



ANP-10304  
Revision 0

**U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth  
Methodology Technical Report**

May 2009

AREVA NP Inc.

---

(c) 2009 AREVA NP Inc.

Non-Proprietary

**Copyright © 2009**

**AREVA NP Inc.  
All Rights Reserved**

## ABSTRACT

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

The U.S. EPR addresses these concerns with a two-fold approach. First, the U.S EPR I&C architecture incorporates features that are designed to prevent a CCF of the safety I&C systems, and features that mitigate the effects of a postulated CCF of the safety I&C systems. Second, a methodology is utilized to evaluate the adequacy of the design with respect to diversity and defense-in-depth (D3). This methodology is designed to address the NRC's regulatory guidance.

This report describes the I&C systems that comprise the overall I&C architecture. The U.S. EPR defense-in-depth concept is discussed, and is compared to the echelons of defense discussed in NUREG/CR-6303. Design features that are used to prevent CCFs in the safety I&C systems, as well as mitigate the effects of a postulated CCF in the safety I&C systems are presented. A methodology to evaluate the adequacy of the U.S. EPR I&C design with respect to D3 is presented.



## Contents

|  | <u>Page</u> |
|--|-------------|
| 1.0 INTRODUCTION .....   | 1-1         |
| 1.1 Scope.....   | 1-1         |
| 1.2 Background.....  | 1-1         |
| 2.0 U.S. EPR I&C ARCHITECTURE .....  | 2-1         |
| 2.1 Level 2—Supervisory Control .....  | 2-3         |
| 2.2 Level 1—System Level Automation .....  | 2-4         |
| 2.3 Level 0—Process Interface.....   | 2-6         |
| 2.4 U.S. EPR I&C Defense-In-Depth Concept.....   | 2-6         |
| 2.5 Comparison of U.S. EPR I&C Defense-in-Depth Concept<br>and NUREG/CR-6303 Echelons of Defense.....                | 2-8         |
| 3.0 DIVERSITY AND DEFENSE-IN-DEPTH FEATURES OF THE U.S.<br>EPR I&C ARCHITECTURE .....                                | 3-1         |
| 3.1 Features that are Designed to Prevent a CCF of the I&C<br>Safety Systems (Main Line of Defense).....             | 3-1         |
| 3.1.1 Equipment Design.....  | 3-1         |
| 3.1.2 Safety I&C System Design.....  | 3-3         |
| 3.1.3 Application Software Development Process .....   | 3-5         |
| 3.2 Features that are Designed to Mitigate a Postulated CCF of<br>the I&C Safety Systems (Main Line of Defense)..... | 3-5         |
| 3.2.1 Diversity between the Main Line of Defense and the<br>Risk Reduction Line of Defense.....                      | 3-6         |
| 3.2.2 Independence between Main Line of Defense and the<br>Risk Reduction Line .....                                 | 3-11        |
| 4.0 DIVERSITY AND DEFENSE-IN-DEPTH METHODOLOGY .....   | 4-1         |
| 4.1 Step 1 - Susceptibility Analysis of Safety I&C Systems to<br>CCF .....   | 4-1         |
| 4.2 Step 2 - Qualitative Evaluation of AOOs and Postulated<br>Accidents .....  | 4-1         |
| 4.3 Step 3 - Determine Inventory of Diverse Controls and<br>Indications.....   | 4-4         |

|       |   |     |
|-------|---|-----|
| 4.3.1 | Hardwired Controls on SICS .....  | 4-4 |
| 4.3.2 | Controls on PICS .....  | 4-4 |
| 4.3.3 | Indications on PICS.....  | 4-4 |
| 4.4   | Step 4 - Quantitative Analyses of AOOs and Postulated<br>Accidents .....  | 4-4 |
| 4.5   | Step 5 - Human Factors Engineering Verification and<br>Validation .....   | 4-5 |
| 4.6   | Step 6 – Platform Diversity Analysis .....  | 4-5 |
| 5.0   | CONCLUSIONS .....   | 5-1 |
| 6.0   | REFERENCES .....  | 6-1 |
| 6.1   | U.S. Regulations .....  | 6-1 |
| 6.2   | U.S. Regulatory Guidance .....  | 6-1 |
| 6.3   | Regulatory Review Precedent .....   | 6-2 |
| 6.4   | AREVA NP Documents.....   | 6-2 |
| 7.0   | APPENDIX – D3 METHODOLOGY STEP 2 – QUALITATIVE<br>EVALUATION OF ANTICIPATED OPERATIONAL<br>OCCURRENCES AND POSTULATED ACCIDENTS ..... | A1  |
| 7.1   | Approach .....  | A1  |
| 7.2   | Evaluation .....  | A1  |
| 7.2.1 | Increase in Heat Removal by Secondary System .....  | A3  |
| 7.2.2 | Decrease in Heat Removal by Secondary System.....   | A5  |
| 7.2.3 | Decrease in RCS Flow Rate .....   | A6  |
| 7.2.4 | Reactivity & Power Distribution Anomalies .....   | A8  |
| 7.2.5 | Increase in RCS Inventory .....   | A9  |
| 7.2.6 | Decrease in RCS Inventory.....  | A10 |
| 7.2.7 | Primary Side Pressure Transients.....   | A12 |
| 7.2.8 | Radioactive Release from a Subsystem or<br>Component .....  | A12 |
| 7.3   | Summary and Conclusions .....   | A13 |

### List of Tables

|   |     |
|---|-----|
| Table 2-1—I&C Systems and Associated Platforms .....      | 2-1 |
| Table 2-2—U.S. EPR Lines of Defense .....                 | 2-9 |
| Table A-1—U.S. EPR Initiating Events – Sheet 1 of 3 ..... | A16 |
| Table A-1—U.S. EPR Initiating Events – Sheet 2 of 3 ..... | A17 |
| Table A-1—U.S. EPR Initiating Events – Sheet 3 of 3 ..... | A18 |
| Table A-2a—Plant Systems Used in Accident Analysis .....  | A19 |
| Table A-2b—Plant Systems Used in Accident Analysis .....  | A21 |
| Table A-2c—Plant Systems Used in Accident Analysis .....  | A22 |
| Table A-2d—Plant Systems Used in Accident Analysis .....  | A23 |
| Table A-2e—Plant Systems Used in Accident Analysis .....  | A24 |
| Table A-2f—Plant Systems Used in Accident Analysis .....  | A25 |
| Table A-2g—Plant Systems Used in Accident Analysis .....  | A26 |
| Table A-3—D3 Qualitative Results.....                     | A27 |

### List of Figures

|   |      |
|---|------|
| Figure 2-1—U.S. EPR I&C Architecture .....                          | 2-2  |
| Figure 2-2—Lines of Defense and I&C Functions .....                 | 2-7  |
| Figure 3-1—Diversity for Initiating Reactor Trip .....              | 3-8  |
| Figure 3-2—Diversity for Executing Reactor Trip .....               | 3-9  |
| Figure 3-3—Diversity for Actuation and Control of ESF Systems ..... | 3-10 |
| Figure 3-4—Diversity of Indications and Alarms .....                | 3-12 |

## Nomenclature

| <b>Acronym</b> | <b>Definition</b>                                      |
|----------------|--|
| ALWR           | Advanced Light-Water Reactor                           |
| AOO            | Anticipated Operational Occurrence                     |
| ATWS           | Anticipated Transients Without Scram                   |
| BDBE           | Beyond Design Basis Event                              |
| BOP            | Balance of Plant                                       |
| CCF            | Common-Cause Failure                                   |
| CRDCS          | Control Rod Drive Control System                       |
| D3             | Diversity and Defense-in-Depth                         |
| DAS            | Diverse Actuation System                               |
| DBE            | Design Basis Event                                     |
| DCD            | Design Control Document                                |
| DEG            | Double-Ended Guillotine                                |
| EBS            | Extra Borating System                                  |
| EFWS           | Emergency Feedwater System                             |
| ESF            | Engineered Safety Feature                              |
| FWLB           | Feedwater Line Break                                   |
| HMI            | Human-Machine Interface                                |
| HVAC           | Heating, Ventilation, Air Conditioning                 |
| I&C            | Instrumentation and Control                            |
| IOPSRV         | Inadvertent Opening of Pressurizer Safety Relief Valve |
| IRWST          | In-Containment Refueling Water Storage Tank            |
| LOCA           | Loss of Coolant Accident                               |
| LOOP           | Loss of Offsite Power                                  |
| LPD            | Linear Power Density                                   |
| MCR            | Main Control Room                                      |
| MFW            | Main Feedwater   |
| MHSI           | Medium Head Safety Injection                           |
| MSIV           | Main Steam Isolation Valve                             |
| MSRT           | Main Steam Relief Train                                |
| MSSV           | Main Steam Safety Valve                                |

---

| <b>Acronym</b> | <b>Definition</b>                             |
|----------------|---|
| NI             | Nuclear Island                                |
| OS             | Operating System                              |
| PACS           | Priority and Actuation and Control System     |
| PAM            | Post Accident Monitoring                      |
| PAS            | Process Automation System                     |
| PICS           | Plant Information and Control System          |
| PLD            | Programmable Logic Device                     |
| PRA            | Probabilistic Risk Assessment                 |
| PS             | Protection System                             |
| PSRV           | Pressurizer Safety Relief Valve               |
| PZR            | Pressurizer                                   |
| QDS            | Qualified Display System                      |
| RCCA           | Rod Cluster Control Assembly                  |
| RCP            | Reactor Coolant Pump                          |
| RCS            | Reactor Coolant System                        |
| RCSL           | Reactor Control, Surveillance and Limitation  |
| RSS            | Remote Shutdown Station                       |
| RT             | Reactor Trip                                  |
| SA             | Severe Accident                               |
| SA I&C         | Severe Accident Instrumentation and Control   |
| SAS            | Safety Automation System                      |
| SBLOCA         | Small Break LOCA                              |
| SBO            | Station Blackout                              |
| SGTR           | Steam Generator Tube Rupture                  |
| SI             | Safety Injection                              |
| SICS           | Safety Information and Control System         |
| SIS            | Safety Injection System                       |
| SIVAT          | (Software) Simulation and Validation Tool     |
| SRM            | Staff Requirements Memorandum                 |
| SSSS           | Standstill Seal System                        |
| SWCCF          | Software Common Cause Failure                 |
| TG I&C         | Turbine Generator Instrumentation and Control |

| <b>Acronym</b> | <b>Definition</b>           |
|----------------|-----------------------------|
| TI             | Turbine Island              |
| TSC            | Technical Support Center    |
| TXS            | TELEPERM XS                 |
| UV             | Undervoltage                |
| V&V            | Verification and Validation |
| VDU            | Video Display Unit          |

## Definitions

*Operational I&C function*—An instrumentation and control (I&C) function that provides for control of plant systems during normal operation.

*Limitation I&C function*—An I&C function that executes one or more of the following actions: 1. Prevents plant disturbances from causing normal operating limits to be exceeded; 2. Alerts the operator when normal operating limits have been exceeded; 3. Prevents disturbances from leading to a design basis event.

*Platform* – A packaged, generic set of hardware devices (e.g, processors, I/O modules, and communication cards) and system software (e.g., operating system (OS), runtime environment, function block libraries) that can be configured for a variety of I&C applications.

*Risk Reduction I&C function*—An I&C function that is used to mitigate the effects of beyond design basis events (BDBE). These include events such as CCF of safety I&C systems, station blackout (SBO), and severe accident (SA).

*Safe Shutdown*—For design basis events, safe shutdown is defined as cold shutdown for the U.S. EPR. For beyond design basis events, safe shutdown is defined in accordance with regulatory guidelines for particular events (e.g., SBO - hot standby).

*Safety I&C function*—An I&C function that either: 1. Actuates or controls one of the processes or conditions essential to maintain plant parameters within acceptable limits established for a design basis event (DBE), or 2. Controls the processes or conditions required to reach and maintain safe shutdown.

## **1.0 INTRODUCTION**

### **1.1 *Scope***

The purpose of this report is to describe a methodology to assess the adequacy of the U.S. EPR instrumentation and control (I&C) design with respect to diversity and defense-in-depth (D3).

To support the discussion of the methodology, this report describes the I&C systems that comprise the overall I&C architecture. The U.S. EPR defense-in-depth concept is discussed, and is compared to the echelons of defense discussed in NUREG/CR-6303 (Reference 7). Design features that are used to prevent a common-cause failure (CCF) of the safety I&C systems, as well as mitigate the effects of a postulated CCF of the safety I&C systems, are presented.

The methodology used to assess the adequacy of the U.S. EPR I&C design with respect to D3 is presented. The results demonstrating that the design is sufficient with respect to D3 will be provided in future submittals to the NRC.

### **1.2 *Background***

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

An early attempt to address these types of CCF was provided in NUREG-0493 (Reference 6). Subsequently, in SECY 91-292 (Reference 5), the staff included discussion of its concerns about common-cause failures in digital systems used in nuclear power plants. As a result of the reviews of advanced light-water reactor (ALWR) design certification applications for designs that use digital protection systems, the NRC documented its position with respect to common-cause failures in digital systems and defense-in-depth. This position was documented as Item II.Q in SECY 93-087 (Reference 8) and was subsequently modified in the associated staff requirements memorandum (SRM), (Reference 9). NUREG-0800 BTP 7-19 (Reference 3) was developed to provide further guidance and clarification of D3 design and acceptance criteria.

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

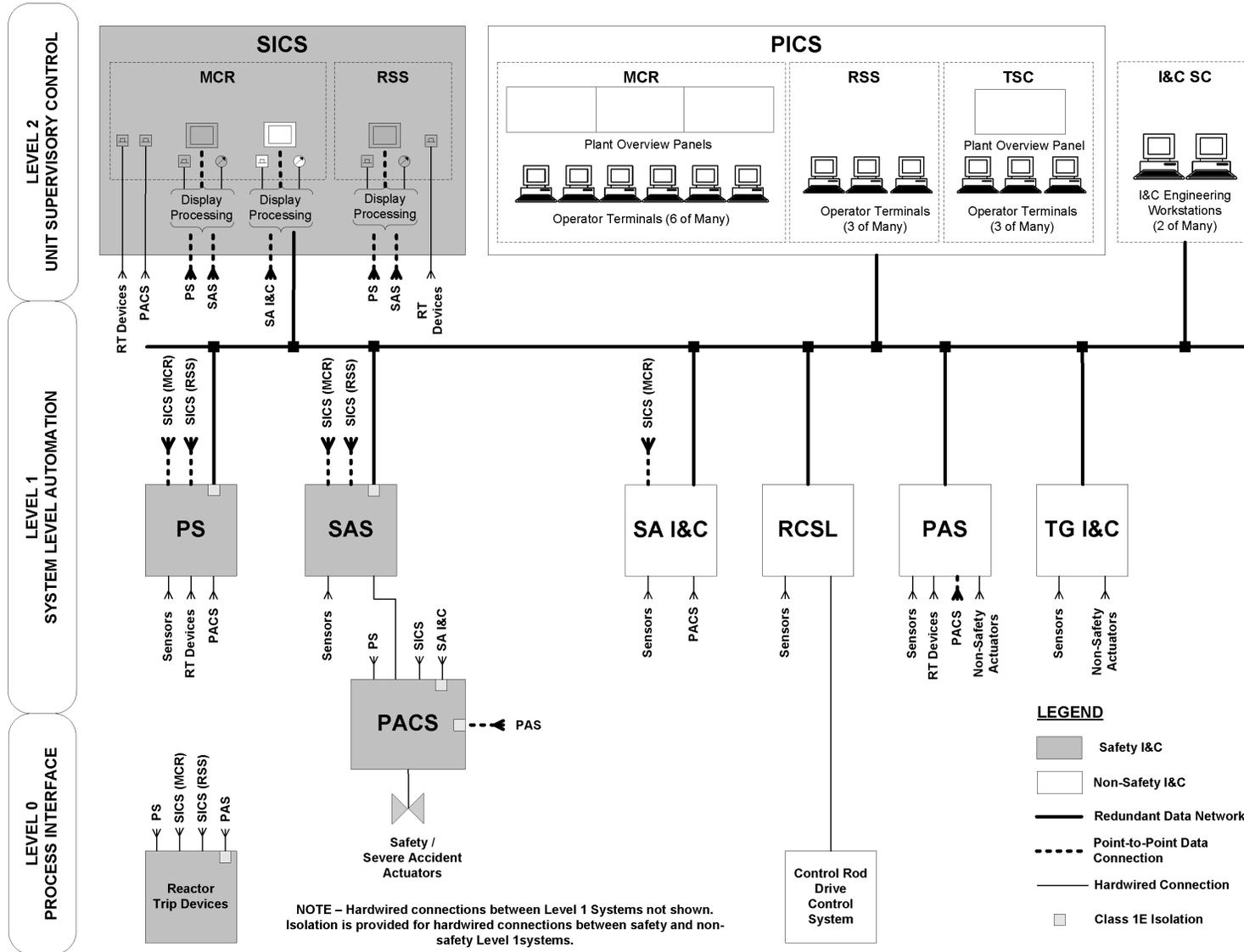
## 2.0 U.S. EPR I&C ARCHITECTURE

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

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

| <b>System</b>                                 | <b>Platform</b>                |
|---|--------------------------------|
| Process Information and Control System        | Computerized, diverse from TXS |
| Safety Information and Control System         | TXS (QDS)/Hardwired            |
| Protection System                             | TXS                            |
| Safety Automation System                      | TXS                            |
| Priority and Actuator Control System          | TXS (AV42)                     |
| Severe Accident Instrumentation and Control   | TXS                            |
| Reactor Control, Surveillance and Limitation  | TXS                            |
| Process Automation System                     | Computerized, diverse from TXS |
| Turbine Generator Instrumentation and Control | Supplied by turbine vendor     |

Figure 2-1—U.S. EPR I&C Architecture



## **2.1 Level 2—Supervisory Control**

There are two systems within Level 2—the process information and control system (PICS) and the safety information and control system (SICS).

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

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

- Monitoring and control of essential non-safety-related systems to provide for safe, steady-state plant operation for a limited time, as well as to reach and maintain hot standby (MCR only).
- Monitoring and control of safety-related-systems. This includes the following capabilities:
  - System level actuation of reactor trip (MCR and RSS).
  - System level actuation of engineered safety features (ESF) systems (MCR only).

- Monitoring and control of safety systems to reach and maintain safe shutdown (MCR and RSS).
- Monitoring and control of plant equipment necessary to mitigate a severe accident (MCR only).

For the initiation of protective actions at the system level (e.g., reactor trip, safety injection), conventional means (i.e., buttons, switches) are provided on the SICS. For ESF system initiations, these signals are either acquired by TXS computers and combined with the automatic actuation logic, or are hardwired directly to priority and actuator control system (PACS) modules. For reactor trip (RT) initiation, the signals are hardwired directly to the reactor trip devices to bypass the TXS computers.

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

The safety related portions of the SICS are designed to meet the requirements of 10 CFR 50.55a(h) (Reference 1).

## **2.2 Level 1—System Level Automation**

The protection system (PS) is an integrated RT system and ESF actuation system. It is a safety-related system. The PS detects the conditions indicative of an anticipated operational occurrence (AOO) or postulated accident and actuates the plant safety features to mitigate these events. This is accomplished primarily through the execution of automatic safety I&C actuation functions, specifically RT and actuation of ESF systems. The PS has four redundant, independent divisions. Each division is located in a physically separated Safeguards Building. Each division of the PS contains two independent subsystems to implement functional diversity. The PS utilizes the TXS

platform, and is designed to meet the requirements of 10 CFR 50.55a(h). For more detail on the PS, see AREVA NP Topical Report ANP-10281P (Reference 12).

The safety automation system (SAS) is a safety-related system. The SAS processes automatic control functions as well as manually initiated control functions to mitigate AOOs and postulated accidents and to reach and maintain safe shutdown. The SAS has four independent divisions. Each division is located in a physically separated Safeguards Building. Additional SAS equipment is located in the two physically separated Emergency Diesel Generating Buildings. There are redundant controllers within each division of the SAS for maximum reliability. The SAS utilizes the TXS platform, and is designed to meet the requirements of 10 CFR 50.55a(h).

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

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

The process automation system (PAS) executes the majority of plant control functions. Specifically, it performs operational and limitation I&C functions except those performed by RCSL or the turbine-generator instrumentation and control (TG I&C). It also executes those risk reduction I&C functions required to mitigate BDBEs other than severe accidents, including anticipated transients without scram (ATWS), SBO, and CCF of the safety I&C systems. It consists of four main subsystems:

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

- Diverse Actuation System (DAS).

The PAS is a non-safety-related system and is implemented with a digital I&C platform diverse from TXS.

The TG I&C performs turbine and generator control and protection functions. It is implemented with a platform supplied by the turbine vendor.

The PACS is a safety-related system. It performs the following functions: priority control, drive actuation, drive monitoring, and essential component protection. The PACS is implemented in four independent divisions, with each division located in a physically separate Safeguards Building. The PACS consists of individual PAC modules associated with each actuator. The PACS utilizes the AV42 priority module, which is part of the TXS family of components. The AV42 is designed to meet the requirements of 10 CFR 50.55a(h). More information on the AV42 is found in AREVA NP Topical Report ANP-10273P (Reference 11).

### **2.3 Level 0—Process Interface**

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

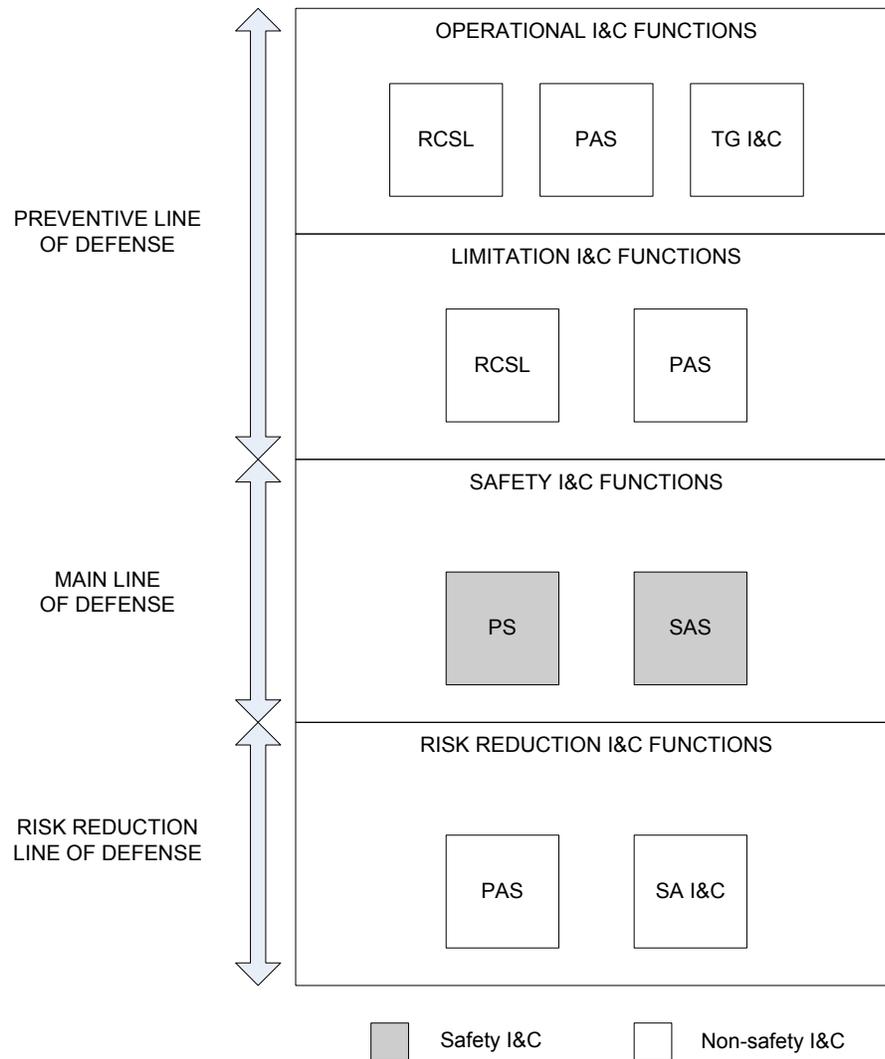
### **2.4 U.S. EPR I&C Defense-In-Depth Concept**

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

- Preventive Line (RCSL, PAS, and TG I&C).
- Main Line (PS and SAS).
- Risk Reduction Line (PAS and SA I&C).

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

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



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

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

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

In general, the lines of defense apply to the architecture level 1 automation systems. The PACS prioritizes actuation requests from I&C systems within each of the lines of defense and therefore does not belong to any single line of defense. The prioritization of actuation requests incorporates the D3 concepts and is described in Section 7.1 of the U.S. EPR Final Safety Analysis Report (FSAR). The PICS is used as long as it is available, and the SICS implements a backup Class 1E human-machine interface (HMI) that is always available for use even when the PICS is unavailable. The PICS and SICS therefore do not belong to any single line of defense.

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

The original concept of "Echelons of Defense" was discussed in NUREG-0493. This study identified three conceptual, functional echelons of defense (control, RT, and ESF) that were to be used to an acceptable degree so that the postulated CCF events do not lead to unacceptable consequences. This approach was expanded by using four different echelons of defense in NUREG/CR-6303. The four echelons were designated 1) control, 2) RT, 3) ESF, and 4) monitoring and indication. These four echelons of defense were based on a conceptual design approach to be used for analyzing CCFs within and between the echelons of defense, and are not required by NRC regulations..

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

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

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

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

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

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

The U.S. EPR I&C architecture is designed to withstand the effects of various CCFs which could prevent performance of the required safety functions. In general, the design utilizes two types of feature:

- Those features designed to prevent a CCF of the safety I&C systems (main line of defense) that could disable a safety function.
- Those features that mitigate the effects of a postulated CCF that has disabled the safety function of the I&C safety systems (main line of defense).

As discussed previously, the main line of defense consists of the automatic safety functions performed by the PS, SAS, and PACS; therefore, these are the systems of interest when considering CCFs.

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

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

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

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

The TXS platform has been designed with many features that enhance reliability and availability. These features are described in detail in Siemens Topical Report EMF-2110 (NP)(A), Revision 1 (Reference 13) and Siemens Topical Report EMF-2267(P), Revision 0 (Reference 14). Both submittals were approved in Reference 10.

The following list summarizes the features of TXS that are designed to prevent a CCF of the platform and the respective relevant reference.

1. Cyclic, deterministic, asynchronous operation—see Section 2.4.3.4 of Reference 13 and Sections 9.1 and 9.3 of Reference 14.
2. Interference-free communications—see Section 2.9 of Reference 13 and Section 9.1 of Reference 14.
3. Independence of the TXS platform operation (including both hardware and system software) from the application software program—see Section 2.4.2.2.1 of Reference 13 and Section 9.4 of Reference 14.
4. Fault tolerance—see Section 2.7 of Reference 13.
5. Equipment and system software qualification—see Section 2.2 of Reference 13
6. The use of a standard library of application function blocks with operating experience—see Section 2.1.3.1 of Reference 13.

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

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

The TXS platform benefits from having extensive operating experience. Internationally, TXS has been in use for over 10 years with over 62 million processor hours of operation. Section 5.2 of Reference 13 describes a configuration management plan, including a change control process. According to problem reports gathered as a result

of the change control process, there have been no reported CCFs of the TXS platform system software to date.

### **3.1.1.2 AV42 Priority Module Design**

The AV42 is a prioritization module that is part of the TXS product family, and meets the requirements of 10 CFR 50.55a(h). The AV42 operates independently of, and diverse to, the operational principles of the digital TXS platform discussed in Section 3.1.1.1. The AV42 is a qualified device that contains a programmable logic device (PLD) that is qualified to perform safety functions, and a Profibus controller to interface to the PAS to execute non-safety functions. The PLD is a simple hardware device that contains no operating system or software. The design of the PLD has been fully tested and its safety function has been independently verified. During manufacturing, the PLD is checked to verify that the appropriate design has been applied. The PLD is periodically tested during operation to verify proper functionality.

Based on the design features and testing described above, the AV42 is not susceptible to a CCF. This is consistent with NRC guidance in NUREG-0800, BTP 7-19 on simple devices being precluded from the consideration of a CCF. The AV42 is described in detail in Reference 11.

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

### **3.1.2.1 PS Design**

The PS is described generally in Section 2.2 of this report. A detailed description of the PS architecture is provided in Reference 12. The PS is implemented with the TXS platform. In addition to the features inherent to TXS, the PS design incorporates the following features that are designed to prevent a CCF of the system:

- Functional diversity—see Section 10 of Reference 12.
- Fail safe/fault tolerant design—see Sections 7.3, 7.4, 8.2 of Reference 12.
- Independence —see Section 14.9 of Reference 12.

- Diversity of RT devices—see Sections 7.7-7.10 of Reference 12.

The design of the PS is the direct result of the experience AREVA NP has developed in the area of digital protection systems installed internationally. This heuristic experience demonstrates that the dominant CCF mode for digital I&C systems is due to errors in the specification of the requirements (i.e., application software), not in the platform itself (hardware and system operating software). To specifically address this type of CCF, the concept of functional diversity was developed, and is implemented in the design of the PS. The CCF prevention features discussed in Section 3.1.1 prevent a CCF associated with application software from impacting the operating system software and propagating to diverse functions. Functional diversity as defined by AREVA NP is referred to as *signal diversity* in NUREG/CR-6303.

Diversity in RT devices is addressed further in Section 3.2.1.1 of this report.

### **3.1.2.2 SAS Design**

The SAS is implemented with the TXS platform. In addition to the features inherent to TXS, the design provides for independence between the four divisions of the SAS, and between the SAS and interfacing non-safety systems. The characteristics of this independence are physical separation, electrical isolation, and communications independence.

### **3.1.2.3 PACS Design**

The PACS is implemented with the AV42 priority module. In addition to the features inherent to the AV42, the design provides for independence between the four divisions of the PACS, and between the PACS and interfacing non-safety systems. The characteristics of this independence are physical separation, electrical isolation and communications independence.

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

The processes used to develop, test, and maintain application software for the I&C safety systems using TXS processors are described in AREVA NP Topical Report ANP-10272 (Reference 15). These processes include the following:

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

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

The TXS platform provides important tools to implement the software development processes and reduce the likelihood of a programming error. Function block programming and automatic code generation significantly reduces the complexity of the application software programming task as compared to command line programming. The built in software simulation and validation tool, SIVAT, provides the ability to test the application software against its requirements to verify proper functionality. These tools are described in detail in Reference 15.

### **3.2 Features that are Designed to Mitigate a Postulated CCF of the I&C Safety Systems (Main Line of Defense)**

The features described in Section 3.1 reduce the likelihood of a CCF. In addition, a conservative approach has been applied that postulates a CCF due to a TXS platform failure which prevents the TXS based I&C systems from performing their functions when required. This postulated CCF is such that the design features discussed in 3.1 are ineffective at preventing the failure. A platform diverse from TXS is provided to cope

with a loss of the safety I&C systems. This platform will be part of the PAS and can be used to automatically initiate required safety functions, or allow manual execution of required safety functions by the operator.

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

Given the postulated CCF, diversity is provided for different types of safety functions. In general, diversity exists for accident mitigation capability from event initiation to achievement of safe shutdown.

Only the portion of the risk reduction line of defense provided to directly mitigate the loss of the main line of defense is required to be diverse from TXS. In the U.S. EPR I&C design, the PAS performs these functions, and is implemented with a digital I&C platform diverse from TXS. The SA I&C system provides for mitigation of severe accidents, and is not required to be diverse from the safety I&C systems.

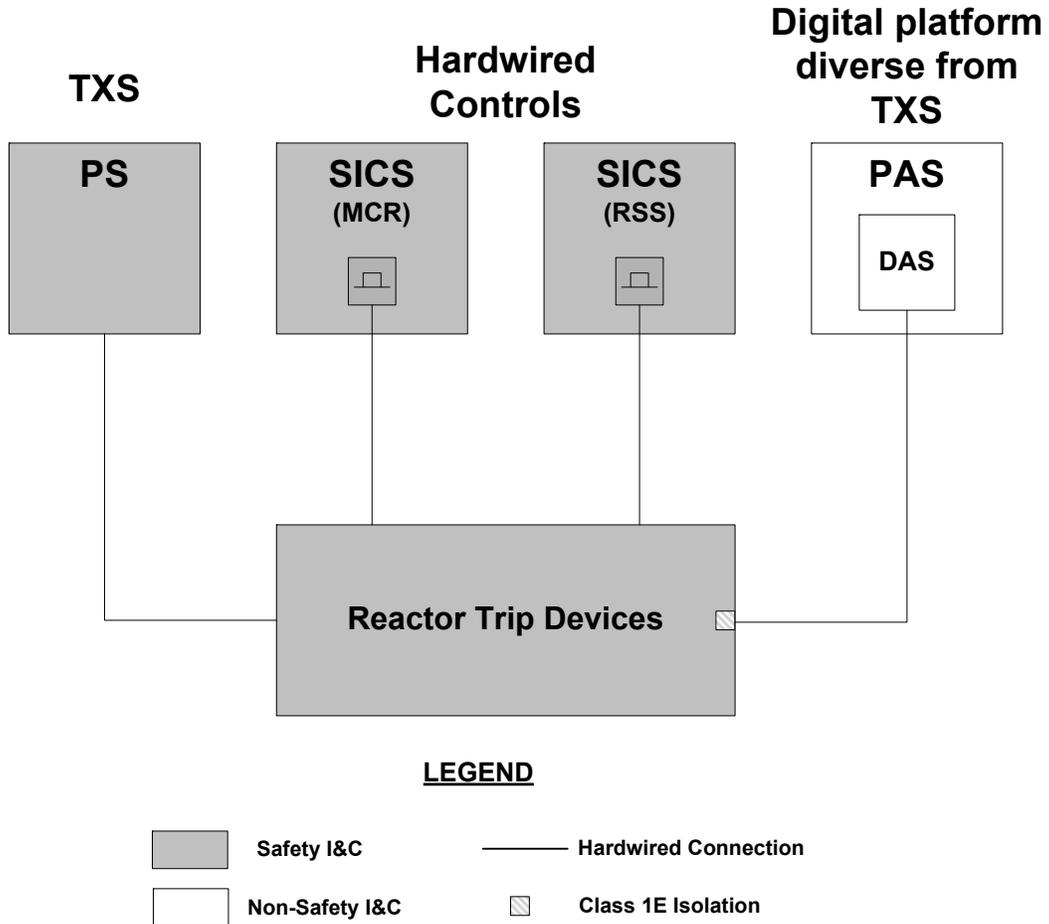
#### **3.2.1.1 Reactor Trip**

The PS is the primary means of initiating RT. Assuming a postulated CCF renders the PS inoperable, there are two diverse means of initiating a RT. If a RT is required to be automatically initiated, it is performed by the DAS, a subsystem of the PAS. If automatic initiation is not required, a manual, hardwired means of initiating a RT is provided on the SICS from either the MCR or RSS. The hardwired controls on SICS to initiate RT, as discussed in Section 2.1 of this report, are provided to address Point 4 of NUREG-0800, BTP 7-19. These controls consist of four switches, each assigned to an independent safety division. The controls are diverse because a software failure of the safety systems will not affect the operation of the hardwired controls. Diversity for initiating a RT is shown in Figure 3-1.

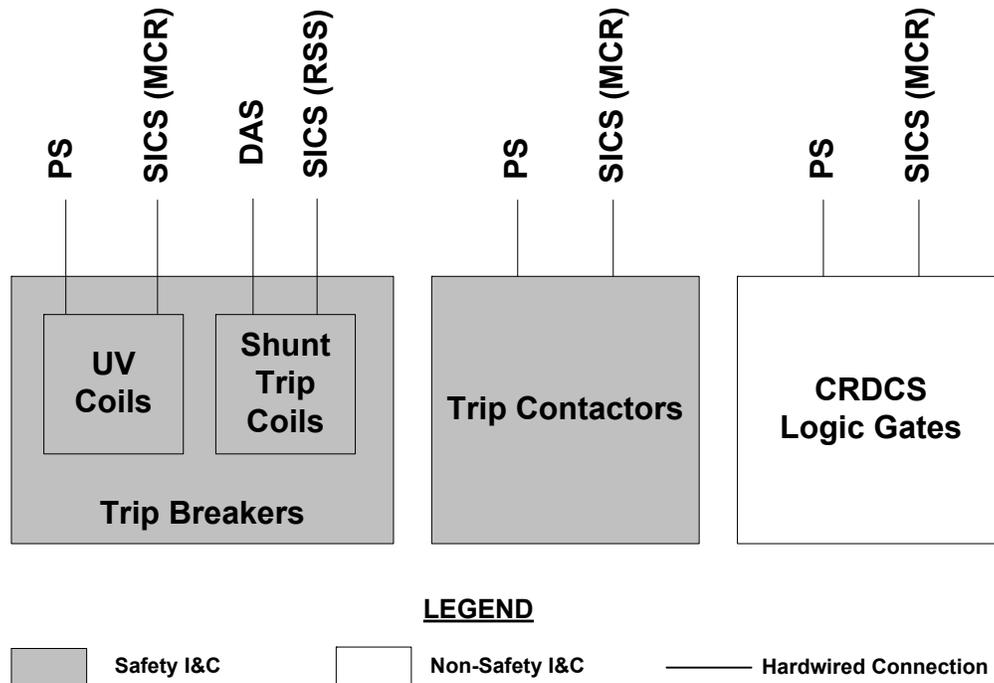
The power supply for the control rods can be interrupted in several diverse ways, for high reliability of the reactor trip function. The safety-related reactor trip breakers contain both an undervoltage (UV) coil and a diverse shunt trip coil. Power to the UV

coil can be interrupted by a signal from either the PS or the SICS in the MCR. The shunt trip coil receives signals from the DAS and the SICS in the RSS. The safety related trip contactors are diverse from the trip breakers, and receive actuation signals from the PS or the SICS in the MCR. The non-safety-related control logic gates in the control rod drive control system (CRDCS) are diverse from the trip breaker and trip contactors, and receive a signal to interrupt power from the PS or the SICS in the MCR. Diversity for executing a RT is shown in Figure 3-2.

**Figure 3-1—Diversity for Initiating Reactor Trip**



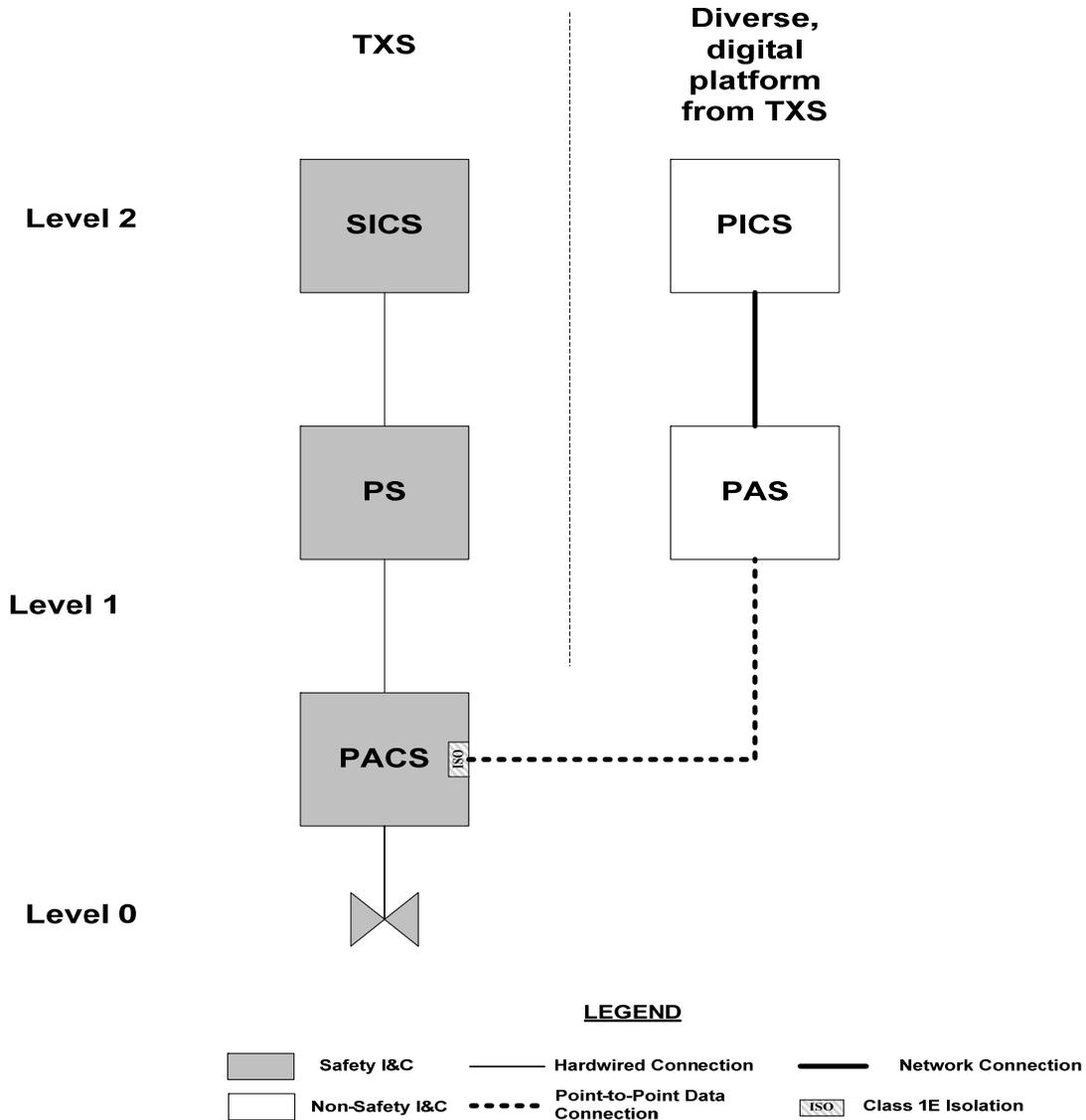
**Figure 3-2—Diversity for Executing Reactor Trip**



**3.2.1.2 ESF Actuation**

The PS is the primary means of performing ESF actuations. Assuming a postulated CCF renders the PS inoperable, there are two diverse means of performing an ESF actuation. If an ESF actuation is required to be automatic, it is performed by the DAS, a subsystem of the PAS. If automatic actuation is not required, manual means of actuating an ESF system are provided at the component level from the PICS via the PAS. The controls are diverse because a software failure of the safety systems will not affect the operation of the PICS or PAS.

**Figure 3-3—Diversity for Actuation and Control of ESF Systems**



**3.2.1.3 ESF Control**

The SAS is the primary means of performing ESF control functions. Assuming a postulated CCF renders the SAS inoperable, the DAS is available as a diverse means of executing ESF control functions. The controls provided in DAS address the guidance of Section 7.3 of NUREG-0800 on diversity of ESF controls. This diversity is shown in Figure 3-3.

Diversity is provided for safety-related ESF control functions performed by the SAS.

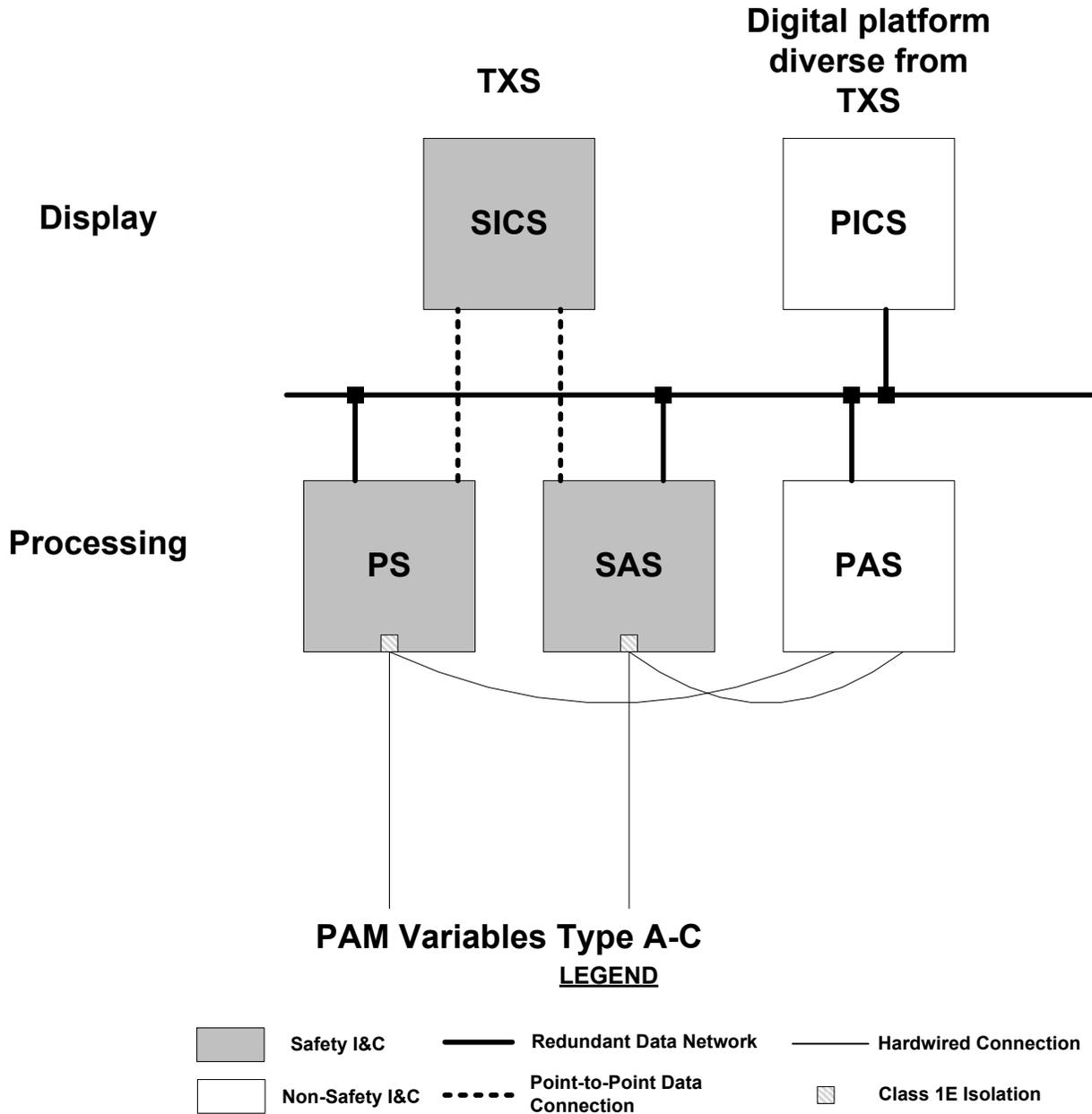
#### **3.2.1.4 *Indications and Alarms***

Diversity is provided for the processing and display of indications and alarms necessary to alert the operator to abnormal plant conditions, including type A, B and C post-accident monitoring variables as defined in Regulatory Guide 1.97 (Reference 4). The PS and SAS are the credited means of processing these variables, and the SICS is the credited means for display. The PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS software. The PICS, which is used during all plant conditions, as long as it is available, provides a diverse display. This diversity is shown in Figure 3-4. The indications provided via PAS and PICS conform to NRC guidance on diversity for post-accident monitoring in Regulatory Guide 1.97 and guidance on diverse indications per Point 4 of NUREG-0800, BTP 7-19.

#### **3.2.2 *Independence between Main Line of Defense and the Risk Reduction Line***

Independence is provided between the systems comprising the main line of defense (PS, SAS, PACS) and the risk reduction line of defense (PAS, SA I&C). Specifically, the safety I&C systems are designed to meet the requirements for independence between safety and non-safety systems per 10 CFR 50.55a(h). This prevents a CCF from affecting both the main line of defense and the risk reduction line of defense.

**Figure 3-4—Diversity of Indications and Alarms**



## 4.0 DIVERSITY AND DEFENSE-IN-DEPTH METHODOLOGY

To verify that the overall I&C architecture design is adequate with respect to D3, and that specific NRC requirements and guidance are met, a D3 methodology is presented. This methodology is to be followed throughout the basic and detailed design phases of the U.S. EPR. The methodology addresses the guidance in NUREG-0800, BTP 7-19, and is consistent with the methodology outlined in NUREG/CR-6303.

### 4.1 *Step 1 - Susceptibility Analysis of Safety I&C Systems to CCF*

An analysis of the safety I&C systems will be performed to determine their susceptibility to a CCF. This analysis addresses Point 1 of NUREG-0800, BTP 7-19. The following assumptions will be used when performing this analysis:

- A CCF of the TXS platform is postulated (conservative assumption). This postulated CCF is such that the TXS based I&C systems do not perform their functions when required. This CCF is such that the design features discussed in 3.1 are ineffective at preventing the failure.
- The AV42 is not affected by a CCF of the TXS process computers. It is not considered to be susceptible to a software CCF.
- The platform used for PICS and PAS is diverse from TXS and not susceptible to the same CCF as the TXS platform.

### 4.2 *Step 2 - Qualitative Evaluation of AOOs and Postulated Accidents*

A qualitative evaluation of the AOOs and postulated accidents listed in U.S. EPR FSAR Tier 2, Chapter 15 will be performed assuming any postulated CCFs determined in Step 1. This process may be performed in conjunction with, before, or after ATWS evaluations to determine required functionality of the DAS for ATWS mitigation. This evaluation addresses Points 2 and 3 of NUREG-0800, BTP 7-19.

This evaluation will be performed with a team comprised of individuals from the following technical disciplines (at a minimum):

- Safety analysis.
- PRA.
- I&C.
- Human factors.

The evaluation will be performed using, at a minimum, the following best estimate assumptions:

- All systems (safety and non-safety) that are not affected by a postulated CCF identified in Step 1 are credited for use.
- Any additional best-estimate assumptions that are used during the process will be documented along with the results of the evaluation.

The evaluation will be performed using the following process:

- Each AOO and postulated accident will be evaluated assuming a postulated CCF identified in Step 1 has occurred concurrent with that event.
- The acceptance criteria for each event is the following:
  - AOOs
    - Radiation release less than 10 percent of the guidelines of 10 CFR 100 (Reference 2).
    - No violation of the integrity of the primary coolant pressure boundary.
  - Postulated accidents
    - Radiation release less than the guidelines of 10 CFR 100.
    - No violation of the integrity of the primary coolant pressure boundary.

- No violation of the integrity of the containment.
- If it is judged that the automated plant response using the I&C systems not affected by the postulated CCF is sufficient to meet the acceptance criteria, no further action is needed.
- If it is judged that the automated plant response using the I&C systems not affected by the postulated CCF will not be sufficient to meet the acceptance criteria stated in NUREG-0800, BTP 7-19, one of the following actions will be performed:
  - Identify additional functionality to mitigate the event.
  - Determine if there is adequate justification to preclude adding additional functionality.
- For any additional functionality, a judgment will be made as to whether it can be performed manually or automatically. Operator action will be allowed to be used if it is judged to be feasible by the participants given the event description and assumed CCF. This determination will be made in accordance with the function allocation criteria described in AREVA NP Topical Report ANP-10279 (Reference 16).
- If a function is allocated for manual actuation, then it is assigned to the appropriate I&C system using the process described in Step 3.
- If a function is allocated for automatic actuation, then it will be assigned to the DAS subsystem of the PAS.
- If qualitative evaluations are insufficient to verify that acceptance criteria are met for specific AOOs or postulated accidents, then quantitative analysis of those events will be performed in Step 4.

Detailed results of Step 2 of the D3 methodology is provided in Appendix A (Section 7).

### **4.3 Step 3 - Determine Inventory of Diverse Controls and Indications**

Inventory of diverse controls and indications is determined for SICS and PICS in the following manner. This process addresses Point 4 of NUREG-0800, BTP 7-19. The inventory is validated during the human factors verification and validation per Step 5.

#### **4.3.1 Hardwired Controls on SICS**

Safety-related controls are provided on the SICS. However, these controls are not credited for providing diverse manual initiation of ESF systems in case of a software CCF of the safety systems. Hardwired controls provided on SICS for reactor trip are credited in the D3 analysis.

#### **4.3.2 Controls on PICS**

Safety-related plant equipment will have the capability of being controlled manually at the component level from the PICS via the PAS and PACS. The functions that were credited for manual operator action in Step 2 are performed via these PICS controls.

#### **4.3.3 Indications on PICS**

The inventory of indications on PICS required for diversity is determined in the following manner.

- Type A-C post-accident monitoring variables will be processed by PAS and displayed on PICS. This is provided to address the guidance of Regulatory Guide 1.97.
- Any additional indications or alarms required to ensure the operator has sufficient awareness of plant conditions.

### **4.4 Step 4 - Quantitative Analyses of AOOs and Postulated Accidents**

As discussed in Step 2, quantitative analyses might be required for some events to confirm that the applicable acceptance criteria are met. The best estimate methods

used to perform these analyses will be described in the analytical results documentation.

If quantitative analyses do not demonstrate that the design meets the acceptance criteria, the evaluation process will be performed again for that event using the quantitative results as input to achieve an acceptable design.

These analyses address Points 2 and 3 of NUREG-0800, BTP 7-19.

#### **4.5 Step 5 - Human Factors Engineering Verification and Validation**

For those events that manual operator action was credited in providing adequate event mitigation, a Human Factors Engineering Verification and Validation (V&V) activity will be performed as described in Reference 16. The objective of this activity is to verify that the operator has sufficient time, indications and controls to perform the required actions.

If it is determined that the operator does not have sufficient time to perform the required actions, those functions will be re-allocated to be automatically performed by the DAS, a subsystem of the PAS.

If it is determined that the operator has insufficient indications and controls to perform the required actions, those indications and controls will be identified and added to the design.

This is provided to address Points 2, 3 and 4 of NUREG-0800, BTP 7-19.

#### **4.6 Step 6 – Platform Diversity Analysis**

An analysis will be performed to demonstrate that the digital platform implemented for the PAS and PICS is diverse from TXS. This analysis will be performed using the diversity principles discussed in NUREG/CR-6303 as a guide, which are:

- Human diversity.
- Design diversity.

- Software diversity.
- Functional diversity.
- Equipment diversity.

Signal diversity (referred to as functional diversity with respect to the U.S. EPR) is specific to the application of a digital I&C system. While signal diversity is a very important design feature that reduces the likelihood of a CCF, the platform diversity analysis is aimed at demonstrating that the digital I&C platforms are diverse. Therefore, signal diversity is not considered in the platform diversity analysis.

Specific attributes to be considered include differences in:

- Manufacturer.
- Hardware.
- OS.
- Programming language.
- Run Time Environment.
- Function blocks.

## **5.0 CONCLUSIONS**

The I&C systems designed for the U.S. EPR have been design to perform required functionality and meet applicable regulatory requirements. The U.S. EPR I&C architecture incorporates a robust defense-in-depth strategy.

The D3 features of the safety I&C systems minimize the likelihood of a CCF. These features have been developed and are proven though years of AREVA NP operating experience with digital safety I&C systems internationally. A conservative approach is taken that provides for a diverse means of performing safety functions in case of the inability of the safety I&C systems to perform their required functions due to a CCF.

The methodology proposed to evaluate the adequacy of the I&C design with respect to D3 meets applicable NRC regulatory requirements and guidance.

## **6.0 REFERENCES**

### **6.1 U.S. Regulations**

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

### **6.2 U.S. Regulatory Guidance**

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

### **6.3      *Regulatory Review Precedent***

10. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, 'Acceptance for Referencing of Licensing Topical Report EMF-2110 (NP), Revision 1', "TELEPERM XS: A Digital Reactor Protection System" (TAC NO. MA1983) May 2000.

### **6.4      *AREVA NP Documents***

11. AREVA NP Topical Report, ANP-10273P, Revision 0, "AV42 Priority Actuation and Control Module," November 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report," NRC:06:054, November 28, 2006.
12. AREVA NP Topical Report, ANP-10281P, Revision 0, "U.S. EPR Digital Protection System", Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10281P, "U.S. EPR Digital Protection System Topical Report," NRC:07:011, March 27, 2007.
13. Siemens Topical Report, EMF-2110 (NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," May 2000.
14. Siemens Topical Report, EMF-2267(P), Revision 0, "Siemens Power Corporation Methodology Report for Diversity and Defense-In-Depth," September 1999.
15. AREVA NP Topical Report, ANP-10272, Revision 0, "Software Program Manual for TELEPERM XS Safety System Topical Report," December 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10272, "Software Program Manual TELEPERM XS Tm Safety Systems Topical Report," NRC:06:061, December 2006.

16. AREVA NP Topical Report, ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program Topical Report," January 2007, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10279, "U.S. EPR Human Factors Engineering Program Topical Report," NRC:07:004, January 2007.

## APPENDIX A

### 7.0 D3 METHODOLOGY STEP 2 – QUALITATIVE EVALUATION OF ANTICIPATED OPERATIONAL OCCURRENCES AND POSTULATED ACCIDENTS

#### 7.1 *Approach*

The approach used in this evaluation is to review the design basis events analyzed in the accident analysis assuming a software common cause failure (SWCCF) in the PS, which includes both the RT and ESF actuation functions. The evaluation is performed in a strictly qualitative manner.

The PS has built-in features to both prevent common failures and to clearly identify failures that occur to preclude unidentified common mode failures. However, for conservatism the entire PS platform is assumed to fail to function for the purpose of this evaluation, and all other TXS based systems are assumed to also fail as-is concurrently. Limitation functions in RCSL share the same platform as the PS and, therefore, are also assumed to fail.

An initial inventory of functions implemented in the diverse actuation system (DAS) is assumed based on engineering judgment. These DAS functions are credited in the evaluation. Limitation and control functions implemented in the PAS are also credited in the evaluation.

#### 7.2 *Evaluation*

The initial inventory of DAS functions assumed is the following:

- RT on high neutron flux.
- RT on low loop flow rate – two loops.
- RT on low-low loop flow rate – one loop.

- RT on high pressurizer (PZR) pressure.
- RT on low hot leg pressure.
- RT on low steam generator pressure.
- RT on high steam generator pressure.
- RT on low steam generator level.
- RT on safety injection system (SIS) actuation.
- RT on emergency feedwater system (EFWS) actuation.
- SIS actuation on low PZR pressure.
- EFWS actuation on low steam generator level.
- Main steam isolation on low steam generator pressure.
- Containment isolation on SIS actuation.
- Turbine trip on RT confirmation.
- Alarm on MCR heating, ventilation, air conditioning (HVAC) high radiation.
- Alarm on rod cluster control assembly (RCCA) bottom position.

Table A-1 identifies the design basis events analyzed as part of the U.S. EPR FSAR Tier 2, Chapter 15 accident analysis. Table A-2 identifies the protective functions associated with each design basis event in the U.S. EPR FSAR Tier 2, Chapter 15 accident analysis. Using these tables and the assumed DAS inventory, each event category is reviewed assuming a SWCCF in the PS and all other TXS based systems.

In the following sections each event category is evaluated as a group. Within each group the AOOs and postulated accidents are evaluated separately. Results of the qualitative evaluation are summarized in Table A-3. Table A-3 also lists the DAS functions expected for each event. It should be noted that the evaluation is performed with the assumption that SWCCF in the shutdown modes is not considered.

The results of the evaluation were reviewed by a multi-disciplinary team representing systems engineering, PRA, HFE and I&C engineering disciplines.

### **7.2.1 Increase in Heat Removal by Secondary System**

This category includes the following postulated events for the U. S. EPR:

- Feedwater malfunction decrease in feedwater temperature.
- Feedwater malfunction increase in feedwater flow.
- Emergency feedwater (EFW) actuation.
- Excess increase in steam flow.
- Spurious actuation of the partial cooldown system.
- Spurious opening of main steam bypass or turbine inlet valves.
- Inadvertent opening of steam generator (SG) relief or safety valve.
- Steam system piping failures.

For the events in this category the U.S. EPR FSAR Tier 2, Chapter 15 accident analysis relies on the following reactor trip functions.

- Low departure from nucleate boiling ratio (DNBR).
- High linear power density (LPD).
- High core power.
- High SG level.
- Low SG pressure.
- High SG  $\Delta P$ .

The DAS functions that are expected to backup these trips for the overcooling events are the low SG pressure and high neutron flux trips because all the events in this category result in a reduction in SG pressure or an increase in neutron flux.

According to the U.S. EPR FSAR Tier 2, Chapter 15 analysis, feedwater malfunction events that result in either a feedwater temperature reduction or increase in feedwater flow would result in a low DNBR reactor trip or a trip on neutron flux. Since the primary protection for the feedwater malfunction events in the U.S. EPR FSAR Tier 2, Chapter 15 analysis is low DNBR, these events require detailed analysis to confirm the effectiveness of the DAS function “RT on High Neutron Flux” for the spectrum of feedwater malfunctions.

Oversteam demand and steam piping failures would result in a reduction in SG pressure and would be protected by the DAS function “RT on Low SG Pressure”.

Additionally, the overcooling events in this category rely on several ESF functions in the U.S. EPR FSAR Tier 2, Chapter 15 analysis. For this category of events the ESF functions of interest are:

- Main steam relief trains (MSRT).
- Main steam isolation valve (MSIV) closure.
- Main feedwater/start-up and shutdown system (MFW/SSS) isolation.
- SIS and partial cooldown.

If the DAS reactor trip occurs in a timely fashion for the spectrum of events in this category as compared to the U.S. EPR FSAR Tier 2, Chapter 15 analysis, the pre-trip response should behave similarly. In the post-trip response the U.S. EPR FSAR Tier 2, Chapter 15 analysis credits the MSRT isolation function and MFW/SSS isolation to limit the cooldown imposed on the primary system. Opening of the MSRTs provides decay heat removal in the long term for each overcooling event once the event is over and once the system heats back up to operating temperature. SIS provides injection of boron from the in-containment refueling water storage tank (IRWST) to maintain shutdown in the long-term.

Under best estimate conditions, all control rods would be expected to insert (no stuck rod as assumed in the Chapter 15 analysis) and there would be a greater amount of negative reactivity than considered in the Chapter 15 analysis to suppress the reactivity transient. It is judged that this additional negative reactivity would offset the effects of not isolating MFW/SSS. Therefore, this function is not expected to be needed in the DAS for this category of events.

The DAS function “Main Steam Isolation on Low SG Pressure” is expected to occur for the spectrum of overcooling events.

It is concluded that events in this category require detailed analysis to confirm the adequacy of the DAS functions (Table A-3) and whether the MSRT isolation function is required. It may be possible to demonstrate that manual operator control of MSRTs is sufficient.

### **7.2.2      *Decrease in Heat Removal by Secondary System***

This category includes the following postulated events for the U. S. EPR:

- Loss of load/ turbine trip.
- Loss of Condenser Vacuum.
- Inadvertent closure of one MSIV.
- Closure of all MSIVs.
- Loss of offsite power (LOOP).
- Loss of normal feedwater.
- Feedwater line break.

These events result in challenges to the primary and secondary pressure boundary and or the heat removal capability of the EFW system.

It is expected that the DAS functions “RT on High SG Pressure” and “RT on High PZR Pressure” will result in a timely RT under high pressure conditions.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, pressure relieving devices that contribute to mitigating the overpressure challenges include the pressurizer safety relief valves (PSRV), main steam safety valves (MSSV) and main steam relief trains (MSRT). The PSRVs (in hot conditions) and the MSSVs do not rely on I&C systems to open, and are available in the event of SWCCF. However, the MSRTs would not be available in the event of a SWCCF. For overpressure events, the peak primary and secondary pressure is limited by the timing of the reactor trip and action of the primary and secondary relieving devices. The assumed DAS functions do not include actuation of the MSRTs. Thus, if no further analysis is performed, MSRT opening and control would be required to maintain pressures less than the appropriate limits for the overpressure events. However, detailed analysis could show that the MSSVs are sufficient in maintaining secondary pressures within limits.

The loss of offsite power event will be covered in the next category, decrease in reactor coolant system (RCS) flow.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, the loss of normal feedwater relies on SG level to trip the reactor and initiate EFWS. The MSRTs are required for long-term heat removal. For feedwater line break, the reactor is tripped by low SG level or low SG pressure. MSIV closure is relied upon to limit the effects to one SG. MSRTs are relied upon to maintain secondary pressures and remove decay heat.

The DAS functions “RT on Low SG Level” and EFWS Actuation on Low SG Level” are expected to occur for these events. The assumed DAS functions do not include actuation of the MSRTs. Thus, if no further analysis is performed, MSRT opening and control is required to maintain pressures less than the appropriate limits for these events. However, detailed analysis could show that the MSSVs are sufficient in maintaining secondary pressures within limits.

### **7.2.3      *Decrease in RCS Flow Rate***

This category includes the following postulated events for the U. S. EPR:

- Partial loss of flow.
- Complete loss of flow.
- Reactor coolant pump (RCP) seizure or shaft breakage.

In the Chapter 15 analysis, the loss of flow events in this category (including the loss of offsite power from the previous category) rely on the various low-flow reactor trip functions. These include:

- RT on low loop flow rate – two loops.
- RT on low-low loop flow rate – one loop.
- RT on low RCP speed - two loops.

Additionally, the MSRTs and EFWS are relied upon for long-term heat removal. The PSRVs are relied upon to suppress any short-term pressure transient.

The DAS functions “RT on Low Loop Flow Rate – Two Loops” and “RT on Low-Low Loop Flow Rate – One Loop” are available for these events.

For the complete loss of flow or loss of offsite power the U.S. EPR FSAR Tier 2, Chapter 15 analysis relies upon the RCP pump speed reactor trip. The assumed DAS functions do not include an equivalent trip that would respond as quickly. It is not clear whether best-estimate conditions for flowrate and power distributions would be enough to offset the delayed trip such that acceptance limits could be met. An equivalent trip function in DAS could be added, or this event would require detailed analysis for confirmation.

In conclusion, because of limited margin for these events, and what could be gained from best estimate assumptions, loss of flow events would need detailed analysis unless equivalent trips are provided. It is expected that a detailed analysis of loss of flow events would show that the existing DAS functions would be successful in meeting the relaxed acceptance criteria for D3.

#### **7.2.4 Reactivity & Power Distribution Anomalies**

This category includes the following postulated events for the U. S. EPR:

- RCCA withdrawal at power.
- RCCA sub-group withdrawal.
- RCCA withdrawal from low power or subcritical.
- RCCA withdrawal from a shutdown state.
- Single RCCA withdrawal.
- RCCA drop.
- RCP startup.
- RCCA ejection.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, events in this category do not rely on ESF functions except for MSRTs for long term decay heat removal.

For the events in this category the U.S. EPR FSAR Tier 2, Chapter 15 accident analysis relies on the following reactor trip functions.

- High flux rate (power range).
- Low DNBR.
- High LPD.
- High core power.

These trips cover the entire range of reactivity addition events from fast to slow to maintain conditions within acceptance limits. The DAS function “RT on High Neutron Flux” is intended to provide backup for these trips. However, the range of events may not be fully protected by the DAS trip on neutron flux alone. This is because many events in this category are protected by low DNBR in the U.S. EPR FSAR Tier 2, Chapter 15 analysis, and there is no equivalent trip included in the assumed DAS

functions. Detailed analysis is required to confirm that the backup function is sufficient to cover the spectrum of reactivity addition events.

Single rod withdrawal, rod drops, and rod ejection events are special forms of reactivity event. The rod ejection appears to be covered by the DAS function “RT on High Neutron Flux”. The single rod withdrawal and rod drop events are protected by the low DNBR trip in the U.S. EPR FSAR Tier 2, Chapter 15 analysis, and there is no equivalent trip in the DAS. These events require confirmatory analysis to assess the adequacy of the assumed DAS functions.

### **7.2.5 Increase in RCS Inventory**

This category includes the following postulated events for the U. S. EPR:

- Spurious startup of SIS.
- Chemical and volume control system (CVCS) malfunction.
- Extra borating system (EBS) malfunction.

Spurious startup of SIS at power is inconsequential for the U.S. EPR. The shutoff head of the safety injection (SI) pumps are below normal operating pressure, thus no injection occurs if the pumps inadvertently started.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, a CVCS malfunction that results in an increase in RCS inventory relies on the high pressurizer level reactor trip and the CVCS shutdown on high level. The assumed DAS functions do not include either of these. However, if credit is taken for the pressurizer limitation and control functions in PAS the CVCS charging flow is isolated, and the event terminated prior to PSRV lift. This is a non-safety function that can be credited in a best estimate analysis.

For a CVCS malfunction that dilutes the RCS boron concentration, manual action may be required to maintain sufficient shutdown margin.

The EBS malfunction is bounded by the CVCS malfunction.

### **7.2.6      *Decrease in RCS Inventory***

This category includes the following postulated events for the U. S. EPR:

- Inadvertent opening of PSRV.
- Steam generator tube rupture (SGTR).
- CVCS malfunction.
- Loss of coolant accidents (LOCA).

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, the inadvertent opening of a PSRV (IOPSRV) relies on the low pressurizer pressure trip and SIS/partial cooldown functions. The assumed DAS functions include “RT on Low Hot Leg Pressure” and “SIS Actuation on Low PZR Pressure”. The assumed DAS functions do not include partial cooldown. It is not clear that the RCS pressure would decrease below the shutoff head of the medium head safety injection (MHSI) for this event without a partial cooldown. Thus, an analysis of the IOPSRV without the partial cooldown function is required if the DAS does not include partial cooldown. Pressurizer level and pressure control and limitation functions in PAS can prolong the response and possibly justify manual initiation of the partial cooldown function.

The SGTR event is concerned with offsite dose consequences. Offsite dose consequences are limited by terminating the leak through the broken tube. The leak is terminated by brining the primary pressure in equilibrium with the secondary pressure in the affected SG by a series of manual actions. The timing is such that all actions can be performed manually, including tripping the reactor. The manual functions would be available through PAS and PACS. These functions are those listed in Table A-2 for the SGTR event. The operator should be able to manually perform these actions and they are not required for thirty minutes.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, CVCS malfunction that results in an inventory decrease relies on low pressure trip function to trip the reactor. The RCS pressure decrease is sufficient to result in a SIS actuation and partial cooldown. The

partial cooldown function is required to assure injection flow from the MHSI pumps to makeup the inventory lost from the letdown flow.

The DAS functions “RT on Low Hot Leg Pressure” and “SIS Actuation on Low PZR Pressure” would provide a timely RT and SIS actuation. A detailed analysis of the CVCS malfunction without partial cooldown is required to determine if credit for pressurizer control function offsets the need for automatic actuation of partial cooldown.

LOCAs range from very small breaks to the double-ended guillotine (DEG) break of a large RCS pipe (cold leg or hot leg). Small break LOCAs are considered over the range from a break size of 2 inches to 10 percent of the RCS pipe ( $\approx$  10 inches). For breaks in the range of 6 inches and beyond, the RCS depressurizes quickly and the accumulators inject early in the event. For these cases, it may be possible to demonstrate that breaks with accumulator injection allow sufficient time for operator action to initiate partial cooldown and achieve MHSI injection to maintain core cooling. For the intermediate breaks (3–6 inches) accumulator injection occurs late after MHSI injection. In these cases, pumped injection is important to maintain core cooling in the early part of the event. For these intermediate breaks, the partial cooldown function is important to reduce RCS pressure to allow MHSI to inject. Thus, for the 3-6 inch breaks, SIS and partial cooldown is critical and it is difficult to judge that sufficient time exists to credit operator action for these breaks. It is necessary to perform confirmatory analysis (with credit for operator action to initiate partial cooldown) to demonstrate that core cooling is maintained.

In the U.S. EPR FSAR Tier 2, Chapter 15 analysis, the RCP trip function is important for certain small breaks. The confirmatory analysis mentioned above should include an evaluation of the feasibility to credit manual RCP trip by the operator.

For large breaks, the DAS functions “RT on Low Hot Leg Pressure” and “SIS Actuation on Low PZR Pressure” will provide a timely RT and SIS actuation. Partial cooldown for large breaks is not important since the RCS depressurizes quickly to below the shutoff

head of the MHSI pumps. The assumed DAS functions are adequate for large break LOCA.

### **7.2.7 Primary Side Pressure Transients**

This category includes the following postulated events for the U. S. EPR:

- Inadvertent operation of pressurizer heaters.
- Inadvertent operation of pressurizer sprays.

These events do not rely on ESF functions except for MSRTs for long term heat removal. The DAS functions “RT on Low Hot Leg Pressure” and “RT on High PZR Pressure” provide sufficient backup for these events.

### **7.2.8 Radioactive Release from a Subsystem or Component**

For offsite dose consequences and control room doses are evaluated for the following events:

- Small line break outside containment.
- LOCAs.
- SGTR.
- Feedwater line breaks (FWLB).
- Locked rotor.
- Rod ejection.
- Fuel handling accident.

The dose analysis credits isolation functions for the control room HVAC, annulus vents and a portion of the HVAC system in the Safeguard Building. These systems are isolated by the PS on either a containment isolation signal or a radiation monitor signal. These functions would not be available in case of SWCCF. The assumed DAS functions include an alarm function to alert the operator of high radiation level in the

control room. A confirmatory evaluation is required to determine whether this DAS function is adequate for the spectrum of conditions.

### **7.3 Summary and Conclusions**

This document provides an evaluation of the events analyzed as part of the U.S. EPR FSAR Tier 2, Chapter 15 Accident Analysis for the U.S. EPR. The evaluation makes use of assumed DAS functions to judge the effects of SWCCF on each accident sequence on a qualitative basis. We reached the following conclusions:

- Since the primary protection for the feedwater malfunction events is low DNBR, these events require detailed analysis to confirm the effectiveness of the DAS function “RT on High Neutron Flux” for the spectrum of feedwater malfunctions.
- For overcooling events, we conclude that detailed analysis is needed to confirm the adequacy of the DAS functions and whether the MSRT isolation function is required. It may be possible to demonstrate that manual operator action is sufficient.
- For overpressure mitigation in the presence of a SWCCF, MSRT opening is required to maintain pressures less than the appropriate limits without detailed analysis. Detailed analysis may show that the MSSVs are sufficient in maintaining secondary pressures within limits.
- Because of limited margin for LOFA events, and what could be gained from best estimate assumptions, LOFA events need detailed analysis unless equivalent trips are provided. We expect that the LOFA events are acceptable with the relaxed criteria for D3.
- Detailed analysis is required to confirm that the DAS functions are sufficient to cover the spectrum of reactivity addition events.
- The single rod withdrawal and rod drop events need confirmatory analysis to confirm adequacy of assumed DAS functions.
- An analysis of the IOPSRV is required to justify exclusion of the partial cooldown

function from automation in DAS. Credit for pressurizer level control systems in PAS can prolong the response and may justify manual initiation of the partial cooldown function.

- A detailed analysis of the CVCS malfunction without partial cooldown is required unless the partial cooldown function is added to DAS. This analysis will determine if credit for pressurizer control functions offsets the need for automatic actuation of partial cooldown.
- For the 3-6 inch breaks, SIS and partial cooldown is critical and it is difficult to judge whether sufficient time exists to credit operator action for these breaks. It is necessary to perform confirmatory analysis in the detailed design phase (with credit for operator action to initiate partial cooldown) to demonstrate that core cooling is maintained. The confirmatory analysis should include an evaluation of the feasibility to credit manual RCP trip by the operator.
- DAS contains an alarm function to alert the operator of high radiation level in the control room. A confirmatory evaluation is required to determine whether this DAS function is adequate for the spectrum of conditions.

***Events requiring detailed analysis (quantitative analysis and human factors verification and validation):***

- Oversteam demands without the MSRT isolation function.
- Overpressure events without MSRT function.
- Complete loss of flow without equivalent RCP pump speed reactor trip.
- Single rod withdrawal and rod drop without low DNBR trip and possibly other withdrawal events to cover the spectrum with only flux trips.
- IOPSRV without partial cooldown function.
- Intermediate small break loss of coolant accidents (SBLOCA) without partial cooldown function and manual RCP trip.

- Radiological events without isolation functions.

***Functions that if added to DAS could avoid detailed analysis:***

- Equivalent trip on RCP pump speed for complete loss of flow.
- MSRT opening on SG pressure.
- SIS and partial cooldown on hot leg pressure.
- DNBR equivalent trip.
- MSRT isolation.

**Table A-1—U.S. EPR Initiating Events – Sheet 1 of 3**

| <b>Event</b>   | <b>Classification</b>             |                            |
|--|-----------------------------------|----------------------------|
|  | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
| <b>Increase in Heat Removal By Secondary System</b>                  |                                   |                            |
| Feedwater malfunction resulting in decrease in feedwater temperature | AOO                               | Condition II               |
| Feedwater malfunction resulting in increase in feedwater flow        | AOO                               | Condition II               |
| EFWS actuation   | AOO                               | Condition II               |
| Spurious actuation of partial cooldown system                        | AOO                               | Condition II               |
| Spurious open of MSB   | AOO                               | Condition II               |
| Inadvertent opening of SG relief or safety valve                     | AOO                               | Condition II               |
| Spurious opening of MSRT   | AOO                               | Condition II               |
| Spurious opening of MSSV   | AOO                               | Condition II               |
| Steam system piping failures   | Postulated Accident <sup>1</sup>  | Condition IV               |
| <b>Decrease in Heat Removal By Secondary System</b>                  |                                   |                            |
| Loss of load/turbine trip  | AOO                               | Condition II               |
| Loss of condenser vacuum   | AOO                               | Condition II               |
| Inadvertent closure of one MSIV                                      | AOO                               | Condition II               |
| Closure of all MSIVs   | AOO                               | Condition II               |
| Loss of offsite power  | AOO                               | Condition II               |
| Loss of normal feedwater   | AOO                               | Condition II               |
| Feedwater line break   | Postulated Accident               | Condition IV               |
| <b>Decrease in RCS Flow Rate</b>                                     |                                   |                            |
| Partial loss of flow   | AOO                               | Condition II               |
| Complete loss of flow  | AOO                               | Condition III              |
| RCP seizure and shaft break  | Postulated Accident               | Condition IV               |

**Table A-1—U.S. EPR Initiating Events - Sheet 2 of 3**

| Event  | Classification                    |                            |
|--|-----------------------------------|----------------------------|
| <b>Reactivity &amp; Power Distribution Anomalies</b>             | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
| RCCA withdrawal at power   | AOO                               | Condition II               |
| RCCA subgroup withdrawal   | AOO                               | Condition II               |
| RCCA withdrawal from low power or subcritical condition          | AOO                               | Condition II               |
| Single RCCA withdrawal   | AOO                               | Condition III              |
| RCCA misalignment/drop   | AOO                               | Condition II               |
| Heterogeneous boron dilution RCP startup                         | AOO                               | Condition II               |
| CVCS malfunction boron dilution                                  | AOO                               | Condition II               |
| Misloading and operation with fuel assembly in improper position | AOO                               | Condition III              |
| RCCA ejection  | Postulated Accident               | Condition IV               |
| <b>Increase in RCS Inventory</b>                                 | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
| Inadvertent operation of SIS                                     | AOO                               | Condition II               |
| CVCS malfunction   | AOO                               | Condition II               |
| Inadvertent operation of EBS                                     | AOO                               | Condition II               |
| <b>Decrease in RCS Inventory</b>                                 | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
| Inadvertent Opening of PSV                                       | AOO                               | Condition II               |
| CVCS malfunction   | AOO                               | Condition II               |
| SG tube rupture  | Postulated Accident <sup>1</sup>  | Condition IV               |
| LOCA   | Postulated Accident <sup>1</sup>  | Condition IV               |

**Table A-1—U.S. EPR Initiating Events – Sheet 3 of 3**

| <b>Primary Side Pressure Transients</b>                  | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
|--|-----------------------------------|----------------------------|
| Inadvertent operation of pressurizer sprays              | AOO                               | Condition II               |
| Inadvertent operation of pressurizer heaters             | AOO                               | Condition II               |
| <b>Radioactive Release from a subsystem or component</b> | <b>AOO or Postulated Accident</b> | <b>ANSI Classification</b> |
| Small line break outside containment                     | Postulated Accident               | Condition IV               |
| LOCA   | Postulated Accident               | Condition IV               |
| SGTR   | Postulated Accident               | Condition IV               |
| MSLB   | Postulated Accident               | Condition IV               |
| FWLB   | Postulated Accident               | Condition IV               |
| Locked rotor/broken shaft                                | Postulated Accident               | Condition IV               |
| Rod ejection   | Postulated Accident               | Condition IV               |
| Fuel handling accident                                   | Postulated Accident               | Condition IV               |

1. Minor leaks or breaks are considered AOOs.

**Table A-2a—Plant Systems Used in Accident Analysis**

| Incident   | Reactor Trip Functions <sup>1</sup>                                     | ESF Functions <sup>2</sup>   | Other Equipment |
|--|---|--|-----------------|
| <b>Increase in Heat Removal by Secondary System</b>                              |   |  |                 |
| Feedwater system malfunctions that result in a decrease in feedwater temperature | Low DNBR<br>High LPD<br>High Core Power                                 | MSRTs  |                 |
| Feedwater system malfunctions that result in an increase in feedwater flow       | High SG Level<br>Low DNBR<br>High LPD                                   | MSRTs<br>MFW/SSS Isolation   |                 |
| EFWS actuation   |   |  |                 |
| Spurious actuation of partial cooldown system                                    | Low DNBR<br>High LPD<br>High Core Power<br>Low SG pressure<br>Low SG ΔP | MSRTs<br>MFW/SSS Isolation<br>SIS and partial cooldown<br>MSRT Isolation<br>MSIV closure |                 |
| Spurious opening of MSB  | Low DNBR<br>High LPD<br>High Core Power<br>Low SG pressure<br>Low SG ΔP | MSRTs<br>MFW/SSS Isolation<br>SIS and partial cooldown<br>MSRT Isolation<br>MSIV closure |                 |
| Inadvertent opening of a steam generator relief or safety valve                  | Low DNBR<br>High LPD<br>High Core Power<br>Low SG pressure<br>Low SG ΔP | MSRTs<br>MFW/SSS Isolation<br>SIS and partial cooldown<br>MSRT Isolation<br>MSIV closure |                 |
| Steam system piping failure  | High Core Power<br>Low SG pressure<br>Low SG ΔP                         | MSRTs<br>MFW/SSS Isolation<br>SIS and partial cooldown<br>MSRT Isolation<br>MSIV closure |                 |

17. A reactor trip results in a turbine trip and high load MFW isolation.

18. MSRTs are used in each event for long-term decay heat removal once the plant has achieved a stable condition.

**Table A-2b—Plant Systems Used in Accident Analysis**

| Incident  | Reactor Trip <sup>1</sup><br>Functions  | ESF Functions <sup>2</sup>   | Other<br>Equipment |
|---|---|--|--------------------|
| <b>Decrease in Heat Removal by Secondary System</b> |   |  |                    |
| Loss of external electrical load                    | High SG pressure<br>High PZR pressure   | MSRTs  | PSRVs<br>MSSVs     |
| Turbine trip (stop valve failure)                   | High SG pressure<br>High PZR pressure   | MSRTs  | PSRVs              |
| Inadvertent closure of main steam isolation valves  | Low DNBR<br>High SG pressure<br>High PZR pressure                                     | MSRTs  | PSRVs              |
| Loss of condenser vacuum                            | High SG pressure<br>High PZR pressure   | MSRTs  | PSRVs              |
| Coincident loss of onsite and external (offsite) AC | Low RCP speed<br>Low RCS flow rate<br>High PZR pressure                               | EFWS on SG level   | PSRVs              |
| Loss of normal feedwater flow                       | Low DNBR<br>Low SG level  | EFWS on SG level   | PSRVs              |
| Feedwater pipe break                                | Low DNBR<br>Low SG pressure<br>Low SG ΔP<br>High Containment Pressure<br>Low SG Level | EFWS on SG level<br>MSIV Closure<br>SIS<br>MFW/SSS Isolation<br>EFW alignment<br>MSRTs | PSRVs              |

1. A reactor trip results in a turbine trip and high load MFW isolation.
2. MSRTs are used in each event for long-term heat removal once the plant has achieved a stable condition.

**Table A-2c—Plant Systems Used in Accident Analysis**

| <b>Incident</b>                                     | <b>Reactor Trip<sup>1</sup><br/>Functions</b>                               | <b>ESF Functions<sup>2</sup></b> | <b>Other Equipment</b> |
|---|---|----------------------------------|------------------------|
| <b>Decrease in Reactor Coolant System Flow Rate</b> |   |                                  |                        |
| Partial Loss of flow                                | RCS loop flow less than<br>25 %<br><br>RCS flow less than 85<br>% (2 loops) | MSRTs<br><br>EFWS                | PSRVs                  |
| Complete loss of forced<br>reactor coolant flow     | RCP speed is less than<br>91%   | MSRTs<br><br>EFWS                | PSRVs                  |
| Reactor coolant pump<br>shaft seizure               | RCS loop flow less than<br>25%.   | MSRTs<br><br>EFWS                | PSRVs                  |
| Reactor coolant pump<br>shaft break                 | RCS loop flow less than<br>25%.   | MSRTs<br><br>EFWS                | PSRVs                  |

1. A reactor trip results in a turbine trip and high load MFW isolation.
2. MSRTs are used in each event for long-term heat removal once the plant has achieved a stable condition.

**Table A-2d—Plant Systems Used in Accident Analysis**

| Incident  | Reactor Trip Functions   | ESF Functions | Other Equipment |
|---|--|---------------|-----------------|
| <b>Reactivity and Power Distribution Anomalies</b>  |  |               |                 |
| RCCA bank withdrawal from a subcritical or low-power startup condition                        | High Flux Rate (PR)  |               |                 |
| RCCA bank withdrawal at power   | Low DNBR<br>High LPD<br>High Core Power<br>High Flux Rate (PR) |               |                 |
| RCCA subgroup withdrawal  | Low DNBR<br>High LPD<br>High Core Power<br>High Flux Rate (PR) |               |                 |
| Single RCCA withdrawal  | Low DNBR   |               |                 |
| RCCA misalignment/drop  | Low DNBR   |               |                 |
| Startup of an inactive reactor coolant pump at an incorrect temperature                       | NA   |               |                 |
| CVCS malfunction that results in a decrease in the boron concentration in the reactor coolant | Low DNBR<br>High Core power                                    |               | Anti-Dilution   |
| Inadvertent loading and operation of a fuel assembly in an improper position                  | NA   |               |                 |
| Spectrum of RCCA ejection accidents   | High Flux Rate (PR)<br>High Flux (IR)                          |               |                 |

**Table A-2e—Plant Systems Used in Accident Analysis**

| Incident   | Reactor Trip Functions                               | ESF Functions   | Other Equipment               |
|--|--|---|-------------------------------|
| <b>Increase in RCS Inventory</b>   |  |   |                               |
| Inadvertent operation of the SIS during power operation  | NA   | NA  | PSRVs in shutdown mode (LTOP) |
| CVCS malfunction that increases reactor coolant inventory  | High PZR level                                       | CVCS Isolation  |                               |
| Inadvertent operation of EBS   | High PZR level                                       |   |                               |
| <b>Decrease in RCS Inventory</b>   |  |   |                               |
| Inadvertent opening of a pressurizer safety or relief valve  | Low PZR pressure                                     | SIS/partial cooldown<br>Containment Isolation   | RCP trip                      |
| CVCS malfunction that results in a decrease in RCS inventory   | Low PZR pressure<br>Low DNBR<br>Low hot leg pressure |   |                               |
| Steam generator tube failure   | Low DNBR<br>Low PZR pressure                         | SIS/partial cooldown<br>SG level/partial cooldown<br>MSRTs<br>EFWS Isolation<br>MSRT setpoint increase<br>MSIV closure<br>MFW/SSS isolation<br>CVCS isolation | EBS                           |
| Loss-of-coolant accidents resulting from a spectrum of postulated piping breaks within the reactor coolant pressure boundary | Low PZR pressure<br>High Containment pressure        | SIS/partial cooldown<br>Containment Isolation<br>MSRTs  | RCP trip                      |

**Table A-2f—Plant Systems Used in Accident Analysis**

| Incident                                     | Reactor Trip Functions                           | ESF Functions | Other Equipment |
|--|--|---------------|-----------------|
| <b>Primary side pressure transients</b>      |  |               |                 |
| Inadvertent operation of pressurizer sprays  | Low PZR pressure<br>Low DNBR<br>Hot Leg pressure |               |                 |
| Inadvertent operation of pressurizer heaters | High PZR pressure                                |               |                 |

**Table A-2g—Plant Systems Used in Accident Analysis**

| Incident   | Reactor Trip Functions | ESF Functions | Other Equipment                                  |
|--|------------------------|---------------|--|
| <b>Radioactive release from a subsystem or component</b> |                        |               |  |
| Small line break outside containment                     |                        |               | MCR HVAC   |
| LOCAs  |                        |               | MCR HVAC<br>Annulus HVAC<br>Safeguard build HVAC |
| SGTR   |                        |               | MCR HVAC   |
| FWLBs  |                        |               | MCR HVAC   |
| Locked Rotor/Broken Shaft                                |                        |               | MCR HVAC   |
| Rod Ejection   |                        |               | MCR HVAC<br>Annulus HVAC<br>Safeguard build HVAC |
| Fuel handling Accident                                   |                        |               | MCR HVAC   |

1. MCR HVAC isolates on either containment isolation or high radiation monitor.
2. Annulus HVAC isolation on containment isolation.
3. Safeguard Building HVAC isolation on high radiation monitor.

**Table A-3—D3 Qualitative Results**

**6 Sheets**

| <b>Event</b>   | <b>Classification</b>             |  |                                   |                          |
|--|-----------------------------------|--|-----------------------------------|--------------------------|
| <b>Increase in Heat Removal By Secondary System</b>                  | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>         | <b>DAS Reactor Trip Functions</b> | <b>DAS ESF Functions</b> |
| Feedwater malfunction resulting in decrease in feedwater temperature | AOO                               | Analysis needed to confirm Low DNBR not required | High neutron flux                 |                          |
| Feedwater malfunction resulting in increase in feedwater flow        | AOO                               | Analysis needed to confirm Low DNBR not required | High neutron flux                 |                          |
| EFWS actuation   | AOO                               | Bounded by increase in feedwater flow.<br>MSRTs  | High neutron flux                 |                          |
| Spurious actuation of partial cooldown system                        | AOO                               | MSRTs isolation may be required in DAS           | Low SG pressure                   | MSIV Closure             |
| Spurious open of MSB   | AOO                               | MSRTs isolation may be required in DAS           | Low SG pressure                   | MSIV Closure             |
| Inadvertent opening of SG relief or safety valve                     | AOO                               | MSRTs isolation may be required in DAS           | Low SG pressure                   | MSIV Closure             |

| <b>Event</b>  | <b>Classification</b>             |  |                                       |                          |
|---|-----------------------------------|--|---------------------------------------|--------------------------|
| Spurious opening of MSRT                            | AOO                               | MSRTs isolation may be required in DAS   | Low SG pressure                       | MSIV Closure             |
| Spurious opening of MSSV                            | AOO                               | MSRTs isolation may be required in DAS   | Low SG pressure                       | MSIV Closure             |
| Steam system piping failures                        | Postulated Accident <sup>1</sup>  | MSRTs isolation may be required in DAS   | Low SG pressure                       | MSIV Closure             |
| <b>Decrease in Heat Removal By Secondary System</b> | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b> | <b>DAS Reactor Trip Functions</b>     | <b>DAS ESF Functions</b> |
| Loss of load/turbine trip                           | AOO                               | MSRTs may be required in DAS             | High SG pressure<br>High PZR pressure |                          |
| Loss of condenser vacuum                            | AOO                               | MSRTs may be required in DAS             | High SG pressure<br>High PZR pressure |                          |
| Inadvertent closure of one MSIV                     | AOO                               | MSRTs may be required in DAS             | High SG pressure<br>High PZR pressure |                          |
| Closure of all MSIVs                                | AOO                               | MSRTs may be required in DAS             | High SG pressure<br>High PZR pressure |                          |
| Loss of offsite power                               | AOO                               | See complete loss of flow                | Low RCS flow<br>High PZR pressure     | EFWS on SG level         |
| Loss of normal feedwater                            | AOO                               | MSRTs may be required in DAS             | Low SG Level                          | EFWS on SG level         |
| Feedwater line break                                | Postulated                        | MSRTs may be                             | Low SG Level                          | EFWS on SG level         |

| <b>Event</b>  | <b>Classification</b>             |   |  |                          |
|---|-----------------------------------|---|--|--------------------------|
|   | Accident                          | required in DAS                                   |  | MSIV closure             |
| Decrease in RCS Flow Rate                               | AOO or Postulated Accident        | Results of Qualitative Evaluation                 | DAS Reactor Trip Functions             | DAS ESF Functions        |
| Partial loss of flow                                    | AOO                               | DAS functions should be adequate                  | Low RCS flow                           |                          |
| Complete loss of flow                                   | AOO                               | Analysis needed or RCP speed trip                 | Low RCS flow                           |                          |
| RCP seizure and shaft break                             | Postulated Accident               | DAS functions should be adequate                  | Low RCS flow                           |                          |
| <b>Reactivity &amp; Power Distribution Anomalies</b>    | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>          | <b>DAS Reactor Trip Functions</b>      | <b>DAS ESF Functions</b> |
| RCCA withdrawal at power                                | AOO                               | Full spectrum may not be covered by DAS functions | High neutron flux<br>High PZR pressure |                          |
| RCCA subgroup withdrawal                                | AOO                               | Analysis confirmation required                    | High neutron flux                      |                          |
| RCCA withdrawal from low power or subcritical condition | AOO                               | DAS functions should be adequate                  | High neutron flux                      |                          |
| Single RCCA withdrawal                                  | AOO                               | Analysis confirmation required                    | High neutron flux                      |                          |
| RCCA misalignment/drop                                  | AOO                               | Analysis confirmation                             | Alarm on rod bottom indication         |                          |

| <b>Event</b>   | <b>Classification</b>             |   |                                   |                          |
|--|-----------------------------------|---|-----------------------------------|--------------------------|
|  |                                   | required for no trip                                      |                                   |                          |
| Heterogeneous boron dilution RCP startup                         | AOO                               | NA  | NA                                |                          |
| CVCS malfunction boron dilution                                  | AOO                               | Manual action may be required for loss of shutdown margin | High neutron flux                 |                          |
| Misloading and operation with fuel assembly in improper position | AOO                               | NA  | NA                                |                          |
| RCCA ejection  | Postulated Accident               | DAS functions should be adequate                          | High neutron flux                 |                          |
| <b>Increase in RCS Inventory</b>                                 | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>                  | <b>DAS Reactor Trip Functions</b> | <b>DAS ESF Functions</b> |
| Inadvertent operation of SIS                                     | AOO                               | NA  |                                   |                          |
| CVCS malfunction   | AOO                               | Manual action may be required for loss of shutdown margin | High PZR pressure                 |                          |
| Inadvertent operation of EBS                                     | AOO                               | Bounded by CVCS malfunction                               | High PZR pressure                 |                          |
| <b>Decrease in RCS Inventory</b>                                 | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>                  | <b>DAS Reactor Trip Functions</b> | <b>DAS ESF Functions</b> |
| Inadvertent Opening of PSV                                       | AOO                               | Partial cooldown may be required in DAS                   | Low hot leg pressure              | SIS                      |
| CVCS malfunction   | AOO                               | Partial cooldown may be required in                       | Low hot leg pressure              |                          |

| <b>Event</b>   | <b>Classification</b>             |  |                                   |                          |
|--|-----------------------------------|--|-----------------------------------|--------------------------|
|  |                                   | DAS  |                                   |                          |
| SG tube rupture  | Postulated Accident <sup>1</sup>  | DAS functions should be adequate                         | Low hot leg pressure              |                          |
| LOCA   | Postulated Accident <sup>1</sup>  | Partial cooldown may be required for intermediate breaks | Low hot leg pressure              | SIS                      |
| <b>Primary Side Pressure Transients</b>                  | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>                 | <b>DAS Reactor Trip Functions</b> | <b>DAS ESF Functions</b> |
| Inadvertent operation of pressurizer sprays              | AOO                               | DAS functions should be adequate                         | Low hot leg pressure              |                          |
| Inadvertent operation of pressurizer heaters             | AOO                               | DAS functions should be adequate                         | High PZR pressure                 |                          |
| <b>Radioactive Release from a subsystem or component</b> | <b>AOO or Postulated Accident</b> | <b>Results of Qualitative Evaluation</b>                 | <b>DAS Reactor Trip Functions</b> | <b>DAS ESF Functions</b> |
| Small line break outside containment                     | Postulated Accident               | Isolation functions may be required                      | MCR HVAC alarm                    |                          |
| LOCA   | Postulated Accident               | Isolation functions may be required                      | MCR HVAC alarm                    |                          |
| SGTR   | Postulated Accident               | Isolation functions may be required                      | MCR HVAC alarm                    |                          |
| MSLB   | Postulated Accident               | Isolation functions may be required                      | MCR HVAC alarm                    |                          |
| FWLB   | Postulated                        | Isolation functions                                      | MCR HVAC alarm                    |                          |

| Event                     | Classification      |                                     |                |  |
|---------------------------|---------------------|-------------------------------------|----------------|--|
|                           | Accident            | may be required                     |                |  |
| Locked rotor/broken shaft | Postulated Accident | Isolation functions may be required | MCR HVAC alarm |  |
| Rod ejection              | Postulated Accident | Isolation functions may be required | MCR HVAC alarm |  |
| Fuel handling accident    | Postulated Accident | Isolation functions may be required | MCR HVAC alarm |  |

Note:

1. Minor leaks or breaks are considered AOOs.