ANP-10284
Revision 0

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

June 2007

AREVA NP Inc.

Non-Proprietary

For information address: AREVA NP Inc.
An AREVA and Siemens Company
3315 Old Forest Road
Lynchburg, VA 24506

U.S. Nuclear Regulatory Commission

Disclaimer

Important Notice Concerning the Contents and Application of This Report
Please Read Carefully

This report was developed based on research and development funded and conducted by AREVA NP Inc., and is being submitted by AREVA NP to the U.S. Nuclear Regulatory Commission (NRC) to facilitate future licensing processes that may be pursued by licensees or applicants that are customers of AREVA NP. The information contained in this report may be used by the NRC and, under the terms of applicable agreements with AREVA NP, those customers seeking licenses or license amendments to assist in demonstrating compliance with NRC regulations. The information provided in this report is true and correct to the best of AREVA NP's knowledge, information, and belief.

AREVA NP's warranties and representations concerning the content of this report are set forth in agreements between AREVA NP and individual customers. Except as otherwise expressly provided in such agreements with its customers, neither AREVA NP nor any person acting on behalf of AREVA NP:

- Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, nor the use of any information, apparatus, method, or process disclosed in this report.
- Assumes any liability with respect to the use of or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

ABSTRACT

Generally, in previous designs of safety instrumentation and control (I&C) systems for nuclear power plants, common-cause failures (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 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.

Nature of Changes

Item	Section(s) or Page(s)	Description and Justification

Contents

List of Tables

List of Figures

Nomenclature

Acronym	Definition
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
DAS	Diverse Actuation System
DBE	Design Basis Event
DCD	Design Control Document
D3	Diversity and Defense-in-Depth
ESF	Engineered Safety Feature
HMI	Human-Machine Interface
I&C	Instrumentation and Control
MCR	Main Control Room
NI	Nuclear Island
OS	Operating System
PACS	Priority 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
QDS	Qualified Display System
RCSL	Reactor Control, Surveillance and Limitation
RSS	Remote Shutdown Station
RT	Reactor Trip
SA	Severe Accident

Acronym	Definition
SA I&C	Severe Accident Instrumentation and Control
SAS	Safety Automation System
SBO	Station Blackout
SICS	Safety Information and Control System
SIVAT	(Software) Simulation and Validation Tool
SRM	Staff Requirements Memorandum
TG I&C	Turbine Generator Instrumentation and Control
TI	Turbine Island
TSC	Technical Support Center
TXS	TELEPERM XS
UV	Undervoltage
V&V	Verification and Validation
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 (BDBEs). 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.

AREVA NP requests the approval of the following items in this report:

- The U.S. EPR defense-in-depth concept.
- The adequacy of the proposed design features to mitigate the consequences of a postulated CCF in the safety I&C systems.
- The methodology used to evaluate the adequacy of the I&C design with respect to D3.

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.

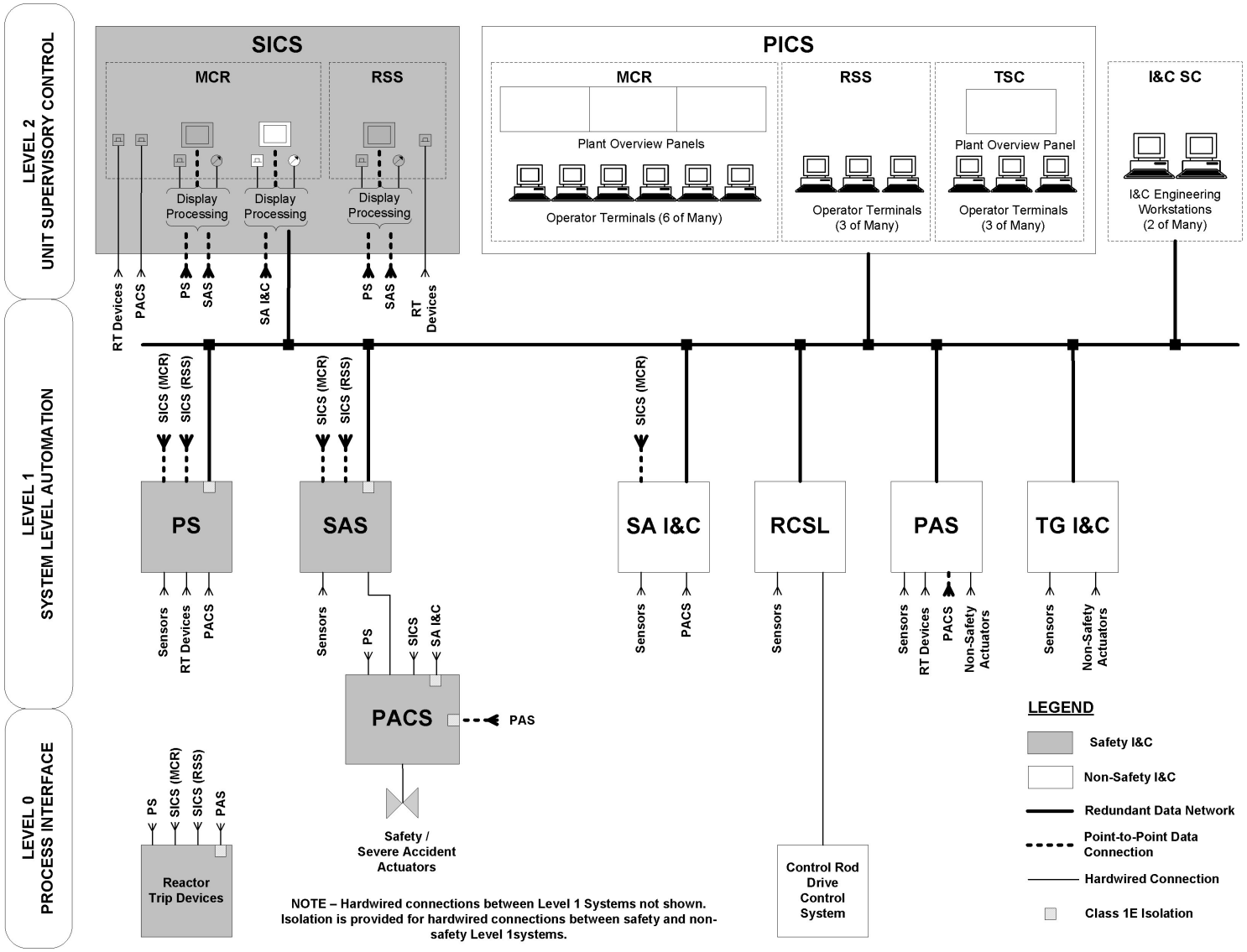
2.0 U.S. EPR I&C ARCHITECTURE

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

System	Platform
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 critical safety functions at the system level (e.g., reactor trip, safety injection), conventional means (i.e., buttons, switches) are provided on the SICS. These signals bypass the TXS computers and are hardwired directly to actuation devices (e.g., reactor trip devices or priority actuation and control (PAC) modules).

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 reactor trip (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 Generator 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 Safeguards 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.

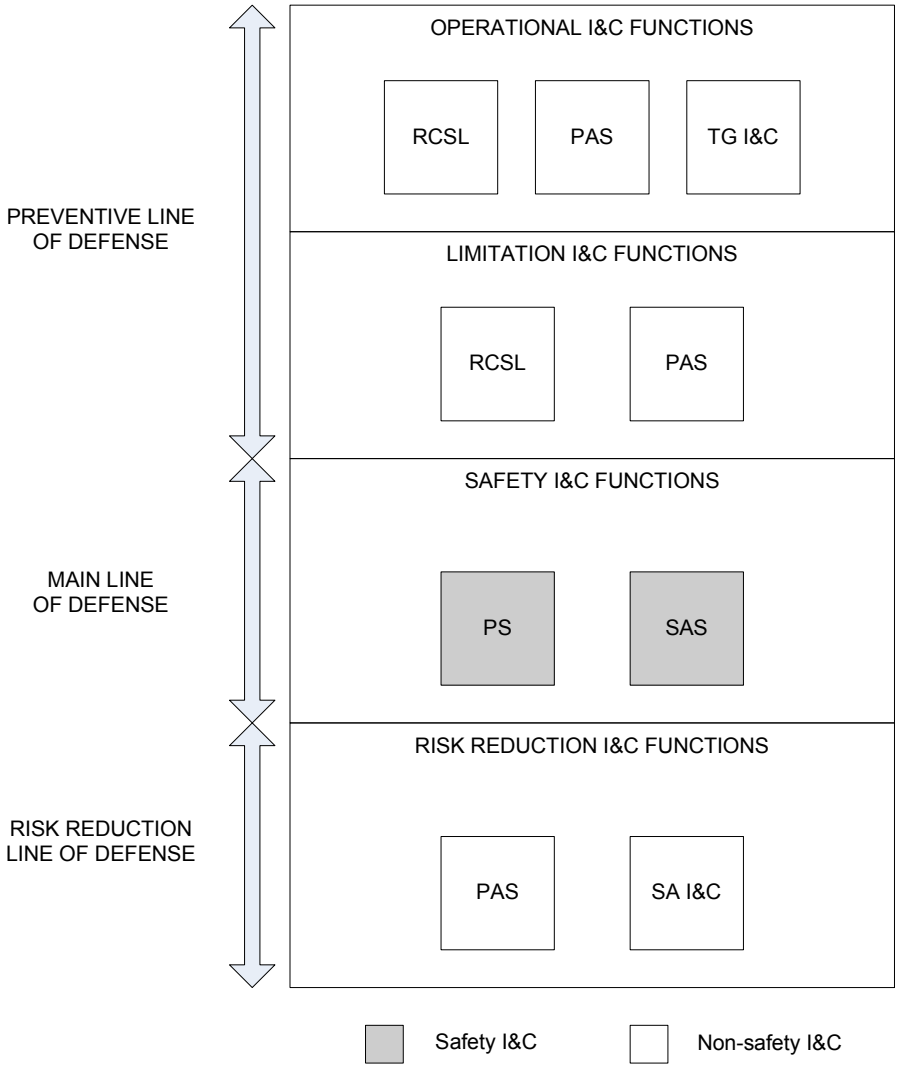
2.4 *U.S. EPR I&C Defense-In-Depth Concept*

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 is used to prioritize actuation requests from the various I&C systems. The PICS is used as long as it is available, and the SICS implements a backup Class 1E 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 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 features:

- 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, and 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 approved the TXS platform in 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) and highlighted below. 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 CCFs are not credible 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

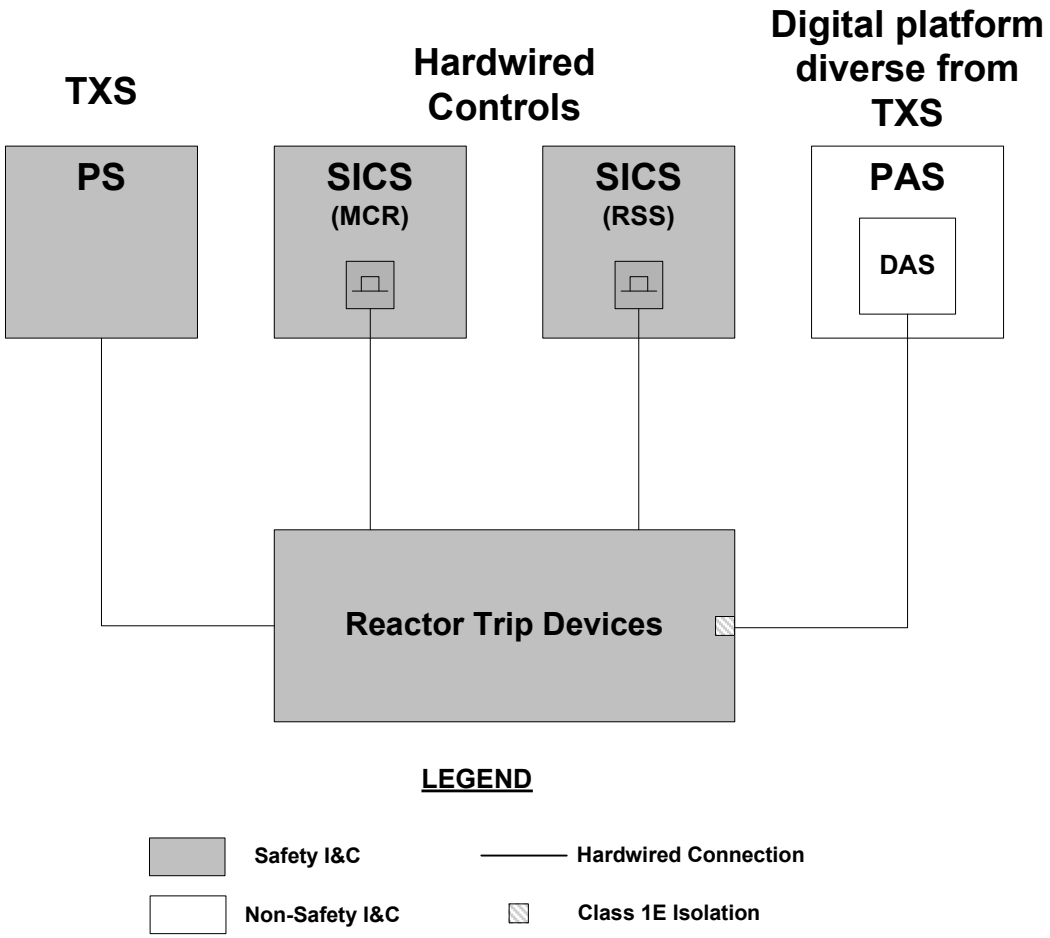
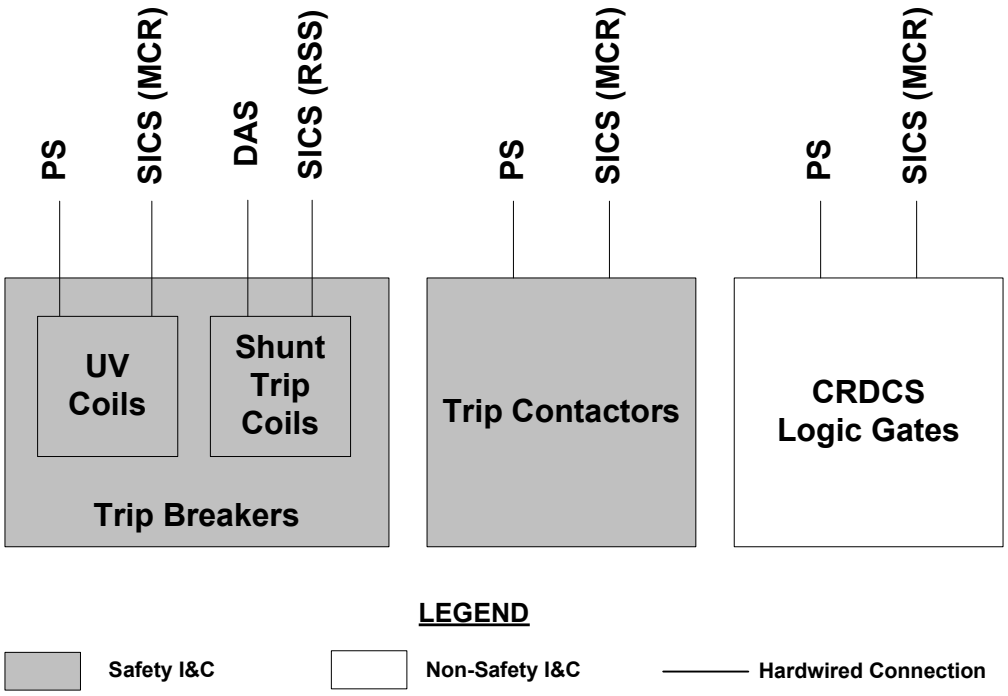


Figure 3-2—Diversity for Executing Reactor Trip

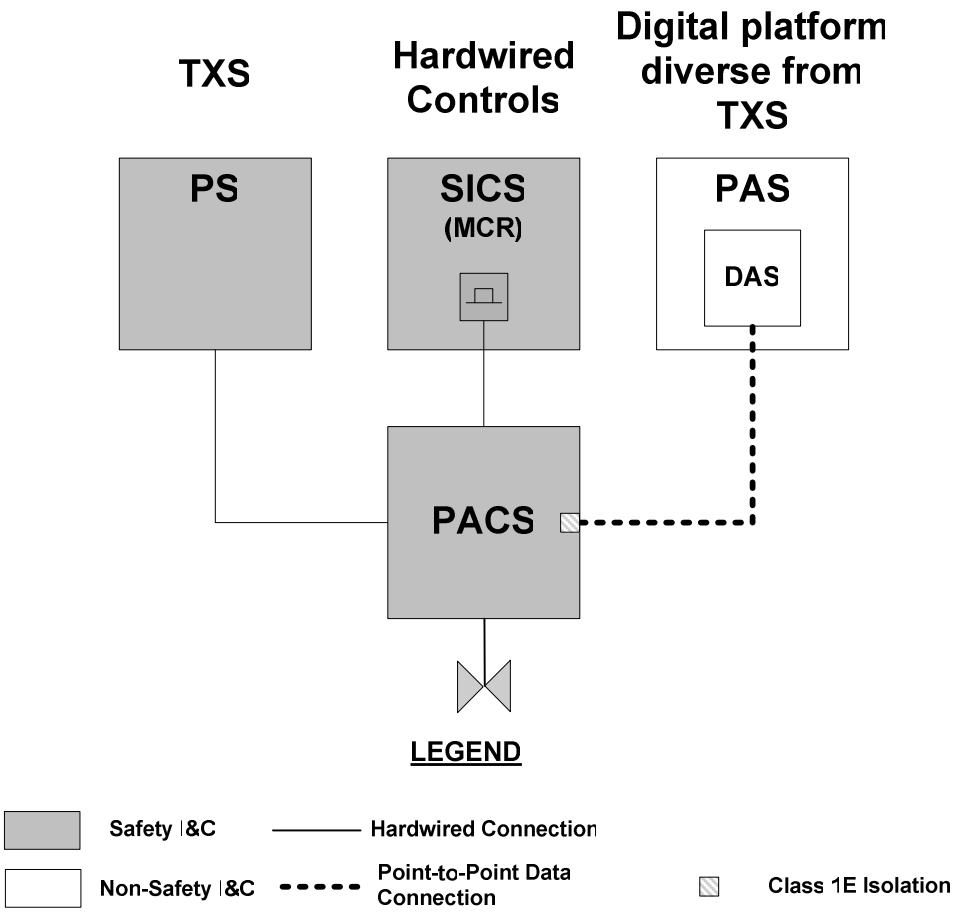


3.2.1.2 *ESF Actuation*

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 is provided on the SICS in the MCR. These means are provided to address Point 4 of NUREG-0800, BTP 7-19. These are hardwired controls that are assigned to the independent safety divisions. The controls are diverse because a software failure of the safety systems will not affect the operation of the hardwired controls. This diversity is shown in Figure 3-3.

In addition, diverse actuation of ESF systems at the component level is provided from PICS via PAS.

Figure 3-3—Diversity for Actuation of ESF Systems

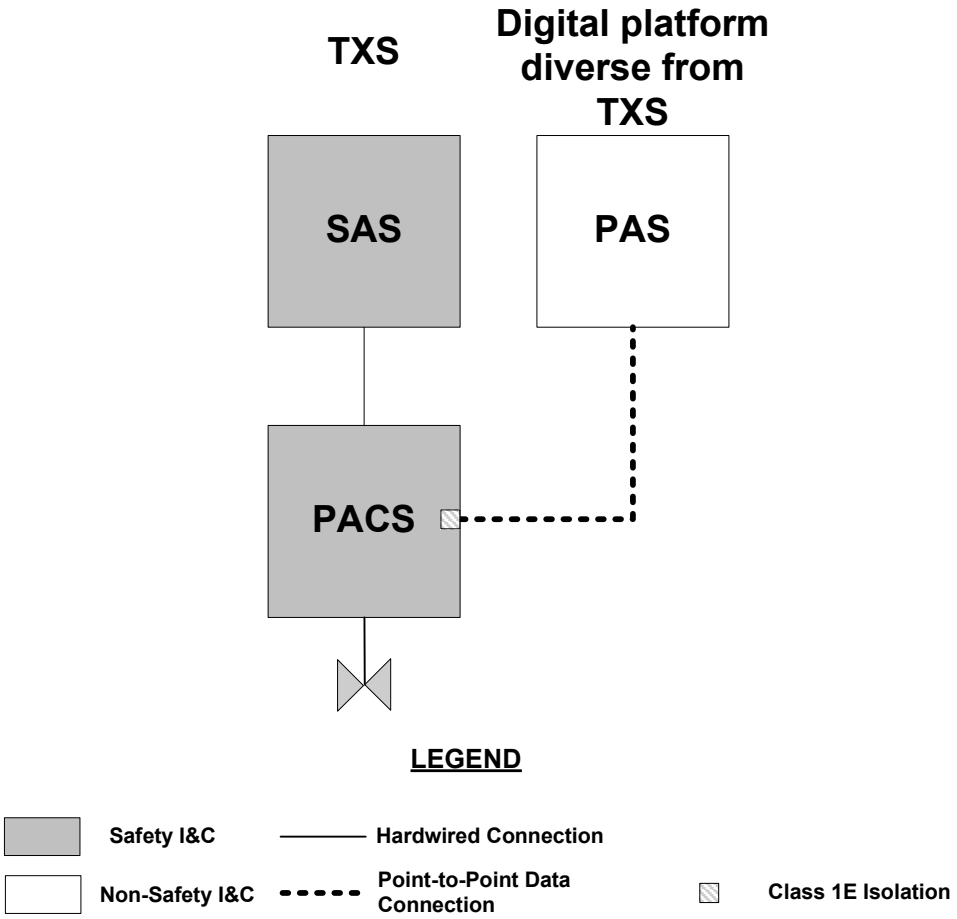


3.2.1.3 *ESF Control*

The SAS is the primary means of performing ESF control functions. Assuming a postulated CCF renders the SAS inoperable, the PAS is available as a diverse means of executing ESF control functions. The controls provided in PAS address the guidance of Section 7.3 of NUREG-0800 on diversity of ESF controls. This diversity is shown in Figure 3-4.

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

Figure 3-4—Diversity for Control of ESF Systems

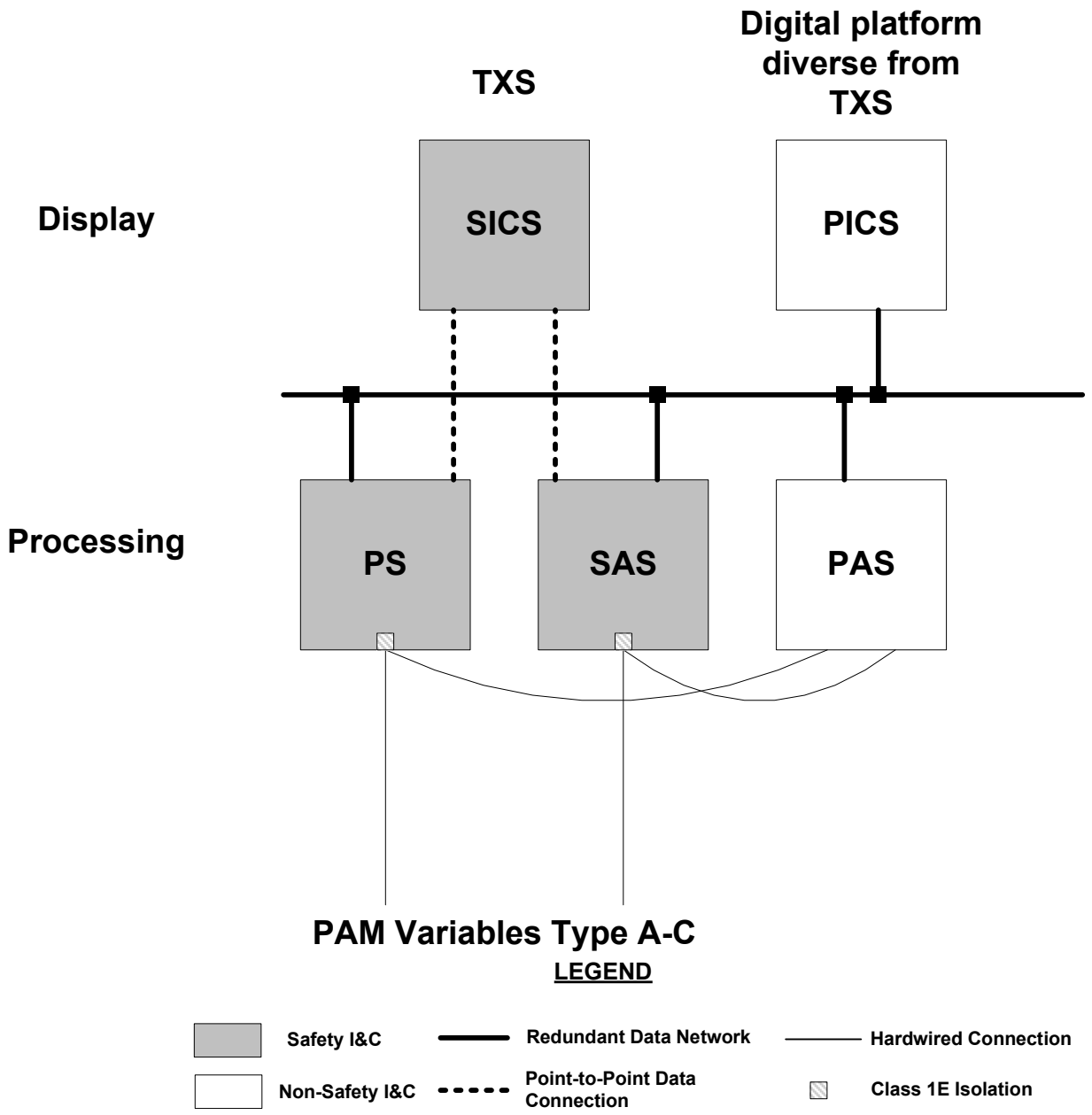


3.2.1.4 *Indications and Alarms*

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 3-5. 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.

Figure 3-5—Diversity of Indications and Alarms



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.

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.

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, and will be performed using NUREG/CR-6303 as a model. The following assumptions are to 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 Chapter 15 of the U.S. EPR Design Control Document (DCD) 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, then 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.

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

The inventory of hardwired controls on SICS is developed using the following requirements:

- System-level manual actuation for critical safety functions, which include: reactor shutdown, core inventory control, decay heat removal, containment isolation and containment integrity.
- System level manual actuation of those safety functions that were credited for manual operator action in Step 2.

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. This will fulfill the requirement of performing manual functions that don't require system level manual actuation.

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.

AREVA NP requests the approval of the following items in this report:

- The U.S. EPR defense-in-depth concept.
- The adequacy of the proposed design features to mitigate the consequences of a postulated CCF in the safety I&C systems.
- The methodology used to evaluate the adequacy of the I&C design with respect to D3.

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.