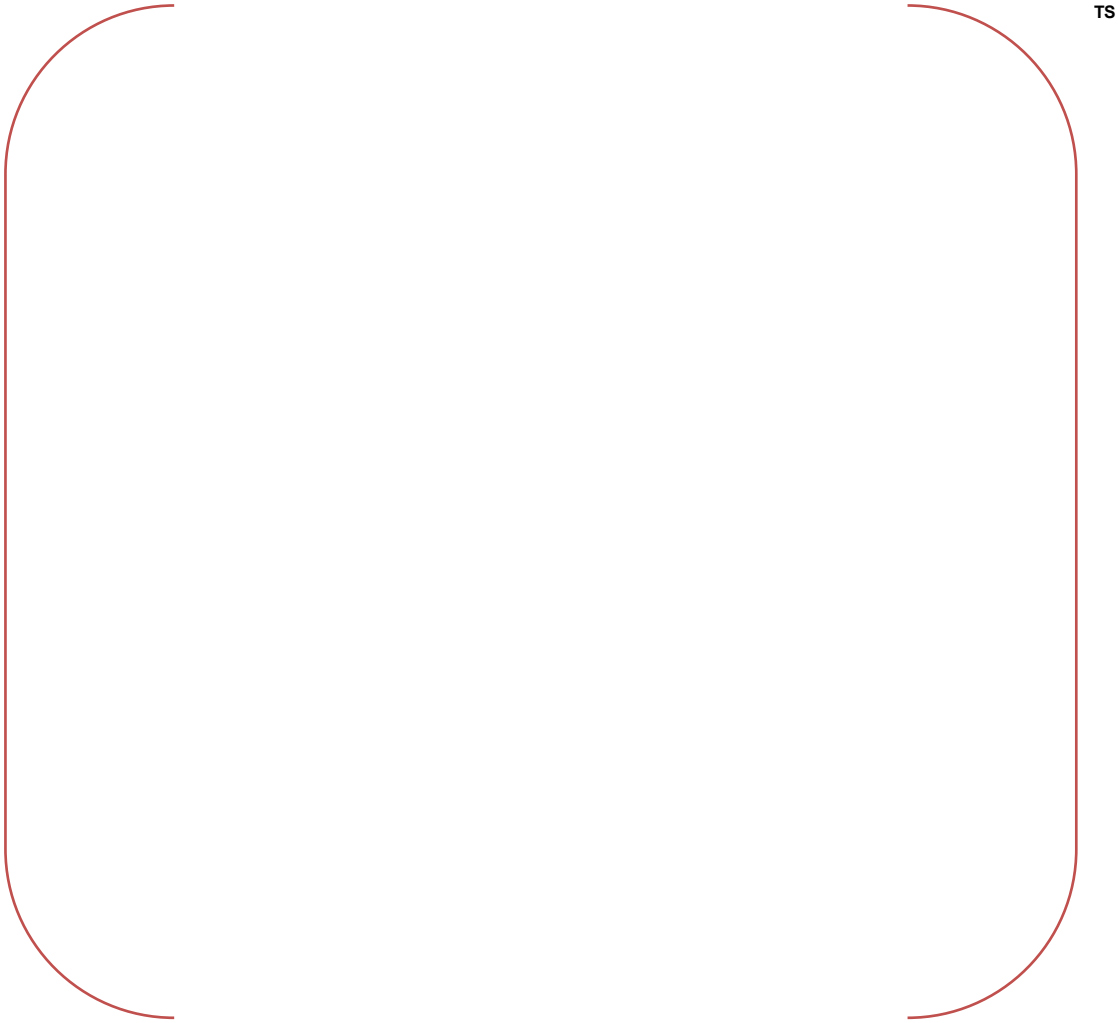

Figure 5-22 RCP SS/SB with a CCF in the PPS/ESF-CCS; Reactor Coolant Temperature vs. Time

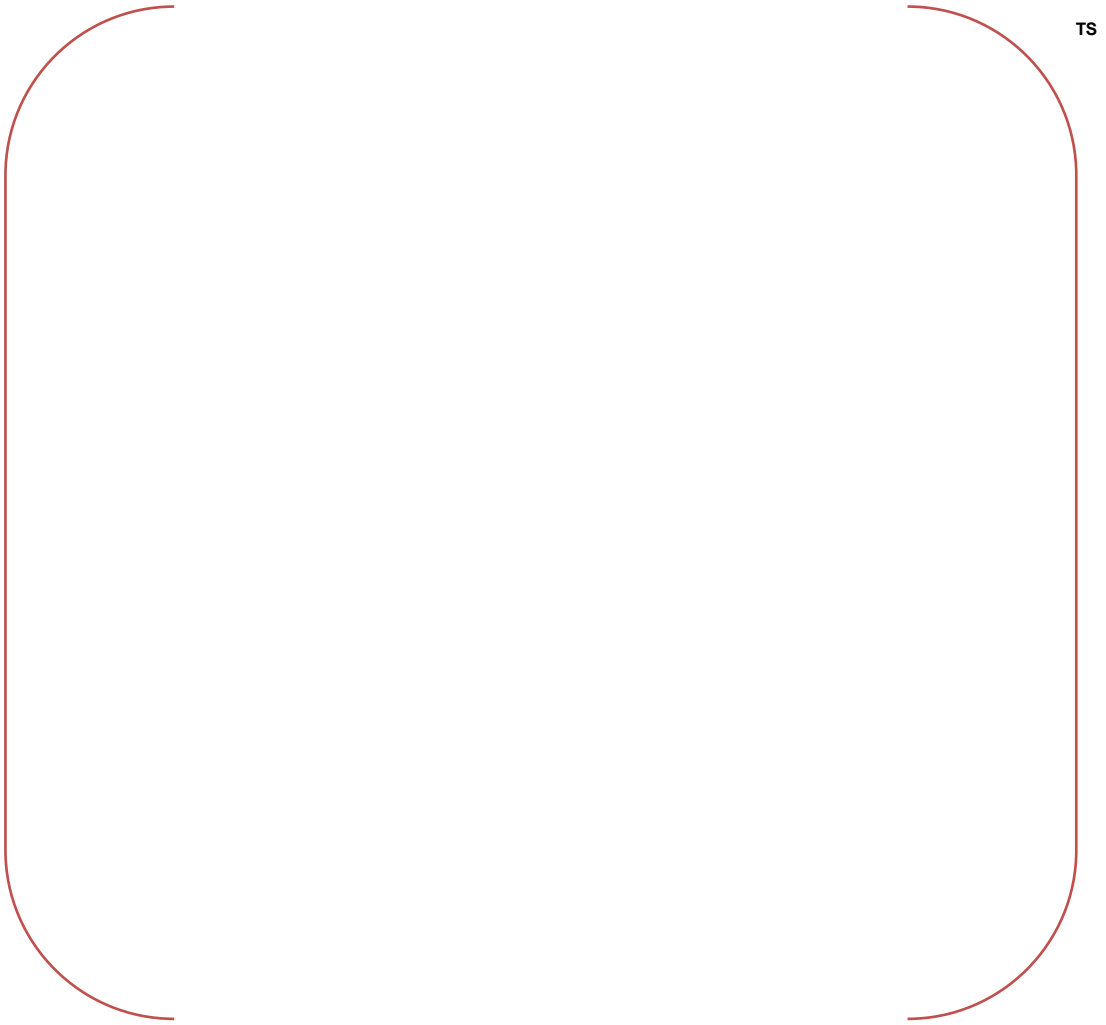

Figure 5-23 RCP SS/SB with a CCF in the PPS/ESF-CCS; Core Flow Rate vs. Time (Long Term)

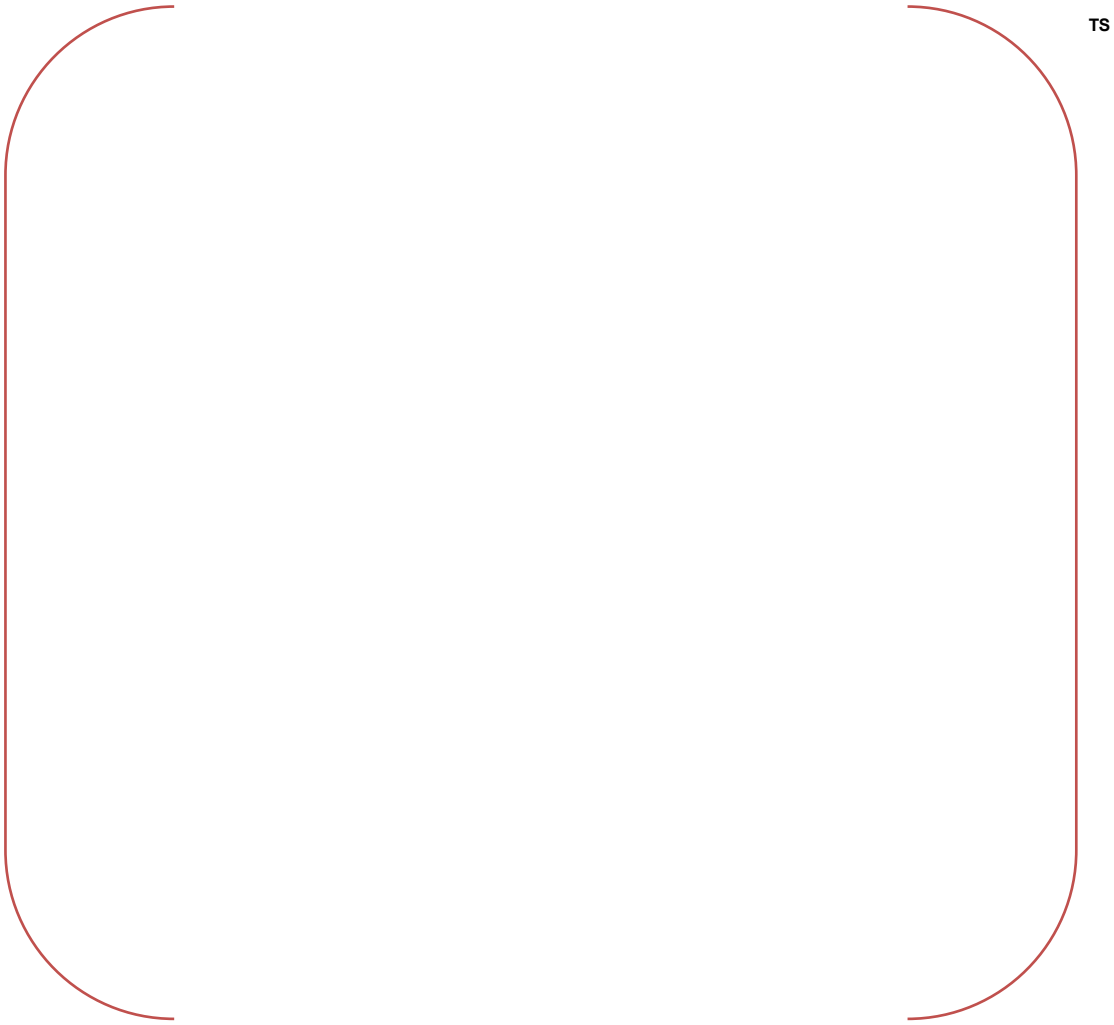

Figure 5-24 RCP SS/SB with a CCF in the PPS/ESF-CCS; Core Flow Rate vs. Time (Short Term)

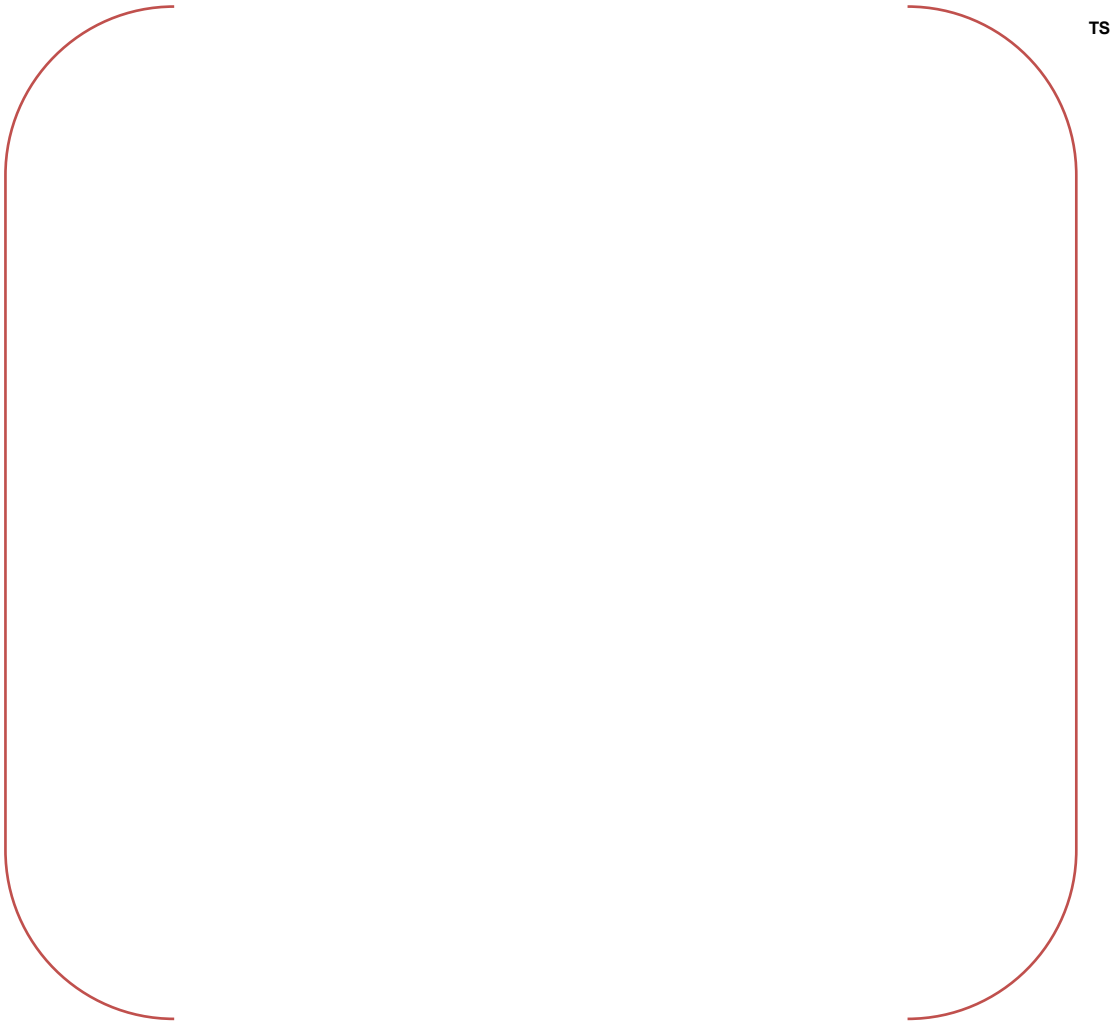

Figure 5-25 RCP SS/SB with a CCF in the PPS/ESF-CCS; DNBR vs. Time (Short Term)

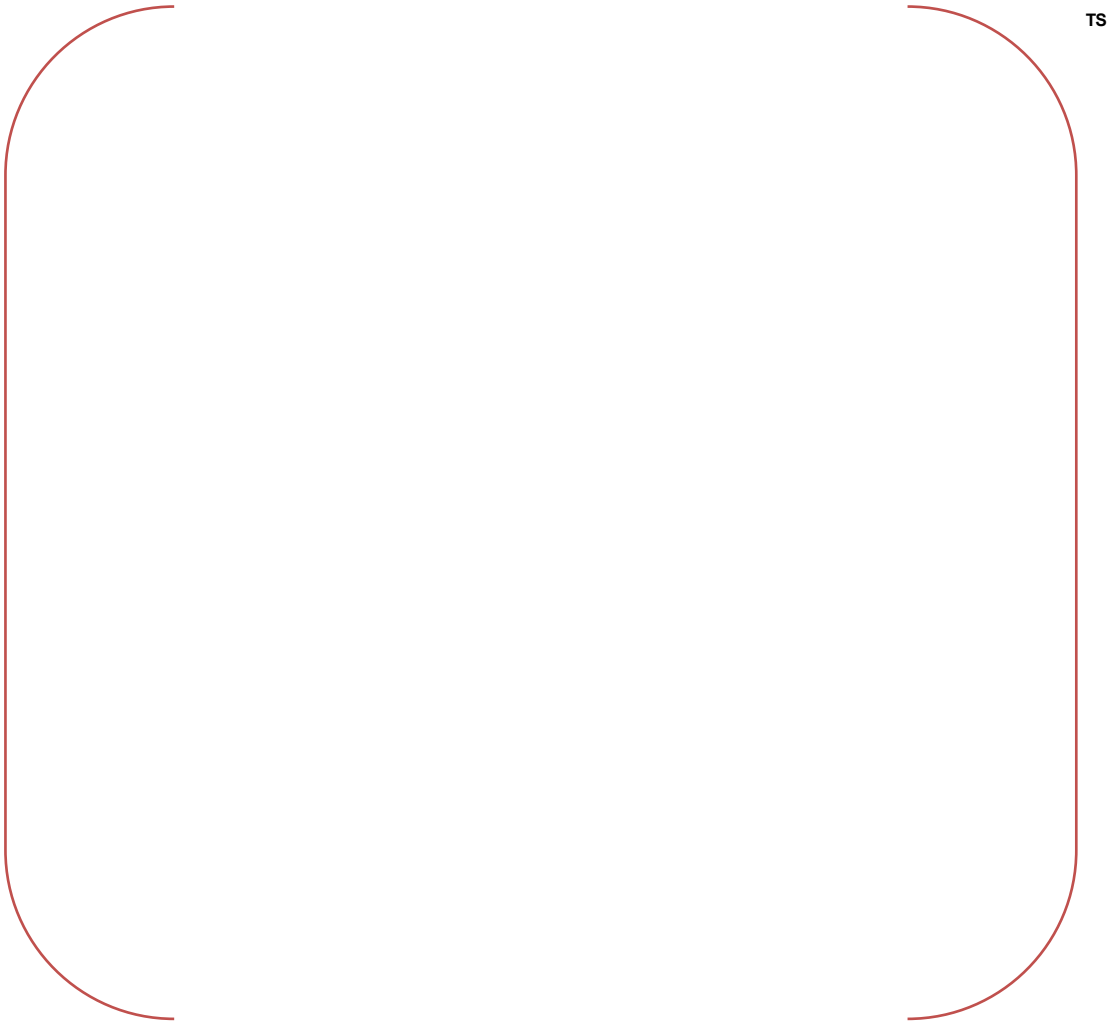

Figure 5-26 RCP SS/SB with a CCF in the PPS/ESF-CCS; DNBR vs. Time (Long Term)

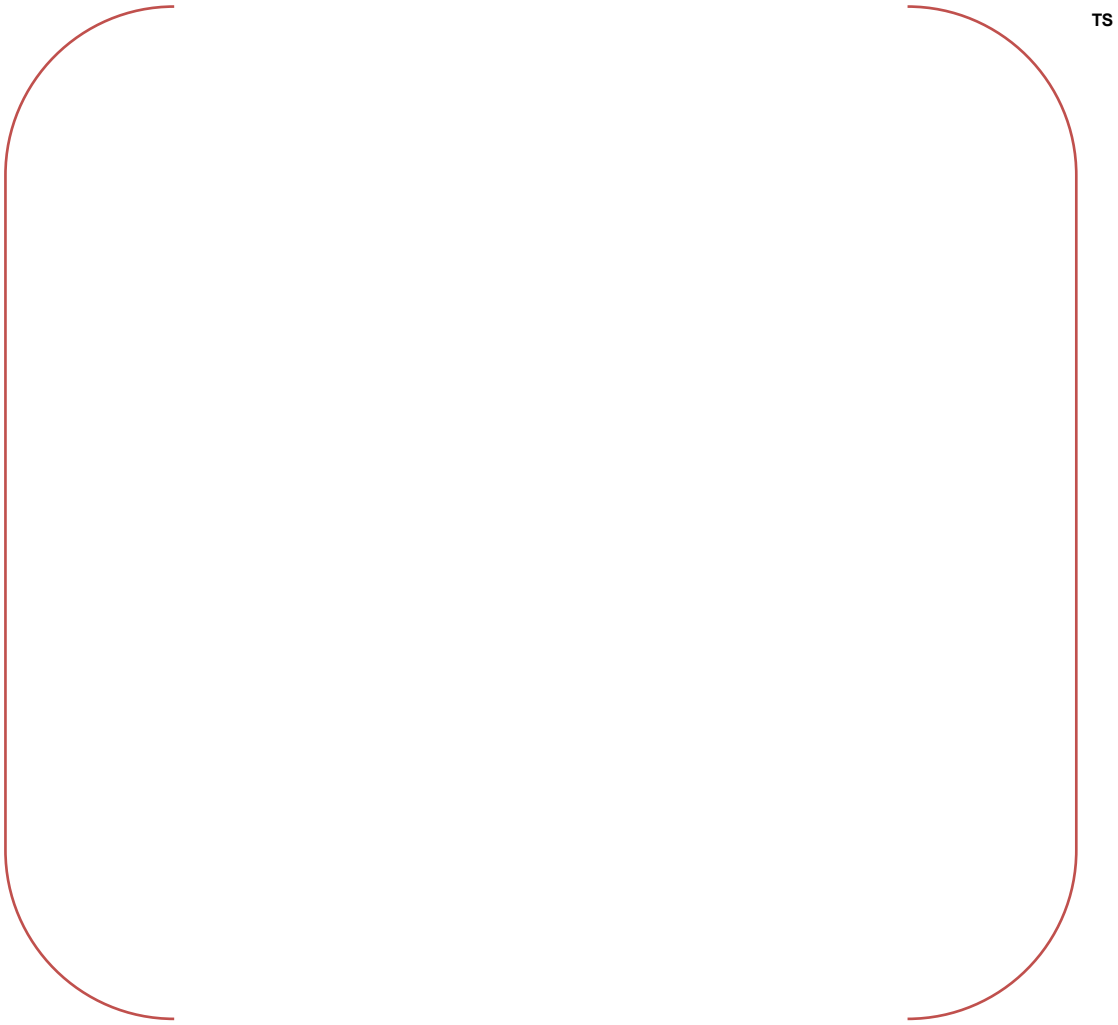

Figure 5-27 CEA Ejection with a CCF in the PPS/ESF-CCS; Core Power vs. Time

TS

Figure 5-28 CEA Ejection with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

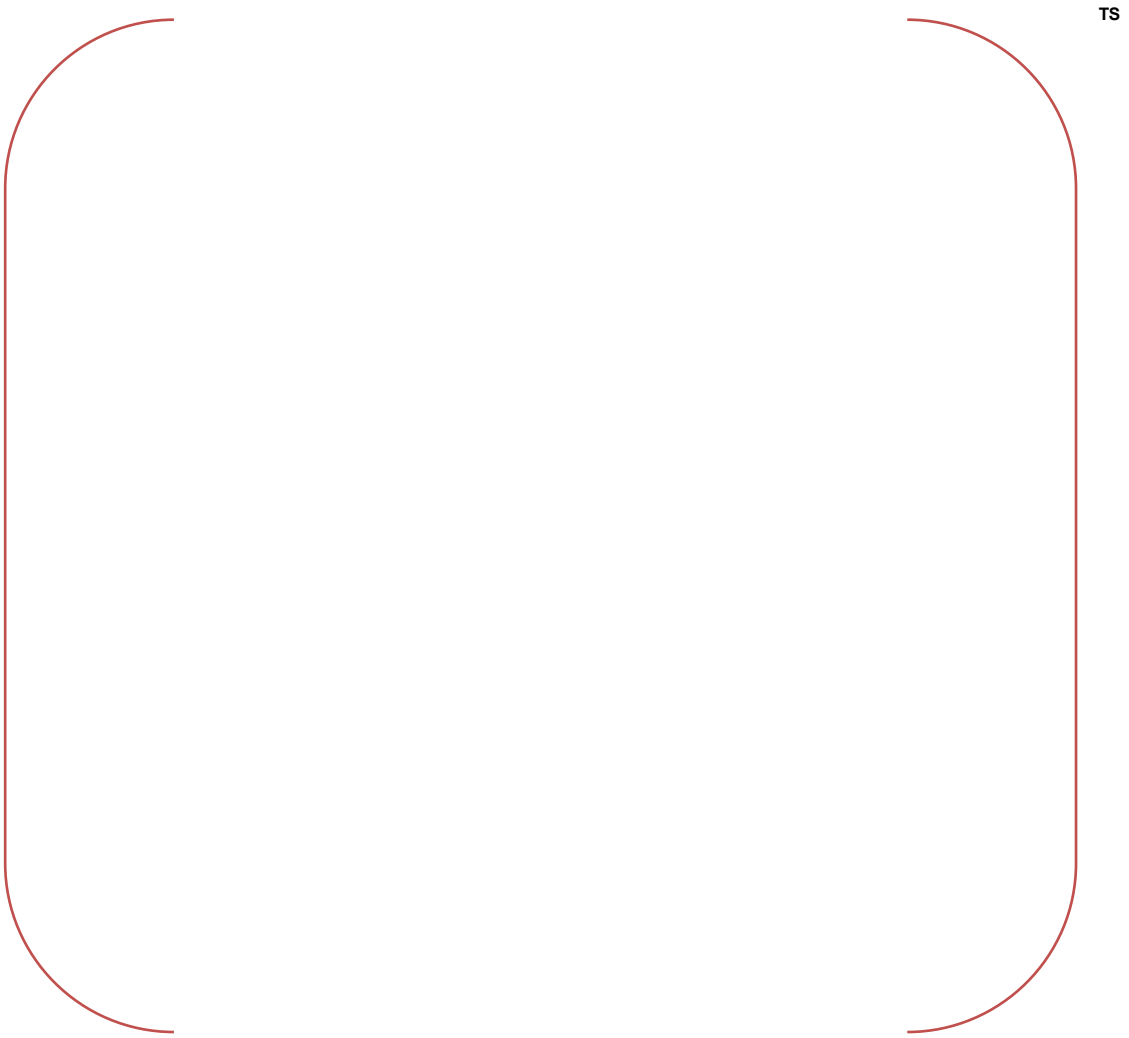

Figure 5-29 CEA Ejection with a CCF in the PPS/ESF-CCS; Reactor Coolant Flow Rate vs. Time

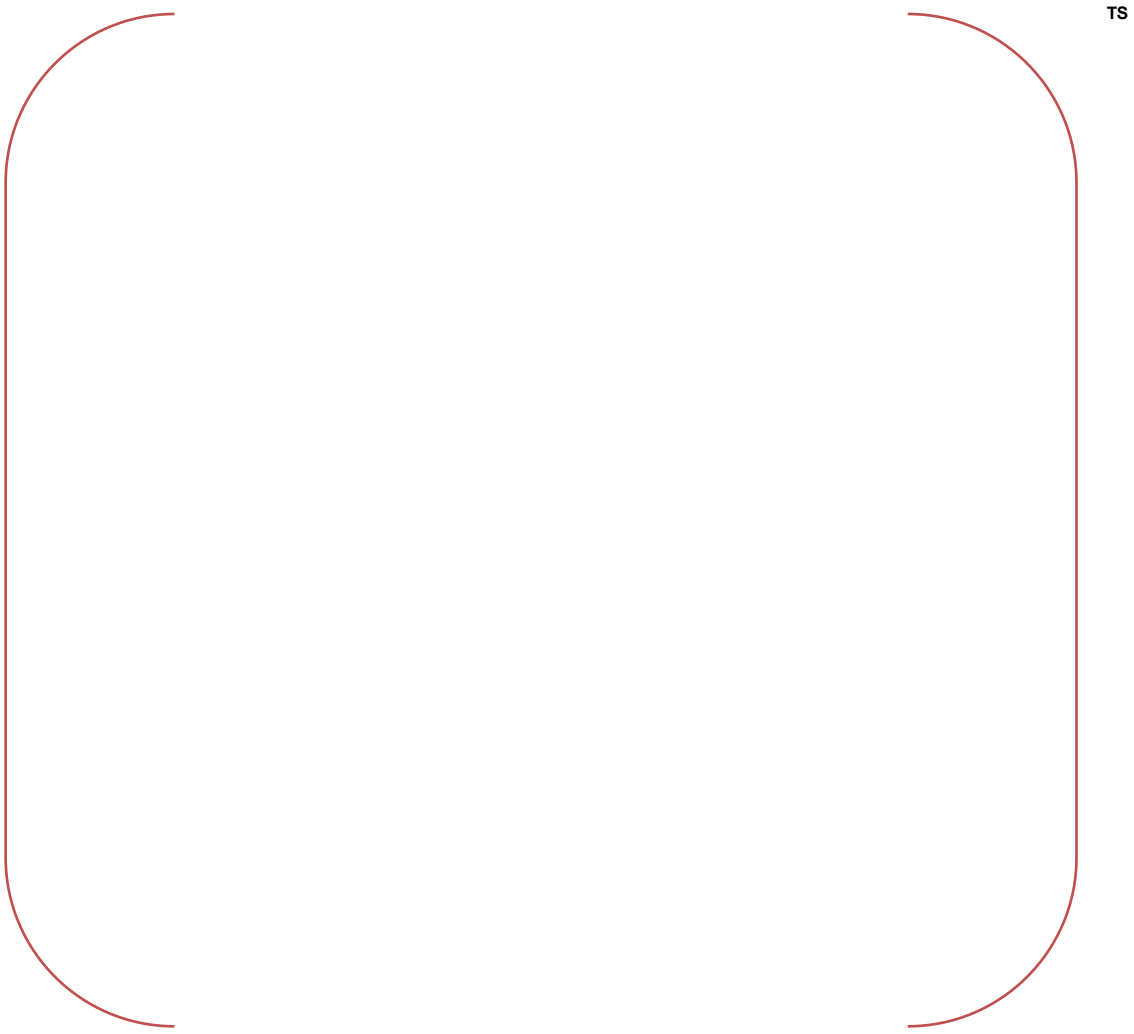

Figure 5-30 CEA Ejection with a CCF in the PPS/ESF-CCS; Reactor Coolant Temperature vs. Time

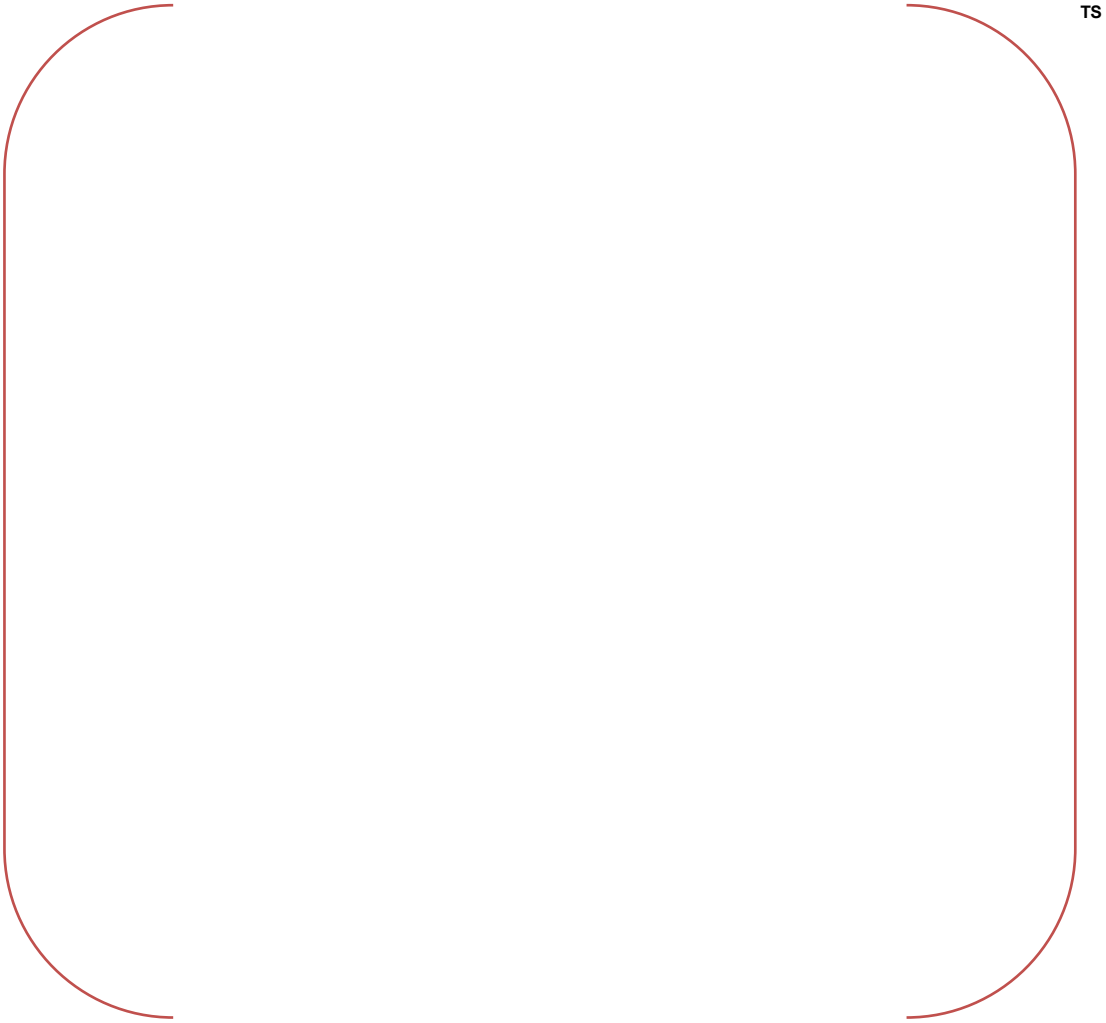

Figure 5-31 CEA Ejection with a CCF in the PPS/ESF-CCS; DNBR vs. Time

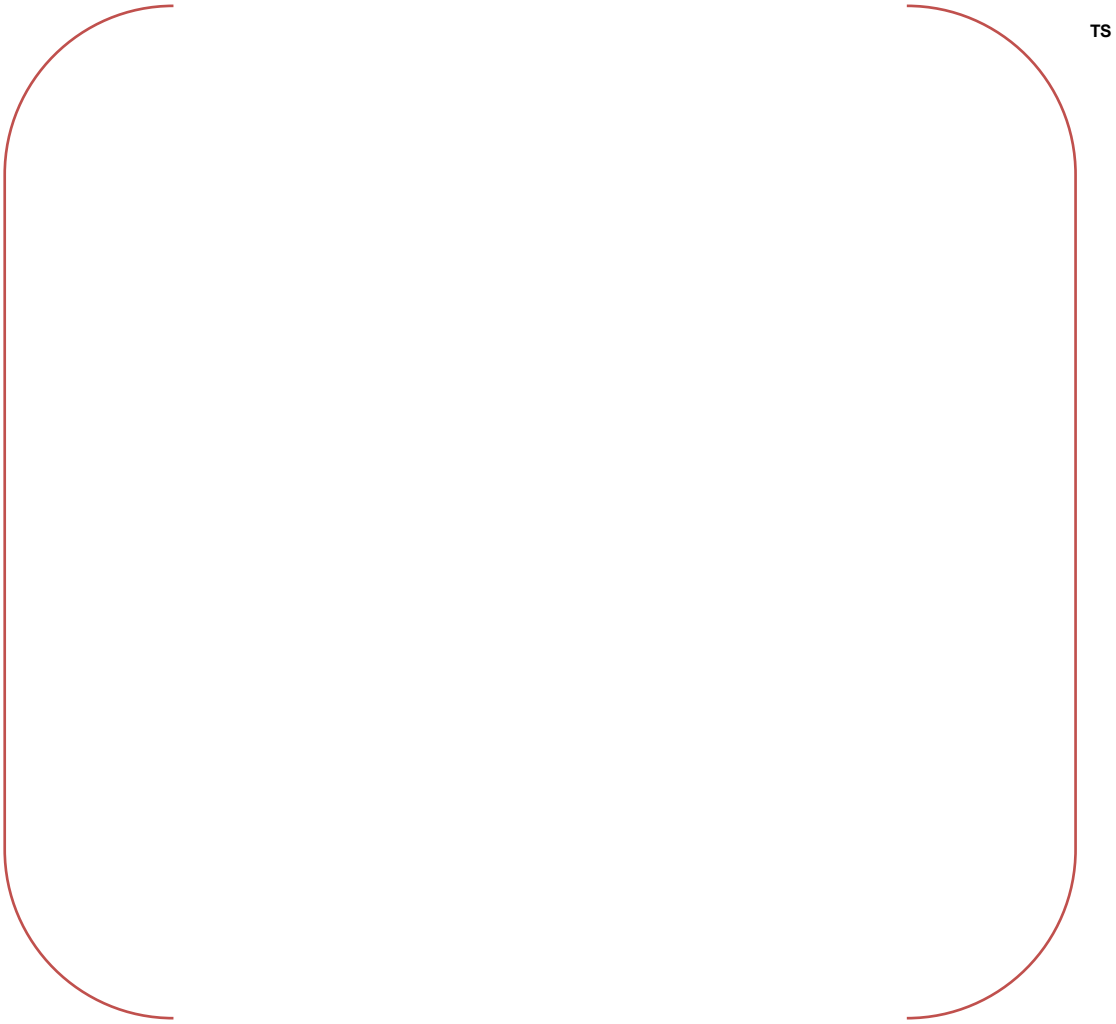

Figure 5-32 CEA Ejection with a CCF in the PPS/ESF-CCS; Fuel Cladding Temperature vs. Time

TS

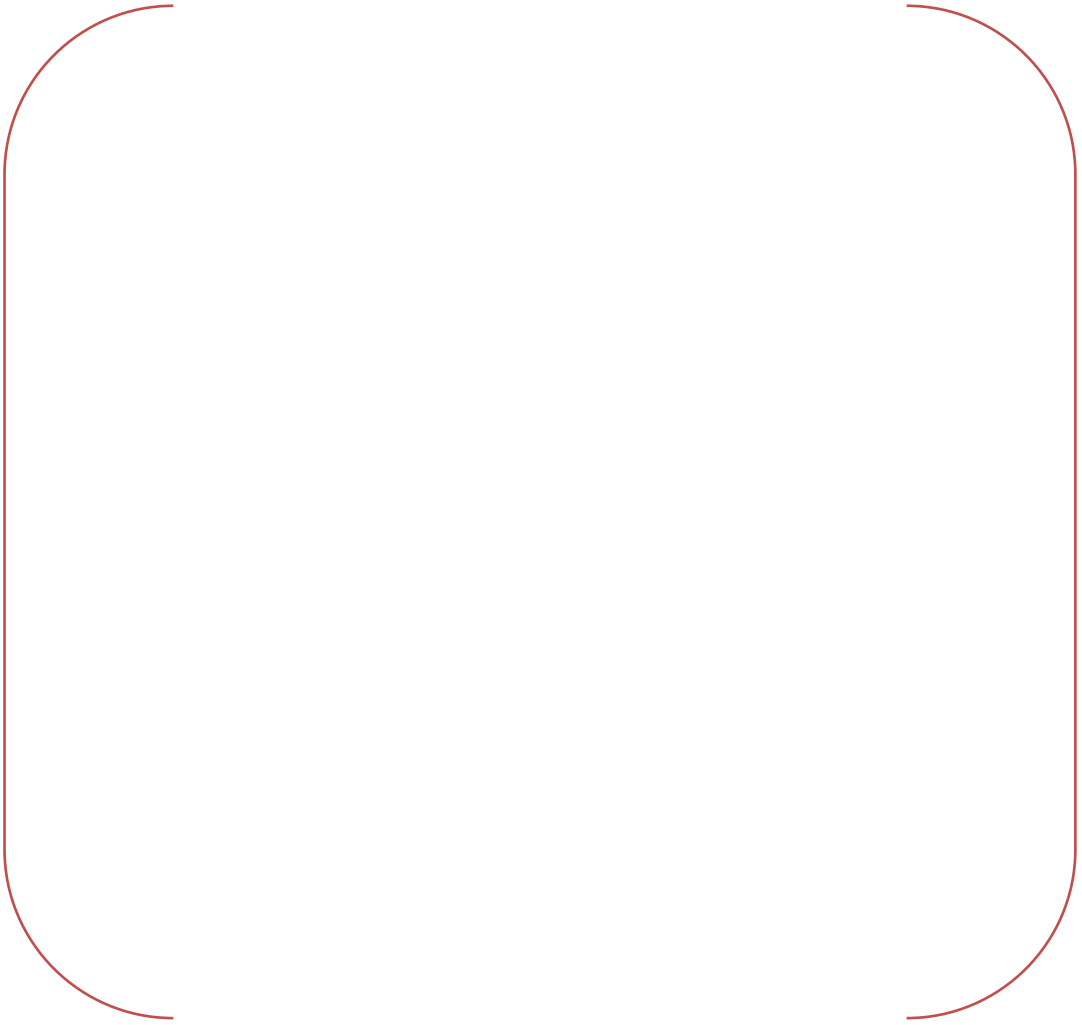

Figure 5-33 CEA Ejection with a CCF in the PPS/ESF-CCS; Fuel Centerline Temperature vs. Time

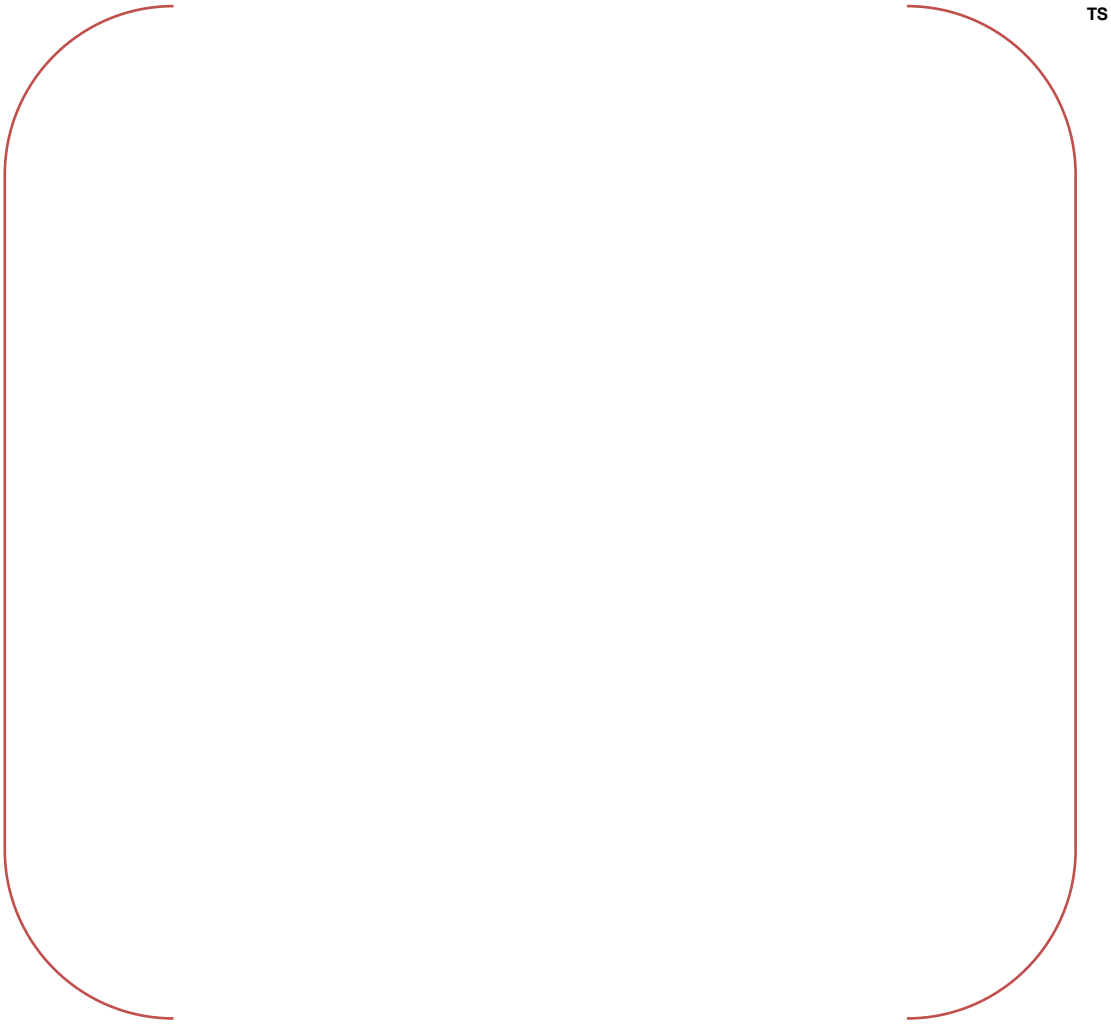

Figure 5-34 SGTR with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

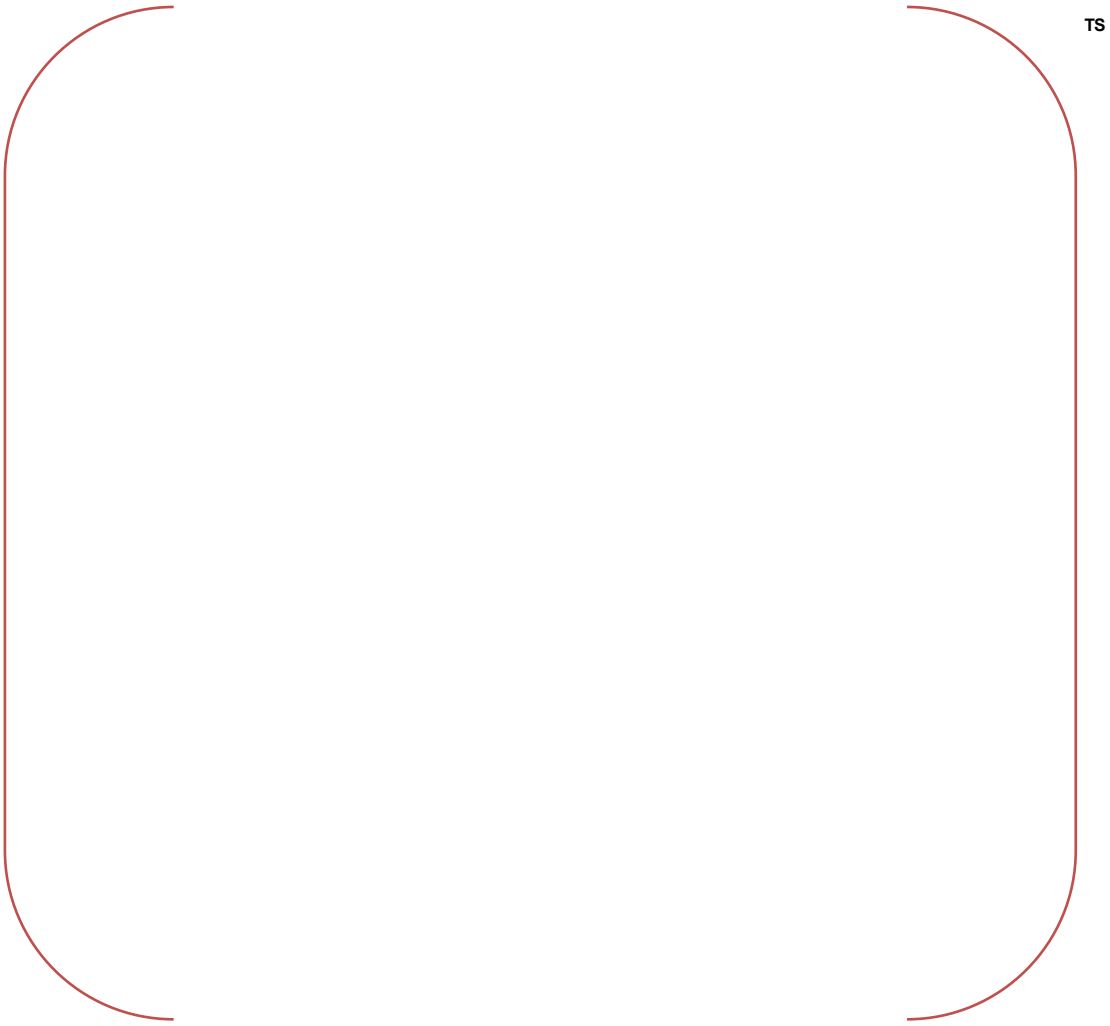

Figure 5-35 SGTR with a CCF in the PPS/ESF-CCS; DNBR vs. Time

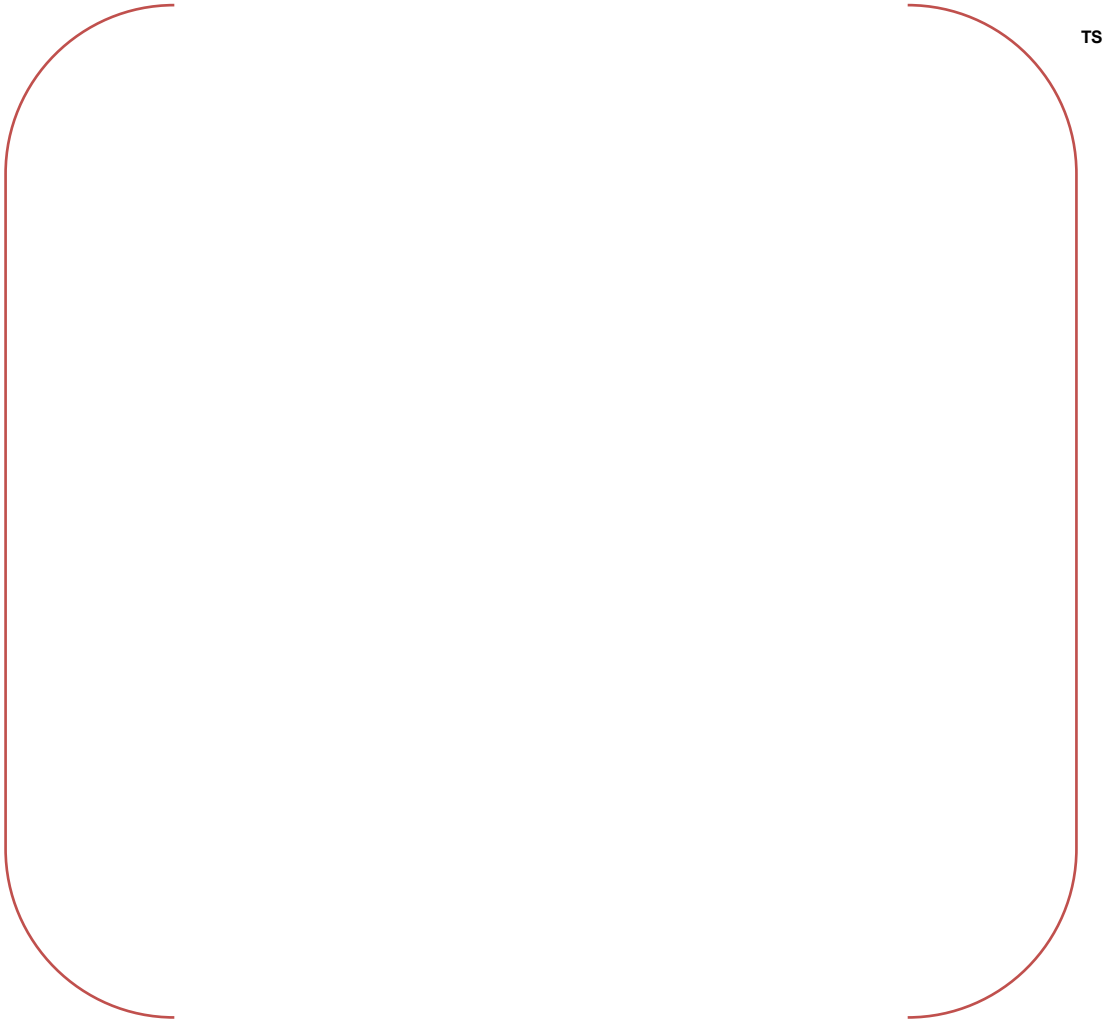

Figure 5-36 SGTR with a CCF in the PPS/ESF-CCS; SG Water Mass vs. Time

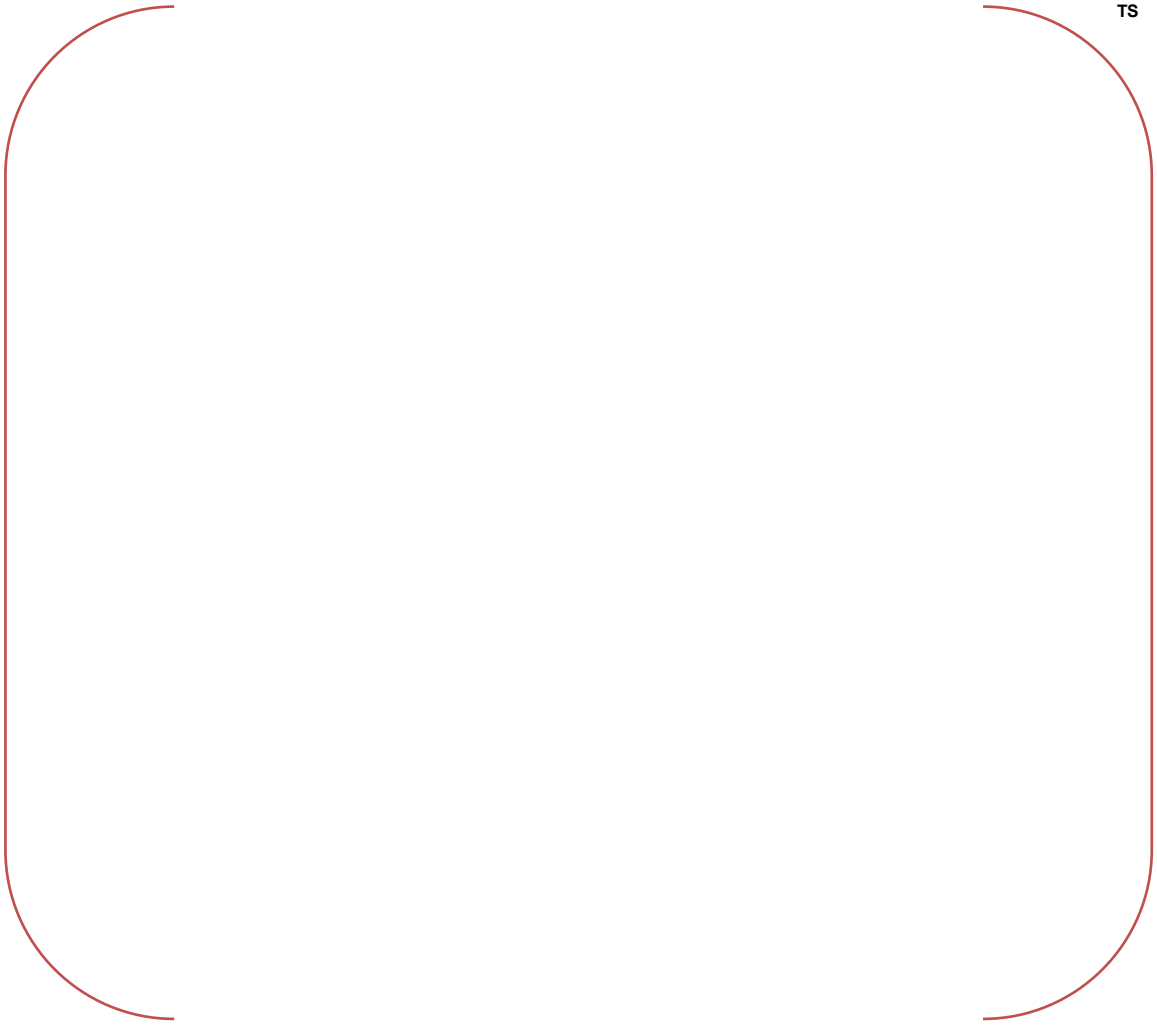

Figure 5-37 LBLOCA with a CCF in the PPS/ESF-CCS; RCS Pressure vs. Time

TS

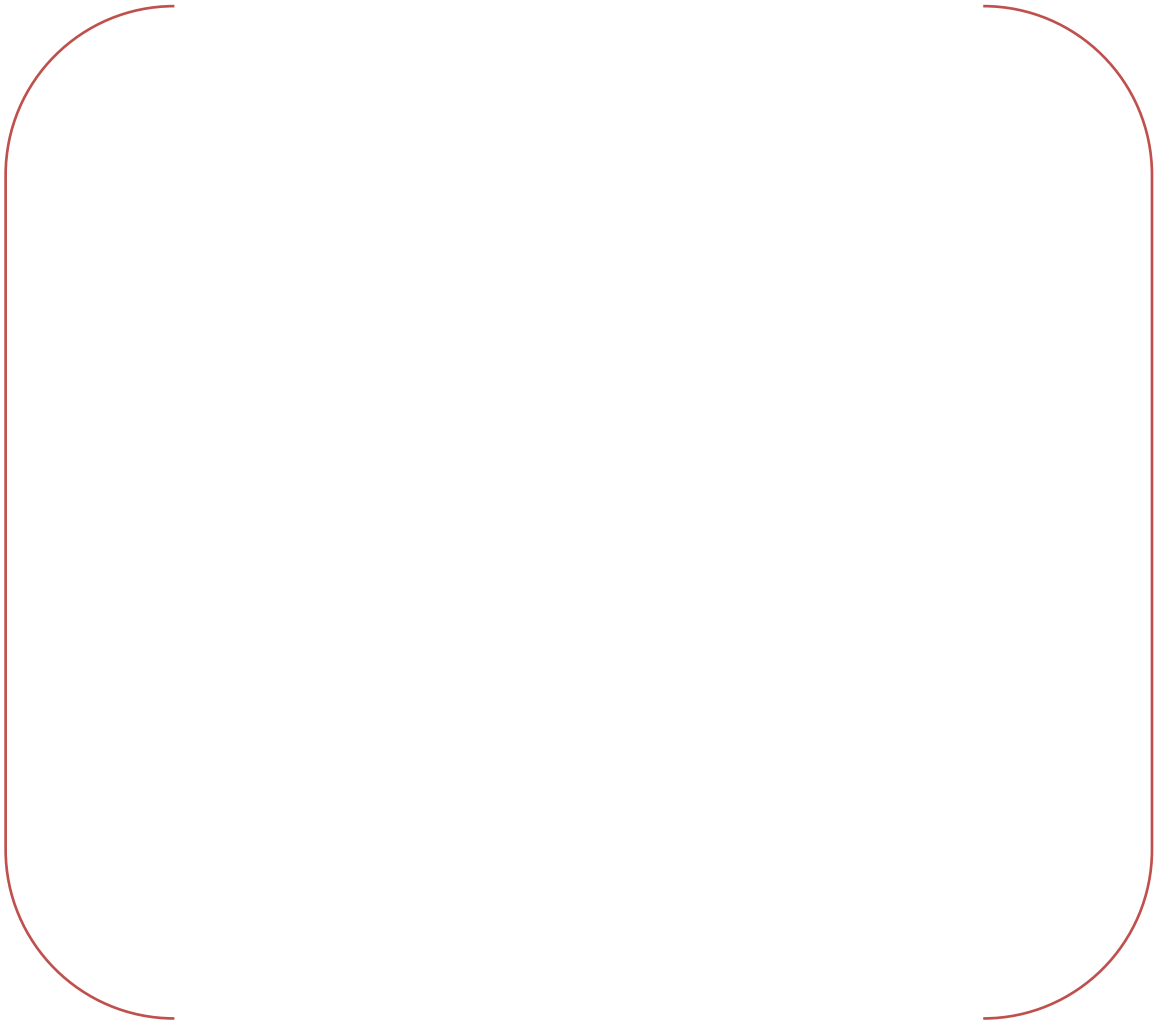

Figure 5-38 LBLOCA with a CCF in the PPS/ESF-CCS; SIT and Safety Injection Flow vs. Time

TS

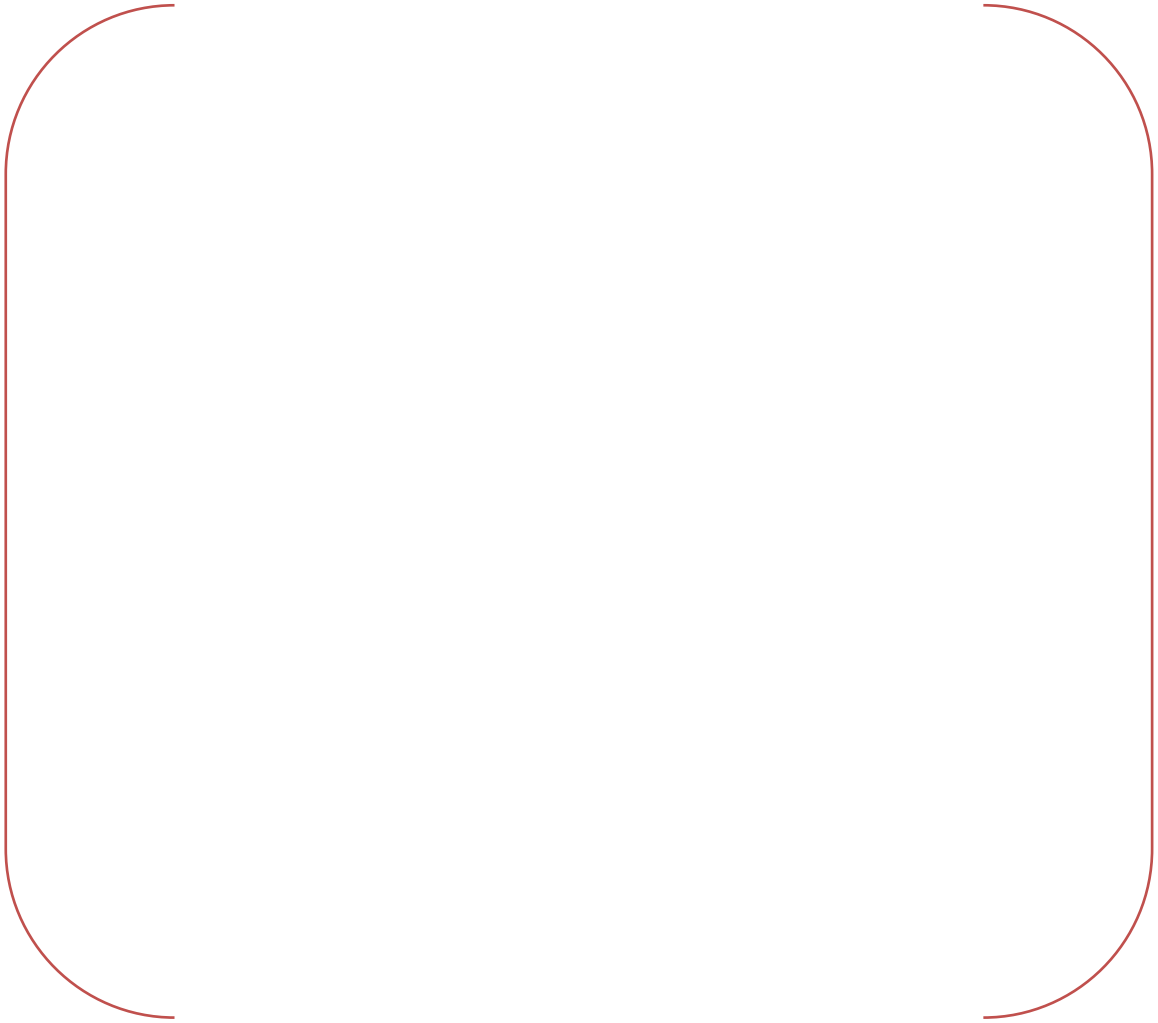

Figure 5-39 LBLOCA with a CCF in the PPS/ESF-CCS; RV Collapsed Water Level w/o Auto S IAS vs. Time

TS

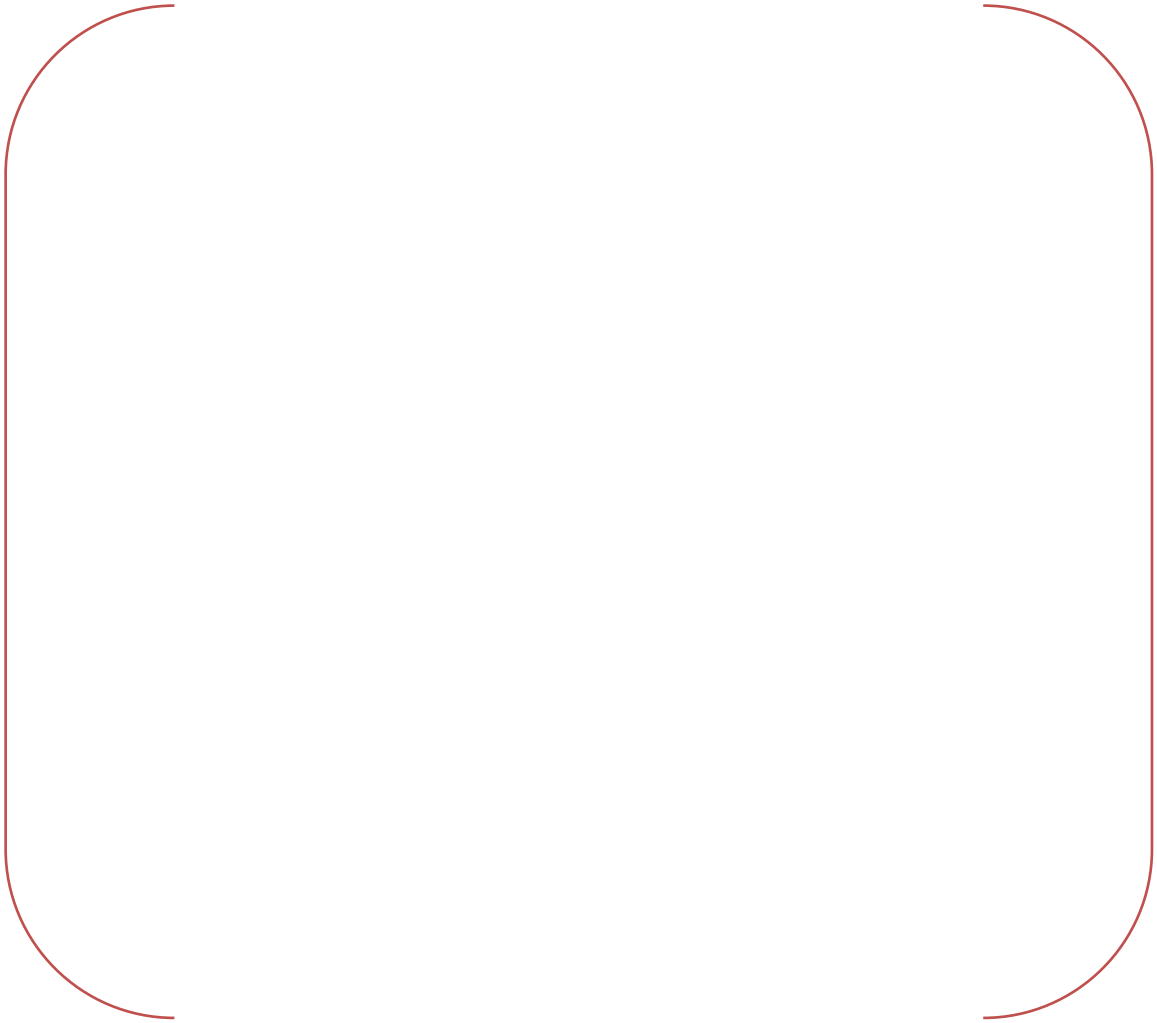

Figure 5-40 LBLOCA with a CCF in the PPS/ESF-CCS; RV Collapsed Water Level with Auto SIAS vs. Time

TS

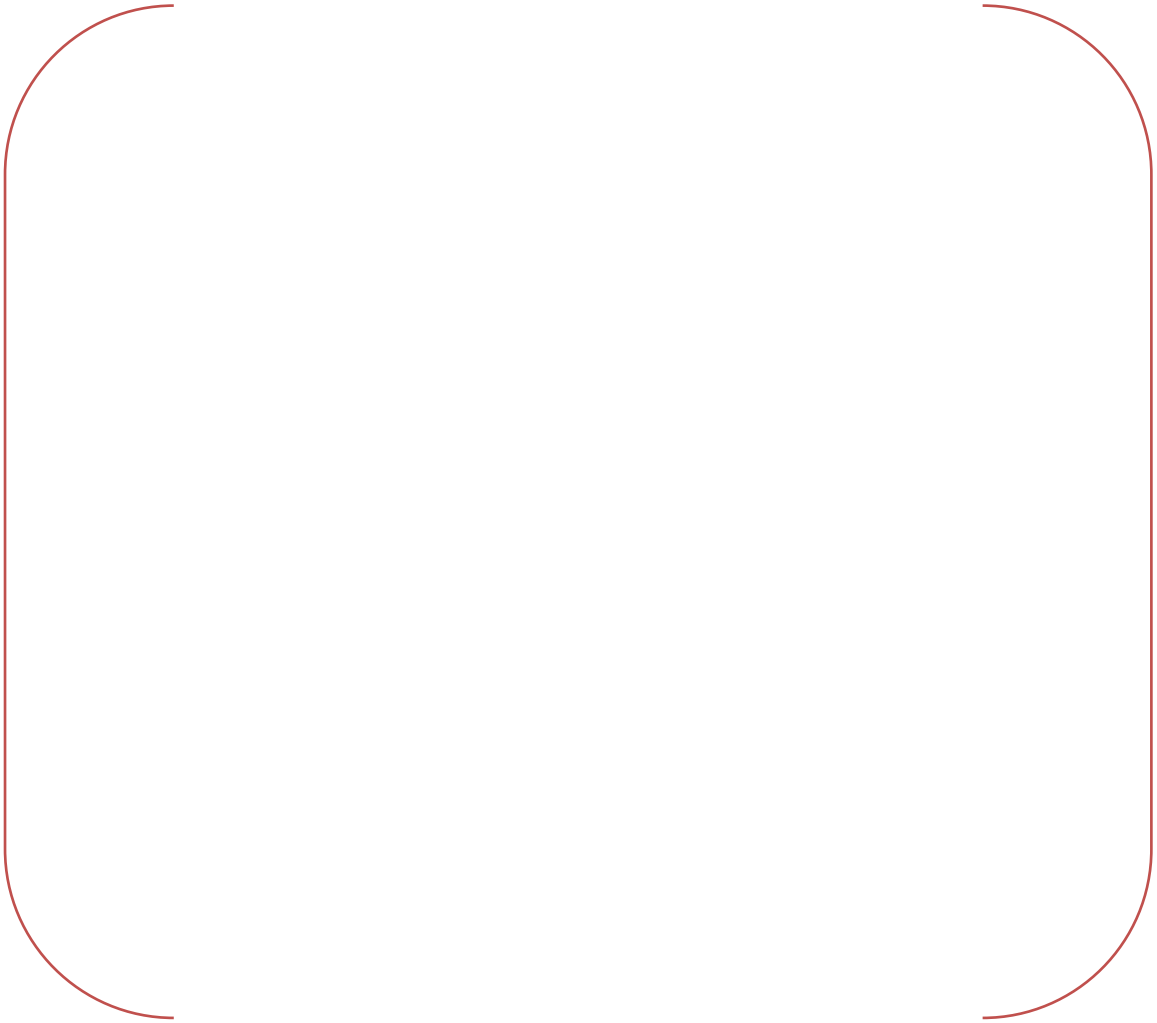

Figure 5-41 LBLOCA with a CCF in the PPS/ESF-CCS; Fuel Cladding Temperature w/o Auto SIAS vs. Time

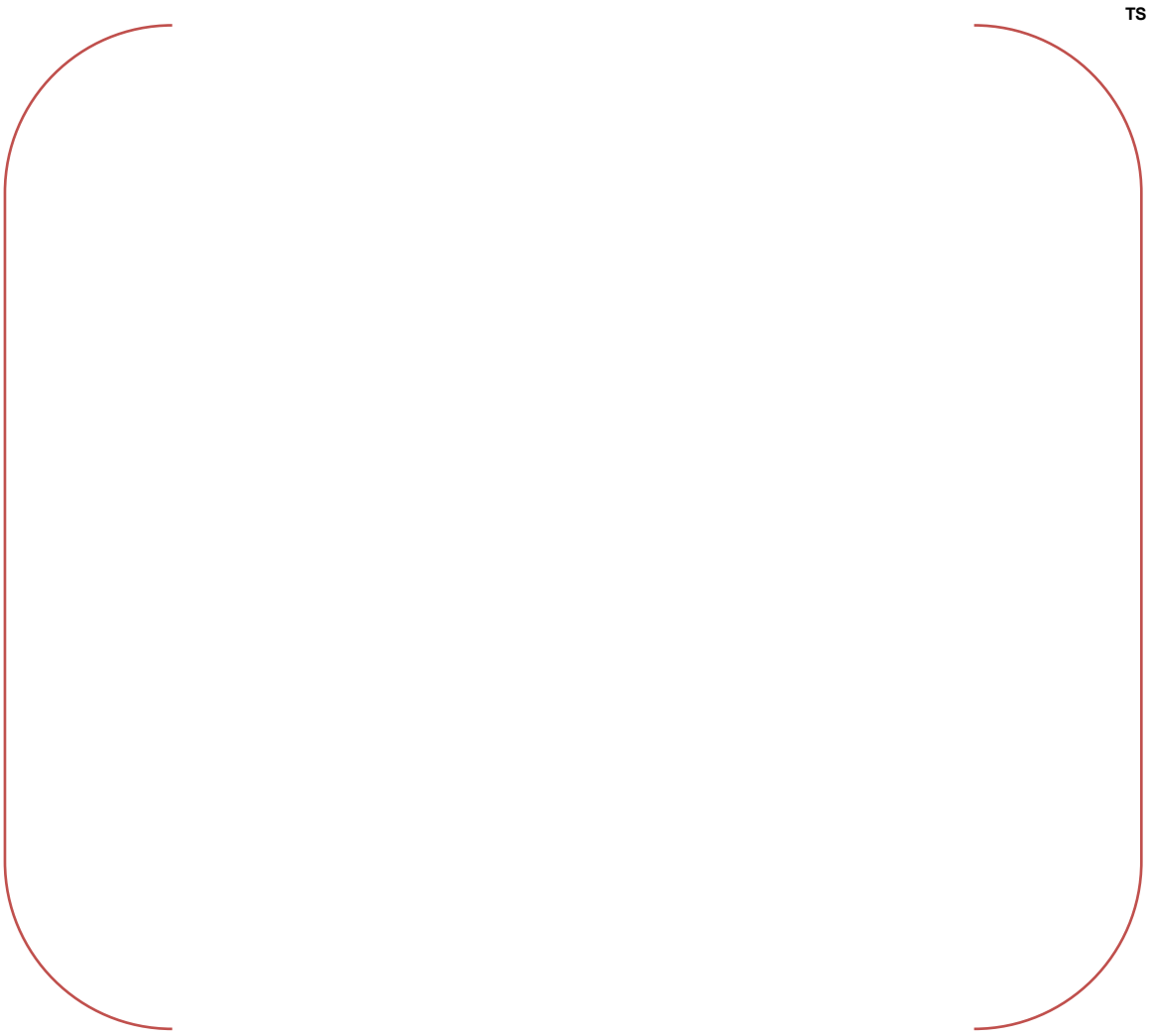

Figure 5-42 LBLOCA with a CCF in the PPS/ESF-CCS; Liquid Fraction with Auto SIAS vs. Time

TS

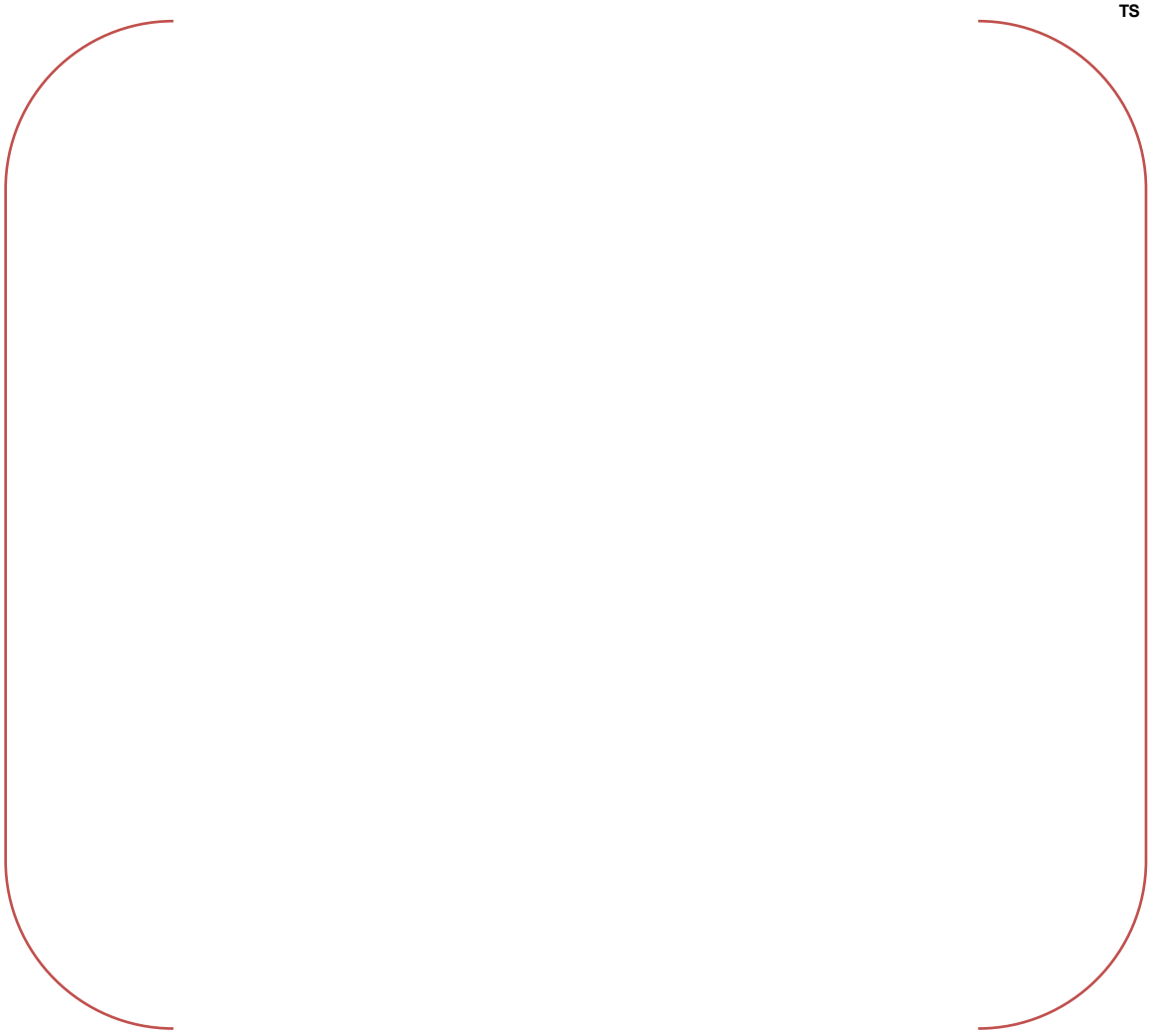

Figure 5-43 LBLOCA with a CCF in the PPS/ESF-CCS; Fuel Cladding Temperature with Auto SIAS vs. Time

TS

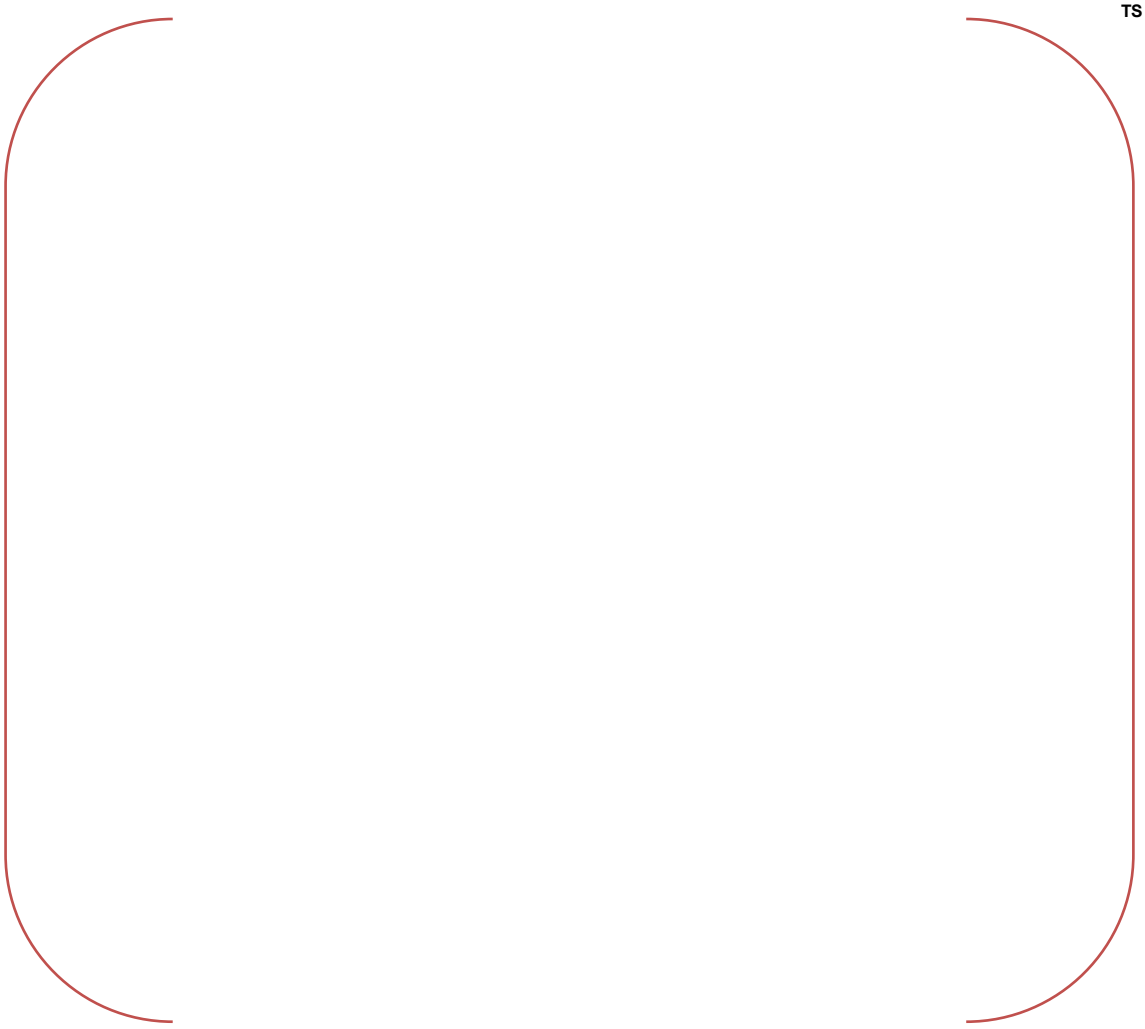

Figure 5-44 SLB with a CCF in the PPS/ESF-CCS (Containment Integrity); Containment Pressure vs. Time

6. CONCLUSIONS

The APR1400 design has digital-based safety I&C systems. Multiple diversity and defense-in-depth characteristics are involved in the digital safety I&C systems to achieve a high confidence in the hardware and software reliability. In spite of various design concepts for high reliability to reduce CCF potential, it is very difficult to verify that the digital systems are error-free from CCF. Therefore, a series of evaluations have been performed to demonstrate that the diversity and defense-in-depth capability designed into the APR1400 design provide adequate means to mitigate DCD Chapter 15 events with a postulated CCF.

Based on the realistic plant conditions in case of a pre-existing CCF in the digital safety I&C systems, all of the DCD Chapter 15 events are evaluated. The evaluation approach adopted in this report is to assume that all the digital safety I&C systems could not function correctly as designed, which is conservative enough to cover all possible common cause failure cases in the digital safety I&C systems.

Eight (8) events were identified to be quantitatively analyzed using computer programs, and margins to fuel, RCS, and containment integrity were examined for each event. The contents of the detailed analysis methods and the results are provided.

In summary, the integrities of RCS pressure boundary and the containment are maintained, and the offsite doses resulted from each event are within the acceptance criteria.

7. REFERENCES

1. APR1400-Z-J-NR-14003-P, “Diversity and Defense-in-Depth,” Revision 3, KHNP, May 2018.

2. NUREG-0800, Standard Review Plan, Appendix 18-A, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses,” Revision 0, U.S. Nuclear Regulatory Commission, November 2014.

3. NUREG-0800, Standard Review Plan, BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 6, U.S. Nuclear Regulatory Commission, July 2012.

4. APR1400-F-C-TR-12002-P-A, “KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design”, KHNP, April 2017.

5. LD-82-001 (dated 1/6/82), “CESEC Digital Simulation of a Combustion Engineering Nuclear Steam Supply System,” Enclosure 1-P to letter from A.E. Scherer to D.G. Eisenhut, December 1981(Proprietary).

6. CEN-214(A)-P, “CETOP-D Code Structure and Modeling Methods for Arkansas Nuclear One- Unit 2,” Combustion Engineering, Inc., July 1982(Proprietary).

7. CENPD-135, “STRIKIN-II, A Cylindrical Geometry Fuel Rod Heat Transfer Program,” Combustion Engineering, Inc., April 1974(Proprietary).

8. NUREG/CR-5535(EGG-2596), “RELAP5/MOD3 Code Manual,” EG&G Idaho Inc., USA, June 1990.

9. “Verification of Simulation Results of Mixture Level Transients and Evaporation Processes in Level Measurement Systems Using Needle-shaped Probes”, A. TRAICHEL, W. KASTNER, S. SCHEFTER, V. SCHNEIDER, S. FLEISCHER, T. GOCHT, and R. HAMPEL, Proc. of Measurement techniques of stationary and transient multiphase flow, December 2000.

10. “Description of the SGNPV Digital Computer Code Used in Developing Main Steam Line Break Mass/Energy Release Data for Containment Analysis,” Nuclear Power System, Combustion Engineering, Inc., February 1988.

11. CENPD-140-A, “Description of the CONTRANS Digital Computer Code for Containment Pressure and Temperature Transient Analysis,” R. C. Mitchell, June 1976(Proprietary).