Diversity and Defense-in-Depth

Revision 1

Non-Proprietary

February 2017

REVISION HISTORY

Revision	Date	Page	Description
0	November 2014	All	First Issue
1	February 2017	Pages (Sections)	Revised based on RAI response or editorial correction. (RAI No.)
		viii - xi (Acronyms)	Additional explanation about acronyms
		4 (3.3.1)	CCF in the protection systems → CCF within digital safety I&C systems (RAI 33-7880, Question 07.08-2)
		4, 33 (3.3.1, 8.7)	Correction of Reference (RAI 43-7887, Question 07.01-16)
		5, 32 (3.3.3, 7.2)	Change of reference applied for the HFE evaluation (RAI 315-8091, Question 18-57)
		6 - 8 (3.4.3, 3.4.6, 4.1)	Editorial changes
		10 (Fig. 4-1)	Additional explanation about the RCC interfaces (RAI 356-7881, Question 07-5 Rev.2)
		11 (Fig. 4-2)	Additional description of Note 2 about the PPS interfaces with the TCS (RAI 274-8277, Question 07.01-35)
		18, 21, 22 (Fig. 5-1, 5-3, 5-4)	Editorial changes (removal of inconsistency, figure locations and numbers)
		14 (4.2.3)	Additional explanation about the DPS functions during a postulated software CCF (RAI 342-8291, Question 07.08-7)
		16 (5.1)	Additional explanation about the characteristics of DPS trip functions (RAI 342-8291, Question 07.08-10)
		17 (5.1)	Detailed explanation about the safety class sensors and APC-S (RAI 342-8291, Question 07.08-11)
		17 (5.1)	Additional explanation about the DPS power supply (RAI 342-8291, Question 07.08-13)

Revision	Date	Page	Description
		19, C16 (5.2, App. C)	DIS is diverse from the QIAS-P and QIAS-N. → DIS is diverse from the QIAS-P (RAI 71-7906, Question 14.03.05-7)
		19 (5.2)	Additional explanation about the DIS power supply (RAI 342-8291, Question 07.08-13)
		19 (5.3)	Additional explanation about the characteristics of DMA switches (RAI 342-8291, Question 07.08-10)
		19 - 20 (5.2, Fig. 5-2)	Additional explanation about signal interfaces between DIS and QIAS-P in Fig. 5-2 (RAI 342-8291, Question 07.08-12)
		23 (5.3)	Additional explanation about power supply to the CIM that interfaces with DMA switches (RAI 342-8291, Question 07.08-13)
		23 - 24 (5.3, Fig. 5-5)	Additional explanation about DMA switch and DMA enable switch (RAI 342-8291, Question 07.08-14)
		23 - 24 (5.3)	Additional explanation about diverse M/A stations (RAI 356-7881, Question 07-11)
		26, 33, A4, C1, C10, C11, C13, C16	Editorial changes
		28 (6.2.3)	Editorial changes (RAI 356-7881, Question 07-11)
		31 (7.1.j)	Editorial changes (RAI 315-8091, Question 18-57)
		33 (8.10 - 8.12)	Editorial correction, and deletion of references (RAI 315-8091, Question 18-57)
		33 - 34 (8.19 - 8.20)	Additional description of references: IEEE Std 7-4.3.2-2003 and IEEE 100 (RAI 342-8291, Question 07.08-11)
		35 (9.0)	Additional description of definitions (RAI 342-8291, Question 07.08-11)
		A6 - A7 (App. A)	Detailed explanation about the spurious actuation results of DPS-SIAS (RAI 342-8291, Question 07.08-14)
		A7 (App. A)	Editorial changes (RAI 342-8291, Question 07.08-6)
		B1 (App. B)	Editorial changes (RAI 43-7887, Question 07.01-13)

Revision	Date	Page	Description
		C4 - C6 (App. C)	Correction of the variables displayed on the QIAS-P (RAI 38-7878, Question 07.05-01, Rev.1)

ABSTRACT

This report provides the design description of the diverse actuation system (DAS) and the diversity and defense-in-depth (D3) analysis method which are intended to be used for NRC Design Certification of the APR1400.

The DAS consists of the diverse protection system (DPS) for automatically initiating functions, Diverse Indication System (DIS) for continuously indicating critical variables, and diverse manual ESF actuation (DMA) switches for manually initiating functions to provide the defense against software common-cause failure (or simply CCF hereafter) in the safety I&C systems.

This report describes the D3 design methods and features, and the diversity evaluation results between diverse systems.

This report also describes the CCF coping evaluation methods for D3 assessment, including the event evaluation methods and manual operator action time evaluation methods, necessary to mitigate the short term effects and to accomplish subsequent recovery actions following each design basis event (DBE) concurrent with a postulated CCF in the safety I&C systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

AAC	alternate alternating current
AC	alternating current
ADV	atmospheric dump valve
AFAS	auxiliary feedwater actuation signal
AFWS	auxiliary feedwater system
AMI	accident monitoring instrumentation
AOO	anticipated operational occurrence
APC-S	auxiliary process cabinet – safety
APR1400	Advanced Power Reactor 1400
ATWS	anticipated transients without scram
BOP	balance of plant
BP	bistable processor
CCF	common-cause failure
CEA	control element assembly
CEDM	control element drive mechanism
CET	core exit thermocouple
CFR	code of federal regulations
CH.	channel
CIAS	containment isolation actuation signal
CIM	component interface module
CPCS	core protection calculator system
CPM	control panel multiplexer
CSAS	containment spray actuation signal
CVCS	chemical and volume control system
D3	diversity and defense-in-depth
DAS	diverse actuation system
DBE	design basis event
DC	direct current
DCD	design control document
DCN-I	data communication network - information
DCS	distributed control system
D/G	diesel generator
DIS	diverse indication system
DMA	diverse manual ESF actuation

DPS	diverse protection system
DRCS	digital rod control system
DVI	direct vessel injection
EDG	emergency diesel generator
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOP	emergency operating procedure
ESCM	ESF-CCS soft control module
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety features – component control system
FIDAS	fixed in-core detector amplifier system
FLC	FPGA-based logic controller
FPD	flat panel display
FPGA	field programmable gate array
FWCS	feedwater control system
GDC	general design criteria
GL	generic letter
GTG	gas turbine generator
HDL	hardware description language
HFE	human factors engineering
HJTC	heated junction thermocouple
HSI	human-system interface
I&C	instrumentation and control
ICC	inadequate core cooling
IEEE	Institute of Electrical and Electronics Engineers
IFPD	information flat panel display
IPS	information processing system
IRWST	in-containment refueling water storage tank
ITP	interface and test processor
ITS	important-to-safety
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
LC	loop controller
LCL	local coincidence logic
LDP	large display panel

LOCA	loss of coolant accident
LOOP	loss of offsite power
M/A	manual/auto
MCR	main control room
MG Set	motor generator set
MI	minimum inventory
MS	main steam
MSIS	main steam isolation signal
MTP	maintenance and test panel
N/A	not applicable
NAPS	nuclear application programs
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NR	narrow range
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OM	operator module
PA	postulated accident
P-CCS	process - component control system
PCS	power control system
PLC	programmable logic controller
PLCS	pressurizer level control system
POSRV	pilot operated safety relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
QIAS-N	qualified indication and alarm system – non-safety
QIAS-P	qualified indication and alarm system – p
RCP	reactor coolant pump
RCS	reactor coolant system
RFI	radio frequency interference
RG	regulatory guide
RPCS	reactor power cutback system
RPS	reactor protection system
RRS	reactor regulating system
RSR	remote shutdown room
RT	reactor trip

RTS	reactor trip system
RTSS	reactor trip switchgear system
SAR	safety analysis report
SBCS	steam bypass control system
SDL	serial data link
SDN	safety system data network
SDVS	safety depressurization and vent system
SG	steam generator
SIP	safety injection pump
SIS	safety injection system
SIAS	safety injection actuation signal
SIT	safety injection tank
SODP	shutdown overview display panel
SPTA	standard post trip actions
SRM	staff requirements memorandum
SSE	safe shutdown earthquake
SW	switch
Tavg	average temperature
TBN	turbine
TCS	turbine control system
TeR	technical report
Tref	reference temperature
TS	trade secret
Txs	transmitters
V&V	verification and validation
WR	wide range

Page intentionally blank

1 PURPOSE

This Technical Report (TeR) provides the design description of the diverse actuation system (DAS) and the diversity and defense-in-depth (D3) approach for I&C systems which are intended to be used for the application of the Advanced Power Reactor 1400 Design Certification (APR1400 DC).

2 SCOPE

This TeR describes the design features and system descriptions of the DAS, and the D3 analysis methods used for the APR1400 instrumentation and control (I&C) systems.

This report includes the DAS conformance to regulations and standards, I&C system overview, DAS design description, and D3 analysis method.

The DAS consists of the diverse protection system (DPS), diverse indication system (DIS) and diverse manual ESF actuation (DMA) switches to provide defense against postulated common-cause failures (CCFs) in the safety I&C systems.

The ESF signals from the DPS and DMA switches are connected to the component interface module (CIM) to cope with a CCF of the safety I&C systems. The CIM interfaces with the DPS and DMA switches are described in the Component Interface Module Technical Report (Reference 1).

This report also describes the CCF coping evaluation methods for the D3 assessment. The CCF coping analysis evaluation methods include the event evaluation methods and the manual operator action time evaluation method necessary to mitigate the short term effects and to accomplish subsequent recovery actions following each design basis event (DBE) concurrent with a postulated CCF in the safety systems.

The CCF coping analysis results are described in the CCF Coping Analysis Technical Report (Reference 2). The analysis is performed using a qualitative evaluation for all DBEs and a quantitative analysis for the specific DBEs identified as a result of qualitative evaluation.

The design features and system descriptions of the safety I&C systems, particularly the plant protection system (PPS) and engineered safety features – component control system (ESF-CCS), are addressed in the Safety I&C System Technical Report (Reference 3).

3 APPLICABLE CODES AND REGULATIONS

This section describes the compliance of the DAS with the applicable codes and regulations.

3.1 10 CFR Parts 50, 52, and 100

a. 10 CFR 50.55a(h), “ Protection and Safety Systems”

The DAS is a non-safety system and conforms to IEEE Std 603-1991 (Reference 4) separation requirements between safety and non-safety systems. The isolators are considered a part of the safety system and are qualified to the same degree as the safety system.

b. 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants” (Reference 5)

The DPS and its related equipment are provided to mitigate the effects of an anticipated operational occurrence (AOO) followed by the failure of the reactor trip portion of the protection system. The conformance to 10 CFR 50.62 is described in Appendix B.

c. 10 CFR 52.47(a)(2)(iv), “Release of Radioactive Material”

The CCF coping analysis is performed to analyze the postulated fission product release in case of DBE with a postulated CCF of protection system. The detailed analysis is provided in the CCF Coping Analysis Technical Report (Reference 2).

d. 10 CFR Part 100, “Reactor Site Criteria”

The CCF coping analysis is performed, and the results are within the limits of 10 CFR 100 acceptance criteria of fission product releases. The detailed analysis is provided in the CCF Coping Analysis Technical Report (Reference 2).

3.2 10 CFR Part 50 Appendix A, General Design Criteria

a. GDC 1, “Quality Standards and Records”

The DAS is designed to comply with the quality assurance guidance of Generic Letter (GL) 85-06 (Reference 6).

b. GDC 13, “Instrumentation and Control”

The DPS is designed to mitigate the effects of ATWS characterized by an AOO concurrent with a failure of the reactor trip portion of the protection system.

The DPS is designed to mitigate the effects of a postulated CCF of the PPS/ESF-CCS digital computer logic, concurrent with a DBE.

The DIS is designed to comply with the NRC Staff Requirements Memorandum (SRM) on SECY-93-087 (Reference 7), item II.Q, and is designed to monitor critical plant variables following a postulated CCF in the digital safety I&C systems. The critical plant variables monitored by the DIS are based on the results of the CCF Coping Analysis Technical Report (Reference 2).

The DMA switches provide the operator with the capability to actuate the engineered safety features (ESF) systems from the main control room (MCR). The DMA switches are diverse from the manual and automatic logic functions performed by digital equipment in the PPS and ESF-CCS.

c. GDC 19, “Control Room”

The MCR safety console is equipped with manual reactor trip initiation switches, manual ESF actuation switches and PPS operator modules (OMs) shared with the ESF-CCS and core protection calculator system (CPCS). Monitoring of the plant is accomplished through the use of the qualified indication and alarm system – P (QIAS-P), qualified indication and alarm system – non-safety (QIAS-N) and information processing system (IPS) displays. The DAS (including DPS, DMA switches, and DIS) equipment are provided to protect against a DBE concurrent with a postulated CCF in the safety I&C systems.

d. GDC 21, “Protection System Reliability and Testability”

The DAS is designed to meet the reliability goal of the plant I&C systems.

e. GDC 22, “Protection System Independence”

The independence between the DAS and the protection systems conforms to the independence requirements of IEEE Std 384-1992 (Reference 8) and IEEE Std 603-1991 (Reference 4).

f. GDC 24, “Separation of Protection and Control System”

The electrical, physical and communication isolations are maintained between the safety I&C systems and the DAS which is a non-safety system.

Where safety sensors are shared between the DAS and the safety I&C systems, the qualified isolators in the auxiliary process cabinet–safety (APC-S) prevent adverse interaction with the safety functions induced by DAS failures.

g. GDC 29, “Protection Against Anticipated Operational Occurrences”

Plant initiating events have been analyzed and the safety I&C systems protect the plant against AOO. The DAS, which is diverse from the safety I&C systems and not subject to CCF in the safety I&C systems, provides backup safety functions for AOO.

3.3 Regulatory Guidances and Reports

3.3.1 SRM on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” Item II.Q, “Defense against Common-Mode Failures in Digital Instrumentation and Control Systems”, July 1993 (Reference 7).

Design features for D3 for the PPS and ESF-CCS are implemented in accordance with SRM on SECY-93-087, as referenced by NUREG-0800.

The DAS is designed to comply with the requirements of defense against a postulated CCF within digital safety I&C systems.

The DPS automatically initiates a reactor trip on high pressurizer pressure, high containment pressure, and turbine trip. The DPS reactor trip on turbine trip is manually enabled from MCR only if the reactor power cutback system (RPCS) is out of service.

The DPS automatically initiates a safety injection actuation signal (SIAS) on low pressurizer pressure, and an auxiliary feedwater actuation signal (AFAS) on low steam generator water level in either steam generator.

The DPS turbine trip signal is automatically generated with three seconds of time delay after the initiation of DPS reactor trip signal.

The DMA switches provide the operators with the capability to manually actuate the ESF functions in the event of a postulated CCF of safety I&C systems. The DMA switches are hardwired directly to the CIM which is allocated at the lowest level of safety control system.

The reactor trip switches are hardwired directly to the reactor trip switchgear system (RTSS) trip circuit breakers.

The DIS displays parameters that monitor inadequate core cooling status, accident monitoring parameters, and parameters for emergency operation.

3.3.2 NUREG-0800, Branch Technical Position 7-19, Rev. 6, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems” (Reference 9)

The DAS is designed to comply with the guidance of BTP 7-19, Rev. 6. The conformance to BTP 7-19 is provided in more detail in Appendix A of this report.

3.3.3 NUREG-0800, Chapter 18-A, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses” (Reference 10)

After the occurrence of a DBE concurrent with a postulated CCF in the safety I&C systems, the operator will immediately take appropriate actions to mitigate the CCF event. These operator actions are evaluated according to NUREG-0800, Appendix 18-A (Reference 10). However, the licensing analysis for a DBE concurrent with a postulated CCF in the safety I&C systems does not credit any operator action conservatively until 30 minutes after event initiation.

3.3.4 NUREG-0800, Section 7.8, “Diverse Instrumentation and Control Systems”

The DAS is designed to comply with the guidance provided in Section 7.8 of NUREG-0800.

3.3.5 NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems”, December 1994 (Reference 13).

The results of D3 analysis performed in accordance with the guidelines of NUREG/CR-6303 are described in Appendix C.

3.3.6 US NRC Generic Letter (GL) 85-06, “Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related,” 1985 (Reference 6).

The DAS is designed to meet the quality assurance guidance provided in Generic Letter 85-06.

3.4 Regulatory Guides

3.4.1 Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Rev. 2 – endorses IEEE Std 379-2000 (Reaffirmed 2008)

The DPS and DMA switches are classified as non-safety system and is not required to meet single failure criterion. However, the DPS is designed to actuate the diverse functions and also prevent spurious actuation following a postulated single failure in the DPS. The DPS is also designed to meet the single failure criterion for the enhancement of system availability by incorporating four channels and 2-out-of-4 coincidence logic for the fault-tolerant capability.

3.4.2 Regulatory Guide 1.62, "Manual Initiation of Protective Actions", Rev. 1

The reactor trip is manually initiated by the reactor trip switches and ESF functions are manually initiated by the DMA switches on the MCR safety console. These hardwired conventional switches are not susceptible to a postulated CCF.

3.4.3 Regulatory Guide 1.75, "Criteria for Independence of Electrical Systems", Rev. 3 – endorses IEEE Std 384-1992

The DPS and DMA switches are classified as non-safety equipment and are isolated from the safety I&C systems by use of qualified isolators. The DPS and DMA switches are also physically separated from the safety I&C systems.

3.4.4 Regulatory Guide 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants", Rev. 3 – endorses IEEE Std 344-1987

The DAS is not required to operate during safe shutdown earthquake (SSE). However, the DMA switches are designed with Class 1E hardware and seismically qualified. The DPS is designed and qualified to withstand their physical integrity during five 1/2 SSEs followed by one SSE. The DIS is classified as non-seismic equipment except the DIS equipment mounted on the safety console, which is qualified to withstand its physical integrity during five 1/2 SSEs followed by one SSE.

3.4.5 Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation", Rev. 3 - endorses Part 1 of ISA-S67.04.01-2006

The setpoints for the DPS automatic functions are determined based on nominal system uncertainties across the range of environmental conditions including the drift. The setpoints are determined to automatically actuate the DPS after the actuation of safety I&C systems through the use of relaxed setpoints and actuation time delays.

3.4.6 Regulatory Guide 1.152, "Criteria for Use of Digital Computers in Safety Systems of Nuclear Power Plants", Rev. 3 - endorses IEEE Std 7-4.3.2-2003

The software for the DIS and DPS is classified as important-to-safety (ITS). The life cycle process for the DAS application software is described in the Software Program Manual Technical Report (Reference 14).

3.4.7 Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control", Rev. 1 - endorses MIL Std 461E-1999, IEEE Std 1050-1996, IEC 61000 - Parts 3, 4 and 6, IEEE Std C62.41-1991, and IEEE Std C62.45-1992

The DAS is a non-safety system and is qualified for electromagnetic compatibility (EMC) necessary to perform its intended functions. The DAS is not susceptible to electromagnetic interference (EMI) / radio frequency interference (RFI) / surge generated externally during normal operation, and does not generate EMI/RFI/surge to the level that may affect the normal operation of other systems.

4 I&C SYSTEM DESCRIPTION

4.1 Overall I&C Systems

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

The safety I&C systems are implemented on programmable logic controllers (PLCs) and the limited number of hardware switches to meet the safety system design criteria in IEEE Std 603-1991.

The safety I&C systems are qualified to meet the 10 CFR 50, Appendix B (Reference 15) requirements for both hardware and software modules. The components of the safety I&C systems are qualified to meet environmental, seismic, and EMI/RFI qualification requirements. The Quality Assurance Manual (Reference 16) and Quality Assurance Program Description (Reference 17) comply with the requirements of 10 CFR 50, Appendix B.

The safety I&C system software is designed, developed, verified and validated using a software life cycle design process. The safety I&C systems implemented on the common safety PLC platform consist of the PPS, ESF-CCS, CPCS and QIAS-P.

The QIAS–N is also implemented on the common safety PLC platform even though it is a non-safety system. The control panel multiplexer (CPM) uses the common safety PLC platform.

Major functions of control, alarm and indication of the non-safety I&C systems are implemented on a distributed control system (DCS) based common platform, and the performance of which is proven by operating experiences from the nuclear industry as well as other industries. The DCS supports component-level control, automatic process control, and high-level group control. The DCS is designed in a redundant and fault-tolerant architecture to achieve high reliability such that a failure of a single component does not cause a spurious plant trip. The non-safety systems implemented in the DCS are the information processing system (IPS), power control system (PCS), and process – component control system (P-CCS) including nuclear steam supply system (NSSS) process control system (NPCS).

The DPS and DIS are implemented on a FPGA-based logic controller (FLC), which is diverse from the common safety PLC platform. The DIS display is implemented on a non-safety flat panel display (FPD) that is independent from the IPS and diverse from the common safety PLC platform. The DMA switches are implemented by conventional switches, which are diverse from common safety PLC platform.

The IPS consists of networking equipment, computer servers, FPDs and peripherals to provide the operator with the plant information and soft control for non-safety components.

There are stand-alone systems which are not installed on a common I&C platform. They have unique hardware and fulfill specific system design requirements. These non-standard systems include the ex-core neutron flux monitoring system (ENFMS), fixed in-core detector amplifier system (FIDAS), NSSS integrity monitoring system (NIMS), APC-S, CIM, turbine control system (TCS), radiation monitoring system, and balance of plant (BOP) monitoring systems.

The plant-wide data networks are composed of safety networks and non-safety networks. The safety network is independent and diverse from the non-safety network. The non-safety network utilizes different communication hardware, software and communication protocol from the safety network.

The I&C system architecture satisfies the independence, separation and diversity requirements as follows:

- Each channel of the safety I&C systems is functionally, physically and electrically independent from each other to meet the single failure criteria.

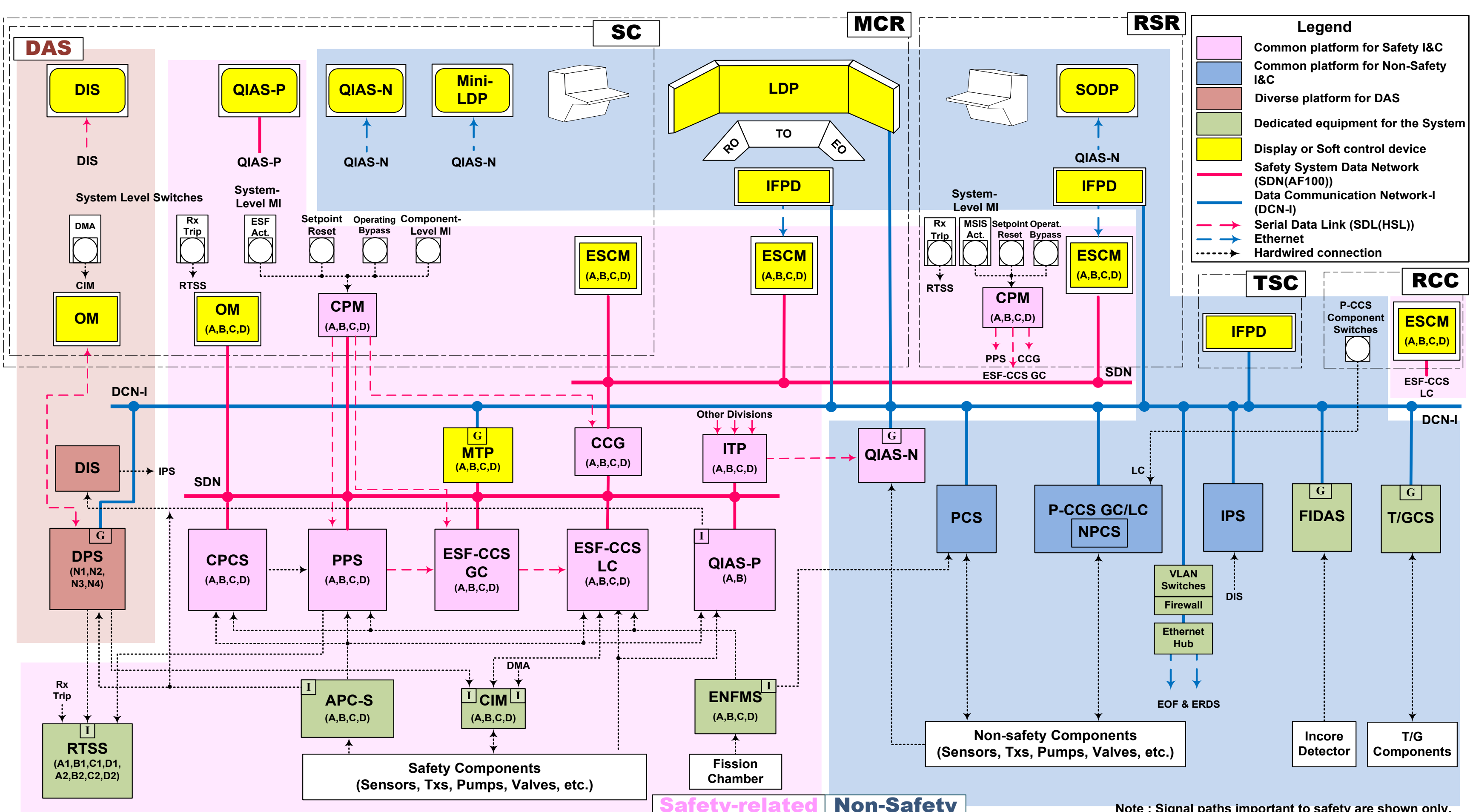
- A safety channel does not receive any information or signals originating from another safety channel or non-safety channel to perform its safety function (except for the 2-out-of-4 voting between channels, and the DPS to CIM interfaces). The bistable outputs from each safety division are shared between safety divisions for the 2-out-of-4 voting.

- The data communication networks of the safety system and non-safety system are independent and diverse from each other. There is no potential for the deterministic cyclic processing of the safety function to be disrupted by any data communication. One way communication from safety systems to non-safety systems and buffering circuits using dual ported memory are commonly used to prevent endangering the safety function.

- The DPS is diverse from the protection systems such as PPS and ESF-CCS in aspects of equipment platform and reactor trip mechanism.

- The DMA switches, manual reactor trip controls, DPS, and DIS are provided to cope with the CCFs of the safety I&C systems.

More detailed descriptions and architecture features are provided in the Safety I&C System Technical Report (Reference 3).



APC-S: Auxiliary Process Cabinet - Safety
CCG: Control Channel Gateway
CIM: Component Interface Module
CPCS: Core Protection Calculator System
CPM: Control Panel Multiplexer
DAS: Diverse Actuation System
DIS: Diverse Indication System
DCN-I: Data Communication Network-Information
DMA: Diverse Manual ESF
DPS: Diverse Protection System
ENFMS: Ex-core Neutron Flux Monitoring System
EOF: Emergency Operation Facility
ERDS: Emergency Response Data System
ESCM: ESF-CCS Soft Control Module
ESF-CCS: Engineered Safety Features - Component Control System
FIDAS: Fixed In-core Detector Amplifier System
G: Gateway
GC: Group Controller
I : Isolator
IFPD: Information Flat Panel Display
IPS: Information Processing System
ITP: Interface and Test Processor
LC: Loop Controller
LDP: Large Display Panel
MCR: Main Control Room
MI: Minimum Inventory
MTP: Maintenance and Test Panel
NPCS: NSSS Process Control System
MSIS: Main Steam Isolation System
OM: Operator Module
P-CCS: Process-Component Control System
PCS: Power Control System
PPS: Plant Protection System
QIAS-P/N: Qualified Indication & Alarm System – P / Non-safety
RCC: Remote Control Center
RSR: Remote Shutdown Room
RTSS: Reactor Trip Switchgear System
Rx: Reactor
SC: Safety Console
SODP: Shutdown Overview Display Panel
T/GCS: Turbine/Generator Control System
TSC: Technical Support Center, Txs: Transmitter

Rev.1

Figure 4-1 Architecture Overview of the APR1400 I&C Systems

TS

Figure 4-2 Diversity Features between PPS/ESF-CCS and DPS/DMA Switches

4.2 Echelons of Defense

For the defense against a postulated CCF in the protection system platform, the following major defense echelons are designed into the APR1400 I&C systems:

a. Control & monitoring systems

b. PPS and ESF-CCS

c. Diverse actuation system

- DPS
- DIS
- DMA switches

Major I&C systems related with the echelons of the defense against a CCF are shown in Figure 4-2 and described in the following sections.

4.2.1 Control & Monitoring Systems

The major non-safety control systems are the PCS and P-CCS.

The PCS is an integrated control system that is designed to control reactor power level including the reactor regulating system (RRS), digital rod control system, and RPCS. The RRS is used to automatically adjust reactor power and reactor coolant temperature to follow turbine load transients within established limits. The RRS receives a turbine load index signal (linear indication of load) and reactor coolant temperature signals. The turbine load index is provided to a reference temperature (Tref) program that establishes the desired average temperature. The hot leg and cold leg temperature signals are averaged (Tavg) in the RRS. The Tref signal is then subtracted from the Tavg signal to provide a temperature error signal. Power range neutron flux is subtracted from the turbine load index to provide compensation to the (Tavg - Tref) error signal generated.

The P-CCS includes NSSS Process Control System (NPCS) and BOP Control System. The NPCS includes the feedwater control system (FWCS), steam bypass control system (SBCS), pressurizer pressure control system (PPCS), and pressurizer level control system (PLCS).

The FWCS is designed to automatically control the steam generator downcomer water level from hot zero power to full power operation.

The SBCS controls the positioning of the turbine bypass valves through which steam is bypassed around the turbine into the unit condenser. The system is designed to increase plant availability by making full utilization of turbine bypass capacity to remove excess NSSS thermal energy following turbine load rejections. This is achieved by the selective use of turbine bypass valves and the controlled release of steam. This avoids unnecessary reactor trips and prevents the opening of pressurizer pilot operated safety relief valve (POSRV) or main steam safety valves. The RPCS is used in conjunction with the SBCS to reduce turbine bypass valve capacity requirements.

The PPCS maintains the reactor coolant system (RCS) pressure within specified limits by the use of pressurizer heaters and spray valves. A pressurizer pressure signal is used to control the proportional heaters. The heaters are controlled to maintain the pressurizer pressure as required. The pressurizer pressure signal is also sent to a spray valve controller. This provides a signal to the spray valves to control their opening.

The PLCS minimizes changes in the RCS coolant inventory by using the charging control valve and letdown orifice isolation valves in the chemical and volume control system (CVCS). It also maintains a vapor volume in the pressurizer to accommodate surges during transients. During normal operations the level is programmed as a function of Tavg in order to minimize charging and letdown flow requirements.

The P-CCS is designed to control non-safety components such as pumps, valves, heaters and fans. The P-CCS performs data acquisition from field instruments and discrete and continuous controls, and provides process variables and their status information to the IPS and QIAS-N for plant monitoring.

Standardized component control logic and I/O interfaces are provided for the various types of components to be controlled. Manual operator controls for the P-CCS are performed through the soft control display on the information FPD (IFPD) driven by the IPS.

4.2.2 PPS and ESF-CCS

The PPS is a safety system which consists of sensors, logic, and other equipment necessary to monitor selected plant conditions and to achieve reliable and rapid reactor trip if any monitored parameter conditions approach specified safety system settings. The functions are to protect the core fuel design limits and RCS pressure boundary following a DBE, and to provide assistance in mitigating the consequences of accidents. Four measurement channels with electrical isolation and physical separation are provided for each parameter used in the generation of trip and actuation signals.

The PPS performs the following functions: bistable trip, local coincidence, reactor trip and/or ESFAS initiation and automatic testing of PPS logic. The bistable processors generate trip signals based on the measured process values exceeding a setpoint. The bistable processors provide their trip signals to the local coincidence logic (LCL) processors located in the four redundant channels. The LCL processors evaluate the local coincidence logic based on the state of the four bistable trip signals and their respective bypasses.

The PPS has four redundant sets of cabinets. Each set of cabinets is located in a separate I&C equipment room. Each set of cabinets contains the signal conditioning devices, bistable processors, LCL processors, interface and test processor (ITP), maintenance and test panel (MTP), and other hardware for the interface with other PPS channels.

Four redundant PPS operator modules (OMs), one per channel, are located in the MCR. Each OM provides the displays for the CPCS, PPS and ESF-CCS. The OM provides the HSI means for entering constants for the CPCS, and the reset function for RPS and ESFAS actuation logic. The conventional switches such as operating bypass and setpoint reset are provided on the MCR safety console and RSR.

A local MTP switch panel, one per channel, also provides trip channel bypasses, operating bypasses, and variable setpoint resets. The MTP FPD is the HSI interface for the maintenance testing, including manual testing of bistable trip functions via the SDN. The redundant MTPs also serve as unidirectional data communication gateways to send selected PPS, CPCS, and ESF-CCS channel status and diagnostic results to the IPS through the DCS gateway servers.

The ITP, one per channel, monitors the PPS and ESF-CCS status and is used to initiate manual and/or automatic surveillance testing based on the user input from the MTP. The ITP interfaces with the RTSS via the SDN for status indication. The ITP also interfaces with the QIAS-N for the data transmission of the safety I&C system status via a serial data link (SDL). The MTP and ITP are shared with other safety I&C systems in each channel (i.e., PPS bistable processor (BP), LCL, ESF-CCS, CPCS and QIAS-P).

The MCR safety console and the RSR console provide means to achieve and maintain the reactor in safe shutdown.

The ESF-CCS receives the ESF actuation signals from the ESFAS portion of the PPS, safety portion of the radiation monitoring system, or the manual ESF system level actuation switches. The ESFAS signals actuate the ESF system equipment. The control circuitry for the components provides the sequences necessary for proper ESF system operation, which utilizes bistable trip functions and coincidence logic in the PPS, and ESF actuation and component control logic in the ESF-CCS. The ESF actuation signals are provided as input signals to the ESF system.

4.2.3 Diverse Actuation System

The DAS performs diverse automatic protection functions, diverse manual ESF actuations, and diverse indication functions. The DAS is designed to meet the following regulatory requirements:

a. ATWS mitigation according to 10 CFR 50.62

b. Points 3 and 4 of the NRC position on D3 in BTP 7-19

The DPS includes diverse automatic trip and actuation functions that are (a) required for ATWS mitigation and (b) for mitigation of DBEs concurrent with a postulated CCF in the safety I&C systems.

If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications are displayed on the DPS operator module (DPS-OM) mounted on the MCR safety console, enabling the operator to be aware of the safety system CCF.

The DMA switches are provided to permit the operator to actuate ESF systems from the MCR after a postulated CCF in the safety I&C systems. To achieve the ESF actuation independently and diversely from the ESF-CCS, the DMA switches are hardwired to the CIM through the isolators for remote manual actuation of the ESF systems.

The DMA switches bypass all PPS digital platform software including CPMs, gateways and the ESF-CCS controllers in order to perform the ESF actuation logic. The DMA switches are connected to fan-out devices in the MCR safety console to distribute the ESF actuation signals to individual component controls.

Two types of manual reactor trip controls are provided. Manual reactor trip switches are hardwired to the RTSS as required by IEEE Std 603-1991. In addition, manual reactor trip controls are also provided through the DPS operator module (DPS-OM) with soft controls.

The DIS displays the information required for operators to place and maintain the plant in a safe shutdown condition following a DBE concurrent with a postulated CCF in the safety I&C systems. The DIS receives field input signals through signal splitters/isolators before they are hardwired to the applicable processors of safety I&C systems. The DIS satisfies the diverse indication guidance provided in the Point 4 position of BTP 7-19. It consists of one channel of non-safety-related equipment. The DIS display device is located on the MCR safety console.

In addition, all process variables input to the safety I&C systems are not affected by the software CCF, and the information derived from those variables are available from the IPS.

5 DIVERSE ACTUATION SYSTEM

The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following subsections. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.

5.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO concurrent with a failure of the reactor trip portion of the protection system. In addition, the DPS is designed to mitigate the consequences of a DBE concurrent with a postulated CCF of the safety I&C system digital computer.

The DPS initiates a reactor trip when either high pressurizer pressure or high containment pressure exceeds the pre-determined value. The DPS also initiates a reactor trip on a turbine trip if the RPCS is out of service. The DPS reactor trip on a turbine trip is manually enabled from the MCR when the RPCS is out of service.

The DPS is designed to transmit reactor trip signals to total eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to total eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the DPS to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.

Once the diverse reactor trip signals are initiated automatically from the DPS cabinet, the diverse reactor trip function is completed by the actuation of shunt trip devices of reactor trip circuit breakers. The diverse reactor trip is completed when the reactor trip circuit breakers open. Deliberate operator action (i.e., reset of reactor trip circuit breakers) is required to clear the diverse reactor trip and close the reactor trip circuit breakers.

The DPS is implemented with a 2-out-of-4 voting logic to ensure a single failure within the DPS does not (a) cause a spurious actuation, and (b) preclude an actuation. The BP provides a channel trip signal to the LCL processor located in the four redundant channels. The LCL processor determines the local coincidence logic trip state and initiates reactor trip, turbine trip and ESF actuations based on the state of the four trip signals.

The DPS actuates the auxiliary feedwater system (AFWS) on low steam generator level in either steam generator when the level decreases below a predetermined value. The auxiliary feedwater actuation signals (AFAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the AFWS. Isolation is provided at the ESF-CCS loop controller (LC) cabinet to maintain electrical isolation between the DPS and the CIM.

A DPS-AFAS occurs when the water level in a SG drops below the DPS-AFAS setpoint, and is reset when the SG water level is recovered to the reset setpoint. The setting and resetting of the DPS-AFAS repeats according to the changes of SG water level during plant transients.

The DPS also actuates the safety injection system (SIS) on low pressurizer pressure when the pressure decreases below a predetermined value. The safety injection actuation signals (SIAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the safety injection of reactor coolant. Isolation is provided at the ESF-CCS LC cabinet to maintain electrical isolation between the DPS and the CIM.

Once the DPS-SIAS is automatically initiated from the DPS, it is maintained until operator resets it. The DPS-SIAS can be reset when the pressurizer pressure is increased above its setpoint.

The DPS also automatically initiates a turbine trip whenever the DPS reactor trip conditions have been met. The DPS turbine trip signal is generated with three seconds of time delay after the initiation of DPS reactor trip signal.

The DPS is implemented on a non-safety platform. Each DPS channel is powered from two non-Class 1E vital buses, which are independent from Class 1E vital buses. The non-Class 1E vital buses are connected with the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DPS is not impacted by a postulated software CCF or loss of offsite power (LOOP) event.

The DPS uses signals from safety class sensors through isolators located at the APC-S. The safety class sensors and the APC-S are conventional analog equipment which do not include any functional programmable unit, as defined in IEEE Std 7-4.3.2. In addition, the APC-S does not use any common software. The signal conditioning/ splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the safety class sensors and APC-S are not susceptible to a postulated software CCF. The configuration and interface of the DPS are shown in Figure 5-1.

TS

Figure 5-1 DPS Functional Block Diagram

5.2 Diverse Indication System

The DIS is diverse from the QIAS-P. The DIS is also diverse from the IPS.

The DIS provides plant operators with the following information that is not susceptible to a postulated CCF in the safety I&C systems. Typical DIS variables are listed in Appendix C and the display parameters are as follows:

- Inadequate core cooling (ICC) monitoring information
- Accident monitoring information
- Emergency operation-related information

The DIS independently calculates a representative core exit temperature, saturation margins and reactor vessel levels for the display. It also provides the heated junction thermo-couple (HJTC) heater power control function for the reactor vessel level detector as a backup of the QIAS-P calculated function which is potentially lost due to a postulated CCF of the safety I&C systems.

The detailed signal interfaces between the DIS and the QIAS-P are shown in Figure 5-2; safety classification, signal flow, and type of signals are also provided in the figure.

The DIS is a single channel of non-safety equipment to meet the requirements of BTP 7-19 Point 4 position on D3 for the safety I&C systems. It receives analog inputs from signal splitters/isolators in the APC-S as well as in the QIAS-P channel A via hardwired interface and displays them on the non-safety DIS FPD at the MCR safety console.

All the software associated with the DIS is classified as ITS.

The DIS is powered by the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DIS is not impacted by a postulated software CCF or LOOP event.

Figure 5-3 shows that the DIS is independent and diverse from the safety I&C system platform.

5.3 Diverse Manual ESF Actuation

The DAS includes conventional DMA switches on the MCR safety console for manual actuation of the ESF components which are required to cope with a DBE concurrent with a postulated CCF in the safety I&C systems. The DMA switches are classified as non-safety system, but designed with Class 1E hardware with augmented quality.

DMA enable switches are essential pieces of equipment which are used to enable the function of the DMA switches for the mitigation of a design bases event which occurs concurrent with a software CCF of the common safety I&C platform.

TS

Figure 5-2 DIS Signal Block Diagram

TS

Figure 5-3 Diversity Features between QIAS and DIS

TS

Figure 5-4 Interfaces of DMA Switches with ESF Components

The DMA enable switch can block the hardwired signal form the DMA switch to the CIM by using an AND gate function, as shown in Figure 5-4. The AND gate function is implemented by a simple configuration using conventional hardwired switches, as shown in Figure 5-5.

A DMA enable switch has contacts that connected to each contact of the DMA switches in series, as shown in Figure 5-5. The DMA enable switch can switch these contacts at the same time to enable the function of DMA switches. Therefore, the operator needs to turn the DMA enable switch to “Enable” and then turn the DMA switch to “Actuate” to send an actuation signal. These actuation signals of the DMA switches are input to the CIM in the ESF-CCS LC cabinets through an interposing relay for isolation. Therefore, the signals from the DMA enable switch and the DMA switch are isolated from the safety I&C systems.

The DMA switches are normally disabled. The functions of the DMA switches can be enabled when the DMA enable switch is switched to enable mode by administratively controlled operator action. The function of the DMA switches is blocked unless operators conclude that safety I&C systems have a CCF. However, this block function is implemented by a simple configuration and the DMA enable switches and DMA switches do not use a software device in order to not be susceptible to a software CCF.

The DMA switches are diverse from the manual and automatic logic functions performed by the PPS and ESF-CCS. The DMA switches provide the ESF actuation as required by SRM on SECY-93-087, and are listed in Appendix C.

The DMA switches provide system-level conventional switches as follows:

- DMA safety injection actuation signal (SIAS) switch - Divisions A and C
- DMA containment spray actuation signal (CSAS) switch - Divisions A and C
- DMA containment isolation actuation signal (CIAS) switch - Division A
- DMA main steam isolation signal (MSIS) switch (1A, 1B, 2A, and 2B) - Division A
- DMA auxiliary feedwater actuation signal-1 (AFAS-1) switch - Division A
- DMA auxiliary feedwater actuation signal-2 (AFAS-2) switch - Division B

The DMA signals are hardwired directly to the CIM through the isolators. The DMA switches send latch signals to the CIM. Therefore, the ESF actuation initiated by the DMA switch continues until completion once initiated. These latch signals will be reset manually when the mitigation function is completed. The CIMs interface directly with plant components through the component control circuitry. The CIMs receive component control signals from the ESF-CCS, DPS, and DMA switches.

In addition, the MCR safety console provides diverse manual/auto (M/A) stations to manually modulate auxiliary feedwater flow/steam generator level as follows:

- DMA auxiliary feedwater flow/steam generator 1 level - Division A
- DMA auxiliary feedwater flow/steam generator 2 level - Division B

The diverse M/A stations are classified as a safety system and implemented by Class 1E qualified devices.

The diverse M/A stations are only enabled when each DMA AFAS is activated in the same division. The diverse M/A stations provide manual analog control and indication of auxiliary feedwater flow and steam generator level. The diverse M/A stations are directly hardwired to the designated components.

The Class 1E 120 Vac I&C power system continuously provides 120 Vac power to the interposing relays of the CIM that interface with the DMA switches. The Class 1E 120 Vac I&C power system is provided power from the DC control center of the Class 1E 125 Vdc power system. Following a LOOP event, the emergency diesel generator (EDG) provides power to the dc control center. If there is a station blackout (SBO) due to EDG failure concurrent with a LOOP event, the alternate alternating current gas turbine generator (AAC GTG) provides power to the DC control center for either the A or the B safety train. In addition, the Class 1E 125 Vdc power system has battery backup power. The design information about the Class 1E 125 Vdc power system and the Class 1E 120 Vac I&C power system is described in Section 8.3.2.1.2 of DCD Tier 2.

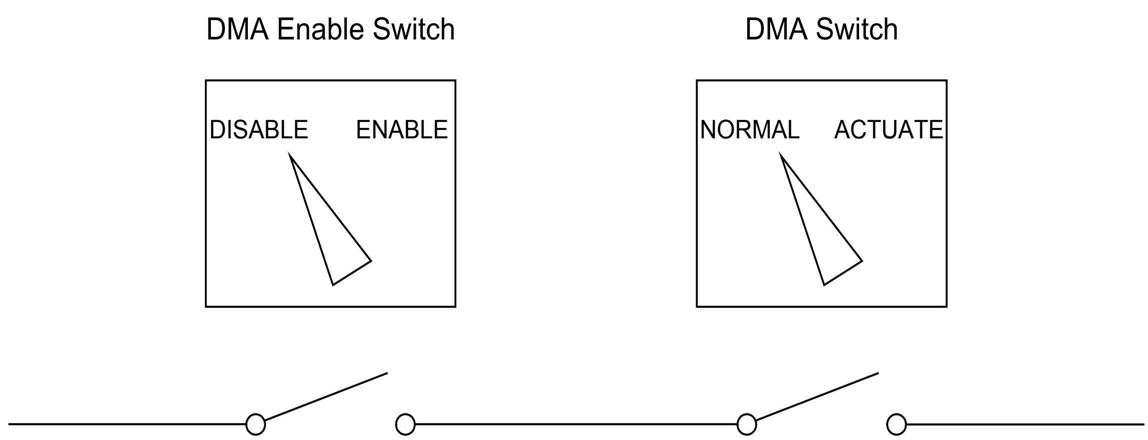


Figure 5-5 Configuration of DMA Switch and DMA Enable Switch

6 DIVERSITY AND DEFENSE-IN-DEPTH ANALYSIS

6.1 Design Approach

The APR1400 design methods and features related with the D3 include the following:

6.1.1 Elimination of Predictable CCFs

The hardware related failures due to common stressors are avoided through environmental, seismic, EMI qualification, aging analyses, and spatial separation of equipment. These are considered predictable CCFs because the testing is designed to reveal susceptibility to external effects that could affect redundant hardware elements in a system (and thus disable the system). Fire is an external effect that is defended by separation of redundant elements of a system, such as placing them in different rooms.

6.1.2 Design of Highly Reliable Software

A rigorous software lifecycle design process is used to minimize postulated CCF errors for the APR1400 safety I&C systems. This approach is summarized as follows:

Deterministic Design – The algorithm execution in the APR1400 safety I&C systems is deterministic. This means that data is updated on a continuous cycle and programs execute on a continuous basis. This approach makes the software easier to design, verify and validate. The potential for hidden errors is significantly lower than in other designs that include event based execution, or event based data communication

Simplicity – The reactor protection and ESF actuation functions are accomplished with PLCs. PLCs are widely used, simple, proven digital devices that utilize logic without branching, interrupts or other complex features. Programming and testing PLCs to accomplish the required functions is easily understood and verified.

Field Proven Products - Operating system software for the APR1400 safety I&C system is selected with field experience in similar applications. These products are mature and, therefore, demonstrated to be free of design errors.

Verification and Validation (V&V) - For custom (application) software, a comprehensive V&V program is employed, including independent document reviews and independent tests. Application software is subject to a documented and rigorous V&V program. Independence is maintained between software development and verification personnel. The configuration controls are also imposed throughout the software life cycle. A rigorous software life cycle design process and associated independent V&V program minimizes the potential for CCF errors throughout the software lifecycle design process as described in the Software Program Manual Technical Report (Reference 14).

Segmentation - Within the APR1400 safety I&C systems, functions are divided among separate processors. There are two (2) bistable racks per PPS channel. Each rack includes one (1) bistable processor (BP) and its own input modules. Both BPs share all monitored process input parameters. One (1) BP executes its trip function in sequence 1 through N while the other BP in the channel executes its trip functions in the reverse sequence N through 1. This approach provides functional diversity within the PPS. The trip outputs from each BP are provided to all LCL racks in four (4) redundant PPS channels. Within ESF-CCS, its functions such as the SIAS and AFAS are distributed to separate control processors. The potential for simultaneous CCF errors in these multiple processors is minimized, since functional diversity is utilized and software execution is asynchronous.

Diversity - Diversity offers the final defense against CCFs. All critical safety functions, such as reactivity control, inventory control and heat removal, can be monitored, automatically controlled, and manual action taken to maintain the safety margins from both the control systems and the safety I&C systems (Table 6-1). These systems are functionally diverse, as are the fluid/mechanical systems they control. In addition, to correspond with the hardware diversity of these fluid/mechanical systems, the APR1400 employs both hardware and software diversity between control and protection I&C systems to eliminate the potential for CCFs. This diversity exists in all software-based aspects of these systems, including processors, multiplexers, communication networks and HSI devices. This same diversity philosophy is applied between the QIAS-P/N and the IPS to ensure availability of control room information.

6.1.3 Evaluation of Defense-in-Depth

Nuclear industry studies of I&C systems have shown systematic ways in which postulated CCFs or sneak-paths can compromise portions of the lines of defense for plant events. These studies have verified that not all such potential faults or paths are identified and/or evaluated during the design process.

The basis for the evaluation documented herein is that CCFs (however slight their potential and no matter how many evaluations are done or how they may occur) can be postulated to occur. As a result, the CCF coping analysis takes credit for diverse functions (automatic, manual, and indication) that are required to meet the applicable acceptance criteria following an initiating event concurrent with a postulated CCF in the protection system.

6.2 Diversity and Defense-in-Depth Analysis

The detailed D3 analysis in accordance with NUREG/CR-6303 guidelines is provided in Appendix C. The appendix demonstrates that the vulnerabilities to CCF have been adequately addressed in the APR1400, and the APR1400 I&C systems have sufficient diversity features using the guidelines 1 through 14 in NUREG/CR-6303 (Reference 13). Refer to Appendix C, Table C-1 for diversity attributes diverse I&C platforms against safety I&C system platform.

6.2.1 Diversity Evaluation between the DPS and the PPS

Detailed analysis results of diversity attributes between the DPS and the PPS are as follows:

Design Diversity – Diverse equipment platform based on different technology is applied to the DPS compared with the PPS. The PPS uses the PLC technology for the digital logic processing, whereas the DPS uses the FPGA logic controllers (FLC) technology for the digital logic processing. In addition, system architectures are diverse between the PPS and the DPS. Therefore, significant design diversity factors are provided between the PPS and the DPS.

Functional diversity – The reactor trip mechanism of the DPS are diverse form that of the PPS. The PPS use the undervoltage trip mechanism, whereas the DPS use the shunt trip mechanism. Therefore, functional diversity is provided between the PPS and the DPS.

Signal diversity – There is no signal diversity between the PPS and the DPS. The safety class sensors and APC-S are shared by both the PPS and the DPS. The sensors and APC-S are analog type equipment. Therefore, these equipment are not affected by the software CCF.

Software diversity – The PPS uses the software for PLC for the digital logic processing, whereas the DPS uses the hardware description language (HDL) for the FLC. Therefore, significant software diversity is provided between the PPS and the DPS.

Equipment diversity – The diverse equipment platform from different manufacturer is applied to the DPS compared with the PPS. The PPS uses the PLC platform for the digital logic processing, whereas the DPS uses the FLC platform. Therefore, significant equipment diversity is provided between the PPS and the DPS.

Human diversity – The DPS is designed and tested by different engineers of different design and test team from the PPS design and test team. Therefore, human diversity is provided between the PPS and the DPS.

6.2.2 Diversity Evaluation between the DIS and the QIAS-P

Detailed analysis results of diversity attributes between the DIS and the QIAS-P are as follows:

Design diversity – Diverse equipment platform based on different technology is applied to the DIS compared with the QIAS-P. The QIAS-P uses the PLC technology for the digital logic processing, whereas the DIS uses the FPGA logic controllers (FLC) technology for the digital logic processing. Therefore, design diversity is provided between the DIS and the QIAS-P.

Functional diversity – There is no functional diversity between the DIS and the QIAS-P.

Signal diversity – There is no signal diversity between the DIS and the QIAS-P.

Software diversity – The QIAS-P uses the software for the digital logic processing in common safety PLC platform, whereas the DIS uses the HDL for the FLC platform. Therefore, significant software diversity is provided between the DIS and the QIAS-P.

Equipment diversity – The diverse equipment platform from different manufacturer is applied to the DIS compared with the QIAS-P. The QIAS-P uses the common safety platform for the digital logic processing, whereas the DIS uses the FLC platform. Therefore, significant equipment diversity is provided between the DIS and the QIAS-P.

Human diversity – The DIS is designed and tested by different engineers of the different design and test team from that of the QIAS-P. Therefore, human diversity is provided between the DIS and the QIAS-P.

6.2.3 Diversity Evaluation of the functions between DMA switches and PPS/ESF-CCS

Detailed analysis results of diversity attributes of the functions between the DMA switches and the PPS/ESF-CCS are as follows:

Design Diversity – The DMA switches are implemented by conventional switches. The ESFAS functions by the PPS and ESF-CCS uses the PLC technology for the digital logic processing, whereas the DMA switches uses the conventional switches for operator manual actions without using digital devices. In addition, the architecture of the DMA switches is diverse from the PPS and ESF-CCS. Therefore, significant design diversities are provided between the DMA switches and the PPS/ESF-CCS.

Functional diversity – There is no functional diversity between the ESF functions of DMA switches and the PPS/ESF-CCS.

Signal diversity – The ESF actuation signals from DMA switches are diverse from the ESF signals from the PPS/ESF-CCS. The ESF signals from the DMA switches are directly connected to the CIM using hardwired cables without using common safety PLC platform like PPS/ESF-CCS. The signals from the DMA switches and the PPS/ESF-CCS are combined in the CIM that are not affected by a software CCF. Therefore, signal diversity is provided between the DMA switches and PPS/ESF-CCS.

Software diversity – The PPS/ESF-CCS uses the software of the PLC for digital logic processing, whereas the DMA switches do not use the software.

Equipment diversity – The PPS/ESF-CCS use the common safety PLC platform for the digital logic processing, whereas the DMA switches are implemented by the conventional analog devices. Therefore, significant equipment diversities are provided between the DMA switches and the PPS/ ESF-CCS.

Human diversity – The DMA switches are designed and tested by different design and test team from the PPS/ESF-CCS design and test team. Therefore, human diversity is provided between the DMA switches and the PPS/ESF-CCS.

6.2.4 Diversity Evaluation between the Actuators/Sensors and Safety I&C Platform

Detailed analysis results of diversity attributes between actuators/sensors and the safety I&C platform are as follows:

Design diversity – Diverse equipment platform based on different technology is applied to the actuators/sensors compared with the safety I&C platform. The actuators/ sensors use the analog technology, whereas the safety I&C platform uses the common safety PLC technology for the signal processing. Therefore, design diversity is provided between the sensors/ actuators and the safety I&C platform.

Functional diversity – There is no functional diversity between the sensors/ actuators and the safety I&C platform. Sensors and actuators provide the functions closely related with the safety I&C systems.

Signal diversity – There is no signal diversity between the sensors/actuators and the safety I&C platform. The safety I&C systems get inputs from various sensors, and provide their outputs to related actuators.

Software diversity – The sensors/actuators do not use the software, whereas the safety I&C platform uses the software for PLC. Therefore, software diversity is not provided between the sensors/actuators and the safety I&C platform.

Equipment diversity – The sensors/actuators are analog type equipment, whereas the safety I&C systems are digital type PLC equipment. Therefore, equipment diversity is provided between the sensors/actuators and the safety I&C platform.

Human diversity – Compared with the safety I&C systems, the sensors/actuators are designed and tested by different design and test team. Therefore, human diversity is provided between the sensors/actuators and the safety I&C platform.

Table 6-1 Critical Functions and I&C Diversity

Critical Function	Non-Safety	Safety	Manual
Reactivity	Rod Control, CVCS Boration	SI System, Reactor Trip Switchgears	Reactor Trip Switchgears
Vital Auxiliaries(AC) (DC)	Main Transformers, Station Batteries	Emergency D/Gs (EDGs), Station Batteries	
RCS Inventory	CVCS	Safety Injection (SI)	Safety Injection (SI)
RCS Pressure	Heaters/Spray, CVCS	SI System, POSRV, Main Steam Safety Valves	SI System, Safety Depressurization and Vent System (SDVS), Atmospheric Dump Valves (ADVs)
Core Heat Removal	Forced Circulation	Natural Circulation	
RCS Heat Removal	Main Feedwater	Auxiliary Feedwater, Shutdown Cooling, SI system	Auxiliary Feedwater, SI System, SDVS, ADV
Containment Isolation	N/A	Isolation Valves	Isolation Valves
Containment Environment	Fan Coolers, Hydrogen Igniters	Containment Spray, Hydrogen Re-combiners	Containment Spray
Radiation Emission	Monitor and Control Radiation Release Paths	Isolation of Release Paths	Isolation Valves

7 CCF COPING EVALUATION METHODS FOR D3 ASSESSMENT

This section describes the CCF coping evaluation methods used to demonstrate the diversity and defense-in-depth (D3) capability of the APR1400 design by showing the acceptance criteria specified in BTP 7-19 (Reference 9) are met for all AOOs and postulated accidents (PAs) with a concurrent postulated CCF in the safety I&C systems. The CCF coping analysis investigates the scenarios in which (a) the safety I&C systems do not actuate when plant conditions require a trip or actuation, and (b) the safety I&C systems spuriously actuates when plant conditions do not require a trip or actuation. Credit is taken in the CCF coping analysis for the plant systems that are implemented on a platform that is diverse from the safety platform in which a postulated CCF is assumed to have occurred.

7.1 Event Evaluation Methods

The CCF coping analysis which has been performed according to the regulatory guidance meets the following acceptance criteria presented in Section 3.1 of BTP 7-19 for the DBEs with a concurrent postulated CCF in the safety I&C systems:

(1) “For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary reactor coolant pressure boundary. The applicant should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.”

(2) “For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.”

The evaluation consists of two phases. The first phase consists of a qualitative evaluation to identify the events that require more detailed analysis using computer program. The second phase consists of a quantitative analysis for those events that are determined to require further analysis by the qualitative evaluation phase.

Based on BTP 7-19, the CCF coping analysis applies realistic initial conditions and assumptions to both the qualitative and quantitative evaluation phases. Major characteristics of the realistic evaluation methodology different from the Chapters 6 and 15 safety analysis of the DCD are summarized as follows:

a. A CCF of the digital safety I&C systems is postulated, such that reactor trip functions implemented in the reactor protection system (RPS) and the ESF functions implemented in the ESF-CCS do not actuate. The failure includes both automatic and manual actuation (except for the hardwired diverse manual ESF actuation and the hardwired manual reactor trip).

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

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

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

e. The postulated CCF in the digital PPS/ESF-CCS does not prevent the reactor trip on high pressurizer pressure or high containment pressure and the diverse turbine trip which are actuated by the DPS. The DPS uses digital equipment and software that are diverse from the PPS and ESF-CCS.

f. The postulated CCF in the digital PPS/ESF-CCS does not prevent the auxiliary feedwater and safety injection system actuation functions which are actuated by the DPS.

g. Hardwired diverse ESF manual actuations at the system level are provided for:

- Safety Injection
- Containment Spray
- Auxiliary Feedwater Actuation
- Main Steam Isolation
- Containment Isolation, with Letdown Isolation

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

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

j. In the CCF coping analysis, it is assumed conservatively that no operator action is taken during 30 minutes after an event initiation. At 30 minutes after the event, the operators begin administrative control of the plant under the appropriate recovery procedures to achieve a hot shutdown condition. Alarms and indications are provided via equipment not affected by the postulated CCF in the digital safety I&C systems to support operators to perform a controlled cooldown of the plant.

k. A postulated CCF in similar software modules results in similar blocks failing in the same manner, i.e., similar software blocks do not fail in a random manner.

The evaluation method for the manual operator action time is described in Section 7.2 in detail. As a result of the qualitative evaluation, eight (8) events are identified that must be quantitatively analyzed;

a. Increase in feedwater flow

b. Steam line break outside containment (offsite dose)

c. Total loss of reactor coolant flow

d. Single RCP shaft seizure/break

e. CEA ejection

f. Steam generator tube rupture

g. Loss of coolant accident (LOCA)

h. Steam line break inside containment (containment integrity)

Computer programs are used in the quantitative analysis.

A detailed description of the CCF coping analysis including the qualitative evaluation and the quantitative analysis is included in the CCF Coping Analysis Technical Report (Reference 2).

7.2 Manual Operator Action Time Evaluation Methods

Manual operator action can be credited as a diverse means of mitigating AOOs and PAs concurrent with a postulated CCF in the safety I&C systems if the operator action time is evaluated based on the HFE guidance provided in NUREG-0800, Appendix 18-A.

After the occurrence of a DBE concurrent with a postulated CCF in the safety I&C systems, the operator will immediately take appropriate actions to mitigate the CCF event. These operator actions are evaluated according to NUREG-0800, Appendix 18-A (Reference 10). However, the licensing analysis for a DBE concurrent with a postulated CCF in the safety I&C systems does not credit any operator action conservatively until 30 minutes after event initiation. Justification includes assessments of available information from the systems not affected by a postulated CCF in the safety I&C systems, the decision making process, and expected operator action steps leading to the credited action based on the emergency operating guidelines. The justification of operator actions credited prior to 30 minutes includes the following considerations:

a. Operators are well aware of plant conditions requiring manual reactor trip and ESF actuation and are assumed to initiate manual reactor trip and/or manual ESF actuation with appropriate response times. The time of operator actions to be completed are justified based on an evaluation using the methods described in NUREG-0800, Appendix 18-A (Reference 10).

b. The IPS, which is not degraded by the postulated CCF, provides alarms indicating conditions relative to reactor trip and ESF bistable setpoints. Also, the operators can recognize that a reactor trip does not occur successfully by monitoring the PCS core mimic, the normal IPS display of the core power, and the large display panel display of core power and the reactor trip status.

c. The sequence of operator actions in response to a prompting alarm and subsequent indications is performed by the staff in the control room according to the standard post trip actions (SPTAs) in the emergency operating procedure which is initiated immediately after a manual reactor trip. Since it is common for operators to memorize the post trip actions during the training, this procedure is considered to be highly familiar.

d. The time to execute each mitigating step in the SPTAs is justified based on an evaluation using the methods described in NUREG-0800, Appendix 18-A (Reference 10).

e. In order to determine the total time required for each of the manual actions credited in the evaluation, a sequential time line is constructed to sum up the time interval involved for each operator response performed in series, including the time required for the operator to recognize a CCF has occurred in the safety I&C systems.

8 References

1. APR1400-E-J-NR-14001-P, "Component Interface Module", Rev. 1, February 2017

2. APR1400-Z-A-NR-14019, "CCF Coping Analysis", Rev. 1, February 2017

3. APR1400-Z-J-NR-14001-P, "Safety I&C System", Rev. 1, February 2017

4. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

5. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"

6. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related", April 1985

7. SRM on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs", Item II.Q, "Defense against Common-Mode Failures in Digital Instrumentation and Control Systems", July 1993

8. IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"

9. NUREG-0800, "Standard Review Plan," Chapter 7, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Rev. 6, July 2012

10. NUREG-0800, "Standard Review Plan," Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses", Rev. 0, April 2014

11. Deleted.

12. Deleted.

13. NUREG/CR-6303, "Method for Performing Diversity and Defense-in Depth Analyses of Reactor Protection Systems", December 1994

14. APR1400-Z-J-NR-14003-P, "Software Program Manual", Rev. 1, February 2017

15. 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

16. APR1400 DC Quality Assurance Manual

17. APR1400-K-Q-TR-11005-N, "KHNP Quality Assurance Program Description for the APR1400 Design Certification"

18. ANSI/ANS-58.11-1995 (R2002), "Design Criteria for Safe Shutdown following Selected Design Basis Events in Light Water Reactors"

19. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations"

20. IEEE 100 (Seventh Edition), "The Authoritative Dictionary of IEEE Standards Terms"

9 Definitions

1. Safe shutdown: A unit shutdown with: (1) the reactivity of the reactor kept to a margin below criticality, consistent with technical specifications; (2) the core decay heat removed at a controlled rate, sufficient to prevent core or reactor coolant system thermal design limits from being exceeded; (3) radioactive material releases controlled to keep doses within prescribed limits; and (4) operation within design limits of structures, systems, and components necessary to maintain these conditions. Refer to ANSI/ANS-58.11-1995 (Reference 18). Safe shutdown means hot shutdown unless otherwise specified in this document.

2. Hot shutdown: In a PWR, the condition, consistent with technical specifications, in which the reactor is subcritical and the reactor coolant system average temperature is below the temperature required to permit operation of the residual heat removal system (e.g., 350^{o}F) but above the temperature specified in the technical specification (e.g., 200^{o}F). Refer to ANSI/ANS-58.11-1995 (Reference 18).

3. Functional Programmable Unit: Computer that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computation, including numerous arithmetic or logic operations, without human intervention. Refer to Section 3.1.8 of IEEE Std 7-4.3.2-2003 (Reference 19).

4. Common Software: Common software includes software, firmware, and logic developed from software-based development systems. Refer to Section 1.4 of NUREG-0800, BTP 7-19 (Reference 9).

5. Firmware: The combination of a hardware device and computer instructions and data that reside as read-only software on that device. Refer to the explanation in IEEE 100 (Reference 20). Programmable Logic Devices (PLD), Field Programmable Gate Arrays (FPGA), and Application-Specific Integrated Circuits (ASIC) use software to develop the logic (called 'firmware') that later resides within the digital component. The firmware often cannot be changed in an individual component. Refer to Section 3.8 of NUREG-0800, BTP 7-19.

Page intentionally blank

APPENDIX A. CONFORMANCE TO BTP 7-19, REV. 6

The APR1400 I&C systems are designed with the D3 approaches based on BTP 7-19, Rev. 6. Compliance to the guidance statements provided in BTP 7-19 (Bold and in Italics) is provided as follows:

Section 1.4 Four-Point Position

Point 1

"The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed."

The D3 within the APR1400 I&C systems has been assessed in this report. The potential for CCF is minimized based on software quality and diversity between the echelons of defense and within the echelons of defense. The diversity features in the plant and I&C systems are shown in Table 6-1. Table A-1 provides the diversity between the platforms upon which the I&C systems are implemented and the I&C subsystems that are implemented on each platform.

Point 2

"In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using <u>best-estimate methods</u> The vendor or applicant shall demonstrate adequate diversity within the design for each of these events."

A qualitative and quantitative D3 analyses are provided in the CCF Coping Analysis Technical Report (Reference 2) for each AOO and PA with a concurrent CCF in the safety I&C systems. This analysis uses the best-estimate analysis methods described in Section 7 of this report. Adequate diversity is judged by conformance to the acceptance criteria defined in Section 7.1, which is the same as the acceptance criteria in BTP 7-19. The DAS, which is diverse from the safety I&C systems and therefore not subject to the postulated CCF, is credited in this analysis for accident mitigation.

Point 3

"If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. <u>The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions</u>."

The D3 analysis assumes the CCF completely disables all common safety platform based systems.

The analysis credits that the CIM priority logic, the CIM component control functions, and the component control functions downstream of the CIM are implemented using conventional non-programmable hardware. The CIM is fully testable to ensure it has no defect that could lead to a CCF. The analysis also credits that the DAS are not susceptible to the postulated digital defect that led to a CCF in the safety I&C systems. The details of the analysis are described in the CCF Coping Analysis Technical Report (Reference 2).

Adequate coping is judged solely on the capabilities of the diverse systems which include both automatic and manual actuation functions. The diverse systems are defined as those systems that are not subject to the postulated CCF in the safety I&C systems.

The conclusion that the diverse actuation system (DAS) is not subject to the same CCF that disables the safety I&C systems is based on the diversity (as analyzed using NUREG/CR-6303, Reference 13) between the safety systems and diverse systems, which are described in Section 5.

The DPS, DIS and DMA switches are designed with augmented quality in accordance with GL 85-06. The DIS and DMA switches provide sufficient functionality to allow the operators to take credited manual actions within the time available, as determined by the best estimate accident analysis. The time required to take these credited operator actions is determined through a documented human factors engineering analysis and confirmed through human-systems interface testing.

Point 4

"A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above."

The APR1400 has a set of controls (DMA switches) which provides for diverse manual ESF actuation of critical safety functions, and displays (DIS) for monitoring of parameters that indicate the status of those critical safety functions.

The DMA switches and DIS are diverse from the safety I&C systems and not subject to the same defect that results in a CCF of the safety I&C systems. The controls and displays provided by the DMA switches and DIS are used for achieving and maintaining the plant in a safe shutdown condition. Safe shutdown means hot shutdown for most of plant events. However, some events, such as steam generator tube rupture, require further cooldown and depressurization.

The DIS and DMA switches are sufficient for the operator to monitor and control the following critical safety functions: reactivity control, reactor core cooling and heat removal from the primary system, RCS integrity, and containment isolation and integrity. HFE principles and criteria are applied to the selection and design of the displays and controls.

The DMA switches are hardwired to the CIM downstream of the ESF-CCS.

The CIM employs non-programmable conventional hardware which is demonstrated through testing to have no defect that could lead to a CCF. Therefore, the CIM is credited for accident mitigation using the safety I&C systems or accident mitigation using the diverse systems.

The DIS receives analog inputs from signal splitters/isolators in the APC-S via hardwired interface and displays them on the non-safety dedicated DIS FPD on the MCR safety console. The software associated with the DIS is classified as ITS.

Section 1.5 Manual Initiation of Automatically Initiated Protective Actions Subject to CCF

"If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF affecting the automatically initiated protective action, then under Point 3 of the NRC position on D3, a diverse manual means of initiating protective action(s) would be needed (i.e., two manual initiation means would be needed). This diverse means may be safety or non-safety. If the system/division level manual initiation required by IEEE Std 603-1991 is sufficiently diverse, the diverse (second) manual system level or division level actuation would not be necessary for the automated protective actions."

The same potential defect in the safety I&C systems can lead to a CCF of the automatically initiated ESF protective actions and a CCF of the manually initiated ESF protective actions. Therefore, a second backup means for manual initiation of ESF protective actions is provided through the DMA switches.

The signals from DMA switches have higher priority than the ESF-CCS signals to achieve the ESF actuation independently and diversely from the ESF-CCS. The DMA switches are hardwired directly to fan-out devices in the MCR safety console to distribute the ESF actuation signals to individual component controls. The signals are hardwired to the CIMs downstream of the ESF-CCS.

The CIMs interface with the component control logic in ESF-CCS loop controller. The CIMs prioritize component actuation signals from the ESF-CCS, DPS, and DMA switches.

The CIM is designed using hardware devices so that it is not susceptible to a postulated software CCF. The CIM is implemented on the device that is diverse from safety I&C systems.

Manual reactor trip switches are also hardwired directly to the RTSS.

Section 1.6 D3 Assessment

"Therefore, as set forth in Points 1, 2, and 3 of the NRC position on D3, the applicant should perform a D3 assessment of the proposed DI&C system to vulnerabilities to CCF have been adequately addressed. In this assessment, the applicant may use realistic assumptions to analyze the plant responses to DBEs (as identified in the SAR). If a postulated CCF could disable a safety function that is credited in the safety analysis to respond to the DBE being analyzed, a diverse means of effective response (with documented basis) is necessary. The D3 analysis methods used in ALWR DC applications and for operating plant upgrades are documented in NUREG/CR-6303 (Reference 13), which describes an acceptable method for performing such assessments."

A CCF coping analysis has been performed for each initiating event described in Chapter 15 of the DCD concurrent with a postulated CCF. The results of the coping analysis are presented in the CCF Coping Analysis Technical Report (Reference 2). The plant response to each DBE is shown to meet the applicable acceptance criteria specified in Section 3 of BTP 7-19 by one of the following means:

a. The plant attains a new steady state condition that meets the specified acceptance criteria. No manual or automatic trip/actuation is required.

b. The operator has sufficient time to initiate manual reactor trip and take other credited manual action using the DMA switches to mitigate the AOO or PA.

c. The DPS is relied upon to automatically actuate a diverse protective function (i.e., reactor trip, turbine trip, AFWS actuation, and SIS actuation).

Section 1.7 The Diverse Means

"The primary focus of BTP 7-19 is to identify whether a diverse means of performing protective actions is necessary due to an automated safety function being subject to a postulated CCF. Functions performed manually normally would be expected to still be performed manually in the presence of a CCF (even if different equipment is called upon to function). If the manual actuation method could be adversely affected by the postulated CCF, then a diverse manual means is needed to perform the safety function or an acceptable different function."

The DPS automatically actuates a reactor trip on the following signals:

a. High pressurizer pressure

b. High containment pressure

The DPS also automatically initiates turbine trip signals to the turbine control system. The DPS turbine trip signal is generated with a proper delayed time (e.g., three (3) seconds) from the DPS when the DPS generates a reactor trip signal.

The DPS automatically actuates the AFWS on low steam generator water level in either steam generator separately. The DPS automatically actuates safety injection on low pressurizer pressure. The D3 coping analysis demonstrates that these diverse protective functions are sufficient to ensure the plant response meets the applicable acceptance criteria for every initiating event analyzed.

Section 1.8 Potential Effects of CCF: Failure to Actuate and Spurious Actuation

"There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip or actuation is not required by plant conditions."

"A failure of a system to actuate may not be the worst case failure, particularly when analyzing the time required for identifying and responding to conditions resulting from a CCF in an automated safety system."

"Failures of the automated protection system stemming from a software CCF can cause spurious actuations. The plant design basis addresses the effects of certain software CCF-caused spurious actuations."

"Further, the analysis should identify whether adequate coping strategies, whether for prevention or mitigation, exist for these postulated spurious actuations (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures and the reactor operations team)."

TS

TS

TS

TS

Section 1.9 Design Attributes to Eliminate Consideration of CCF

"Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF:

<u>Diversity</u> or <u>Testability</u>

(1) Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within channels can be considered to be appropriately addressed without further action.

(2) Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case."

The response to Point 1 position of BTP 7-19 describes the features of the PPS, ESF-CCS and QIAS-P that minimize the potential for a CCF. Despite those features, a defect that results in a CCF for all PPS, ESF-CCS and QIAS-P functions is assumed in the CCF coping analysis to address Point 2 position of BTP 7-19. The DPS, DIS and DMA switches provide diverse equipment to cope with the postulated CCF in the safety systems. The DPS and DIS are demonstrated to be diverse from the safety systems, through the diversity analysis provided to address Point 3 and 4 positions of BTP 7-19, respectively.

The only safety components for which a design defect leading to a CCF is not assumed are the following:

a. Sensors

b. APC-S

c. CIM

These components are shared by both the safety systems and the diverse backup systems. To eliminate consideration of a CCF, these components use only conventional analog or binary logic technology (i.e., no software-based processing). In addition, the sections of the CIM that are relied upon for both the safety systems and the diverse systems are tested.

Table A-1 Diverse Platforms of I&C Systems

Platform	Subsystems	Comments
Common Safety PLC	PPS Bistable Processor PPS LCL Processor CPCS Processor RT Selective 2-out-of-4 Logic ESF-CCS GC and LC EDG Sequencer (Shed and Load) QIAS-P Controller QIAS-N Controller Operator Module (OM) Control Panel Multiplexers (CPM) ESF-CCS Soft Control Module (ESCM) Maintenance and Test Panel (MTP) Interface and Test Processor (ITP)	Digital system with operating system software and application software developed or commercially dedicated according to IEEE Std 7-4.3.2
Non-Safety DCS	Power Control System NSSS Process Control System BOP Process Control Process - Component Control System (P-CCS) Process Soft Control Workstation Information Processing System (IPS)	Digital system with operating system software and application software that is totally diverse from the common safety PLC
FLC	Diverse Protection System (DPS) Diverse Indication System (DIS)	FPGA-based digital systems without CPU and operating system software
Hardware Based Modules	APC-S Diverse manual ESF actuation (DMA) switches Component Interface Module (CIM) EDG Starting Circuit Ex-core Neutron Flux Monitoring System (ENFMS)	The platform is not a PLC based or implemented on an FPGA, but may not be analog circuitry (e.g., discrete integrated logic circuitry).
Analog Based Modules	Sensors ESF Component Actuated Devices Reactor Trip Switchgear Emergency Diesel Generator (EDG) EDG Output Breakers Offsite AC Power Crosstie Breakers Safety Channel Batteries Safety Channel Inverters	No software involved

APPENDIX B. CONFORMANCE TO 10 CFR 50.62

The DPS provides the ATWS mitigation functions required by 10 CFR 50.62. This appendix describes the conformance of the DPS to the requirements of 10 CFR 50.62 (Reference 5). Italic text in this appendix indicates the extracted requirements from 10 CFR 50.62.

(1) "Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system."

The DPS provides automatic turbine trip and AFWS actuation. Figure 4-2 shows the simplified architecture for diverse automatic AFWS actuation and for the diverse automatic turbine trip. The DPS AFWS actuation is automatically actuated on low steam generator water level in either steam generator.

The DPS turbine trip is also automatically initiated whenever the DPS reactor trip has been actuated. The DPS turbine trip signal will be generated after the initiation of DPS reactor trip signal with three seconds of time delay.

The common safety PLC based platform is used for the reactor trip in the PPS. The DPS is implemented on a FLC platform which is diverse form the common safety PLC platform.

The DPS is designed to perform its function in a fault-tolerant manner, and it is independent from sensor outputs to the shunt trip relays of the RTSS.

(2) "Each pressurized water reactor must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods)."

The reactor trip function from the PPS is diverse and independent from the reactor trip function provided by the DPS. The simplified architecture between the reactor trip function from the PPS and diverse reactor trip function from the DPS is shown in Figure 4-2. A DPS reactor trip function is automatically actuated by high pressurizer pressure, high containment pressure, or turbine trip (only if the RPCS is out of service).

a. The common safety platform is used for the reactor trip in the PPS. The diverse reactor trip is provided by the DPS implemented on a diverse FLC platform.

b. The reactor trip from the PPS breaks the power of the CEDM using the undervoltage trip coils of the reactor trip circuit breakers. The diverse reactor trip from the DPS breaks the power of the CEDM using the shunt trip coils of the reactor trip circuit breakers.

c. The RTSS-1 and RTSS-2 reactor trip breakers are diverse each other to ensure that a diverse means exists to break power to the CEDMs.

d. The process instrumentation (PI) sensors for the safety I&C systems are shared by the DPS. The PI sensor signals are electrically isolated in the APC-S prior to being hardwired to the DPS.

(3) "To develop QA guidance for non-safety-related ATWS equipment, the NRC staff both surveyed quality practices applied to non-safety-related equipment at some operating

plants and reviewed the comments from utilities, industry organization, and other concerned parties. As a result, the staff continues to view the observed industry practices as acceptable for non-safety-related ATWS equipment. The practices that were observed during the plant visits or were described by utilities in their comments generally consisted of the application of quality controls comparable to selected portions of their Appendix B program. However, utility procedures and practices did not specifically reference such controls as Appendix B requirements.

The DAS is designed to meet the quality assurance guidance of GL 85-06 to maintain sufficient quality to perform the necessary functions. The software associated with DAS is qualified as ITS defined in the Software Program Manual, Quality Assurance Manual (Reference 14) and Quality Assurance Program Description (Reference 15).

(4) The QA controls in Appendix B to 10 CFR 50 describe one form of a comprehensive management control system for a complex task. While Appendix B describes only one such system, licenses and applicants have expressed a desire to minimize proliferation of different kinds of management control systems for their plants. The NRC staff concurs with this desire not to establish new and separate management control systems for non-safety-related ATWS equipment.

The DAS is designed to meet the quality assurance guidance of GL 85-06 to maintain sufficient quality to perform the necessary functions. The software associated with DAS is qualified as ITS defined in the Software Program Manual, Quality Assurance Manual (Reference 14) and Quality Assurance Program Description (Reference 15).

(5) The enclosure to this letter provides the explicit QA guidance required by 10 CFR 50.62. The lesser safety significance of the equipment encompassed by 10 CFR 50.62, as compared to safety-related equipment, necessarily results in less stringent QA guidance. We have incorporated this lesser degree of stringency by eliminating requirements for involvement of parties outside the normal line organization and requirements for a formalized program and detailed recordkeeping for all quality practices."

The DAS is designed to meet the quality assurance guidance of GL 85-06 to maintain sufficient quality to perform the necessary functions. The software associated with DAS is qualified as ITS defined in the Software Program Manual, Quality Assurance Manual (Reference 14) and Quality Assurance Program Description (Reference 15).

APPENDIX C. CONFORMANCE TO NUREG/CR-6303 GUIDELINES

This appendix provides an evaluation of the conformance of the APR1400 architecture features to the guidelines presented in NUREG/CR-6303 (Reference 13). Figure 4-1 provides the block level I&C architectural overview of the APR1400 I&C systems.

1. "Guideline 1 – Choosing Blocks"

The Guideline 1 states that "the main criterion for selecting blocks is that the actual mechanism of failure inside a block should not be significant to other blocks." Based on the guideline, the I&C systems are categorized into five major blocks implemented on the diverse platforms, such as common safety PLC, FPGA, non-safety DCS, hardware based modules and analog based modules, as shown in Table A-1.

The systems implemented on common safety PLC are reactor trip system (RTS), ESF-CCS, QIAS-P; and QIAS-N. The DPS and DIS are implemented on FPGA. The IPS and non-safety control system are implemented on DCS.

The D3 analysis assumes the total functional loss of common safety PLC based systems in case of a CCF in the block and normal operation of the other systems since the CCF in the common safety PLC block does not propagate and is not significant to the other diverse blocks.

A brief description of each of these systems is provided.

a. Reactor Trip System

The RTS includes the CPCS and the hardwired manual reactor trip controls.

The automatic reactor trip functions are:

i. Variable Overpower

ii. High Logarithmic Power Level

iii. High Local Power Density

iv. Low Departure from Nucleate Boiling Ratio

v. High Pressurizer Pressure

vi. Low Pressurizer Pressure

vii. High Steam Generator Water Level

viii. Low Steam Generator Water Level

ix. Low Steam Generator Pressure

x. Low Reactor Coolant Flow

xi. High Containment Pressure

The automatic RTS actuation signal path is segregated into the following blocks:

i. Sensors

ii. APC-S and CPCS

iii. Bistable Processor

iv. Local Coincidence Logic (LCL) Processor

v. Selective 2-out-of-4 Logic

vi. Reactor Trip Switchgear

Remote manual switches are also provided in the MCR for manual reactor trip. These switches are hardwired directly to the RTSS.

b. Engineered Safety Features – Component Control System (ESF-CCS)

The ESF-CCS includes the automatic ESFAS system-level actuation system functions; the manual ESF system-level actuation switches; the ESF component-level controls; and the manual component-level ESF-CCS soft control module (ESCM) controls.

The automatic ESFAS system-level actuation signals are

i. Safety Injection Actuation Signal (SIAS)

- Low Pressurizer Pressure (Wide Range: WR)
- High Containment Pressure (Narrow Range: NR)

ii. Containment Isolation Actuation Signal

- Low Pressurizer Pressure (WR)
- High Containment Pressure (NR)

iii. Containment Spray Actuation Signal

- High-High Containment Pressure (WR)

iv. Main Steam Isolation Signal

- High Containment Pressure (NR)
- Low Steam Generator Pressure
- High Steam Generator Level (NR)

v. Auxiliary Feedwater Actuation Signal 1

- Low Steam Generator 1 Level (WR)

vi. Auxiliary Feedwater Actuation Signal 2

- Low Steam Generator 2 Level (WR)

vii. Control Room Emergency Ventilation Actuation Signal

- Low Pressurizer Pressure (WR)
- High Containment Pressure (NR)

viii. Fuel Handling Area Emergency Ventilation Actuation Signal

- High Spent Fuel Pool Area Radiation Level

ix. Containment Purge Isolation Actuation Signal

- High Containment Operating Area Radiation Level

The automatic ESFAS actuation signal path is segregated into the following blocks:

i. Sensors

ii. APC-S

iii. Bistable Processors

iv. LCL Processors

v. ESF-CCS (including Component Control Logics)

vi. CIM

vii. ESF Components

Remote manual hardwired switches are also provided in the MCR for manual ESF system-level actuation and component-level control of ESF components.

The remote manual hardwired switches provided for the ESF system-level actuation include the following system-level controls:

i. Safety Injection Actuation (Divisions A, B, C, and D)

ii. Containment Spray Actuation (Divisions A, B, C, and D)

iii. Auxiliary Feedwater Actuation (Divisions A, B, C, and D for SG 1)

iv. Auxiliary Feedwater Actuation (Divisions A, B, C, and D for SG 2)

v. Containment Isolation Actuation (Divisions A, B, C, and D)

vi. Main Steam Isolation (Divisions A, B, C, and D)

vii. Main Steam Isolation (Divisions A and B in RSR only)

The remote manual hardwired switches for component-level ESF component control consist of the minimum inventory (MI) switches for ESF components necessary to achieve and maintain a safe reactor shutdown following an initiating event.

The ESF system-level actuation and component-level MI switch signals are input to the CPM and then data linked to the ESF-CCS, i.e., the signals are susceptible to a postulated CCF.

c. Qualified Indication and Alarm System – P

The QIAS-P displays the RG 1.97, Rev. 4, Types A, B, and C variables. The Types A, B and C variables are displayed on the QIAS-P display device on the MCR safety console. The QIAS-P is implemented on the same platform as the safety I&C system, but the software is classified as ITS.

The variables displayed on QIAS-P display device are as follows:

i. Pressurizer Pressure (WR)

ii. Pressurizer Level

iii. Hot Leg Temperature (WR)

iv. Cold Leg Temperature (WR)

v. Steam Generator 1 Pressure

vi. Steam Generator 2 Pressure

vii. Steam Generator 1 Level (WR)

viii. Steam Generator 2 Level (WR)

ix. Logarithmic Reactor Power

x. Core Exit Temperature

xi. RCS Subcooling Margin

xii. CET Subcooling Margin

xiii. RV Upper Head Subcooling Margin

xiv. Reactor Vessel Level

xv. RCS Pressure

xvi. Containment Pressure (Extended Range)

xvii. Containment Pressure (WR)

xviii. Containment Level

xix. Containment Operating Area Radiation

xx. Containment Upper Operating Area Radiation

xxi. Containment Isolation Valve Position

xxii. IRWST Level

xxiii. IRWST Temperature

xxiv. Holdup Volume Tank Level

xxv. Spent Fuel Pool Radiation

xxvi. SIP DVI Flow Rate

xxvii. Reactor Cavity Level

xxviii. MS ADV Position

xxix. Auxiliary Feedwater Flow

In addition to the above displayed variables, several parameters are calculated from those variables and displayed on QIAS-P display device. These include:

i. Representative Core Exit Temperature

ii. Highest CET Temperature (Quadrant 1, 2, 3, 4)

iii. Next Highest CET Temperature (Quadrant 1, 2, 3, 4)

iv. Temperature Saturation Margin (Upper Head, RCS, CET)

v. Pressure Saturation Margin (Upper Head, RCS, CET)

vi. Differential Junction Temperature

vii. Heated Junction Thermocouple Relative Liquid Inventory (1 thru 8)

viii. Liquid Reactor Vessel Level (Head, Plenum)

The QIAS-P display path for Types A, B and C is segregated into the following blocks:

i. Sensors

ii. APC-S

iii. QIAS-P Processor

iv. QIAS-P Display Device

d. Qualified Indication and Alarm System – Non-Safety

The QIAS-N displays the RG 1.97, Rev. 4, Types A, B, C, D, and E variables. The QIAS-N is implemented on the same platform as the QIAS-P, but is non-safety system and seismically qualified.

The QIAS-N variables include the Types A, B, and C variables of QIAS-P in addition to the Types D and E variables.

The variables also constitute the minimum inventory of variables necessary to monitor the status of the plant critical safety functions, and to provide information to the operator concerning the need to manually actuate a manual reactor trip or ESFAS protective function.

The QIAS-N display path is segregated into the following blocks:

i. Sensors

ii. APC-S / IPS

iii. QIAS-P Controller / Gateway

iv. Interface and Test Processor (ITP) / QIAS-N Maintenance and Test Panel (MTP)

v. QIAS-N Controller

vi. QIAS-N Display Device

e. Diverse Actuation System (DAS)

The DAS includes the diverse automatic reactor trip functions and the diverse automatic ESFAS functions (DPS), the diverse indication system (DIS) and the hardwired diverse manual ESF actuation (DMA) switches. The DAS is implemented on a platform that is diverse from the safety I&C systems.

The DPS automatic reactor trip functions are initiated on the following signals:

i. High Pressurizer Pressure

ii. High Containment Pressure

iii. Turbine Trip

The DPS automatically actuates turbine trip upon the DPS reactor trip (with time delay) due to the following reactor trip actuation signals:

i. DPS Reactor trip on High Pressurizer Pressure

ii. DPS Reactor trip on High Containment Pressure

The DPS automatically actuates the following diverse ESF functions:

i. Safety Injection Actuation Signal

- Low Pressurizer Pressure (WR)

ii. Auxiliary Feedwater System Actuation Signal 1

- Low Steam Generator 1 Level (WR)

iii. Auxiliary Feedwater System Actuation Signal 2

- Low Steam Generator 2 Level (WR)

The hardwired DMA switches include:

i. Safety Injection Actuation (2 switches)

ii. Containment Spray Actuation (2 switches)

iii. Auxiliary Feedwater System Actuation (1 switch for SG 1)

iv. Auxiliary Feedwater System Actuation (1 switch for SG 2)

v. Main Steam Isolation (2 switches for SG 1)

vi. Main Steam Isolation (2 switches for SG 2)

vii. Containment Isolation Actuation (2 switches)

viii. Auxiliary Feedwater Flow / Steam Generator 1 Level (1 switch)

ix. Auxiliary Feedwater Flow / Steam Generator 2 Level (1 switch)

The DIS displays the following variables

i. Inadequate Core Cooling (ICC) Monitoring Information

- Upper Head Temperature Saturation Margin
- Upper Head Pressure Saturation Margin – Plenum
- RCS Temperature Saturation Margin
- RCS Pressure Saturation Margin
- CET Temperature Saturation Margin
- CET Pressure Saturation Margin
- Representative Core Exit Temperature
- Reactor Vessel Level – Head
- Reactor Vessel Level – Plenum
- Upper Head Temperature

ii. Accident Monitoring Information

- Reactor Power
- RCS Hot Leg Temperature
- RCS Cold Leg Temperature
- RCS Pressure
- Pressurizer Pressure
- Pressurizer Level
- Steam Generator 1 Wide Range (WR) Level
- Steam Generator 2 WR Level
- Steam Generator 1 WR Pressure
- Steam Generator 2 WR Pressure
- AFW Flow to Steam Generator 1
- AFW Flow to Steam Generator 2
- AFW Storage Tank A Level
- AFW Storage Tank B Level
- Containment Pressure
- Containment Water Level
- Containment Temperature
- Containment Hydrogen Concentration
- Containment Area Radiation
- In-Containment Refueling Water Storage Tank (IRWST) Level
- IRWST Temperature
- IRWST Hydrogen Concentration

iii. Emergency Operation-related Information

- SI Flow to Direct Vessel Injection A
- SI Flow to Direct Vessel Injection B
- Charging Flow
- Containment Spray Flow
- Safety Injection Tank (SIT) 1 WR Pressure
- Aux Building Sump Level

The DPS reactor trip signal path is segregated into the following blocks:

i. Sensors

ii. APC-S

iii. DPS Signal Processing Modules

iv. Reactor Trip Breakers (Shunt Trip Devices)

The DPS ESF actuation signal path is segregated into the following blocks:

i. Sensors

ii. APC-S

iii. DPS Signal Processing Modules

iv. CIM

v. ESF Components

The DMA signal paths are segregated into the following blocks:

i. Hardwired Switches

ii. CIM

iii. ESF Components

The DIS signal display path is segregated into the following blocks:

i. Sensors

ii. APC-S / QIAS-P

iii. DIS Processor

iv. DIS Display

f. Information Processing System (IPS)

The IPS displays all sensor values; specified calculated parameters; system status; plant alarm system information; sequence of event time history; and nuclear application programs (NAPS) information on the information FPD (IFPD).

The IPS obtains its information from the following blocks:

i. QIAS-N

ii. MTP

iii. DPS

iv. DIS

v. Control and Monitoring Systems

vi. Other Non-safety Systems (e.g., NIMS, FIDAS)

All the above subsystems have a gateway or data link to the DCN-I network. The IFPD can then display any of the data on the DCN-I network. The IPS is implemented on a platform that is diverse from the safety I&C systems. However, the signals received from QIAS-N and the MTP may be degraded due to a postulated CCF in the protection system. The signals from the other blocks are not susceptible to a postulated CCF in the protection system.

g. Control Systems

The control system includes the PCS and the P-CCS. The control system is implemented on a non-safety DCS platform that is diverse from the safety I&C systems.

h. Class 1E Power System

The Class 1E power system includes the EDG; the off-site AC power crosstie breakers; the vital bus load shed breakers; EDG starting circuit ; the EDG output breaker; the vital bus batteries; and the vital bus inverters.

The Class 1E power system is segregated into the following blocks:

i. Vital Bus Voltage Sensors

ii. EDG Starting Circuit

iii. ESF-CCS Group Controller (including EDG Loading Sequencer, EDG Load Shedding)

iv. ESF-CCS Loop Controller (including Component Control Logics)

v. CIM

vi. ESF Components

2. “Guideline 2 – Determining Diversity”

The APR1400 I&C systems are implemented on five major platforms. The platforms and the subsystems implemented on them are summarized in Table A-1.

NUREG/CR-6303 (Reference 13) discusses six diversity attributes. The attributes are listed below with a brief description of each attribute provided.

a. Design

Different technologies, different approaches, different architecture

b. Equipment

Different manufacturers of different designs

c. Functional

Different underlying mechanism, different function

d. Human

Different design organization, different management team, different designers

e. Signal

Different process parameters, different redundant sensors

f. Software

Different algorithms, different operating system, different computer language

Table C-1 provides a summary of the diversity attributes that are shared in the design of the five different platforms used in the implementation of the plant I&C systems.

Table C-1 Diversity Attributes Between I&C System Platforms

Diverse I&C Platforms (Refer to Table A-1.)		Diversity Attributes against Common Safety PLC Platform					
		Design	Equipment	Functional	Human	Signal	S/W
Non-Safety DCS		O	O	O	O	O	O
FPGA	DPS	O	O	O	O		O
	DIS	O	O		O		O
Hardware Based Device (CIM)		O	O		O		N/A
Analog (Actuator)		O	O		O		N/A
Analog (Sensor)		O	O		O		N/A

O: Diverse, N/A: Not Applicable

Explanatory Notes:

a. The information provided in the table is with respect to the diversity features shared between the platforms, i.e., the reader should observe the information in each column for each diversity feature.

b. Non-safety DCS platform has functional diversity against the common safety PLC platform. The common safety PLC platform provides ON/OFF trip and monitoring functions, whereas the non-safety DCS platform provides continuous control and monitoring functions.

c. A different design team from the common safety PLC design team is responsible for the design of DPS and DIS, and the systems implemented on the Non-safety DCS platform. Detailed analysis results of diversity attributes between the DPS and the PPS are described in Section 6.2.

d. PPS sensor signals are also used in Non-safety DCS systems through qualified isolators.

e. Sensors and APC-S are shared by both PPS and DPS. The analog sensors and APC-S are analog equipment, and they are not affected by the software CCF.

f. There is no commonality in software modules used among the common safety PLC platform, the Non-safety DCS, and the FPGA platforms. Therefore, the occurrence of concurrent CCF of different platform equipment is not considered in the D3 analysis.

g. There are a few areas in which several diversity attributes are shared between platforms, but that is only because more than one platform is used within an actuation path. For example, for an ESFAS actuation path, the instrumentation channel contains analog sensors, APC-S, PPS, ESF-CCS, CIM, electrical panel, and ESF actuated devices. The complete instrumentation channel is designed within the same safety group, so there is human commonality in the design of the applicable modules.

h. Reactor trip mechanism of the DPS is diverse from that of the PPS. In addition, trip setpoints of the DPS are different from those of the PPS. Therefore, some functional diversity features are provided between the DPS and the PPS.

The RTS and ESFAS functions are implemented on the same common safety PLC platform. Hence, a postulated CCF in the common safety PLC platform could degrade both the reactor trip and ESFAS functions. However, BTP 7-19, Section 1.3, states

"NRC regulations do not require nor does the guidance imply that RTS and ESFAS echelons of defense must be independent or diverse from each other with respect to a CCF."

Based upon the above diversity evaluation, it is concluded that sufficient diversity exists between the platforms/devices such that they can be categorized as diverse.

3. "Guideline 3 – System Failure Types"

NUREG/CR-6303 (Reference 13) defines three different failure types.

a. Type 1 Failures : Interaction between echelons of defense

The APR1400 I&C systems include many features that preclude the occurrence of a Type 1 failure. There are no sensors shared between the plant control system echelon and the reactor trip and ESF echelon of defense (except sensors for DPS, which are shared with safety I&C systems). Therefore, a failure of an input sensor to the control system echelon has no impact on the reactor trip echelon and the ESF echelon of defense.

In addition, even though the reactor trip and ESF echelons of defense share sensor inputs, the sensor signals are split in the non-software based APC-S module and hardwired independently to the reactor trip bistable module and the ESF bistable module. Hence, a postulated failure in an input signal module in the reactor trip echelon of defense does not degrade the input signal to the ESF echelon of defense.

b. Type 2 Failures : Failures of safety I&C systems to respond upon demand

Table C-1 illustrates the diversity of the platforms utilized in the APR1400 plant I&C systems. As indicated, the plant control system platform is diverse from the reactor trip and ESF platform. The reactor trip and ESF functions share a common platform. The DAS is implemented on a platform that is not susceptible to a postulated CCF in the protection system. As demonstrated in the CCF Coping Analysis Technical Report (Reference 2), the plant response to an initiating event concurrent with a postulated CCF in the safety platform meets the acceptance criteria specified in Section 3 of BTP 7-19. The diverse functions implemented on DAS and the plant control systems are credited for mitigating the initiating event such that the acceptance criteria are met.

c. Type 3 Failures : Failure of sensors to detect abnormal conditions

These types of failures occur when the consequences of the initiating event result in the failure of sensors to detect abnormal conditions in the plant. The initiating event may result in anomalous indications due to plant conditions following the initiating event. For example, the inadvertent opening of a pressurizer safety valve due to a mechanical failure could result in an indicated high pressurizer water level even though the initiating failure eventually results in an actual low water level. Even though the display in the control room potentially provides ambiguous information to the operator, functionally diverse sensors are installed to address this type of failure. The initiating failure eventually results in uncovering the core if the SIAS is not actuated. The SIAS is actuated on low pressurizer pressure which is not degraded by an uncontrolled steam/water release from the top of the pressurizer. Hence, an automatic SIAS signal is generated on low pressurizer pressure and the water level in the RCS is maintained such that no core damage occurs.

No scenarios have been identified in which the consequences of the initiating event results in degradation of the sensed process variable such that an automatic or manual ESFAS function is not actuated. This type of failure is not a problem on the APR1400 due to the diversity of process variable input to the reactor trip and ESFAS protective functions.

4. "Guideline 4 – Echelon Requirement"

The RTS, ESF-CCS, QIAS-P and QIAS-N are implemented on the common safety PLC platform. The DPS is implemented on a FLC platform. The non-safety FLC platform, the DCS platform and the common safety PLC platform are diverse as illustrated in Table C-1. Hence, a postulated CCF in the common safety PLC platform could degrade the reactor trip, ESFAS, and safety monitoring echelons of defense.

However, sufficient diversity exists for the functions implemented on DAS (i.e., DPS, DIS and DMA switches) and the plant control systems such that for each initiating event concurrent with a postulated CCF, the plant response meets the applicable acceptance criteria as specified in Section 3 of BTP 7-19. The plant transient results are presented in the CCF Coping Analysis Technical Report (Reference 2).

5. "Guideline 5 – Method of Evaluation"

All initiating events (AOO and PA) that are evaluated in the APR1400 Chapter 15 of the DCD are also evaluated concurrent with a postulated CCF using "best-estimate methods" as discussed in BTP 7-19, Point 2. The "best-estimate" assumptions and initial conditions utilized in the analysis are described in Section 7.1.

The acceptance criteria that must be met are specified in Section 3 of BTP 7-19.

The transient analyses assume that the postulated CCF occurs simultaneously in all software blocks that contain the same or identical software, i.e., in all redundant safety channels. A software block is chosen to be at the processor level (e.g., bistable processor, LCL processor, ESF-CCS processor, etc.) in an effort to view the CCF "at a level of abstraction that eliminates superfluous detail." Each software block is treated as a "black box" and the consequences of a postulated CCF are only addressed for the inputs and outputs of the block.

6. "Guideline 6 – Postulated Common-Cause Failure Blocks"

The CCF coping analysis assumes that the postulated CCF occurs simultaneously in all software blocks that contain the same or identical software, i.e., in all redundant safety channels. Two failure modes are evaluated:

a. postulated CCF that results in all common block outputs to fail low (i.e., failure to respond)

b. postulated CCF that results in all common block outputs to fail high (i.e., spurious trip or actuation).

7. "Guideline 7 – Use of Identical Hardware and Software Modules"

The APR1400 architecture has four redundant safety channels in the RTS and the ESFAS. For the purposes of the D3 evaluation, the software blocks that perform similar functions in all four channels (e.g., bistable logics, 2-out-of-4 voting logics) are assumed to use the same or identical blocks. Hence when a failure of a software block is postulated, the identical blocks in all four channels are assumed to fail in a similar manner.

8. "Guideline 8 – Effect of Other Blocks"

Only one postulated CCF is postulated to occur in similar or identical blocks. All other software blocks are expected to operate as designed during the evaluation in response to the output of the failed software block.

9. "Guideline 9 – Output Signals"

The analysis assumes a postulated failure in the software block such that one or more output signals either fail high or fail low. However, a software failure assumed in similar blocks results in the output signals for all similar blocks failing to the same failure mode. For example, for a BP module, all bistable outputs are assumed to either fail high or fail low, i.e., random failures are not assumed for similar software block output signals.

10. "Guideline 10 – Diversity for Anticipated Operational Occurrences"

Each AOO analyzed in the Chapter 15 of the DCD is analyzed concurrent with a postulated CCF. The results of the D3 analyses are described in the CCF Coping Analysis Technical Report (Reference 2). The following diverse manual and automatic functions are credited in order to meet the applicable acceptance criteria provided in Section 3 of BTP 7-19.

a. Reactor trip on high pressurizer pressure and high containment pressure

b. Reactor trip on turbine trip (if the RPCS is out of service only)

c. AFWS actuation on low steam generator level in either steam generator

d. Turbine trip on reactor trip

e. Safety Injection actuation on low pressurizer pressure

f. Manual reactor trip switches

11. "Guideline 11 – Diversity for Accidents"

Each postulated accident (PA) analyzed in the Chapter 15 of the DCD is analyzed concurrent with a postulated CCF. The results of the D3 analyses are described in the CCF Coping Analysis Technical Report (Reference 2). The following diverse automatic and manual ESFAS functions are credited in order to meet the applicable acceptance criteria presented in Section 3 of BTP 7-19.

a. AFWS actuation on low steam generator level in either steam generator

b. Safety injection system actuation on low pressurizer pressure

c. Reactor trip on high pressurizer pressure, high containment pressure, and turbine trip (only if RPCS is out of service)

d. Turbine trip on reactor trip

e. Manual system-level SIAS actuation

f. Manual system-level CS actuation

g. Manual AFWS actuation

h. Manual component-level steam generator #1 steamline isolation

i. Manual component-level steam generator #2 steamline isolation

j. Manual system-level Containment Isolation

12. "Guideline 12- Diversity among Echelons of Defense"

The diversity characteristics between the five platforms upon which plant I&C systems are implemented are provided in Tables A-1 and C-1.

13. "Guideline 13 - Plant Monitoring"

The DIS is implemented on a diverse platform from the common safety PLC platform upon which the QIAS-P is implemented. The DIS indications are listed in the response to Guideline 1, item (c).

14. "Guideline 14 - Manual Operator Action"

Point 4 of BTP 7-19 requires

"A set of … controls located in the main control room … for manual, system-level actuation of critical safety functions."

A set of hardwired controls are implemented on the DMA switches that are hardwired directly to the CIM. The controls by DMA switches are listed in the response to Guideline 1, item (e).

The operator response time assumed in the evaluation of the AOOs and PAs is provided in the CCF Coping Analysis Technical Report (Reference 2).