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

<table>
<thead>
<tr>
<th>Item/Project</th>
<th>YGN5&amp;6</th>
<th>UCN5&amp;6</th>
<th>SKN3&amp;4</th>
<th>APR1400</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plant Protection System (PPS)</strong></td>
<td>Analog</td>
<td>PLC(Common-Q)</td>
<td>PLC(Common-Q)</td>
<td>PLC</td>
<td></td>
</tr>
<tr>
<td><strong>Control System</strong></td>
<td>PLC(Omron)</td>
<td>PLC(Omron)</td>
<td>DCS(Ovation)</td>
<td>DCS</td>
<td></td>
</tr>
<tr>
<td><strong>Diverse Protection System (DPS)</strong></td>
<td>PLC(Modicon)</td>
<td>PLC(Modicon)</td>
<td>DCS(Ovation)</td>
<td>DCS</td>
<td></td>
</tr>
<tr>
<td><strong>Diverse Indication System (DIS)</strong></td>
<td>x</td>
<td>x</td>
<td>DCS(Ovation)</td>
<td>DCS</td>
<td></td>
</tr>
<tr>
<td><strong>Diverse Manual ESF Actuation (DMA)</strong></td>
<td>x</td>
<td>H/W SW.</td>
<td>H/W SW.</td>
<td>H/W SW.</td>
<td></td>
</tr>
</tbody>
</table>

### DPS Output Signals

<table>
<thead>
<tr>
<th>DPS Output Signals</th>
<th>ATWS</th>
<th>D3</th>
<th>D3 Analysis TR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ATWS</strong></td>
<td>RT</td>
<td>RT</td>
<td>RT</td>
</tr>
<tr>
<td><strong>AFAS</strong></td>
<td>AFAS</td>
<td>AFAS</td>
<td>AFAS</td>
</tr>
<tr>
<td><strong>D3</strong></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>D3 Analysis TR</strong></td>
<td>x</td>
<td>Done</td>
<td>Done</td>
</tr>
</tbody>
</table>

**Remark:**
- PZR PR
- S/G LVL
- CNMT PR (MSLB)
- SIAS
- PZR PR (LBLOCA)

**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)

APR1400-R-I-I(EC)-11002-N APR1400
4 Echelons of Defense
## Echelons of Defense (1/2)

### Combining Diversity Attributes (NUREG guideline 2)

<table>
<thead>
<tr>
<th>PROTECTION &amp; SAFETY MONITORING SYSTEM</th>
<th>CONTROL &amp; MONITORING SYSTEM</th>
<th>DIVERSE ACTUATION SYSTEM (DAS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPS</td>
<td>Power Control System (PCS)</td>
<td>DPS</td>
</tr>
<tr>
<td>ESF-CCS</td>
<td>P-CCS</td>
<td>DPS</td>
</tr>
<tr>
<td>QIAS-P</td>
<td>IPS</td>
<td>DIS</td>
</tr>
<tr>
<td>Manual ESFAS Initiation Switch</td>
<td>N/A</td>
<td>DMA Switch</td>
</tr>
<tr>
<td>RTSG</td>
<td>PCS</td>
<td>MG-Set (Output Breaker)</td>
</tr>
<tr>
<td>RTS/ESFAS Echelon</td>
<td>CONTROL Echelon</td>
<td>MONITORING &amp; INDICATOR Echelon</td>
</tr>
</tbody>
</table>
Echelons of Defense (2/2)

Diversity between Protection and Diverse Actuation System

Safety Console

- QIAS-P
- QIAS-N
- RT Initiation
- Minimum Inventory
- Man. ESFAS Initiation
- DMA Switch
- Point 4 Display
- Dedicated H/W switches

PPS
CPM
RTSG
ESF-CCS

RT
ESFAS

CPM: Control Panel Multiplexer

ESF components

RT
DPS

MG-Set
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)

<table>
<thead>
<tr>
<th>Item/System</th>
<th>PPS/ESF-CCS</th>
<th>DPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical Class</td>
<td>Class 1E</td>
<td>Non-1E</td>
</tr>
<tr>
<td>Controller</td>
<td>PLC</td>
<td>DCS</td>
</tr>
<tr>
<td>Actuation Signals</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open RTSG circuit breaker</td>
<td>Open M-G set Output Breaker</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESFAS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESF-CCS output is sent to ESF equipment via CIM</td>
<td>DPS output is sent to ESF equipment via CIM</td>
</tr>
</tbody>
</table>
Diverse Protection System (4/5)

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

Dedicated Safety Sensors (4 Ch)

ENFMS (4 Ch)

CPCS (4 Ch)

Non-safety Sensors (2 Ch)

PPS

Ch A

Ch B

Ch C

Ch D

ESF-CCS

Ch A

Ch B

Ch C

Ch D

ESF Components

DMA Switches

CIM

ESF Actuation Signals

RTSS

RT

AFAS

SIAS

CIM

MG set

G

M

DRCS

C

A

B

D

N1

N2

CAMP: 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

Operator Station
- Manual RT
- TBN Trip Enable

Engineer Workstation
- Test

Control & Monitoring Network

DPS Channel 1
- Bistable function
- 2/2 coincidence function
- RT to MG-1
- AFAS-1 SIAS

DPS Channel 2
- Bistable function
- 2/2 coincidence function
- RT to MG-2
- AFAS-2 SIAS

TBN Trip Status 1
ENABLE
S/G#1 LVL 1
S/G#2 LVL 1
PZR PR 1
CNMT PR 1

TBN Trip Status 2
ENABLE
S/G#1 LVL 2
S/G#2 LVL 2
PZR PR 2
CNMT PR 2

4th Pre-application Meeting
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

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

*Note: The table above illustrates the differences in hardware, safety class, seismic class, application software, input source, and display parameter for QIAS-P, QIAS-N, and DIS.*
Diverse Indication System (4/4)

Diversity between QIAS and DIS

- AMI & ICC parameters
- EOP parameters
- Information (AMI, ICC, EOP) for manual operation during CCF

QIAS-P → QIAS-N → DIS

AMI parameters

Control & Monitoring Network

Gateway

Safety Network

ITP

QIAS-N Network

CETs / HJTCs

S: Splitter
I: Isolator

AMI & ICC parameters

DIS (Ch.A)

CETs / HJTCs

APC-S (4 Ch)

Sensors & Transmitters
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

Manual ESFAS Initiation Switches

Diverse Manual ESF Actuation (DMA) Switches

Hardwired Interface
Serial Data Link

Sensor

APC-S

I/E

RPS
ESFAS

PPS

2/4 Coincidence Logic

Component Control Logic

ESF-CCS

PPS

GC
LC

CPM

ESF Components (Pump, Valve, …)

CIM

APR1400-R-I-I(EC)-11002-N APR1400
**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
## Functional Diversity in Systems

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

- RCS Integrity has been confirmed ($\leq 3200$ psig)
  - Max. RCS peak pressure: 2580 psia from SLB accident
- CNMT Integrity has been confirmed ($\leq 123.7$ 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)

<table>
<thead>
<tr>
<th>Available Alarms &amp; Indications</th>
<th>Operator Response Time</th>
<th>Credited Response Time in Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reactivity Control</strong></td>
<td>N/A</td>
<td><strong>Automatic Reactor Trip by DPS</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CNMT Spray – 27 min.</td>
</tr>
</tbody>
</table>
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.