

ArevaEPRDCPEm Resource

From: WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
Sent: Thursday, March 29, 2012 3:54 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy (AREVA); CRIBB Arnie (EXTERNAL AREVA); DELANO Karen (AREVA); HATHCOCK Phillip (AREVA); LEIGHLITER John (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); MEACHAM Robert (AREVA); HUDSON Greg (AREVA)
Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7, Question 07.08-50
Attachments: RAI 512 Question 07.08-50 Response US EPR DC - DRAFT.pdf

Getachew,

Attached is a DRAFT response for Question 07.08-50 of RAI No. 512 (FSAR Ch. 7) in advance of the May 30, 2012 final date.

Let me know if the staff has any questions or if this response can be sent as final.

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.

7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Friday, February 17, 2012 4:17 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7, Supplement 2

Getachew,

AREVA NP provided a schedule on October 13, 2011 for a technically correct and complete response to the one question in RAI 512. On January 10, 2012, AREVA NP provided Supplement 1 to revise the schedule for the one question.

The schedule for providing a technically correct and complete response to Question 07.08-50 has been changed as shown below in bold.

Question #	Response Date
RAI 512 — 07.08-50	May 30, 2012

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.

7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (CORP/QP)
Sent: Tuesday, January 10, 2012 4:57 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7, Supplement 1

Getachew,

AREVA NP provided a schedule on October 13, 2011 for a technically correct and complete response to the one question in RAI 512.

The schedule for providing a technically correct and complete response to Question 07.08-50 has been changed as shown below in bold.

Question #	Response Date
RAI 512 — 07.08-50	April 5, 2012

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.

7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, October 13, 2011 5:24 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 512 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the one question cannot be provided at this time.

The following table indicates the respective pages in the response document, "RAI 512 Response US EPR DC.pdf," that contain AREVA NP's response to the subject question.

Question #	Start Page	End Page
RAI 512 — 07.08-50	2	3

A complete answer is not provided for the one question. The schedule for a technically correct and complete response to this question is provided below.

Question #	Response Date
RAI 512 — 07.08-50	January 10, 2012

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.

7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: Tesfaye, Getachew [<mailto:Getachew.Tesfaye@nrc.gov>]
Sent: Wednesday, September 14, 2011 3:35 PM
To: ZZ-DL-A-USEPR-DL
Cc: Mott, Kenneth; Zhang, Deanna; Morton, Wendell; Spaulding, Deirdre; Truong, Tung; Zhao, Jack; Mills, Daniel; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on September 13, 2011, and discussed with your staff on September 14, 2011. No change is made to the draft RAI as a result of that discussion. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/NARP
(301) 415-3361

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 3848

Mail Envelope Properties (2FBE1051AEB2E748A0F98DF9EEE5A5D4BAF6C8)

Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 512 (6048), FSAR Ch. 7, Question 07.08-50
Sent Date: 3/29/2012 3:54:04 PM
Received Date: 3/29/2012 3:52:10 PM
From: WILLIFORD Dennis (AREVA)

Created By: Dennis.Williford@areva.com

Recipients:

"BENNETT Kathy (AREVA)" <Kathy.Bennett@areva.com>
Tracking Status: None
"CRIBB Arnie (EXTERNAL AREVA)" <arnie.cribb.ext@areva.com>
Tracking Status: None
"DELANO Karen (AREVA)" <Karen.Delano@areva.com>
Tracking Status: None
"HATHCOCK Phillip (AREVA)" <Phillip.Hathcock@areva.com>
Tracking Status: None
"LEIGHLITER John (AREVA)" <John.Leighliter@areva.com>
Tracking Status: None
"ROMINE Judy (AREVA)" <Judy.Romine@areva.com>
Tracking Status: None
"RYAN Tom (AREVA)" <Tom.Ryan@areva.com>
Tracking Status: None
"MEACHAM Robert (AREVA)" <Robert.Meacham@areva.com>
Tracking Status: None
"HUDSON Greg (AREVA)" <Greg.Hudson@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: auscharm02.adom.ad.corp

Files	Size	Date & Time	
MESSAGE	5322	3/29/2012 3:52:10 PM	
RAI 512 Question 07.08-50 Response US EPR DC - DRAFT.pdf			965596

Options

Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Response to

**Request for Additional Information No. 512 (6048), Revision 0,
Question 07.08-50**

9/14/2011

U. S. EPR Standard Design Certification

AREVA NP Inc.

Docket No. 52-020

SRP Section: 07.08 - Diverse Instrumentation and Control Systems

Application Section: ANP-10304 Revision 4

**QUESTIONS for Instrumentation, Controls and Electrical Engineering 1
(AP1000/EPR Projects) (ICE1)**

DRAFT

Question 07.08-50:**OPEN ITEM****Follow-up to RAI 303, Question 07.03-28**

Clarify the role of the safety automation system (SAS) regarding defense-in-depth and diversity (D3) and the plant response if it were to fail due to a postulated common-cause failure (CCF). Identify automatic or manual actions that would compensate for such failure.

10 CFR Part 50, Appendix A, General Design Criteria 22, states, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. One of the purposes of the diversity analysis method described in NUREG/CR-6303 is to postulate common-cause failures and to determine what portions of a design are uncompensated with regards to D3.

NUREG/CR-6303 also states that manual operator action is permissible as a diverse means of response to postulated CCF if, among other things, sufficient information and time is available for the operator to detect, analyze, make decisions, take action, and correct reasonably probable errors of operator function.

In Table A.2-1 of Technical Report ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," Revision 4 (ML11188A198), the applicant classifies "Decrease in feedwater temperature," "Increase in feedwater flow," "Increase in steam flow," "Inadvertent opening of SG relief or safety valve," and "Loss of normal feedwater flow" events as anticipated operational occurrences (AOOs). In the event of a postulated software CCF of the protection system, if necessary, the diverse actuation system (DAS) would actuate the emergency feedwater (EFW) system upon the low steam generator (SG) level actuation setpoint being reached. Once EFW is initiated by DAS, the operator is credited for controlling the EFW system manually to maintain SG level and to remove decay heat. Technical Report ANP-10304 states that, after DAS initiation of EFW on low SG level, the operator action credited is:

- For loss of normal feedwater flow event, manual operation of the EFW flows is required for the operators to prevent SG overfill, during long-term control. It takes approximately one hour to fill the SG with EFW from the low level EFW actuation setpoint to the protection system EFW isolation setpoint. Therefore, there is sufficient time for the operator to manually control SG level with the EFW system.
- For decrease in feedwater temperature event, main feedwater may be isolated on high SG level (a DAS function). If main feedwater is isolated, EFW actuates once SG level decreases to the low level DAS setpoint. The operator then controls SG level to remove decay heat using the EFW system. It takes more than 60 minutes for the level to recover from the EFW actuation setpoint, giving the operator sufficient time to manually control SG level.
- For increase in feedwater flow event, the operator controls the EFW system manually to maintain SG level and remove decay heat. It takes approximately 60 minutes for the SG level to recover to its nominal value from the EFW actuation setpoint. This provides the operator adequate time to manually control SG level.
- For inadvertent opening of an MRST or MSSV event, after 30 minutes, the operator terminates EFW flow to the affected SG.

In Technical Report ANP-10304, the staff found that SAS is only credited to *limit EFW flow* to a depressurized SG. It appears the stated times for SG fill up after EFW actuation by the DAS include the EFW flow limitation by SAS. Furthermore, if operator action is used for limiting EFW flow in other events, why is the SAS credited to limit flow for a depressurized SG? For example, is the limit flow function of SAS to prevent SG overfill, to prevent pump runout, or to prevent a rapid cooldown of the RCS and therefore mitigate a pressurized thermal shock event or reactor restart? From the staff's observation, SAS is the only system that can provide this limit flow function. Given a common-cause failure of SAS, an AOO or postulated accident, and other systems functioning properly, what type of automatic or manual actions would address the loss of EFW limit flow function provided by SAS? If operator actions are used, discuss the basis for why use of operator actions is acceptable.

Response to Question 07.08-50:

The sections referring to the process automation system (PAS) signal diversity will be removed from ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," due to the fact that PAS and the Protection System (PS) share a number of common sensors.

The SAS is not credited with the actions for Diversity and Defense-in-Depth due to the fact that SAS shares a number of common sensors with PS and is designed on the same TXS platform. Therefore, Technical Report ANP-10304 will be revised to say that SAS is not credited for being diverse from the PS.

The SAS EFW flow control function limits EFW pump flow to a depressurized SG to prevent pump runout and provides closed-loop control of the EFW flow to a desired setpoint. This function is performed by the EFW flow control valves. The valves include two adjustable mechanical stops. One mechanical stop limits the maximum flow to approximately 490 gpm. The second mechanical stop provides a minimum flow of approximately 270 gpm. The valve is positioned on the "minimum flow" mechanical stop during normal plant operation. During EFW pump operation, the valve is automatically positioned by a flow controller (SAS) based on the difference between the setpoint value of 400 gpm and the EFW Pump flow as measured by a flow sensor.

During events requiring EFW actuation, the SAS EFW flow control function is assumed to be operational. Flow from each EFW pump is maintained at 400 gpm. Based on this flow, it takes approximately 53 minutes for the SG level to recover to the high level isolation setpoint (89 percent wide range) from the EFW actuation setpoint. SG level control is performed by the EFW SG level control valves. The operator is credited with manual control of the level control valves after 30 minutes.

In the event of a CCF of the SAS concurrent with an AOO or PA requiring actuation of EFW, the flow control function would be lost. Two scenarios are examined, maximum flow and minimum flow.

If the flow control valve fails open, then maximum flow to the SG would occur. Because of the mechanical stop on the valve, the flow would be limited to approximately 490 gpm. Based on this higher flow rate, it would take approximately 43 minutes for the SG level to recover to the high level isolation setpoint (89 percent wide range) from the EFW actuation setpoint. There is adequate time for the operator to control SG Level with the level control valve. The EFW pump would be protected from runout at this flow rate. This higher flow also remains within the

bounds assumed in the Main Steam Line Break safety analysis for the maximum EFW flow to a depressurized SG.

If the flow control valve failed closed or if the SAS CCF occurred before EFW actuation, then a minimum flow to the SG would occur. Because of the mechanical stop, approximately 270 gpm would still be allowed to flow through the valve. This is sufficient flow following a loss of normal feedwater or feedwater line break to remove decay heat and recover SG levels. The operator would be able to modulate the valve position after 30 minutes if necessary for long term control.

In summary, there are no automatic or manual actions credited to address the loss of EFW flow control in the event of a SAS CCF. The mechanical stops on the flow control valves will protect the pump from runout and provide sufficient flow to an affected SG, even in the absence of a control signal from SAS.

FSAR Impact:

The U.S. EPR FSAR will be not be revised as a result of this response.

Technical Report ANP-10304 will be revised to as described in the response and indicated on the enclosed markups.

DRAFT

**ANP-10304—U.S. EPR
Diversity and Defense-
in-Depth Assessment
Technical Report
Markups**

DRAFT

Nature of Changes

Revision	Sections or Pages	Description and Justification
1	All	Complete revision to incorporate I&C architectural design changes and to reflect completion of analysis rather than methodology to perform future analysis.
2	All	Complete revision to incorporate I&C architectural design changes.
3	Pages 2-4, 4-15, 4-20, A-5, A-119	Clarified terminology of AOO/PA versus DBE.
	Page 3-6	Clarified DAS interfaces with CRDCS and nature of DAS trip signal as energize to actuate.
	Pages 4-24, 4-25	Updated Figures 4-1 and 4-2 to accurately reflect the new DCS architecture.
	Page 4-22	Clarified the role of PAS in the D3 assessment.
	All	Clarified terminology describing I&C technology
4	Page 2-1	Clarified basis of SICS
	Pages 2-6, 3-3	Clarified digital terminology
	Page 3-3	Clarified temperature inputs for DAS
	Page 5-2	Corrected References
	<u>5</u>	<u>Page 2-3</u>
	<u>Pages 4-2 and 4-3</u>	<u>Added discussion of SWCCF in SAS</u>
	<u>Pages 4-5 and 4-6</u>	<u>Added clarification for SICS design and software diversity</u>
	<u>Pages 4-10 and 4-11</u>	<u>Added clarification for DAS human and software diversity</u>
	<u>Figures 4-1 and 4-2</u>	<u>Replaced</u>
	<u>Appendix A</u>	<u>Revised to reflect treatment of SWCCF in SAS and to clarify results for Increase in Steam Flow Event</u>

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

Guideline 7. AREVA NP believes this approach, while consistent with the intent of NUREG/CR-6303, would result in an extensive and lengthy NRC review, which is undesirable. Additionally, the U.S. EPR design includes a diverse actuation system conservatively designed to mitigate AOOs and PAs, assuming a complete PS failure. The U.S. EPR design can satisfy D3 criteria without credit taken for any portion of the PS functioning correctly. Therefore, AREVA has chosen a more conservative block representation to use in performing the D3 assessment.

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

The resulting block diagram used to perform the U.S. EPR D3 assessment is shown in [Figure 4-1](#). The connections are general purpose interfaces between systems that represent connections to perform all of the interfacing functions between those systems.

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

Safety Automation System

The SAS performs automatic and manual grouped control functions to perform safety-related controls during normal operations, mitigate the effects of AOOs and PAs, and to achieve and maintain safe shutdown. This functionality could be very useful, if credited in the assessment to mitigate a PS SWCCF. SAS is implemented in the same technology as the PS and acquires many of the same measurements as the PS, but has significantly different functionality than the PS. This results in very different application software and allows a sound argument to be made

that SAS would not be subject to the same SWCCF as the PS, concurrent with an AOO or PA. However, because of the multiple similarities between the PS and SAS, a conservative decision is made not to credit the SAS to terminate events in the D3 assessment. Based on an evaluation of the SAS functions it was determined that the only function on SAS that would help in the D3 assessment is the EFW flow control function. The impact of the loss of this function is discussed in the Appendix A assessment for those events where EFW is actuated.

Reactor Control Surveillance and Limitation System

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

Process Information and Control System

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

Process Automation System

In the D3 assessment, no failures beyond the SWCCF of the PS are postulated. PAS is therefore considered operational. As part of best estimate assumptions, normally operating control functions in PAS, such as pressurizer level control and pressurizer pressure control, continue to operate following a SWCCF. The only PAS function that relies on a PS output is the partial cooldown actuation. Because it relies on a PS output, this function is not assumed to be operational in the D3 analysis. This assumption allows the event progression to be accurately

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

~~• Signal diversity—The vast majority of sensors acquired by the PAS are not acquired by the PS, and vice versa. A small set of sensors may be used by both systems; however, these signals would be used for fundamentally different purposes (e.g., signal selection algorithms for closed loop control in PAS vs. coincidence voting logic for actuation in PS). The PAS largely uses different process sensor measurements than the PS, which is a “more effective” characteristic of signal diversity.~~

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

Safety Automation System:

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

- ~~Design diversity—The SAS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and is clearly different from the PS architecture. Most significantly, SAS is a single layer system (only a control unit layer) while the PS is a multi-layer system (APU, actuation logic unit). Different architecture is a “less effective”, but still relevant, characteristic of design diversity.~~
- ~~Functional diversity—The SAS fulfills a fundamentally different purpose, and performs different types of functions, than the PS. The SAS performs automated control functions of safety-related plant systems, to regulate those systems during normal operation. The SAS also processes commands from the PIGS and SIGS to allow the operator to manually control the safety-related plant systems. The PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. Two systems with different purposes and functions require significantly different application software structures. This greatly reduces the risk of the same latent software defect existing in the two systems. Different purpose and function is a “more effective” characteristic of functional diversity.~~
- ~~Signal diversity—The vast majority of sensors acquired by the SAS are not acquired by the PS, and vice versa. A small set of sensors is used by both systems; however, those signals are used for fundamentally different purposes (e.g., signal selection algorithms for closed loop control in SAS vs. coincidence voting logic for actuation in PS). Additionally, the functions in SAS that use the same sensors as the PS rely on PS outputs for initiation and are therefore not credited to mitigate a PS failure in the D3 assessment. The use of different process parameters as inputs is a “more effective” characteristic of signal diversity.~~

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

Diverse Actuation System:

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

- Design diversity–The DAS will implement technology that is not microprocessor based PE technology (i.e., electrical, electronic, or programmable electronic other than microprocessor based). This constitutes, at a minimum, a different approach within a technology, as listed in Guideline 2. The DAS architecture is shown in U.S. EPR FSAR Tier 2, Section 7.1, and it is clearly different from the PS architecture. This combination of multiple design characteristics establishes a “more effective” case of design diversity.
- Equipment diversity–At a minimum, the DAS equipment will be a fundamentally different design than the PS equipment. Section 3.2.1 identifies this commitment. The use of a fundamentally different design is a “more effective” characteristic of equipment diversity.
- Functional diversity–The DAS is designed with the intent of allowing the PS to actuate before the DAS, in response to a DBE. This results in different setpoint parameters and delay times for the DAS functions, compared to the PS. Different response timescale is a “less effective”, but still relevant, characteristic of functional diversity.
- Human diversity–Different design organizations (i.e., different management, engineers, designers, and programmers) will be responsible for the design of the two systems. This establishes a more effective case of human diversity.~~At a minimum, different engineers will be responsible for the design of the DAS and PS. It is likely that different design organizations will be responsible for the design of the two systems (the most effective characteristic of human diversity. This will not be determined until the detailed design of these systems is in progress. To be conservative, only the use of different engineers is~~

Figure 4-1—Block Diagram for D3 Assessment

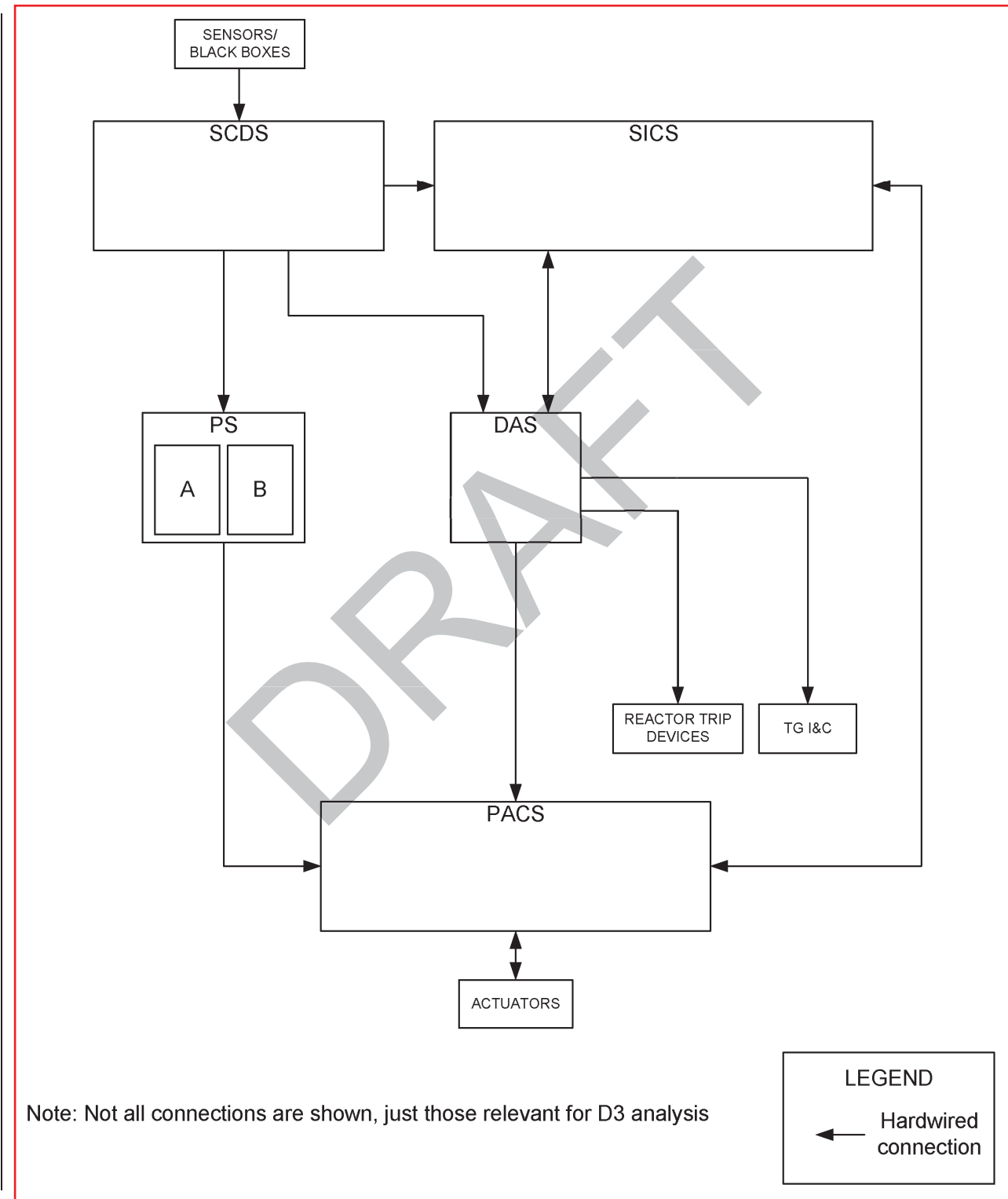
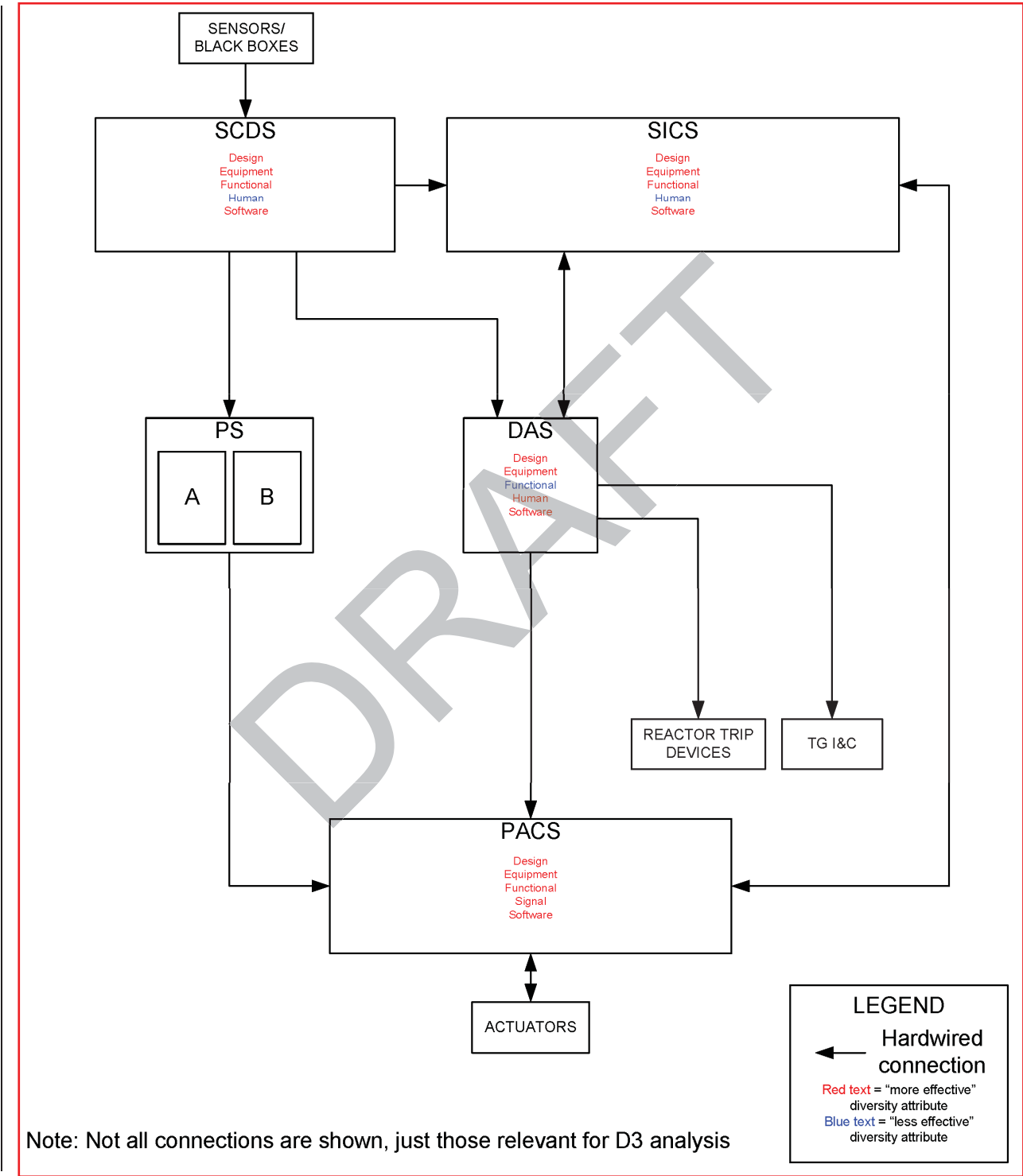


Figure 4-2—Block Diagram with Diversity Attributes



A.1 INTRODUCTION

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

The method of assessment used is to analyze, assuming an SWCCF in the PS, the DBEs analyzed in the U.S. EPR FSAR safety analysis. An SWCCF in the SAS is also evaluated. The DBEs are identified in Section A.2.3.

The purpose of this appendix is to present the U.S. EPR D3 plant response analysis that assesses conformance with Point 2 of NUREG-0800 BTP 7-19. The D3 plant response analysis entails a quantitative evaluation of U.S. EPR FSAR Chapter 15 AOOs and PAs in the presence of an SWCCF that renders the PS ineffective. For a SWCCF in the SAS the only important function is EFW flow control. An SWCCF is evaluated for those events where EFW is actuated.

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

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

is limiting. For a SWCCF in SAS, EFW flow control is the only important function to consider (see Section 4.1).

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

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

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

This appendix provides a review of the U.S. EPR safety analysis in support of D3. The scope of the review included the U.S. EPR FSAR safety analysis (U.S. EPR FSAR Tier 2, Chapter 15), radiological consequence analysis (U.S. EPR FSAR Tier 2, Chapter 15) and the containment analysis (U.S. EPR FSAR Tier 2, Chapter 6). This review was performed to disposition the

various analyses assuming an SWCCF in the PS and SAS. A number of DAS functions were identified in the course of the review to demonstrate that, in the event of an SWCCF ~~in the PS~~, the acceptance criteria of BTP-7-19 are met. Events were found acceptable by engineering argument or specific engineering analysis. Events where additional analyses were performed include:

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

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

The U.S. EPR design, including DAS functions, available plant control systems, and manual operator actions, are determined to be sufficient in maintaining the acceptance criteria of BTP 7-

19 for an AOO or PA concurrent with a SWCCF ~~of the PS~~.

A.2 D3 PLANT RESPONSE ANALYSIS APPROACH

A.2.1 Method

The method used in this analysis is to review the U.S. EPR AOOs or PAs analyzed in the U.S. EPR FSAR safety analysis, assuming an SWCCF in the PS that renders the PS ineffective. An SWCCF in SAS is also considered for those events where EFW is actuated. The events considered are identified in Section A.2.3. The D3 plant response analysis considers the I&C functionality as described in Section A.2.2.

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

The analysis assumes the plant is operating under full power nominal conditions (no uncertainties) with all equipment available (i.e., no preventative maintenance and no single failures). RCCAs are maintained in their normal full power position (i.e., all RCCAs are out, with the lead control bank slightly inserted). The analysis employs best estimate core neutronic parameters and power distributions expected at full power conditions (hot channel factors accounting for engineering uncertainties, RCCA bow, or assembly bow are excluded). The best

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

A.2.2.1 SWCCF in PS

The U.S. EPR DCS architecture is described in Section 2 of this report. The plant response analysis assumes an SWCCF in the PS that renders the PS ineffective during a DBE.

Functions that require initiation from the PS are assumed to be lost as a result of the SWCCF

(i.e., partial cooldown). The analysis assumes that ~~SAS and~~ PAS functions that do not rely on a PS output continue to operate. The analysis conservatively assumes the SAS and RCSL ~~is~~ are not available as ~~a~~ credited mitigation systems. RCSL is assumed to function during an event when its correct operation would make the response of the event more severe. The assessment of the I&C systems that reaches these conclusions is presented in Section 4.

The following are specific I&C functions that are either assumed to operate normally (~~SAS and~~ PAS functions) or provided specifically as a diverse means to mitigate events in the D3 evaluation of an SWCCF in the PS during a postulated AOO or PA. These functions are described in the evaluation presented in Section A.3. Essential auxiliary support systems required for these functions are either in continuous operation (controlled by ~~SAS or~~ PAS and not affected by PS SWCCF), or are initiated as part of the DAS actuation of the associated ESF function. The loss of SAS functions would not affect the performance of the essential auxiliary support systems for at least 30 minutes, at which point the operator would take over long-term control. The operator actions listed are not assumed to occur until 30 minutes after the initiating event, unless otherwise noted.

Automatic control functions:

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

- SAS/PACS–EFW flow control (limits flow to a depressurized SG). This function is also lost for a SWCCF in SAS (see Section A.2.2.2).

Manual functions:

- SICS/DAS/Reactor Trip Devices–manual RT.
- SICS/PACS–manual EDG start.
- SICS/PACS–manual diesel generator loading (emergency diesel generators or SBOs).
- SICS/DAS/PACS–manual EFW actuation.
- SICS/PACS–manual operation of EFW for long-term SG level control.
- SICS/PACS–manual SI switchover to hot leg injection.
- SICS/PACS–manual MSIV closure.
- SICS/PACS–manual feedwater isolation (MFW and EFW).
- SICS/DAS/PACS–manual initiation of medium head safety injection (MHSI).
- SICS/PACS–manual control of MHSI.
- SICS/PACS–manually extend partial cooldown.
- SICS/PACS–Manual depressurize RCS with pressurizer sprays.
- SICS/PACS–manual actuation of EBS.
- SICS/PACS–manual control room HVAC reconfiguration.
- SICS/PACS–manual CVCS isolation.
- SICS/PACS–manual MSRT⁴.
- SICS/DAS/PACS–manual Stage 1 containment isolation¹.
- SICS/DAS/PACS–manual opening of containment hydrogen mixing dampers¹.

Automatic DAS functions:

¹ BTP 7-19 Point 4

(RT) or signal application to actuators (ESF). These DAS functions are credited in the analysis presented in Section A.3. These functions are enabled/disabled by separate permissives.

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

A.2.2.2 SWCCF in SAS

The SAS is a Class 1E control system. The SAS performs automatic and manual grouped control functions to execute safety-related controls during normal operations, mitigate the effects of AOOs and PAs, and to achieve and maintain safe shutdown. As discussed in Section 4.1, under D3 conditions (four trains available), the only important SAS function is the EFW control function.

Therefore, if an SWCCF occurs in SAS, the EFW flow control function would not be available. The EFW flow control function would make 400 gpm available to each SG under normal conditions and would limit the flow to a depressurized SG to 490 gpm. In the event of a CCF of SAS concurrent with an AOO or PA requiring actuation of EFW, the Flow Control function would be lost. Two scenarios are examined, maximum flow and minimum flow.

If the flow control valve fails open, then maximum flow to the SG would occur. Because of the mechanical stop on the valve, the flow would be limited to approximately 490 gpm. Based on this higher flow rate, it would take approximately 43 minutes for the SG level to recover to the high level isolation setpoint (89 percent wide range) from the EFW actuation setpoint. There is

adequate time for the operator to manually control SG Level with the level control valve. The EFW Pump would be protected from run-out at this flow rate. In addition, this higher flow remains within the bounds assumed in the MSLB safety analysis for the maximum EFW flow to a depressurized SG.

If the flow control valve fails closed or if the SAS CCF occurred before EFW actuation, then a minimum flow to the SG would occur. Because of the mechanical stop, approximately 270 gpm would still be allowed to flow through the valve. This is sufficient flow, following a loss of coolant flow (LOCF) or FWLB event, to remove decay heat and recover SG levels. The operator would be able to modulate the valve position after 30 minutes if necessary for long term control. An SAS CCF is described in further detail in each section where the actuation of EFW is discussed.

The loss of SAS functions would not affect the performance of the essential auxiliary support systems for at least 30 minutes, at which point the operator would take over long-term control.

A.2.3 Postulated Events

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

A.2.4 Acceptance Criteria

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

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

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

A.3 EVALUATION RESULTS

A.3.1 General

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

A.3.2 Increase in Heat Removal by Secondary System

A.3.2.1 Decrease in Feedwater Temperature

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

Following the DAS reactor trip, normal pressurizer pressure and level controls maintain RCS pressure and pressurizer level. The normal MFW control system reacts to control SG level. Depending on the speed of control of the MFW to match decay heat, MFW may be isolated on high SG level (a DAS function). If MFW is isolated, EFW actuates once SG level decreases to the low level DAS setpoint. The operator then controls SG level, to remove decay heat using the EFW system. It takes ~~more than~~approximately 60 minutes for the level to recover from the EFW actuation setpoint to the high level isolation setpoint (89 percent wide range level), giving the operator sufficient time to manually control SG level. After RT, the turbine bypass system

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

many events. In the event of an SWCCF in SAS, the EFW level control function would not be available and the EFW flow could be governed by the high flow mechanical stop on the EFW control valve. Under these conditions it would take approximately 43 minutes before level is recovered and the high level isolation setpoint (89 percent wide range) is challenged. This is sufficient time for the operator to terminate EFW before the steam generator is full.

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

A.3.2.2 Increase in Feedwater Flow

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

Following the DAS reactor trip, normal pressurizer pressure and level controls maintain RCS pressure and pressurizer level. Because MFW is isolated DAS actuates EFW when SG level decreases to the low level DAS setpoint. The operator controls the EFW system manually to maintain SG level and remove decay heat. It takes approximately 60 minutes for the SG level to recover ~~to its nominal value~~ the high level isolation setpoint (89 percent wide range) from the EFW actuation setpoint. As discussed in the event of an SWCCF in SAS this time would be reduced to approximately 43 minutes. This provides the operator adequate time to manually control SG level. After RT, the TBS opens, to control primary pressure through the maintenance of secondary system pressure in a stable, controlled condition.

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

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

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

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

$T(^{\circ}F) \times DF\left(\frac{\%}{^{\circ}F}\right)$ is negative, the indicated reactor power is lower than the current reactor power, and the RT on high neutron flux is delayed.

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

Core power peaks at 131.1 percent in 825 seconds, ~~but power is and remains~~ fairly constant at a value of approximately 130 percent power, ~~from 130 seconds until the transient is terminated by the operator.~~ For this event, ~~a reactor trip is not assumed to~~ does not occur, ~~either by manual or automatic action.~~ Indicated core power does not reach a level high enough to cause a DAS-initiated reactor trip on excure high neutron flux. Instead, the system moves to a higher steady-state power level and remains there. SG levels are maintained during the transient, even with actual core power at 130 percent as the MFW pumps are conservatively modeled to match the increasing steam demand. ~~The MFW pumps are able to match the demand, due to the decreased pressure on the secondary side.~~ (This is a conservative assumption because matching the demand results in the highest core power.) Figure A.3.2-1 through Figure A.3.2-11 provide the response of key parameters for the limiting Increase in Steam Flow event.

~~Under best estimate conditions,~~ If the MFW system was modeled realistically, the feed train will likely trips, as a result of the reduced feedwater system pressures and the feedwater system would not be able to match steam demand at 130 percent reactor power. If the MFW pumps are unable to keep up with demand, SG levels decrease and the reactor trips on low SG level.

MSIV closure and MFW isolation will be initiated by DAS on low SG pressures. DAS will then actuate EFW on low SG level to provide long term cooling. The operator controls EFW manually to maintain SG level. For long-term heat removal, manual operation of the MSRTs is available. These features were not credited in the analysis of this event to evaluate the proximity to fuel design limits.

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

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

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

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

In the event of a SWCCF in the SAS the EFW flow control function would not be available. However, the EFW flow to a depressurized steam generator would be limited by the high flow mechanical stop on the EFW flow control valve. These conditions are bounded by the analysis of steam system piping failures.

A.3.2.4 Inadvertent Opening of an MSRT or MSSV

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

In the event of a SWCCF in SAS the EFW flow to a depressurized steam generator would be limited to 490 gpm by the high flow mechanical stop on the flow control valve. Thus, a SWCCF in SAS has no impact on Steam System Piping Failures.

DRAFT

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

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

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

In the event of a SWCCF in SAS and the EFW flow control function fails EFW flow could be limited to 270 gpm to each SG based on the minimum flow control valve mechanical stop. In this case three EFW pumps would be required to provide sufficient flow.

The U. S. EPR Emergency Procedure Guidelines/Emergency Operating Procedures are still under development. Symptom-based recovery instructions for the secondary inventory loss scenarios are planned to not require a special D3 coping procedure.

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

A.3.3.4 Loss of Normal Feedwater Flow

The Loss of Normal Feedwater event is an AOO initiated by the complete termination of MFW flow. This condition can be caused by a loss of power to the main feedwater pumps or a malfunction of the feedwater control system or equipment. The U.S. EPR FSAR criterion for this event is to confirm the ability of the EFW system to maintain SG inventories sufficient for decay heat removal. DNBR limits are not challenged, and, because the event progresses fairly slowly, peak RCS and secondary system pressures are bounded by the TT and MSIV closure

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

In the event of a SWCCF in SAS and the EFW flow control function fails EFW flow could be limited to 270 gpm to each SG based on the minimum flow control valve mechanical stop. In this case three EFW pumps would be required to provide sufficient flow. As previously noted, four EFW pumps are available.

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

A.3.3.5 Feedwater System Piping Failures

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

The U.S. EPR FSAR analysis covers a complete break spectrum, from very small breaks just beyond what can be handled by the feedwater system, to a complete severance of the main feedwater pipe. The smaller breaks trip the reactor on high pressurizer pressure. Intermediate breaks trip the reactor on low SG level and the larger breaks trip on high SG pressure drop or

low SG pressure. Except for very small breaks, the MSIVs close on high SG pressure drop or low SG pressure. EFW is actuated on low SG level for the entire break spectrum. The MSRTs and MSSVs function to control secondary pressure. The PSRVs limit RCS pressure.

In the case of an SWCCF in the PS, DAS provides the same protection for the range of breaks. DAS has RT functions on high pressurizer pressure, low SG level, and low SG pressure. DAS also has functions for MSIV closure on low SG pressure, MFW isolation in the affected SG on low SG pressure, and EFW actuation on low SG level. The PSRVs and MSSVs are not subject to SWCCF and are still available to limit RCS and secondary pressure. In the long term, decay heat would be removed through the intact MSSVs or through the MSRTs through manual operator action.

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

In the event of a SWCCF in SAS and the EFW flow control function fails EFW flow could be limited to 270 gpm to each SG based on the minimum flow control valve mechanical stop. In this case three EFW pumps would be required to provide sufficient flow to continue to bound the FSAR analysis. As previously noted for D3, three pumps are available feeding intact steam

generators while one feeds the break. For D3, there is no requirement for the operator to realign the EFW pump feeding the break. After 30 minutes the operator would trip RCPs.

DRAFT

ID the loop seal may take several hours to clear. In this case, the operator will need to take manual control and cooldown through the MSRTs to reduce RCS pressure and actuate MHSI. There is sufficient time to manually initiate the cooldown so that the partial cooldown function is not required to be automated on DAS. Figure A.3.7-10 through Figure A.3.7-17 show the response of key parameters for representative breaks at both ends of the spectrum.

In the event of a SWCCF in SAS sufficient EFW flow remains available to maintain SG inventory and remove decay heat.

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

DRAFT

A.3.8.2 MSLB inside containment

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

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

In the event of an SWCCF in SAS the EFW flow to a depressurized SG would still be limited to 490 gpm.

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

A.3.9 Radiological consequences

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

- Small line break outside containment.
- LOCA.
- SGTR.
- MSLB.
- FWLB.

In the event of a SWCCF in SAS and the EFW flow control function fails, sufficient flow remains available to remove decay heat and recover steam generator levels with three EFW pumps even if the flow control valve fails on the low flow mechanical stop. The high flow mechanical stop limits flow to a depressurized SG.

The U.S. EPR design, including DAS functions, available plant control systems and manual operator actions are sufficient to satisfy the acceptance criteria of BTP 7-19 for an AOO or PA concurrent with a SWCCF of the PS and SAS.

A.5 REFERENCES

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