

# Control System CCF Analysis Technical Report

---

- Introduction
- Credible Failure Type
- Control System Design Features
- Evaluation for Control Signals Sent to ESF-CCS
- Evaluation for Failure Type 1
- Evaluation for Failure Type 2
- Evaluation for Failure Type 3
- Evaluation for Failure Type 4
- Summary

# Introduction

## Control System CCF Analysis TeR (APR1400-Z-J-NR-14001)

- **NRC letter comments (Dec. 19, 2013)**
  - The application did not provide sufficient information for the software common cause failures of non-safety related control systems that can lead to spurious actuations of redundant safety and non-safety components.
  
- **KHNP plan proposed at the 13<sup>th</sup> PARM (Feb. 11, 2014)**
  - Committed to submit a new Control system SWCCF Analysis TeR.
  - Proposed four Failure Modes (i.e., four Failure Types).
  - Presented evaluation example of the Failure Type 1.
  - Assumptions for four Failure Types

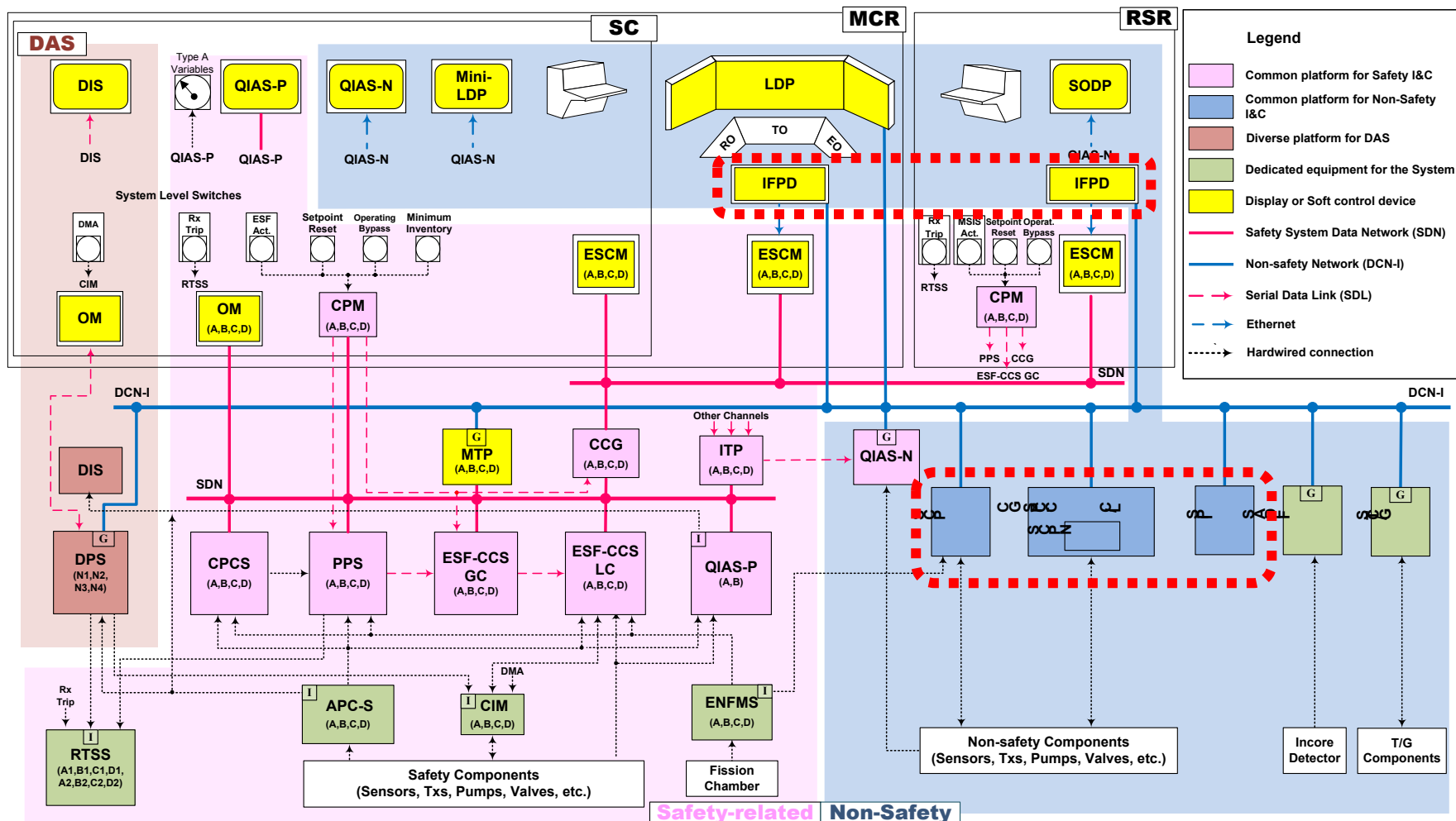
# Introduction

## NRC Major Feedbacks and Comments

TS

# Introduction

## Credible Failure Boundary



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

Rev.1

15th Pre-application Review Meeting

# Introduction

## Control System Overview - Primary & Secondary System

TS

15<sup>th</sup> Pre-application Review Meeting

# Credible Failure Type

## Credible Failure Types of Control System CCF

TS

# Credible Failure Type

Initiating Event Selection for Failure Types 1, 2, 3 & 4

TS

# Credible Failure Type

## Failure Type Overview

TS



# Control System Design Features

## Control System Design Features against CSCCF

- Each control group assigned to separate controller(s) to limit the failure in the control group (**segmentation**)
- Redundant controller for availability enhancement
- **Interlock/ permissive functions** by separate control group or safety system to limit the failure effects (e.g., CEAs withdrawal interlock signals, TBV permissive signals)
- **Control signal validation** to limit a single input failure of redundant channel inputs (i.e., large deviation of redundant inputs)
- **Redundant analog input modules with auto signal selection algorithm** to limit the failure effect of a single module (i.e., out of range)
- **Hardwired signal interface** of shared signals between major control groups<sup>[1]</sup>
- Self-diagnostics and abnormal alarming
- Structured software development process
- Test before and after installation

[1] Major control groups consist of RRS/RPCS, DRCS, PPCS, PLCS, SBCS Main/Permissive, FWCS1/2 and are called as nuclear steam supply system (NSSS) control system.

# Control System Design Features

## Design Features - Segmentation

TS

# Control System Design Features

## Design Features – Segmentation (Cont'd)

TS

# Control System Design Features

## Design Features - Segmentation (Cont'd)

TS

# Evaluation for Control Signals Sent to ESF-CCS

Evaluation Result

TS

# Evaluation for Control Signals Sent to ESF-CCS

Evaluation Result (Cont'd)

TS

# Evaluation for Control Signals Sent to ESF-CCS

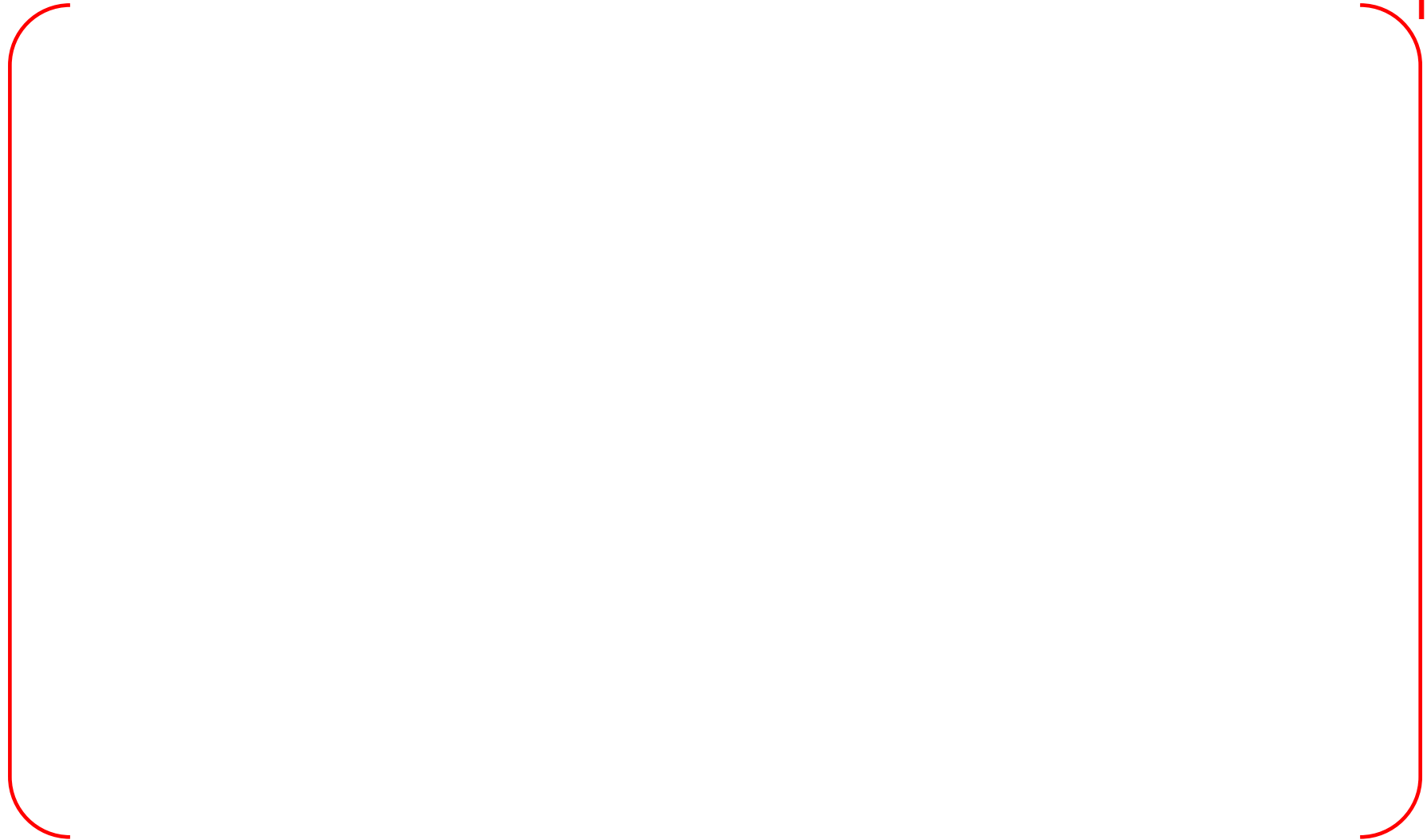
Evaluation Result (Cont'd)

TS

# Evaluation for Failure Type 1

Evaluation Method

TS





# Evaluation for Failure Type 1

## Shared Signal List (1/2)

TS

# Evaluation for Failure Type 1

## Shared Signal List (2/2)

TS

# Evaluation for Failure Type 1

Evaluation Result (example)

TS

# Evaluation for Failure Type 1

Evaluation Result (summary)

TS

# Evaluation for Failure Type 1

## Evaluation Result (summary) (Cont'd)

TS

- Detailed evaluation result will be included in TeR.

# Evaluation for Failure Type 2

Evaluation Method

TS

# Evaluation for Failure Type 2

Evaluation Result (example)

TS

# Evaluation for Failure Type 2

Evaluation Result (example) (Cont'd)

TS



# Evaluation for Failure Type 3

Evaluation Method

TS

# Evaluation for Failure Type 3

Best Estimate Method with Realistic Assumption

TS

# Evaluation for Failure Type 3

Available Systems Credited in the Evaluation

TS

# Evaluation for Failure Type 3

## Qualitative Evaluation

TS

# Evaluation for Failure Type 3

## Quantitative Analysis

TS

# Evaluation for Failure Type 3

Quantitative Analysis Tool : RELAP5

TS

# Evaluation for Failure Type 3

Initialization of RELAP5 for Nominal Initial Condition

TS

# Evaluation for Failure Type 3

Challenge to Fuel Cladding Integrity

TS



# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Fuel Cladding Integrity (Results)

TS



# Evaluation for Failure Type 3

Challenge to Primary System Integrity

TS

# Evaluation for Failure Type 3

## Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

## Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Cont'd)

TS

# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Cont'd)

TS



# Evaluation for Failure Type 3

Challenge to Primary System Integrity (Results)

TS

# Evaluation for Failure Type 4

Evaluation Method

TS

# Evaluation for Failure Type 4

## Evaluation Method (Cont'd)

TS

# Summary

## Summary of Results

TS