Diversity and Defense-in-Depth (D3)

Topical Report

Applicable Codes & Regulations

System Description

Echelons of Defense

Diverse Protection System

Diverse Indication System

Diverse Manual ESF Actuation (DMA) Switches

Diversity & Defense-in-Depth Analysis

D3 Coping Analysis Method

Conformance to BTP 7-19

Conformance to 10 CFR 50.62

Summary

1 Topical Report

Topical Report (1/2)

Proposed Table of Contents

- Purpose
- Scope
- Applicable codes and regulations
- I&C system description
- Diverse Actuation System (DAS)
- Diversity and Defense-in-Depth (D3) analysis
- D3 coping analysis method
- References
- Appendix A. Conformance to BTP 7-19
- Appendix B. Conformance to 10 CFR 50.62

Topical Report (2/2)

D3 Analysis Comparison

Item/Project		YGN5&6	UCN5&6	SKN3&4	APR1400	Remark
Plant Protection System (PPS)		Analog	PLC(Common-Q)	PLC(Common-Q)	PLC	
Control System		PLC(Omron)	PLC(Omron)	DCS(Ovation)	DCS	
Diverse Protection System(DPS)		PLC(Modicon)	PLC(Modicon)	DCS(Ovation)	DCS	
Diverse Indication System (DIS)		x	x	DCS(Ovation)	DCS	
Diverse Manual ESF Actuation(DMA)		x	H/W SW.	H/W SW.	H/W SW.	
DPS Output Signals	ATWS	RT	RT	RT	RT	PZR PR
		AFAS	AFAS	AFAS	AFAS	S/G LVL
	D3	x	RT	RT	RT	CNMT PR (MSLB)
		x	x	x	SIAS	PZR PR (LBLOCA)
D3 Analysis TR		x	Done	Done	To be submitted	

2 Applicable Codes & Regulations

Applicable Codes and Regulations (1/2)

Applicable Codes and Standards

- 10 CFR 50
  - 10 CFR 50.62
  - 10 CFR Part 50 Appendix A, General Design Criteria
- Staff Requirements Memorandum
  - SECY-93-087, II. Q, Defense against Common-Mode Failures in Digital Instrumentation and Control Systems
- Regulatory Guides
  - RG 1.62, Manual Initiation of Protection Action
  - RG 1.75, Criteria for Independence of Electrical Systems
  - RG 1.105, Setpoints for Safety-Related Instrumentation
  - RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
  - RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C

Applicable Codes and Regulations (2/2)

Applicable Codes and Standards

- BTP 7-19, Guidance on Evaluation of D3 in Digital Computer Based I&C Systems
- SRP Ch. 18, Appendix 18-A, Crediting Manual Operator Actions in D3 Analysis
- NUREG/CR-6303, Method for Performing Diversity and Defense-in Depth Analyses of Reactor Protection Systems
- ANSI/ANS 58.8, Time Response Design Criteria for Safety-related Operator Actions
- GL 85-06, Quality Assurance Guidance for ATWS Equipment that is not safety related

3 System Description

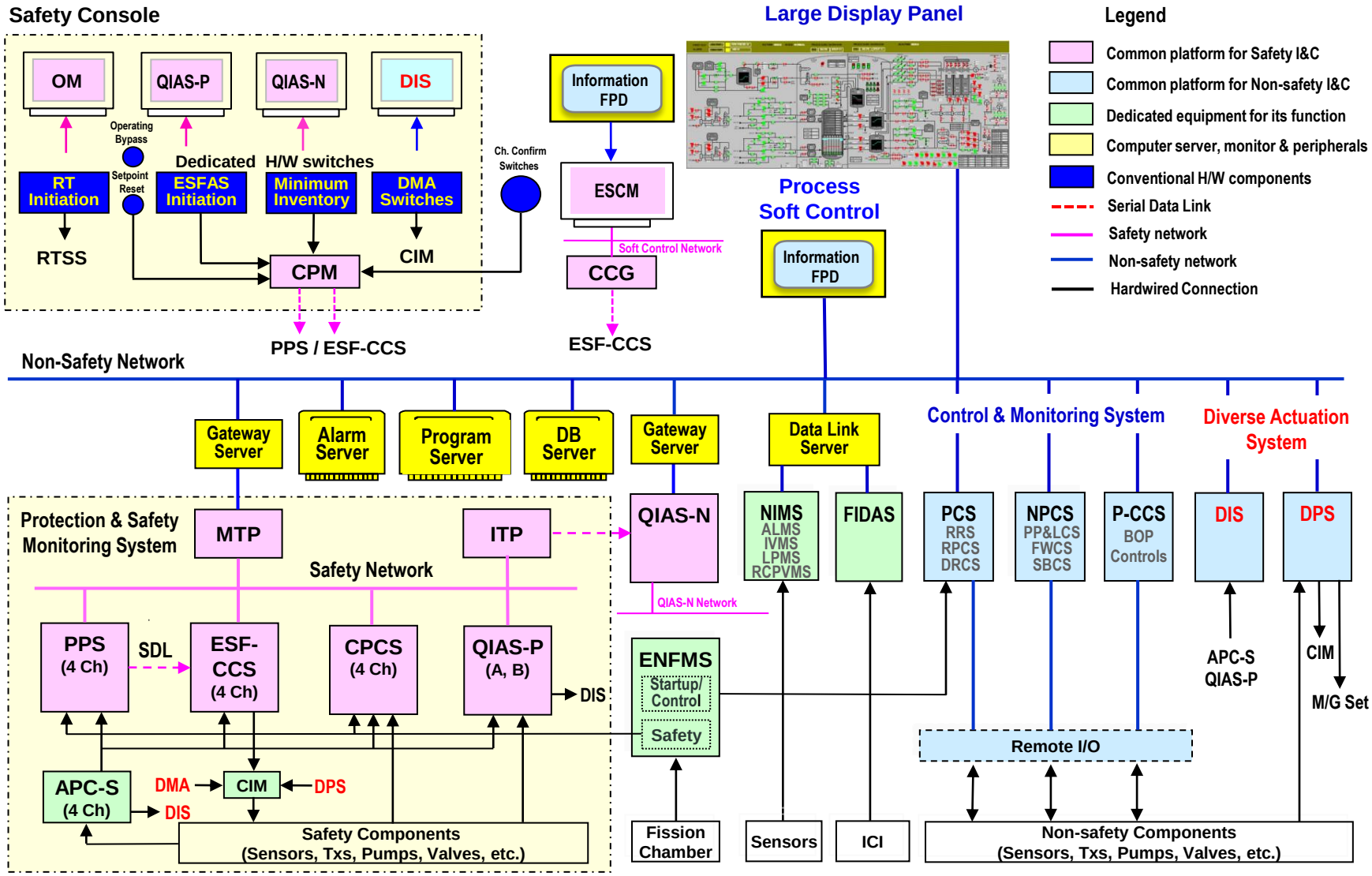
System Description (1/2)

I&C Systems

- Protection & Safety Monitoring System
  - PPS, ESF-CCS, CPCS, QIAS-P (based on PLC)
- Control & Monitoring System
  - QIAS-N (based on PLC)
  - PCS, NPCS, P-CCS (based on DCS)
- Diverse Actuation System
  - DPS, DIS (based on DCS), DMA SW. (conventional switch)
- Dedicated System
  - ENFMS, APC, NIMS, CIM (based on different platform)
- Human-System Interface System
  - MCR, RSR
- Data Communication Network
  - Safety Network and Serial Data Link
  - Non-Safety Network

System Description (2/2)

Overall I&C Architecture



APC-S : Auxiliary Process Cabinet – Safety, CIM : Component Interface Module, CPCS : Core Protection Calculator System, DIS : Diverse Indication System, DMA : Diverse Manual ESF Actuation, DPS : Diverse Protection System, ENFMS : Ex-core Neutron Flux Monitoring System, ESCM : ESF-CCS Soft Control Module FIDAS : Fixed In-core Detector Amplifier System, ICI : In-Core Instrumentation , NIMS : NSSS Integrity Monitoring System, NPCS : NSSS Process Control System, OM : Operator Module, P-CCS : Process Component Control System, PCS : Power Control System, QIAS-P/N : Qualified Indication & Alarm System - PAMI / Non-safety

4 Echelons of Defense

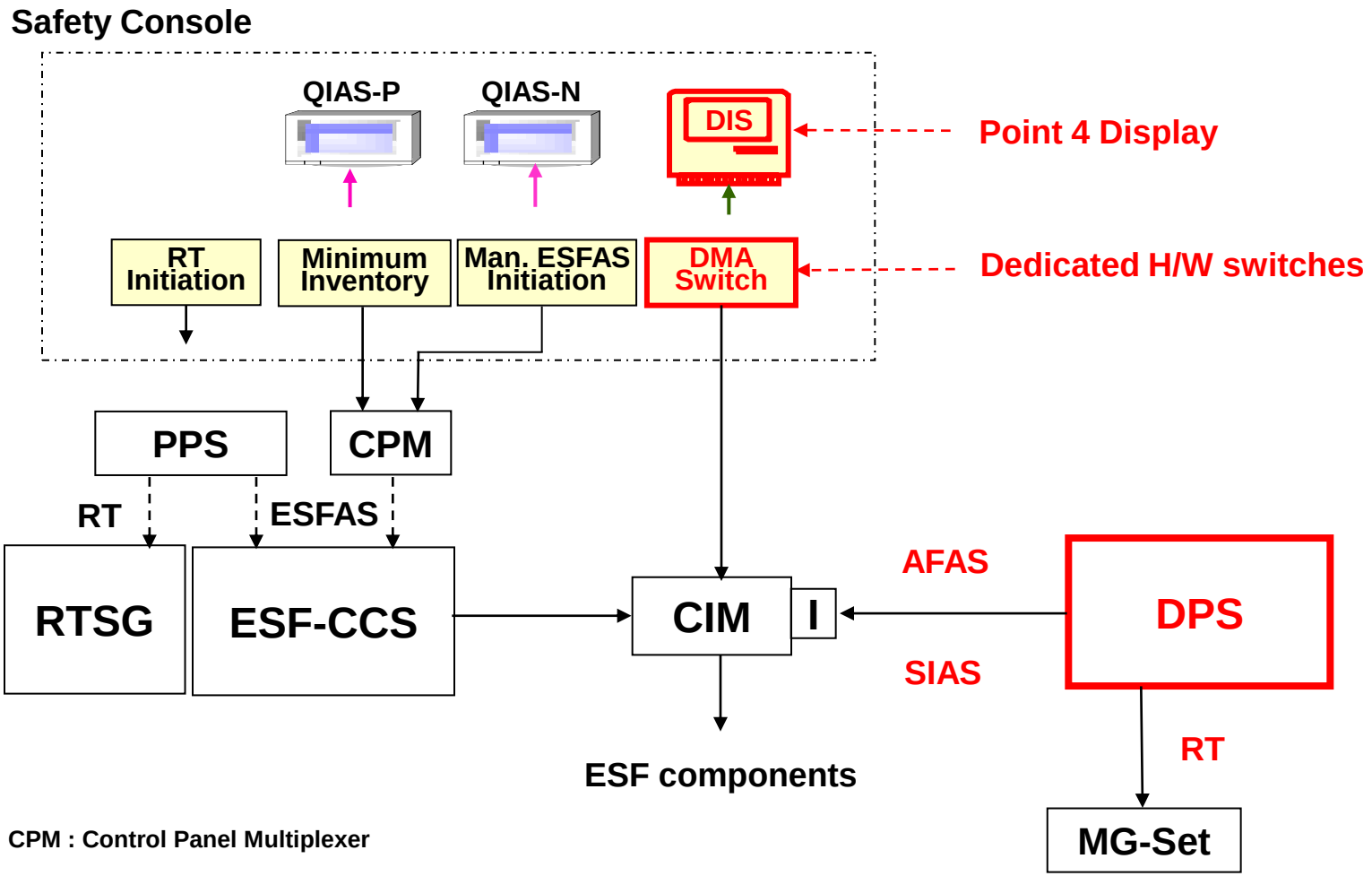
Echelons of Defense (1/2)

Combining Diversity Attributes (NUREG guideline 2)

PROTECTION & SAFETY MONITRING SYSTEM	CONTROL & MONITORING SYSTEM	DIVERSE ACTUATION SYSTEM (DAS)
PPS	Power Control System (PCS)	DPS
ESF-CCS	P-CCS	DPS
QIAS-P	IPS	DIS
Manual ESFAS Initiation Switch	N/A	DMA Switch
RTSG	PCS	MG-Set (Output Breaker)
RTS/ESFAS Echelon	CONTROL Echelon	MONITORING & INDICATOR Echelon

Echelons of Defense (2/2)

Diversity between Protection and Diverse Actuation System



CPM : Control Panel Multiplexer

5 Diverse Protection System

Diverse Protection System (1/5)

Design Features

- Reduction of the risk of ATWS (10 CFR 50.62)
- Provision to cope with CCF of PPS/ESF-CCS (BTP 7-19)
- Diverse from the PPS
  - Diverse equipment from sensor output to final actuation device
- Design to prevent spurious actuation
  - Energized-to-actuate design
  - Two channels and 2/2 coincidence logic
  - Augmented quality (Important to Safety)

Diverse Protection System (2/5)

System Components

- DPS Controller
  - Diverse reactor trip
    - on high PZR pressure (for ATWS mitigation)
    - on high CNMT pressure (for MSLB with CCF)
  - Diverse AFAS actuation
    - on low S/G level (for ATWS mitigation)
  - Diverse SIAS actuation
    - on low PZR pressure (for LOCA with CCF)
- Operator Station
  - System status monitoring and displays
  - Manual actuation
- Engineer Workstation
  - Setpoint change, bypass function
  - Manual and automatic test

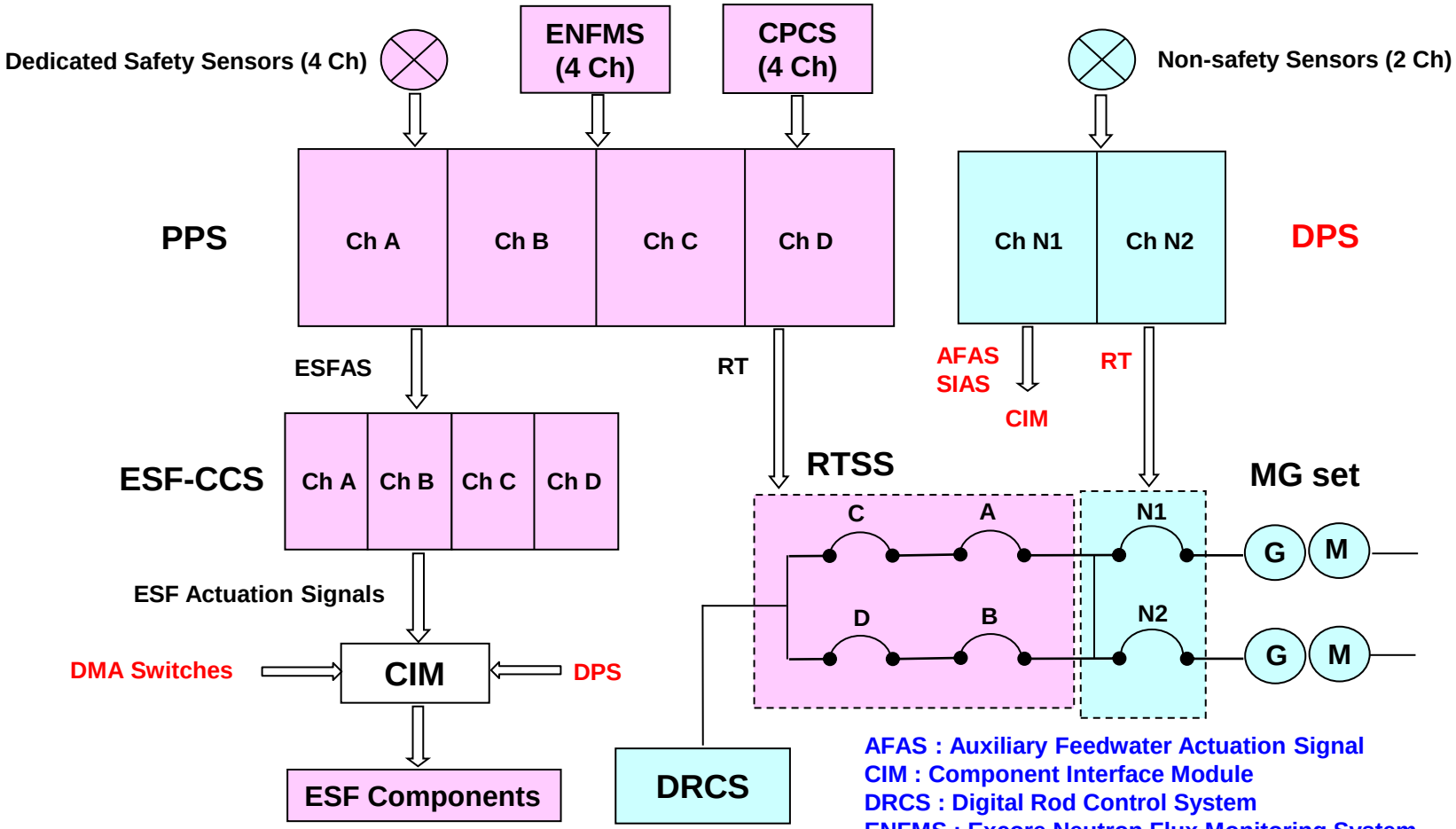
Diverse Protection System (3/5)

Diversity between PPS/ESF-CCS and DPS (1/2)

Item/System		PPS/ESF-CCS	DPS
Electrical Class		Class 1E	Non-1E
Controller		PLC	DCS
Actuation Signals	RT	Open RTSG circuit breaker	Open M-G set Output Breaker
	ESFAS	ESF-CCS output is sent to ESF equipment via CIM	DPS output is sent to ESF equipment via CIM

Diverse Protection System (4/5)

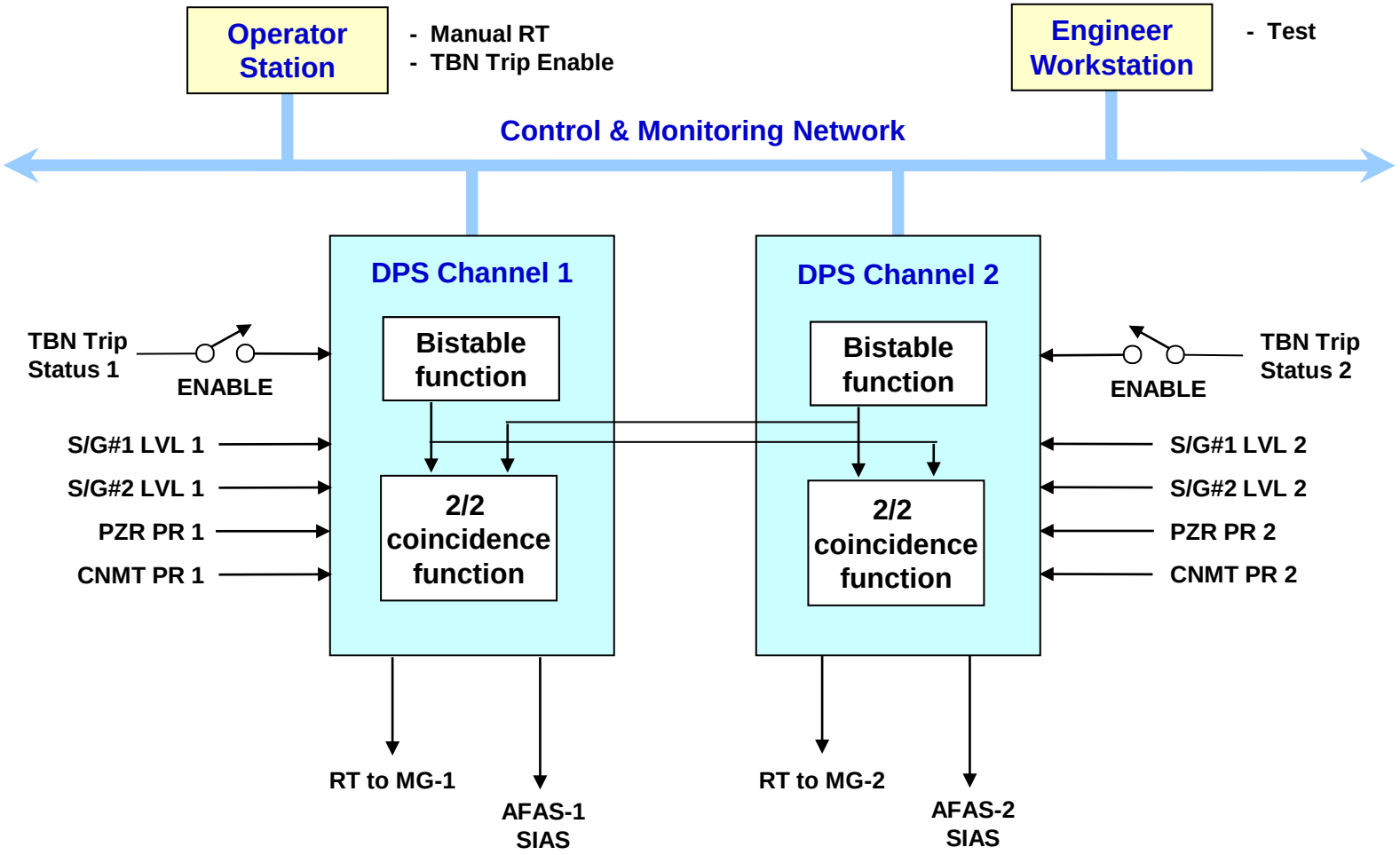
Diversity between PPS/ESF-CCS and DPS (2/2)



AFAS : Auxiliary Feedwater Actuation Signal
CIM : Component Interface Module
DRCS : Digital Rod Control System
ENFMS : Excore Neutron Flux Monitoring System
RTSS : Reactor Trip Switchgear System
SIAS : Safety Injection Actuation Signal

Diverse Protection System (5/5)

Block Diagram



6 Diverse Indication System

Diverse Indication System (1/4)

Design Features

- Diverse Indication System (DIS) provides a set of displays required by BTP 7-19 Point 4.
- DIS is used to monitor the plant state for placing the plant in a safe shutdown condition during DBEs with CCF.
- Displays and controls available on Safety Console during CCF for manual operator action
  - DIS display
  - Information FPDs
  - Diverse manual ESF actuation (DMA) switches
  - Reactor trip initiation switches

Diverse Indication System (2/4)

System Description

- Independent and diverse from QIAS-P/N.
- Displays Point 4 variables based on D3 analysis.
- Provides safety-related information.
  - Accident monitoring instrumentation (AMI)
  - Inadequate core cooling (ICC)
  - Emergency operating procedure (EOP)
- Receives hardwired signals from APC-S and QIAS-P (Ch. A) via splitters/isolators.

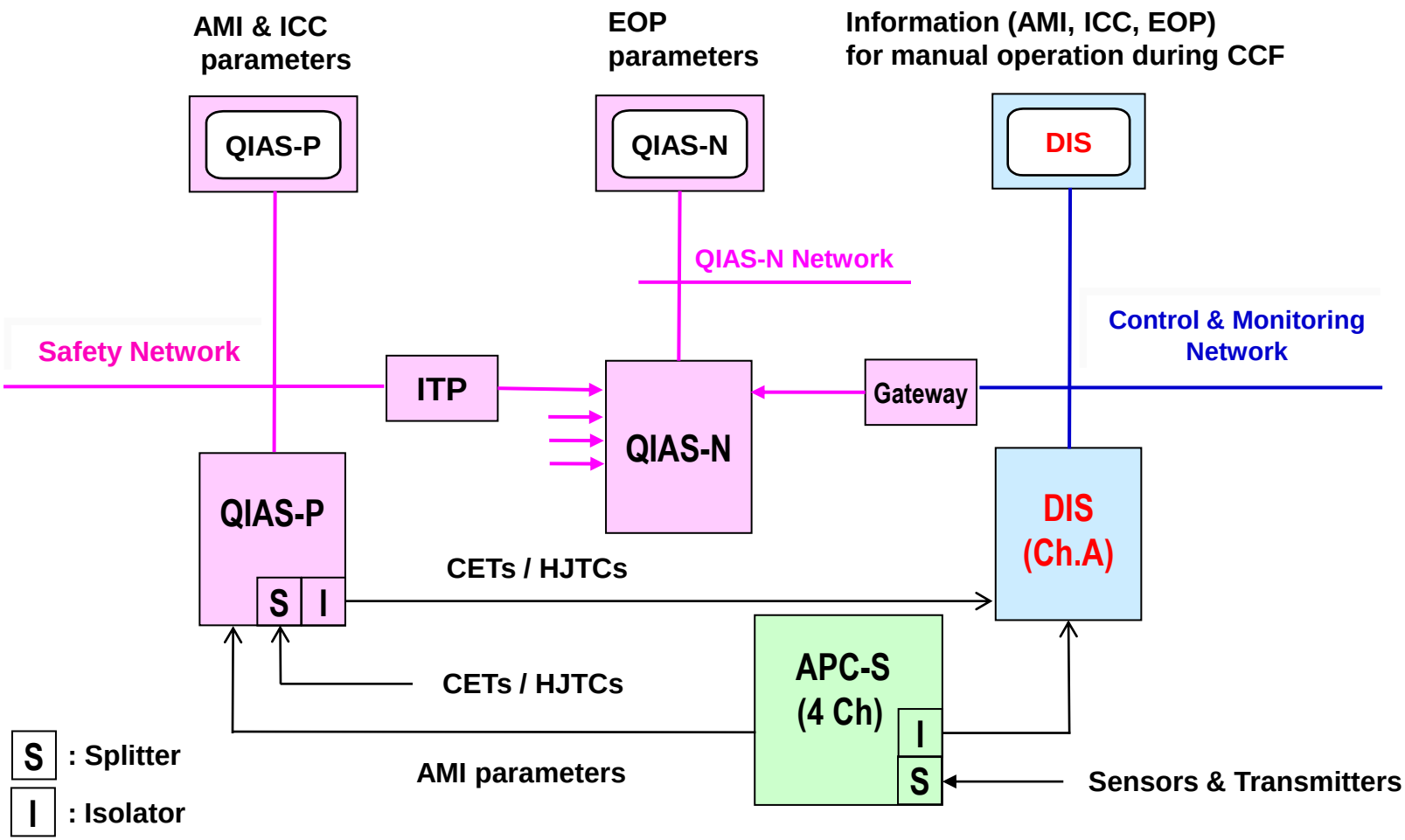
Diverse Indication System (3/4)

Independence and Diversity

Item	QIAS-P	QIAS-N	DIS
Hardware	PLC	PLC	DCS
Safety Class	Safety	Non-safety	Non-safety
Seismic Class	I	I	II
Application Software	ITS	ITA	ITS
Input Source	PPS/ESF-CCS via safety network	PPS/ESF-CCS via ITP	APC-S / QIAS-P via hardwired cable
Display Parameter	- AMI - ICC monitoring	- EOP parameters	- AMI - ICC monitoring - EOP parameters

Diverse Indication System (4/4)

Diversity between QIAS and DIS



7 DMA Switch

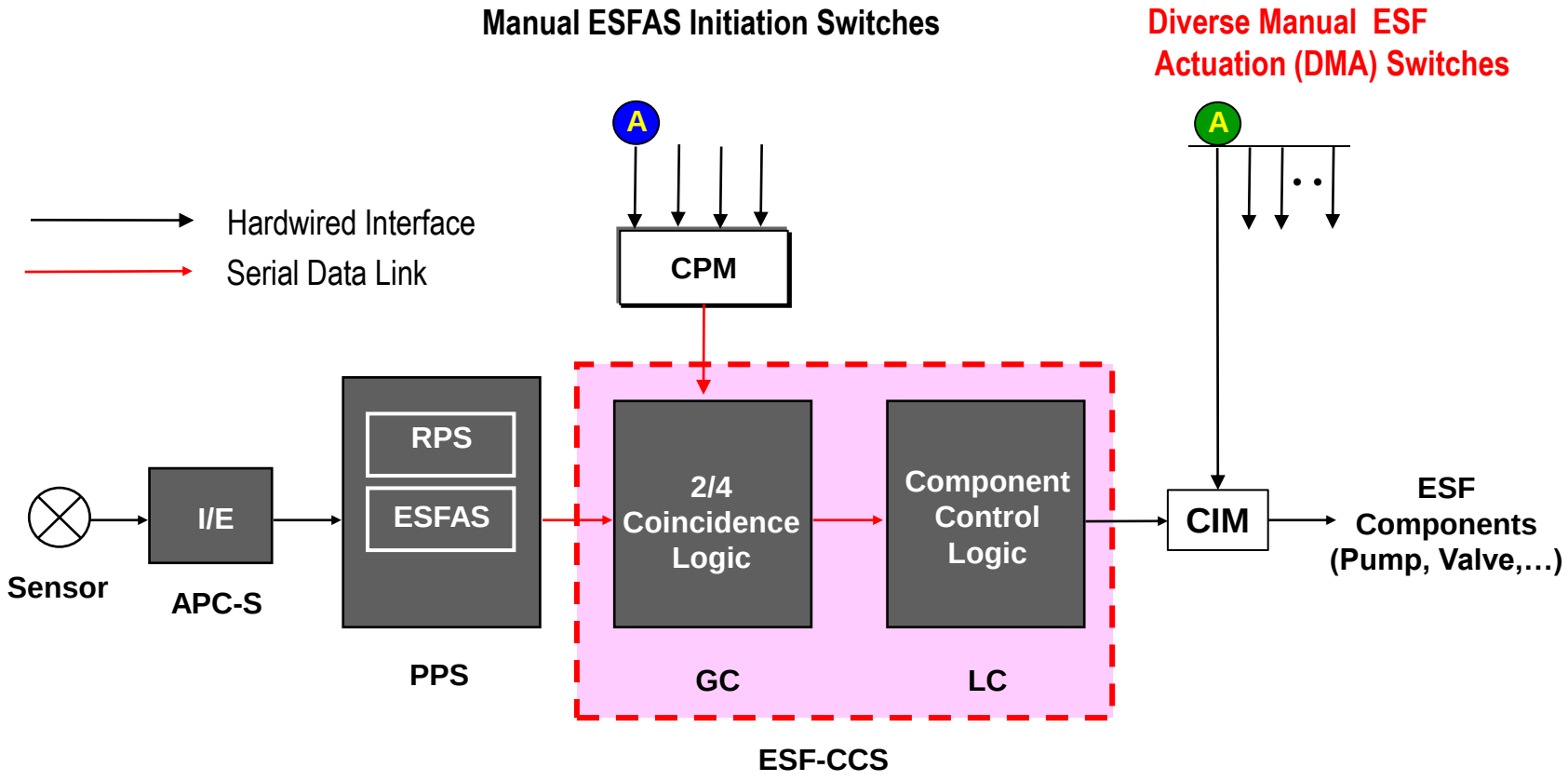
Diverse Manual ESF Actuation Switch (1/3)

Design Features

- A set of controls required by BTP 7-19 Point 4
- Diverse from manual ESFAS initiation switches required by IEEE Std. 603 (section 6.2/7.2)
- Conventional switches for system level ESFAS actuation
- Output signals connected to CIM (downstream of ESF-CCS)

Diverse Manual ESF Actuation Switch (2/3)

Interface to ESF Components



Diverse Manual ESF Actuation Switch (3/3)

Component Interface Module (CIM) (1/2)

- Main functions
  - Integrate component command signals from different control platforms.
  - Arbitrate component command and prioritize control by system-based and state-based priority.
  - Provide power interface from system to the components.
- Hardware-based safety grade module
  - Diverse from safety platform (PPS & ESF-CCS)
  - Permanent logic implemented by solid-state device technology
  - Fully testable design
  - Seismic Category I
  - EMI/RFI qualification

8 D3 Analysis

Diversity & Defense-in-Depth Analysis (1/4)

Design Approach

- Elimination of predictable CCFs
  - Equipment qualification (environmental, seismic, EMI)
  - Geographic separation (different equipment room)
- Design for high reliability
  - Deterministic design
  - Simplicity and Segmentation
  - Field proven product
  - Verification & Validation
  - Diversity
- Diversity and defense-in-depth analysis
  - Evaluates remaining diverse lines of defense to be adequate to deal with CCF (NUREG/CR-6303)

Diversity & Defense-in-Depth Analysis (2/4)

Choosing Blocks and System Failure Types

- The postulated CCF block (systems) with identical H/W and S/W
  - Plant Protection System
  - Core Protection Calculator System
  - Engineered Safety Features – Component Control System
  - Qualified Indication and Alarm System – PAMI / Non-Safety
  - Safety Soft Control
  - Manual ESFAS Initiation Switches
  - Minimum Inventory Switches

- System Failure Types
  - Type 1 Failure : Interaction between echelons of defense (N/A)
  - Type 2 Failure : Failure to respond due to CCF (failure of total block)
  - Type 3 Failure : Anomalous instrument reading (signal diversity)

Diversity & Defense-in-Depth Analysis (3/4)

Plant Monitoring and Manual Operator Action

- Diverse Actuation System (DPS+DIS+DMA switch)
- Aux. Process Cabinet–Safety/Non-safety
- Information Processing System
- Control Systems
  - PCS (RRS, RPCS, DRCS)
  - NPCS (PP&LCS, FWCS, SBCS)
  - P-CCS (BOP discrete and continuous controls)
  - Neutron Flux Monitoring System (ENFMS, FIDAS)
  - NSSS Integrity Monitoring System
  - T/G Control and Monitoring System
- RT Initiation Switches

Diversity & Defense-in-Depth Analysis (4/4)

Functional Diversity in Systems

Critical Function	Non-Safety	Safety	Manual
Reactivity	Rod Control System CVCS Boration	Safety Injection System Reactor Trip Switchgear	DMA SW RT SW
Vital Auxiliaries(AC) (DC)	Main Transformer, Station Batteries	Emergency D/G Station Batteries	
RCS Inventory	CVCS	Safety Injection System	DMA SW
RCS Pressure	Heaters/Spray CVCS	Safety Injection System Safety Depressurization and Vent System	DMA SW
Core Heat Removal	Forced Circulation	Natural Circulation	
RCS Heat Removal	Main Feedwater	Auxiliary Feedwater System Safety Injection System Shutdown Cooling System	DMA SW DMA SW
Containment Isolation	Control Valves	Isolation Valves	DMA SW
Containment Environment	Fan Coolers Hydrogen Igniters	Containment Spray System Hydrogen Re-combiners	DMA SW
Radiation Emission	Monitor and Control Radiation Release Paths	Isolation of Release Paths	

9 D3 Coping Analysis Method

D3 Coping Analysis Method (1/5)

Event Evaluation Method

- Acceptance Criteria (BTP 7-19 / 10 CFR 100 Guideline)
  - For AOOs, radiation release not exceeding 10% and RCPB integrity
  - For PAs, radiation release not exceeding 100% and RCPB/CNMT integrity
- Two Phases Realistic Evaluation
  - Qualitative evaluation to identify events requiring more analysis
  - Quantitative analysis to analyze the events using computer program
- Major Assumptions (SKN 3&4)
  - No additional single failure other than CCF
  - Control systems in automatic mode
  - Nominal plant condition
  - RCP assumed to be operating
  - DAS not affected by CCF

D3 Coping Analysis Method (2/5)

Quantitative Analysis (SKN3&4) (1/2)

- Eight events identified for quantitative analysis (SAR Chapter)
  - Increase in feedwater flow (15.1.1)
  - Steam line break (15.1.5)
    - Non-LOCA
    - Containment Integrity
  - Total loss of reactor coolant flow (15.3.1)
  - Single RCP rotor seizure (15.3.3)
  - CEA ejection (15.4.8)
  - Steam generator tube rupture (15.6.3)
  - Small Break Loss of coolant accident (6.3)

- Large Break LOCA will be included in APR1400 (BTP 7-19)

D3 Coping Analysis Method (3/5)

Quantitative Analysis (SKN3&4) (2/2)

- Summary of Quantitative Results
  - RCS Integrity has been confirmed (≤ 3200 psig)
    - Max. RCS peak pressure: 2580 psia from SLB accident
  - CNMT Integrity has been confirmed (≤ 123.7 psia)
    - Max. CNMT peak pressure: 93.15 psia from SLB accident
  - Offsite dose has been confirmed (10% or 100% of 10 CFR 100)
    - Max. dose from AOO: No fuel failure, Not severe than DBEs
    - Max. dose from PA : Less than 10 CFR 100 dose limit

- Addition of diverse means by analysis
  - Reactor trip by high CNMT pressure (MSLB with CCF)
  - SIAS by high PZR pressure (LBLOCA with CCF) for APR1400

D3 Coping Analysis Method (4/5)

Manual Operator Action Time Evaluation Method

- Manual operator actions based on HFE methodology proposed by NUREG-0800, SRP Appendix 18-A
  - Assessment of available information
  - Decision making process and operator action steps based on emergency operating procedures

- Basis for Operator Response Time Estimates
  - Operators aware of plant conditions requiring reactor trip
  - IPS providing alarms indicating conditions for reactor trip
  - Sequence of operator actions according to Standard Post Trip Action
  - Execution time based on ANSI/ANS 58.8
  - Total elapsed time is sum of operator responses performed in series.

D3 Coping Analysis Method (5/5)

Response Time for Evaluation (SLB - CNMT integrity, SKN3&4)

Available Alarms & Indications		Operator Response Time	Credited Response Time in Evaluation
Reactivity Control	N/A	Automatic Reactor Trip by DPS	Reactor Trip not Credited
RCS Heat Removal	Alarms : Lo SG P, Hi CNMT P, Lo RCS T	Close MFIV – 25 min.	Close MFIV – 30 min.
	Indications : S/G P/L, CNMT P/T, PZR P/L, RCS T	Close MSIV – 26 min.	Close MSIV – 30 min.
		CNMT Spray – 27 min.	CNMT Spray – 30 min.

10 Conformance to BTP 7-19

Conformance to BTP 7-19 (1/1)

Four Point Positions

- Point 1, Assess D3 to address vulnerabilities to CCF.
  - D3 topical report to be submitted.
- Point 2, Analyze postulated CCF for events in SAR and demonstrate adequate diversity using realistic assumptions and analysis methods.
  - Technical report for CCF coping analysis to be submitted.
- Point 3, Identify a diverse means required to perform safety function.
  - Augmented quality DAS to perform necessary functions.
- Point 4, Provide displays & controls to support safety functions.
  - DIS/DMA switches/CIM diverse from safety systems
  - Manual operator actions will be evaluated based on HFE methodology.

11 Conformance to 10 CFR 50.62

Conformance to 10 CFR 50.62 (1/1)

Requirements for Reduction of Risk from ATWS Events

- Diverse Aux. Feedwater System Actuation
  - Diverse sensor for S/G level (AFAS)
  - Diverse hardware (DCS)
  - Diverse actuation device (CIM)
- Diverse Turbine Trip
  - Diverse sensor (DRCS undervoltage relay)
- Diverse Scram System
  - Diverse sensor for pressurizer pressure (RT)
  - Diverse hardware (DCS)
  - Diverse interruption of power to control rod (MG-Set output breaker)

12 Summary

Summary

- DAS(DPS+DIS+DMA SW.) is provided. (10 CFR 50.62, BTP 7-19)
- Diverse Protection System is diverse from PPS.
  - Reactor Trip
  - Auxiliary Feedwater Actuation
  - Safety Injection Actuation
- Diverse Indication System is diverse from QIAS-P/N.
- Diverse Manual ESF Actuation Switch is diverse from Manual ESFAS Initiation Switch.
- Diversity and Defense-in-Depth (D3) Analysis is performed. (NUREG/CR-6303)
- D3 Coping Analysis will be performed to meet acceptance criteria.
  - RTS is added for MSLB with CCF for SKN3&4.
  - SIAS will be added for LB LOCA with CCF for APR1400.