Safety I&C Systems

Topical Report
Applicable Codes and Regulations
Safety I&C System Description
  ✓ Overview
  ✓ PPS
  ✓ ESF-CCS
  ✓ CPCS
  ✓ QIAS-P
  ✓ Data Communication
Software Development and V&V
Equipment Reliability
Design Acceptance Criteria
Summary
1 Topical Report
Topical Report (1/1)

Table of Contents

- Purpose
- Scope
- Applicable Codes and Regulations
- I&C System Description
- Software Reliability
- Equipment Qualification
- Equipment Reliability
- References
- Appendix A. Conformance to IEEE Std. 603-1991
- Appendix B. Conformance to IEEE Std. 7-4.3.2-2003
- Appendix C. Conformance to DI&C ISG-04
2 Applicable Codes and Regulations
Applicable Codes And Regulations (1/8)

10 CFR Part 50 Appendix A, General Design Criteria

- GDC 1, “Quality Standards and Records”
  - Conforms to the requirements of 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants”
- GDC 2, “Design Bases for Protection against Natural Phenomena”
  - Designed as Seismic Category I
  - Installed in the I&C equipment rooms or MCR that provide protection against other natural phenomena
- GDC 10, “Reactor Design”
  - Contributes to reactor design margin by providing conservatism in setpoint calculations and fault-tolerant features
  - Uncertainties and setpoint methodology will be submitted as a separate technical report
Applicable Codes And Regulations (2/8)

10 CFR Part 50 Appendix A, General Design Criteria

- GDC 19, “Control Room”
  - Equipped with manual reactor trip initiation switches and manual ESFAS initiation switches in the MCR safety console
  - Implemented with the displays for safe operation in the MCR.
- GDC 21, “Protection System Reliability and Testability”
  - Maintains the protection function in case of any single credible failure
  - Allows periodic testing without reducing the availability of the protection systems using bypass function
Applicable Codes And Regulations (3/8)

10 CFR Part 50 Appendix A, General Design Criteria

- GDC 22, “Protection System Independence”
  - Consists of four independent measurement channels for each protective parameter
- GDC 23, “Protection System Failure Modes”
  - Designed to fail into a safe state
  - FMEA method will be described in the Topical Report
- GDC 24, “Separation of Protection and Control System”
  - Maintains physical separation from non-safety system
Regulatory Guide

- Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions”
  - Provides complete overlap testing during the reactor operating at power or when shutdown
  - Provides system level alarms when a component is bypassed or inoperable
  - Assures both the reactor safety and resistance to a spurious reactor trip with four channel configuration
Applicable Codes And Regulations (5/8)

Regulatory Guide

  - Provides manual initiation of a protective action at the system level for RPS and ESFAS
  - Provides manual switches on the MCR safety console
  - Located in different geographic fire zones for each channel
  - Electrically isolated using fiber-optic technology
  - Physically separated
  - Provides the accident monitoring instrumentation according to IEEE Std. 497-2002
Applicable Codes And Regulations (6/8)

Regulatory Guide

  - Setpoint methodology conforms to ISA-S67.04-1994
  - Uncertainties and setpoint methodology will be submitted as a separate technical report

  - Designed to be periodically tested in accordance with the criteria of IEEE Std. 338-1987
  - Provides overlapped testing for the RPS and ESFAS without initiating a reactor trip or ESF actuation

  - Conforms to IEEE Std. 7-4.3.2-2003
Applicable Codes And Regulations (7/8)

Regulatory Guide

  - Conforms to IEEE Std. 1012-1998 and IEEE Std. 1028-1997

  - Conforms to IEEE Std. 828-1990 and IEEE Std. 1042-1997

  - Conforms to IEEE Std. 829-1983

  - Conforms to IEEE Std. 1008-1987

  - Conforms to IEEE Std. 830-1993
Applicable Codes And Regulations (8/8)

  - Conforms to IEEE Std. 1074-1995
  - Qualified according to the EMI/RFI requirements of MIL Std. 461E
  - Qualified according to the requirements of IEEE Std. 323-2003
3 Safety I&C System Description
Overview (1/6)

Overall I&C System Architecture

- Safety I&C system uses qualified PLC platform
- Non-safety I&C system uses DCS platform
- Provides 4 channel redundancy for safety I&C system except QIAS-P
  - Installed in physically separated I&C equipment rooms
- Electrical isolation, physical separation and communication independence
  - Between redundant safety channels
  - Between safety system and non-safety system
- Diversity to cope with the CCF of digital safety I&C system
  - Diverse Protection System
  - Diverse Indication System
  - Diverse Manual ESF Actuation Switches
Overview (3/6)

Protection and Safety Monitoring System

- **Plant Protection System**
  - Initiates reactor trip or ESFAS whenever the monitored process values exceed the pre-defined limits

- **Engineered Safety Features-Component Control System**
  - Controls the operation of ESF components
  - Receives manual ESFAS actuation signals from safety console

- **Core Protection Calculator System**
  - Computes DNBR and LPD
  - Provides the trip signal to PPS

- **Qualified Indication and Alarm System – PAMI**
  - Displays Type A, B & C variables required by Reg. Guide 1.97 and the variables for inadequate core cooling monitoring

- **Auxiliary Process Cabinet – Safety**
  - Receives safety field signals and distributes them to PPS, ESF-CCS, CPCS, QIAS-P and DIS
Overview (4/6)

Control and Monitoring System

- **Power Control System**
  - Controls reactor power level
  - Includes Reactor Regulating System, Reactor Power Cutback System and Digital Rod Control System

- **NSSS Process Control System**
  - Controls NSSS processes
  - Consists of Pressurizer Pressure & Level Control System, Feedwater Control System and Steam Bypass Control System

- **Process-Component Control System**
  - Controls BOP processes

- **Qualified Indication and Alarm System – Non-safety**
  - Supports continuous plant operation when Information Processing System is unavailable
  - Provides the indications required for EOP execution, safe shutdown and critical operator action required by PRA and HRA
Overview (5/6)

Diverse Actuation System

- Diverse Protection System
  - Provides defense against CCF of PPS/ESF-CCS (SECY 93-087, BTP 7-19)
  - Reduces the risk of ATWS (10 CFR 50.62)
- Diverse Indication System
  - Displays Position 4 variables (SECY 93-087, BTP 7-19)
- Diverse Manual ESF Actuation Switches
  - Provide Position 4 actuation (SECY 93-087, BTP 7-19)
Overview (6/6)

Human – System Interface

- Large Display Panel
  - Display of overall plant operation
- Operator Consoles
  - Monitor and control all processes
- Safety Console
  - Backup operation during total failure of the operator consoles;
  - EOPs operation and safe shutdown
  - Critical operator actions required by PRA and HRA
  - Manual ESF system level actuation switches and reactor trip switches
  - Alarms, displays, controls needed to perform periodic surveillance test
Plant Protection System (1/5)

Design Features

- Qualified PLC platform
- Reactor Trip & ESFAS initiation function
  - Mitigates the consequences of safety related design bases events
- Four independent channels
- Redundancy within each channel to enhance availability
- Fail-safe design for component failure or loss of electrical power
- Continuous automatic on-line testing
  - Hardware self diagnostics
  - Cross channel comparisons
- Manual testing
  - Computer-aided surveillance testing
Plant Protection System (2/5)

System Description

- **Bistable Processor**
  - Generates trip signals when the process value exceeds a setpoint

- **Local Coincidence Logic Processor**
  - Determines the trip state based on the state of the four channel bistable trip inputs and respective bypasses
  - Generates the initiation signal for RTSS or ESF-CCS

- **Maintenance & Test Panel**
  - Shared with ESF-CCS, CPCS and QIAS-P
  - Provides manual control functions using soft control with Function Enable Key switches to meet DI&C-ISG-04
  - Displays system operating status
Plant Protection System (3/5)

System Description

- **Interface & Test Processor**
  - Transfers the safety system operating status to IPS and QIAS-N
  - Supports surveillance test

- **Operator Module**
  - Shared with ESF- CCS and CPCS
  - Located on the Safety Console
  - Provides PPS control functions using conventional switches on the Safety Console
    - operating bypass, variable setpoint reset
  - Displays system operating status

- **RPS Reactor Trip Initiation Switches**
  - 4 switches in the MCR Safety Console
  - Hardwired directly to the RTSS
Plant Protection System (4/5)

System Configuration

Diagram of Plant Protection System Configuration.

CHANNEL A
CHANNEL B
CHANNEL C
CHANNEL D

TR - SENSOR AND TRANSMITTER
APC-5
ENFM5

SISTABLE PROCESSOR
OM

LCL PROCESSOR
MTP
ITP

INITIATION CIRCUIT
REACTOR TRIP

4th Pre-application Meeting

Safety I&C Systems

ICEP CO
Plant Protection System (5/5)

Testing Function

- Self-testing
  - Continuous and automatic diagnostics for detecting hardware and software error
  - Cross channel comparison for channel operability check

- Manual testing
  - Performs under administrative control
  - Complete overlapped testing
ESF-CCS (1/3)

**Design Features**

- Common platform with PPS
- Consists of 4 channels
- Consists of Group Controller and Loop Controller
- Group Controller
  - Performs 2/4 logic using the ESFAS initiation signals from PPS
  - Performs load sequence logic for emergency diesel generator
- Loop Controller
  - Performs the component control logic

![Diagram of ESF-CCS components](chart)
ESF-CCS (2/3)

System Description (CIM)

- **Main Function**
  - Integrates component command signals from different control platforms
  - Arbitrates component command and prioritize control by system-based and state-based priority.

- **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
ESF-CCS (3/3)

System Description (CIM)

- Priority Logic
  - Hardware-based logic
  - State-based priority (safe state first)
CPCS (1/3)

System Description

- Common platform with PPS
- Four independent channels
- Generates the low DNBR trip and high LPD trip to PPS
- Provides CEA Withdrawal Prohibit signals to the Digital Rod Control System
- Transmits all the CEA positions to the Information Processing System
CPCS (2/3)

System Description

- CPCS consists of CPC, CEAC and CPP
- Core Protection Calculator
  - Calculates Departure from Nucleate Boiling Ratio and Local Power Density based on CEA position and penalty factor
  - Generates Low DNBR / High LPD trip and CWP to PPS
- Control Element Assembly Calculator
  - Monitors CEA positions
  - Calculates CEA position penalty factor
- CEA Position Processor
  - Performs A/D conversion for the signals from the Reed Switch Position Transmitters
  - Transmit the CEA positions to CEAC
CPCS (3/3)

System Description (Function)

- Receives the following signals from the process sensors, RSPT and ENFMS
  - RCS cold leg and hot let temperature
  - Pressurizer pressure
  - Reactor coolant pump speed
  - Ex-core neutron flux power
  - CEA positions
- Calculates DNBR and LPD values
- Compares the calculated DNBR and LPD values to setpoints
- Provides the output to PPS
  - Low DNBR trip, pre-trip
  - High LPD trip, pre-trip
  - CEA Withdrawal Prohibit
QIAS-P(1/2)

System Description

- Common platform with PPS
- Two channel redundancy (Ch. A & B)
- Provides two separate FPDs (continuous and dedicated) at the Safety Console
- Displays accident monitoring instrumentation variables
  - Type A, B and C parameters required by Reg. Guide 1.97 Rev.04
- Displays inadequate core cooling variables (NUREG-0737, Sec.II.F.2)
  - Primary coolant saturation margin
  - Rx vessel level (HJTC)
  - Core exit temperature
QIAS-P (2/2)

QIAS-P Architecture

QIAS-N

Data Link

ITP

QIAS-P

Ch.A(B)

QIAS-P Cabinet Ch.A(B)

CET

HJTC

AMI

Sensors

APC-S

Splitter

DIS

DIS Display (Ch.A only)

Control & Monitoring Network

MTP

Safety network

Data Link

Hardwired

Safety network

Network Data

Isolator

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A

QIAS-N

QIAS-P

IPS

QIAS-P Display Ch. A
Data Communication (1/6)

Data Communication Independence

- Data communication meets the requirements of R.G. 1.75 and DI&C-ISG-04
  - Physical separation: distance between redundant channels
  - Electrical isolation: fiber optic technology
  - Communication independence: broadcast only
- The serial data link transmission is used for transmitting safety signals
  - No acknowledgement from the other side
- The communication and processing section processors share data by means of dual-ported memory
  - Interface via dual-ported memory separate functionally between processing processor and communication processor
Data Communication (2/6)

Data Communication Network

Non-Safety Network

Safety to Non-safety Interface

Safety Network (Ch. A)

CCC Data Link: Cross Channel Communication

CPCS → BP → LCL → GC

From BP in Ch. B, C, D

From LCL in Ch. B, C, D

To LCL in Ch. B, C, D

PPS to ESF-CCS Data Link

ITP Network: ITP’s in Ch. B, C, D

IPF

Gateway Server

QIAS-N

MTP

ITP

QIAS-P

ITP's in Ch. B, C, D

Information Processing System

APR1400-R-I-I(EC)-11001-N

33
Data Communication (3/6)

Data Communication between Redundant Safety Channels

- Between PPS channels
- Between CPCS channels
- Between PPS and ESF-CCS channels
- Between ITPs in each channel

PS : Processing Section
CS : Communication Section

Serial data link between Bistable processor and LCL processor for example
Data Communication (4/6)

Data Communication from Safety to Non-safety system

- Between ITPs in each channel and QIAS-N

- Between MTPs in each channel and Gateway Servers
Data Communication (5/6)

Soft Control Communication

● Replaces the conventional dedicated pushbuttons and M/A station.

● Enable operators to control all ESF components using the ESF-CCS Soft Control Module (ESCM)

● Safety related soft control
  – Selects ESF component to be controlled on the Information FPD
  – Information FPD sends component ID to ESCM
  – Controls the selected ESF component using the component control template the ESCM
  – ESCM control signals are transmitted to the ESF-CCS via Control Channel Gateway (CCG)
  – The control signals are validated by channel confirm switches.
Soft Control Communication

- **Hardwired**
- **Serial Data Link**

CPM: Control Panel Multiplexer
CCG: Control Channel Gateway
ESCM: ESF-CCS Soft Control Module

Diagram:
- Information FPD
- ESCM
- CCG
- ESF-CCS
- Safety components
- Ch. Confirm Switches

4th Pre-application Meeting
4 Software Development and V&V
Software Development and V&V (1/2)

Software Reliability

- **Software design life cycle**
  - Software life cycle model consistent with IEEE Std. 1074
  - Software life cycle activities consistent with NUREG 0800, BTP 7-14
  - Major software plan documents
    - software quality assurance plan – IEEE Std. 730
    - software V&V plan – IEEE Std. 1012
    - software configuration management plan – IEEE Std. 828
    - software safety plan – IEEE Std. 1228

- **Software classification**
  - Classified according to the grade of importance (its function to be performed)
  - Software within a processor have the same classification
  - Most rigorous V&V requirements are applied to protection grade S/W
### Software Development and V&V (2/2)

#### Software Classification

<table>
<thead>
<tr>
<th>IEEE 1012-1998 Criticality</th>
<th>APR1400 Software Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (Level 4)</td>
<td>Protection (Safety Critical)</td>
</tr>
<tr>
<td></td>
<td>- perform RPS control actions</td>
</tr>
<tr>
<td></td>
<td>- perform ESFAS control actions</td>
</tr>
<tr>
<td></td>
<td>- perform safe shutdown control actions</td>
</tr>
<tr>
<td>Major (Level 3)</td>
<td>Important to Safety (ITS)</td>
</tr>
<tr>
<td></td>
<td>- monitor or test protection functions</td>
</tr>
<tr>
<td></td>
<td>- monitor plant critical safety functions</td>
</tr>
<tr>
<td></td>
<td>- provide supplemental means to perform protection functions</td>
</tr>
<tr>
<td>Moderate (Level 2)</td>
<td>Important to Availability (ITA)</td>
</tr>
<tr>
<td></td>
<td>- maintain operation of plant systems and equipment that are necessary to operate the plant</td>
</tr>
<tr>
<td>Low (Level 1)</td>
<td>General Purpose</td>
</tr>
<tr>
<td></td>
<td>- perform functions other than that described in the previous classifications</td>
</tr>
<tr>
<td></td>
<td>- not installed in the on-line plant system.</td>
</tr>
</tbody>
</table>
5 Equipment Reliability
Equipment Reliability (1/3)

Types of Equipment Qualification

- Environmental Qualification
  - Located in mild environments where qualified HVAC is provided
  - IEEE std. 323-2003, as endorsed by RG 1.208

- Seismic Qualification
  - Classified in Seismic category I
  - IEEE std. 343-1987, as endorsed by RG 1.100
  - To be qualified by test, analysis or a combination of both methods

- Electromagnetic Compatibility (EMC)
  - Qualified for EMI/RFI emission / susceptibility and SWC
  - MIL. std. 461E and IEC std. 61000 series, as endorsed by RG 1.180
Equipment Reliability (2/3)

Reliability Analysis (FMEA)

- Potential single failure analysis for hardware components
- Assumes that one of the redundant PPS bistable trip channels is bypassed for maintenance
- Analysis to the level of replaceable modules
- FMEA table includes
  - Component and number
  - Failure mode
  - Symptom and local effect
  - Effect on protective function
  - Method of detection
  - Fault classification
Equipment Reliability (3/3)

Reliability Analysis (Unavailability)

- Probabilistic analysis using fault tree model
  - PPS fails to trip the reactor on demand
  - ESF-CCS fails to actuate the ESF components on demand
- Analysis considers
  - Independent component hardware failures
  - Common cause component hardware failures
  - Unavailability due to trip parameter in bypass
  - Human (operator) errors
- Major components for impacting system reliability
  - Reactor trip : CCF of RTSS, CCF of LCL DO module
  - ESFAS : CCF of Component Interface Module
6 Design Acceptance Criteria
### Design Acceptance Criteria

#### Digital Platform and Safety I&C System

<table>
<thead>
<tr>
<th>System</th>
<th>Design Area</th>
<th>DC Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Platform for Safety System</td>
<td>Hardware Component Detail Design - Response Time - Uncertainty - Deterministic Performance - System Diagnostics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Communication Independence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equipment Qualification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Commercial Grade Dedication</td>
<td>DAC</td>
</tr>
<tr>
<td>Safety System</td>
<td>System Description</td>
<td>Detail Design</td>
</tr>
<tr>
<td>- RPS</td>
<td>Design Bases</td>
<td>Detail Design</td>
</tr>
<tr>
<td>- ESF-CCS</td>
<td>Functional Design</td>
<td>Detail Design</td>
</tr>
<tr>
<td>- CPCS</td>
<td>Software</td>
<td>DAC</td>
</tr>
<tr>
<td>- QIAS-P</td>
<td>Set-point Calculations</td>
<td></td>
</tr>
<tr>
<td>- Data Comm.</td>
<td>Reliability Analysis</td>
<td></td>
</tr>
</tbody>
</table>
7 SUMMARY
Summary

- APR1400 I&C system overview provides the information for:
  - Common PLC for safety I&C and DCS for Non-safety I&C
  - Design feature and system description of PPS, ESF-CCS, CPCS, QIAS-P and data communications
  - S/W design process
  - Safety I&C reliability

- I&C system licensing plan
  - DAC is used for safety system digital platform and software
  - Component design details will be provided for reference

- Safety I&C systems topical report will be submitted