# Control System CCF Analysis

## Revision 2

## Non-Proprietary

## January 2018

# REVISION HISTORY

| Revision | Date | Page | Description |
|---|---|---|---|
| 0 | November 2014 | All | First Issue |
| 1 | February 2017 | (Sections) | Revised based on RAI response or editorial correction (RAI Numbers) |
| | | 2 (2.0) | Description for screening process added (8633-20) |
| | | 3 (3.2) | Description for reference added |
| | | 4 and 5 (4.1) | Description for screening process added (8633-20) |
| | | 5 (4.2) | Supplemental description for Figure 4.2-1 added (7892-5) |
| | | 8 and 9 (4.4.2, 4.4.3 and 4.4.4) | Description for DCS fail-over and fault detection features added, and acronyms applied for DCN-I (7892-4) |
| | | 10 and 11 (4.4.4.1) | Description for environmental qualification of IFPD modified (7892-8) |
| | | 11 and 12 (4.4.5 and 4.4.6) | Description for design features to prevent and cope with broadcast storms modified (7892-6) |
| | | 13 (Figure 4.1-1) | Figure 4.1-1 modified to reflect the revised I&C System Overview Architecture (8281-17) |
| | | 14 (Figure 4.1-2) | Figure 4.1-2 modified to add acronyms (7892-5) |
| | | 16 (Figure 4.2-1) | Figure 4.2-1 added for PCS and other non-safety I&C system internal network (7892-5) |
| | | 22 (4.5.4) | Supplemental description added and Figures 4.5-5 modified for component segmentation 1 (7881-17) |

| | | | |
|---|---|---|---|
| | | 23<br>(4.5.4) | Supplemental description added and Figure 4.5-6 modified for component segmentation 1 (7881-15) |
| | | 26<br>(4.5.6) | Supplemental description added for the assignment of control groups (7881-17) |
| | | 27<br>(Table 4.5-2) | Table 4.5-2 modified to add BOP components (8633-20) |
| | | 28 and 29<br>(Table 4.5-3) | Table 4.5-3 added to reflect results of screening process for all control system (8633-20) |
| | | 30<br>(4.6) | Supplemental description added for redundant control loop (7881-16) |
| | | 30<br>(4.7) | Supplemental description added for Interlock/Permissive functions (7881-15) |
| | | 33 thru 37<br>(4.9) | Description modified, figure 4.9-1 through 4.9-4 modified and changed, figure 4.9-5 through 4.9-7 added, and table 4.9-1 modified to make a complete list and summary for control signals from the P-CCS to the ESF-CCS and provide safety evaluation (7892-8) |
| | | 43<br>(4.10) | PCS and NPCS design information added about embedded devices (7881-8) |
| | | 43 and 44<br>(4.10) | Description added and table 4.10-1 added to provide design information about embedded digital devices (8633-18) |
| | | 48, 50 thru 56<br>(5.1.1, 5.1-4, 5.1.4.1 thru 5.1.4.17) | Description for availability of CSV with PRV function added, and Table 5.1-2 thru Table 5.1-18 are combined into one table and sheet number for Table 5.1-2 added (7881-7) |
| | | 53<br>(5.1.4.7 and 5.1.4.8) | Clarification of failure effects of TLI signal about FWCS and SBCS (7892-7) |
| | | 57<br>(5.2.2) | Description for assumption about EMI/RFI added (7881-10) |
| | | 58<br>(5.2.4.1) | Supplemental description added for SBCS main control group (7881-15) |

| | | | |
|---|---|---|---|
| | | 60<br>(5.2.4.6) | Editorial correction (closing → throttling back) (8456-9) |
| | | 56<br>(5.2.4.7) | Description for safety evaluation of CVCS modified (7892-8) |
| | | 62 and 63<br>(5.2.4.8) | Description for multiple failures of RRS/RPCS control group modified (8456-11) |
| | | 65 and 66<br>(5.2.4.11 thru 5.2.4.13) | Editorial correction (Feedwater HP → HP Feedwater) (8633-20) |
| | | 67 and 68<br>(5.2.4.16) | Description for multiple failures of condenser vacuum control group added and modified (8633-20) |
| | | 68<br>(5.2.4.18) | Description for multiple failures of miscellaneous BOP control group added and modified (8633-20) |
| | | 69<br>(5.3.2) | Description for assumptions about Seismic and EMI/RFI added (7881-10) |
| | | 69 and 70<br>(5.3.2) | Description for assumptions of the basis for selection of the initial parameters added (8456-15) |
| | | 70<br>(5.3.2) | Description for multiple failures causing RCS cooldown added and editorial correction (FW HP → HP FW) (8633-20) |
| | | 70<br>(5.3.4) | Acceptance criteria for Failure Type 3 events are modified according to Table 4.1-1 and DCD Chapter 15, Section 15.0.0.1.2 PA acceptance criteria. |
| | | 71<br>(5.3.5.1) | Description for multiple failures about CEA withdrawal added (8456-16) |
| | | 71<br>(5.3.5.1) | The results for Failure Type 3 including BOP components are modified (8633-20) |
| | | 73 and 74<br>(Table 5.1-1) | Clarification for the physical plant components (7881-7) |
| | | 75 thru 92<br>(Table 5.1-2) | Combination of similar information into a single table and sheet number for Table 5.1-2 added (7881-7) |
| | | 82 and 83<br>(Table 5.1-2) | Clarification of failure effects of TLI signal at low power level (7892-7) |

| | | | |
|---|---|---|---|
| | | 93<br>(Table 5.2-1) | Description added and modified for turbine bypass control (7881-15) |
| | | 93 and 94<br>(Table 5.2-1) | Description added and modified for turbine bypass control, control rod control and HP feedwater heater (7881-9) |
| | | 94<br>(Table 5.2-1) | Description added and modified for control rod control and HP feedwater heater (7892-2) |
| | | 94<br>(Table 5.2-1) | Editorial correction (Feedwater HP → HP Feedwater) (8633-20) |
| | | 95<br>(Table 5.2-1) | Description for multiple failures of condenser vacuum and miscellaneous BOP control group added and modified (8633-20) |
| | | 95<br>(Table 5.2-1) | Description of miscellaneous BOP control modified (7881-4) |
| | | 96 thru 113<br>(Table 5.2-1 thru 5.2-18) | Editorial correction (group → Group) |
| | | 101<br>(Table 5.2-7) | Description modified, and editorial correction (12.7 kg/sec → 11.3 kg/sec) (8456-9) |
| | | 103<br>(Table 5.2-9) | Clarification of failure effects of TLI signal at low power level (7892-7) |
| | | 104<br>(Table 5.2-9) | Description for multiple failures of RRS/RPCS control group modified (8456-10, 8456-11), and editorial correction (AMP → AWP) |
| | | 111<br>(Table 5.2-16) | Description for multiple failures of condenser vacuum control group added and modified (8633-20) |
| | | 113<br>(Table 5.2-18) | Description for multiple failures of miscellaneous BOP control group added and modified (8633-20) |
| | | 114<br>(Table 5.3-1) | Description for multiple failures of condenser vacuum and miscellaneous BOP control group added and modified (8633-20) |
| | | 117<br>(Table 5.3-4) | Sequences of Events for Event 1 are modified as recalculated results reflecting BOP components (8633-20) |

| | | | |
|---|---|---|---|
| | | 119<br>(Table 5.4-1) | Description for multiple failures of condenser vacuum and miscellaneous BOP control group added (8633-20) |
| | | 120<br>(Table 5.4-2) | Description for HP FW heater control group added (7881-15) |
| | | 121 thru 125<br>(Figure 5.3-1 thru Figure 5.3-5) | Dynamic behaviors for Event 1 are modified (8633-20) |
| | | 131<br>(7) | Reference added (7892-8) |
| 2 | January 2018 | vii, 2, 4, 47 thru 55, 56 thru 61, 64 thru 71, 130 | Deletion or changes of TS scope in the sections and figures in the following parentheses (ABSTRACT, 2, 4.1, 5.1, 5.1.1 thru 5.1.4, 5.1.4.1 thru 5.1.4.17, 5.2.1 thru 5.2.4, 5.2.4.1 thru 5.2.4.18, 5.2.5, 5.3.1 thru 5.3.5, 5.3.5.1 thru 5.3.5.2, 5.3.6, 5.4, 6, 7, Figure 4.1-1)<br>Revision bars are omitted because there are no technical changes. |
| | | (Sections) | Revised based on RAI response or editorial correction (RAI Numbers) |
| | | 12<br>(4.4.6) | Editorial correction (HIS → HSI) |
| | | 43<br>(4.10) | Diversity evaluation for ultrasonic level transmitters is moved to the Diversity and Defense-in-Depth TeR, APR1400-Z-J-NR-14002-P (8633-18) |
| | | 131<br>(7) | Reference added (8633-18), and reference publication date modified |

# ABSTRACT

This technical report (TeR) provides the results of the evaluation for postulated non-safety control system common-cause failures (CCFs) for APR1400.

TS

The pertinent features of the control systems, including the architecture of the distributed control system (DCS), credited in this evaluation are described in this technical report.

One key feature of the DCS that ensures the failure of a single non-safety control group does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences (AOOs) in Chapter 15, is that major control functions, such as pressurizer level control and feedwater control, are distributed to separate control groups. Each control group consists of at least one separate controller and includes at least one control system.

The following Failure Types due to a shared signal failure and CSCCFs are evaluated to confirm that the DCD Chapter 15 analysis acceptance criteria are met.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to a CSCCF
- Failure Type 3 : multiple failures of more than one control group due to a CSCCF
- Failure Type 4 : multiple failures of Information Flat Panel Display (IFPD) control commands due to a CSCCF

For all Failure Types above, the failure effect on multiple control functions and multiple plant components is considered.

For Failure Types 1 and 2, the qualitative evaluations are performed. This report concludes that the event consequences of the transients caused by a shared signal failure and the postulated CCFs are bounded by the acceptance criteria of AOOs presented in DCD Chapter 15.

For Failure Types 3 and 4, the worst combinations of multiple failures with respect to fuel cladding integrity and primary system integrity are quantitatively evaluated using the RELAP5 code. This report concludes that the event consequences caused by the postulated CSCCFs are bounded by the acceptance criteria of postulated accidents (PAs) in DCD Chapter 15.

TS

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AMI | automatic motion inhibit |
| AOO | anticipated operational occurrence |
| APR1400 | Advanced Power Reactor 1400 |
| AWP | automatic withdrawal prohibit |
| BAST | boric acid storage tank |
| BOP | balance of plant |
| CCF | common cause failure |
| CCS | component control system |
| CCW | component cooling water |
| CDP | condensate pump |
| CEA | control element assembly |
| CEAC | control element assembly calculator |
| Ch. | 1) Chapter, 2) channel |
| CIAS | containment isolation actuation signal |
| CPCS | core protection calculator system |
| CPC | core protection calculator |
| CSCCF | control system common cause failure |
| CVCS | chemical and volume control system |
| CWP | 1) CEA withdrawal prohibit, 2) circulating water pump |
| DCD | design control document |
| DCN-I | data communication network-information |
| DCS | distributed control system |
| DBE | design basis event |
| DNBR | departure from nucleate boiling ratio |
| DRCS | digital rod control system |
| DV | downcomer valve |
| ESCM | ESF-CCS soft control module |
| ESFAS | engineered safety features actuation system |
| ESF-CCS | engineered safety features – component control system |
| EV | economizer valve |
| FW | feedwater |
| FWCS | feedwater control system |
| HART | highway addressable remote transducer |
| HPPT | high pressurizer pressure trip |

| | |
|---|---|
| HSI | human-system interface |
| HTR | heater |
| HVAC | heating, ventilation, and air conditioning |
| I&C | instrumentation and control |
| I/O | input/output |
| IFPD | information flat panel display |
| IPS | information processing system |
| KHNP | Korea Hydro & Nuclear Power Co. Ltd. |
| LCO | limiting conditions for operation |
| LEL | lower electrical limit |
| LOCV | loss of condenser vacuum |
| LOF | loss of flow |
| LONF | loss of normal feedwater |
| LPD | local power density |
| MCR | main control room |
| MFIV | main feedwater isolation valve |
| MFWP | main feedwater pump |
| Mod. | modulation |
| MSIV | main steam isolation valve |
| MSIS | main steam isolation signal |
| MSSV | main steam safety valve |
| MTC | moderator temperature coefficient |
| NFO | not fully open |
| NIMS | NSSS integrity monitoring system |
| NPP | nuclear power plant |
| NPCS | NSSS process control system |
| NRC | Nuclear Regulatory Commission |
| NSSS | nuclear steam supply system |
| PA | postulated accident |
| Perm. | permissive |
| P&ID | piping and instrumentation diagram |
| PAMI | post accident monitoring instrumentation |
| P-CCS | process-component control system |
| PCS | power control system |
| PLCS | pressurizer level control system |
| POSRV | pilot operated safety and relief valve |

| | |
|---|---|
| PPCS | pressurizer pressure control system |
| PRV | process representative value |
| PZR | pressurizer |
| RCP | reactor coolant pump |
| RCS | reactor coolant system |
| RDT | reactor drain tank |
| RMS | radiation monitoring system |
| RPCS | reactor power cutback system |
| RRS | reactor regulating system |
| RSPT | reed switch position transmitter |
| RSR | remote shutdown room |
| SBCS | steam bypass control system |
| SFADL | specified acceptable fuel design limit |
| SIAS | safety injection actuation signal |
| Tavg | average temperature |
| TBV | turbine bypass valve |
| TBN | turbine |
| Tcold | cold leg temperature |
| TCS | turbine control system |
| Tref | reference temperature |
| VOPT | variable over power trip |
| UEL | upper electrical limit |
| UGS | upper group stop |

Page intentionally blank

# 1. PURPOSE

The purpose of this technical report (TeR) is to determine the effects of the postulated common cause failures (CCFs) on the non-safety control system, describe the methodology for evaluating those function/component effects on the plant, and document the evaluation results for the Advanced Power Reactor 1400 (APR1400) design.

## 2. SCOPE

This TeR provides the evaluation methods and results of the evaluation for the postulated control system CCF (CSCCF).

The non-safety control systems of primary and secondary systems are considered for the evaluation as described in Section 4.1. All control systems of the primary and secondary systems described in the design control document (DCD) Chapter 7.7 and Chapter 15 are included in the evaluation for the postulated CSCCF, TS

TS

Therefore, CCFs within the non-safety control system are considered. The results of screening process for all control systems in the APR1400 plant are presented in Section 4.1 and Table 4.5-3.

TS

The expected failures due to a shared signal failure and CSCCF are divided into four parts as follows.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of Information Flat Panel Display (IFPD) control commands due to CSCCF

TS

Failure Types 1 and 2 are evaluated to meet the AOO acceptance criteria of the DCD Chapter 15. Refer to Sections 5.1 and 5.2 for the evaluation method and the results.

Failure Types 3 and 4 are evaluated to meet the PA acceptance criteria of the DCD Chapter 15. Refer to Sections 5.3 and 5.4 for the evaluation method and the results.

# 3. APPLICABLE CODES AND REGULATIONS

The following subsections provide applicable codes and regulations.

## 3.1. 10 CFR 50.55a(h), “Protection and Safety Systems”

The 10 CFR 50.55a(h) endorses IEEE Std. 603.

## 3.2. IEEE Standard 603

The compliance with Clause 4.8 of IEEE Std. 603-1991 (Reference 3) is described in this TeR.

The non-safety control system is designed to have the compliance with Clauses 4.8 and 5.6.3 of IEEE Std. 603-1991.

IEEE Std. 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

For the compliance with Clauses 4.8 and 5.6.3 of IEEE Std. 603-1991, the evaluation methods and results for the postulated CSCCF are described in this TeR.

# 4. CONTROL SYSTEM DESIGN FEATURES TO PREVENT CCF

This section describes design features of the non-safety control systems and safety systems that (1) prevent failures that could otherwise lead to a CCF, (2) reduce the adverse effect of CCFs or (3) allow coping with CCFs.

## 4.1. Credible Failure Boundary

The primary and secondary control systems are evaluated for the postulated CCFs. Table 5.2-1 shows the control groups of primary and secondary systems evaluated for the postulated CCFs. Each control group consists of at least one separate controller and includes at least one control system. For the major control systems of primary and secondary systems, refer to Figure 4.1-2.

The control systems listed in Table 5.2-1 and described in DCD Chapter 7.7 and Chapter 15 are considered for the evaluation for the postulated CSCCF, TS

TS

A system is identified as being capable of affecting critical safety functions if that control system can affect the reactivity, the RCS pressure, the RCS temperature, the RCS flow, or the RCS inventory of the primary system, because its failure can challenge fuel cladding integrity, or primary system integrity and ultimately can affect critical safety functions. The following critical safety functions which can challenge the analysis acceptance criteria presented in DCD Tier 2, Section 15.0 are considered to determine the limiting initiating events for the control system CCF analysis.

- Challenge to fuel cladding integrity
- Challenge to primary system integrity
- Challenge to offsite dose limit
- Challenge to containment integrity

Most of the control systems are implemented by a DCS-based common platform that has been proven by operating experiences in the nuclear industry and other industries.

The DCS conducts the functions of operator interface, component level control, automatic process control, high-level group control, and data processing for normal operation. The DCS is designed with a redundant and fault-tolerant architecture for high reliability and to minimize and prevent the failure of a single component from causing a spurious plant trip.

Some instrumentation and control (I&C) systems are implemented by self-standing systems.

As the non-safety control systems are software-based systems that are susceptible to a software defect, the design features and evaluation are necessary to prevent CSCCF.

TS

TS

### 4.2. Control System Overview

The non-safety control systems consist of the power control system (PCS) and the process-component control system (P-CCS).

The PCS includes the reactor regulating system (RRS), the digital rod control system (DRCS), and the reactor power cutback system (RPCS).

The P-CCS includes the NSSS process control system (NPCS) and balance of plant (BOP) control systems. The NPCS consists of the feedwater control system (FWCS), steam bypass control system (SBCS), pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), and other miscellaneous nuclear steam supply system (NSSS) control functions.

The BOP control systems provide discrete and continuous control of normally used non-safety BOP processes including radwaste control system.

Major control systems of NSSS are PCS and NPCS which include RRS, RPCS, DRCS, PPCS, PLCS, SBCS, and FWCS. Refer to Figure 4.1-2.

The internal network of PCS and other non-safety I&C systems is shown in Figure 4.2-1.

### 4.3. Credible Failure Types of Control System CCF

Credible failures of the CSCCF are initiating events caused by the control system failure that can affect critical safety functions.

As each major control function is assigned to a separate control group which consists of at least one controller, the following 4 credible Failure Types are assumed as credible failures. Refer to Table 4.1-1.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to CSCCF

Table 4.1-1 Credible Failure Types

| Failure Type | Evaluation Criteria |
|---|---|
| Failure Type 1 : Multiple function failures due to a single failure of a shared signal | To be bounded by DCD Chapter 15 AOO acceptance criteria |
| Failure Type 2 : Multiple failures of a single control group due to CSCCF | |

| Failure Type | Evaluation Criteria |
|---|---|
| Failure Type 3 : Multiple failures of more than one control group due to CSCCF | To be bounded by DCD Chapter 15 PA acceptance criteria |
| Failure Type 4 : Multiple failures of IFPD control commands due to CSCCF | |

Refer to Figure 4.1-3 for the overview of the four Failure Types. The evaluation results of the four Failure Types are described in Section 5.

### 4.4. Control System Design Features

To reduce the likelihood of CSCCF, the control system is designed to have the following design features:

- Each control function in DCD Chapter 7.7 is assigned to separate control group that consists of at least one separate controller to limit the failure in the control group (segmentation)[1]. Refer to Section 4.5.
- A redundant controller for increased availability
- Interlock/permissive functions by a separate control group or safety system to limit the failure effects (e.g., control element assembly (CEA) withdrawal interlock signals, turbine bypass valve (TBV) permissive signals)[2]
- 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 the control groups within PCS and NPCS[3]
- Diagnostic and alarming functions
- Design features of the IFPD to defend against a design basis event (DBE) due to single random hardware failure (e.g., broadcast storm)[1]

[1] Control group segmentation and design features to protect broadcast storm are credited in the evaluation of Failure Types 1 and 2. For the design features of broadcast storm, refer to Section 4.4.5.

[2] Permissive functions of SBCS permissive control group are credited in the evaluation of Failure Types 1 and 2.

[3] Refer to Figure 4.1-3 and Table 5.1-1.

Each design feature listed above is described in the following sections.

#### 4.4.1. Segmentation of Major Functions

Segmentation is a process that separates and groups components, including instrument and control functionality in a non-safety DCS controller.

Functional allocation is performed to minimize the effects of single failures in the nuclear power plant (NPP). Maintaining the dependent and independent relationships established by the plant functional design is achieved by allocating specific functions (e.g., monitoring, control) to specific processors and by allocating specific inputs and outputs to specific input/output (I/O) modules (e.g., boards, personality/base modules).

Segmentation is credited to limit the effects of a single failure within a controller to the functions controlled by that controller. However, even with segmentation, erroneous signals that may result from a single failure, and that propagate to other controllers, are evaluated in this analysis for their effect on the functions controlled by those other controllers.

Segmentation can also be credited to limit the effect of a software defect to a single controller, regardless of that defect existing in multiple controllers. This can be done by demonstrating that each controller has different inputs and application programs. Therefore, the same defect is unlikely to be triggered in multiple controllers concurrently.

Due to the continuous operation of most control systems, triggered failures are self-announcing because they cause component repositioning. Therefore, when the defect is announced, it can be corrected in all controllers, before it causes a CCF of multiple controllers.

The detailed requirements of segmentation are described in Section 4.5. Though the segmentation of control functions makes the concurrent failure of those multiple control functions highly unlikely, multiple concurrent failures of more than one control group due to a CCF is considered as a credible failure and is evaluated in Section 5.3 as a beyond design basis event.

#### 4.4.2. Redundancy

The control system is provided with the following redundancies in the platform design:

- Digital processors
- Input/output modules
- Communication networks
- Power supply

Non-safety system cabinets include redundant power supplies with outputs auctioneered to power the digital processors, I/O modules, and other system peripherals. No loss of function occurs when either power supply is turned off or on, with the other supply being powered.

The non-safety system incorporates network communication configurations that have dual or redundant communication paths.

The non-safety system incorporates digital processors in configurations that have redundant processing. A failure that results in shutdown of the primary processor will automatically hand off system functionality to a backup processor. The non-safety system incorporates redundancy with selected inputs or outputs.

There are different approaches available to incorporate this redundancy. Depending on the approach taken, component and instrument segmentation are considered to that extent needed to preserve the desired fault tolerance for safety analysis.

Failure of the primary controller would result in fail-over to the standby controller and an alarm. Failure of the standby controller would only result in an alarm as the primary controller is already controlling.

TS

Redundancy enhances system availability due to many component failures. However, redundancy cannot prevent the adverse effects from a failure that results in erroneous or spurious signals.

Therefore, redundancy is not credited in the Failure Type 1, 2, 3 or 4 analyses.

#### 4.4.3. Diagnostic and Alarming Functions

For all applications the non-safety DCS controller is provided in a redundant-pair configuration to provide fault tolerance. The non-safety DCS controller is fully redundant with a backup controller designed to operate in a masterless scheme. Each controller in the redundant pair executes the same application with the primary controlling the outputs while the secondary tracks the primary. Fail-over detection and switching control to the backup process controller is done automatically and smoothly.

The non-safety DCS controller utilizes multiple control areas to support multitasking and preemptive task scheduling. The controller has high-capacity control capability. The functions executed within one controller are typically limited only by the amount of memory or flash disk available, to execute simple or complex modulating and sequential control and by the throughput performance required for the application.

TS

[redacted]

Diagnostic and alarming functions are not credited in the Failure Type 1, 2, 3 or 4 analyses.

#### 4.4.4. Design Features of the Information Flat Panel Display

##### 4.4.4.1. Design Features to Prevent Spurious Control Commands

TS

[redacted]

TS

TS

### 4.4.5. Design Features to Prevent CCF Due to Broadcast Storms on the DCN-I Network

TS

TS

[redacted]

#### 4.4.6. Design Features to Cope with Broadcast Storms on the IFPD/ESCM Ethernet Networks TS

[redacted]

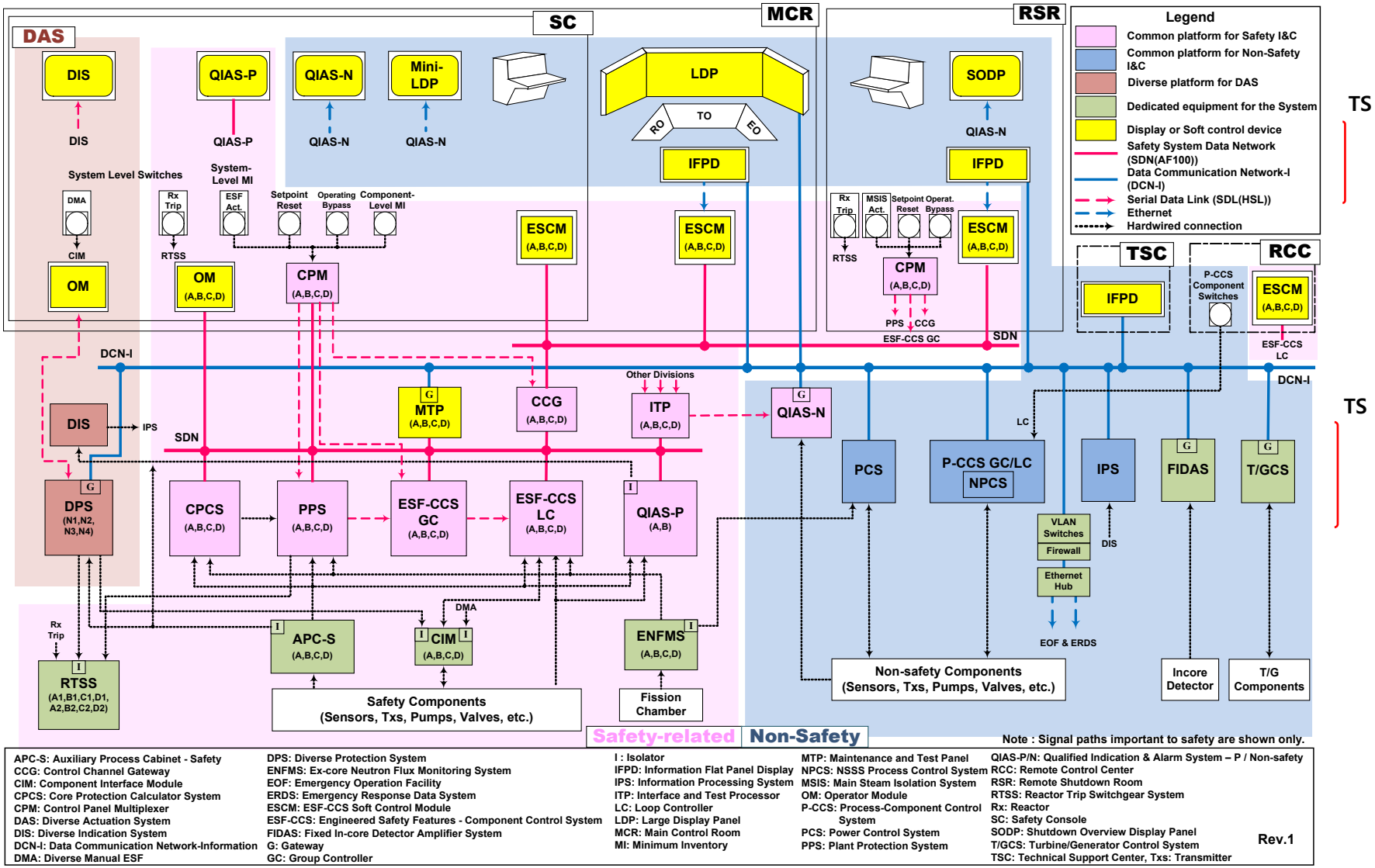


Figure 4.1-1 Credible Failure Boundary of Control System CCF

TS

Figure 4.1-2 Control System Overview

TS

Figure 4.1-3 Overview of 4 Credible Failure Types

TS

Figure 4.2-1 Internal Network of PCS and Other Non-safety I&C Systems

TS

Figure 4.4-1 Data Communication between the IFPD and DCS Controller

### 4.5. Segmentation

A majority of the plant components do not possess a unique functional identity in that they are not individually important to the plant but are collectively important as a part of a subsystem or group. Looking at a system simplistically, the valves in a fluid flow path are of little importance without the pump that drives the fluid unless a major pressure difference exists. Conversely, the pump is of no value if the valves in a fluid flow path cannot be opened. This fundamental observation is the basis for the system configuration of the non-safety control system.

The grouping is performed on the non-safety control system design based on observing two levels of functional based grouping. This task is performed using the following methodology and definitions.

- Functional grouping - The first level of groupings establish a set of groupings that are consistent with functional boundaries of the physical systems, system definitions, and based on an overview of a grouping of systems and functions (e.g., primary systems, secondary systems, and support systems).

- Component groupings - The second level of groupings follow a very simplistic perspective to further group components defined by functional grouping consistent with functional plant processes.

The functional grouping and component grouping are not credited in the Failure Type 1, 2, 3 or 4 analyses.

After the functional grouping and component grouping, for CSCCF functional segmentation and component segmentation are applied to reduce the likelihood of potential credible failures, to mitigate the effects of the potential credible failures. The functional segmentation and component segmentation 1, 2 are described in Section 4.5.3, 4.5.4 and 4.5.5.

The functional segmentation and component segmentation are credited in Failure Type 1 and 2 analyses.

#### 4.5.1. Functional Grouping

TS

TS

Figure 4.5-1 Critical Functions and Success Paths (Example)

#### 4.5.1.1. Power Source Segregation

Plant components and the associated instrument loops are divided into the following power divisions:

**Table 4.5-1 Segregation of Power Source**

| Power Division | Channel Designation |
|---|---|
| Non-Safety 'A' | AB (N1) |
| Non-Safety 'B' | BB (N2) |

Components belonging to each division are grouped and assigned to controllers. Each division AB and BB have the required number of groups depending upon its ability to satisfy the design philosophy.

All controllers are redundant and are powered from two separate power supplies within the same electrical division. Therefore, a credible failure of a power source has no adverse effect on any control functions.

### 4.5.2. Component Grouping

TS

Figure 4.5-2 Independent Configuration (Example)

Figure 4.5-3 Serial Configuration (Example)

TS

Figure 4.5-4 Parallel Configuration (Example)

### 4.5.3. Functional Segmentation

TS

### 4.5.4. Component Segmentation 1

TS

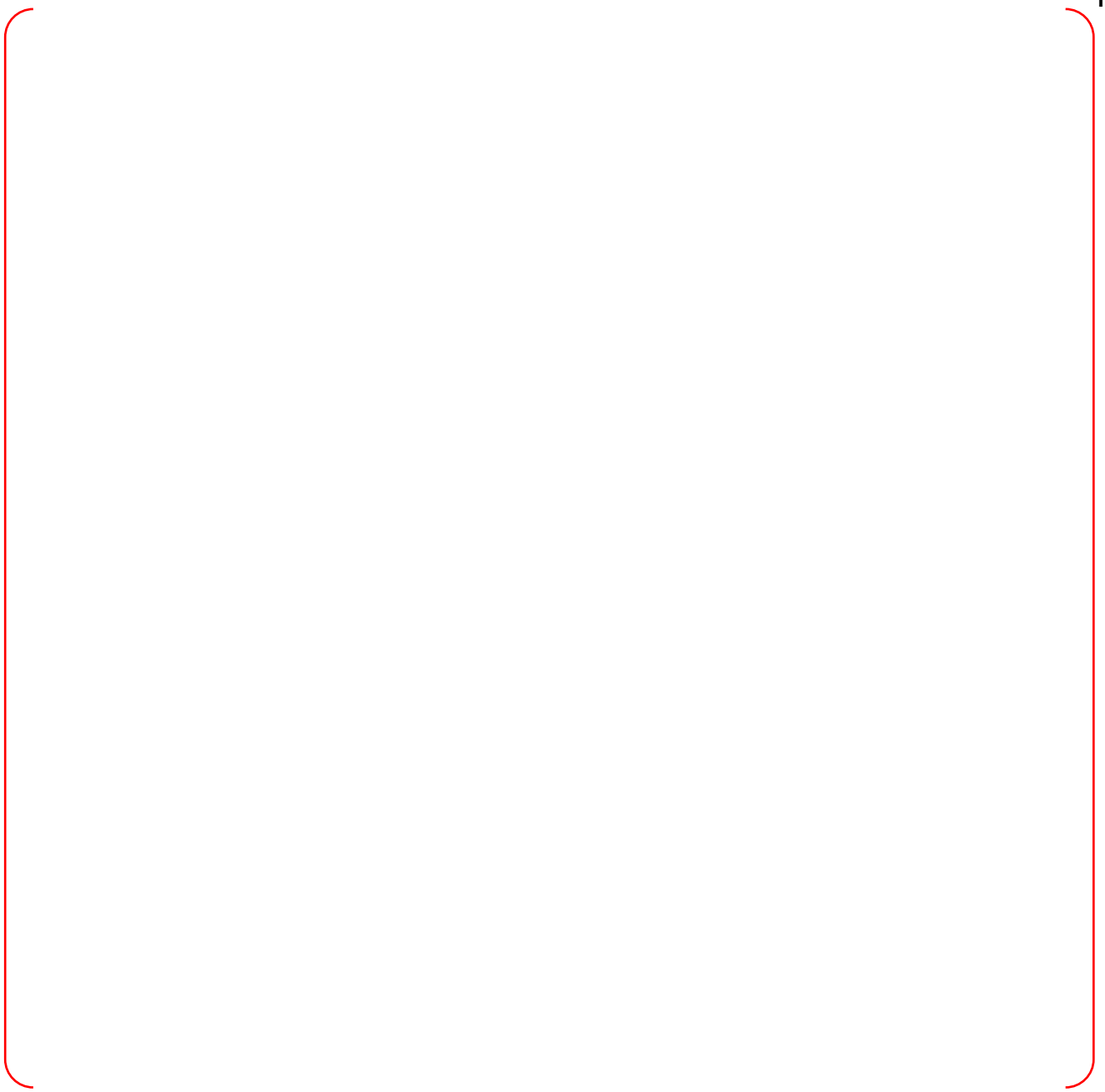

Figure 4.5-5 Component Segmentation 1 for SBCS Turbine Bypass Control

TS

Figure 4.5-6 Component Segmentation 1 for High Pressure FW Heater

TS

TS

Figure 4.5-7 SBCS Main Functional Block Diagram

TS

Figure 4.5-8 SBCS Permissive Functional Block Diagram

TS

Figure 4.5-9 HP FW Heater Functional Block Diagram

### 4.5.5. Component Segmentation 2

TS

### 4.5.6. Control Group

Control groups are assigned in accordance with the functional segmentation and component segmentation 1 and 2.

Refer to Table 4.5-2 for the control groups of non-safety control systems and the applied segmentation methodology.

TS

Table 4.5-2 Control Group

TS

Table 4.5-3 Results of Screening Process for All Control System in the APR1400 Plant (Sh. 1 of 2) TS

Table 4.5-3 Results of Screening Process for All Control System in the APR1400 Plant (Sh. 2 of 2) TS

### 4.6. Redundant Controller for Availability Enhancement

Each DCS controller of PCS and P-CCS is provided with redundant processor, power supply, and data communication network.

For NSSS control functions, PCS and NPCS use redundant control loop and control signal validation design as identified in Sections 4.8 and 5.1.1, Table 5.1-1, and Figure 4.1-3.

For RCP and BOP control functions, the following equipment control logic circuits are designed as completely redundant control loop. The redundant control loop is provided with redundant controllers with two I/O modules. These control circuits perform their functions to be completely separated from each other. The redundant controllers and I/O modules access simultaneously the field data and if one controller or I/O module fail, the other controller or I/O module can perform automatically the functions of controller or data acquisition/signal initiation without bump.

- Control logic for RCPs
- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers
- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

Any one failure is annunciated in the MCR and RSR.

### 4.7. Interlock/Permissive Functions by Separate Control Group or Safety system

TS

Table 4.7-1 Control Limit and Interlocks on Digital Rod Control System

| Conditions of Interlocks | Functions | Signal Path |
|---|---|---|
| Upper electrical limit (UEL) and lower electrical limit (LEL) signals from reed switch position transmitter (RSPT). | Interlock: Blocks control rod withdrawal or insertion on automatic, manual group and manual individual DRCS control modes. | RSPT → DRCS (UEL, LEL) |
| Automatic withdrawal prohibit (AWP) signals from RRS and SBCS when Tavg is much higher than Tref, Tcold is high, or any opening demand of TBVs is generated in accordance with excessive energy in the NSSS. | Interlock: Blocks control rod withdrawal on automatic DRCS control mode. | RRS → DRCS (AWP)<br>SBCS → DRCS (AWP) |
| Upper group stop (UGS) and lower group stop (LGS) function in the DRCS | Control Limit: Blocks control rod withdrawal or insertion on automatic and manual group DRCS control modes. | DRCS (UGS, LGS) |
| CEA withdrawal prohibit (CWP) signal from PPS. | Interlock: Blocks control rod withdrawal on automatic, manual group and manual individual DRCS control modes. | PPS → DRCS (CWP) |

### 4.8. Control Signal Validation

Where there are at least three identical process parameter inputs including control and safety systems, a valid process representative value (PRV) calculated in the information processing system (IPS) are used to select a valid control signal, where necessary.

The control system takes action based on a sensor signal that is selected by a PRV that reflects a valid process representative value. PRV is used only as a reference value for a channel selection. One value is selected among Channel 1 and Channel 2 or average in accordance with control signal validation algorithm.

If the deviation between the input channels exceeds an acceptable level, the input channel that has less deviation from the PRV is used as the control signal.

Therefore, there are fewer challenges to plant safety due to control system errors, since failed sensors are detected and eliminated before they adversely impact control system performance.

IPS failure would affect the control function, only if there is an additional failure of an input channel. Refer to Subsection 7.7.1.1 of DCD.

TS

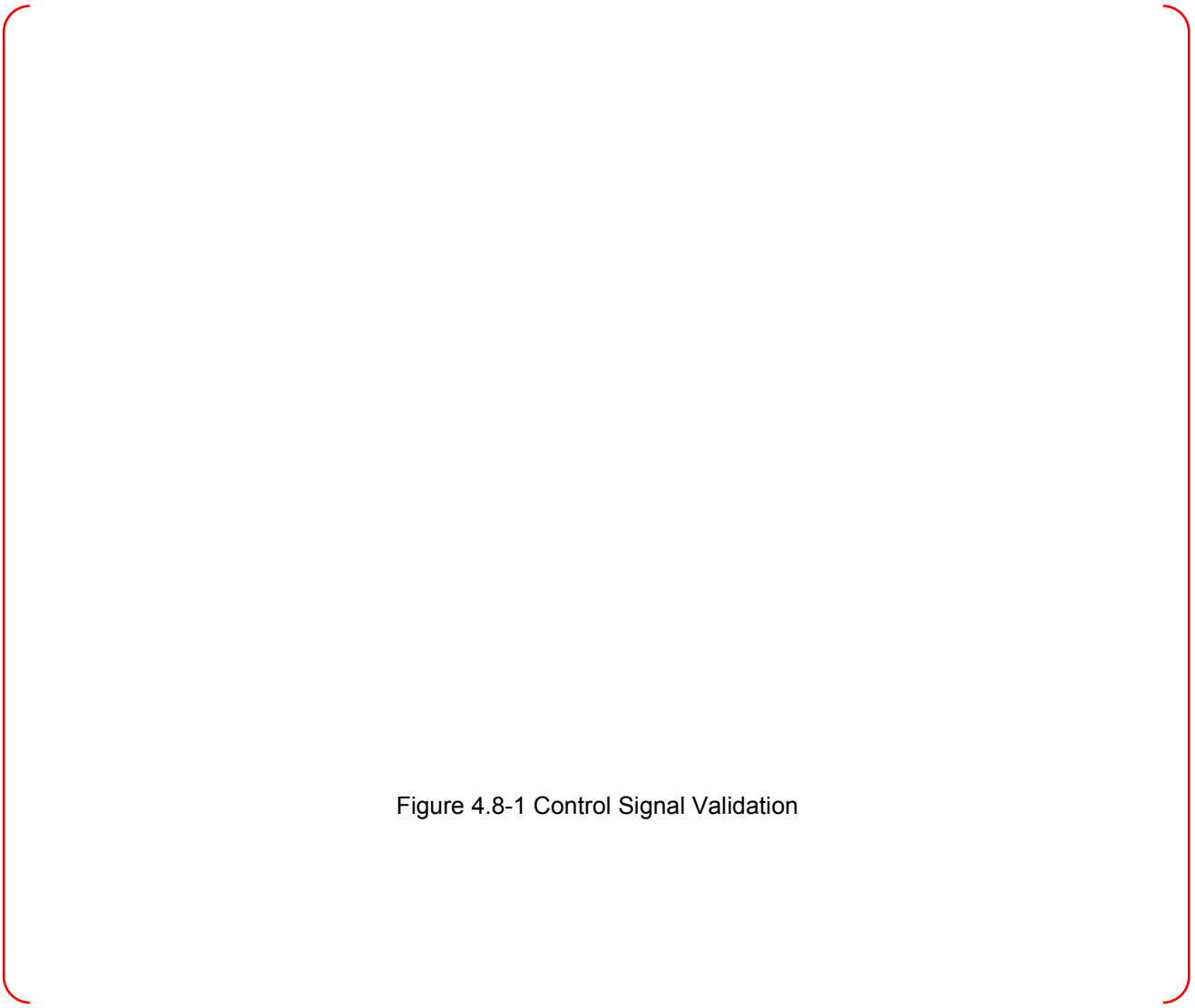

Figure 4.8-1 Control Signal Validation

### 4.9. Non-safety Control Signals Sent to ESF-CCS

TS

[ ]

### 4.9.1. Evaluation of the Non-safety Control Signal for CVCS

TS

[ ]

TS

Figure 4.9-1 Non-safety Control Signals Sent from P-CCS to ESF-CCS for ESF Valves (Typical)

TS

Figure 4.9-2 ESF-CCS Control Logic against Non-Safety Signal Failure

TS

Figure 4.9-3 Non-safety Control Signals Sent from P-CCS to ESF-CCS for Reactor Coolant Makeup

### 4.9.2. Evaluation of the Non-safety Control Signal for Class 1E 4.16kV System

TS

TS

Figure 4.9-4 Configuration of Class 1E 4.16kV Bus

TS

Figure 4.9-5 Simplified Signal Flow for UAT-PCB and SAT-PCB

### 4.9.3. Evaluation of Other Non-safety Control Signals

TS

#### 4.9.3.1. Evaluation of the Non-safety Control Signal for Case A

Figure 4.9-6 Simplified ESF-CCS Control Logic for Case A

#### 4.9.3.2. Evaluation of the Non-safety Control Signal for Case B

TS

Figure 4.9-7 Simplified ESF-CCS Control Logic for Case B

Table 4.9-1 Non-safety Control Signals sent from P-CCS to ESF-CCS (Sh. 1 of 3)

TS

Table 4.9-1 Non-safety Control Signals sent from P-CCS to ESF-CCS (Sh. 2 of 3)

TS

Table 4.9-1 Non-safety Control Signals sent from P-CCS to ESF-CCS (Sh. 3 of 3)

TS

### 4.10. CCF Analysis of Embedded Devices in Field Equipment

TS

[redacted]

#### 4.10.1. Evaluation for the CCF of Non-safety Field Instruments

TS

[redacted]

TS

### 4.10.2. Evaluation for the CCF of Non-safety Field Actuators

TS

### 4.10.3. Evaluation for the Effect on Field Instruments due to Controller Failures

### 4.10.4. Evaluation for the Effect on Field Actuators due to Controller Failures

TS

# 5. EVALUATION METHOD AND RESULTS

This section describes the evaluation methods and results for the postulated CSCCF of the control system. Depending on the Failure Types, limiting initiating events caused by CSCCF are selected and the qualitative evaluations are performed to verify that the results of initiating events are bounded by the same acceptance criteria of the design basis accidents presented in the DCD Chapter 15. Where necessary for some events, quantitative evaluations are performed to confirm that the analysis acceptance criteria are met.

The expected failures due to a shared signal failure and CSCCF are divided into four types as follows.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to CSCCF

Initiating events are those events that upset plant stability and challenge critical safety functions during shutdown as well as power operations. The following critical safety functions which can challenge the analysis acceptance criteria are considered to determine the limiting initiating events for Failure Types 1, 2, 3 and 4.

- Challenge to fuel cladding integrity
- Challenge to primary system integrity
- Challenge to offsite dose limit
- Challenge to containment integrity

However, a challenge to containment integrity is not of concern because a control system failure of any type, including a CCF, cannot cause a pipe break in containment.

### 5.1. Failure Type 1: Multiple Failure due to a Single Failure of Shared Signal

As shown in Table 5.1-1, the shared signals for the APR1400 primary and secondary system consist of reactor power, PZR pressure, RCS average temperature, turbine load index, PZR level, SG steam flow, steam header pressure and non-class 1E 13.8 kV Lo-Lo. Table 5.1-1 addresses all shared signals whose failure causes multiple function failures in two or more control groups.

As shown in Table 5.1-1 and Figure 4.1-3, shared signals are connected to a single control group or more than one control groups. The signal is shared by multiple functions within that control group and by other functions in the other control groups. TS

The cases for the failed shared signal are presented in Table 5.1-1 and are evaluated as Failure Type 1 in Section 5.1.

TS

#### 5.1.1. Assumptions Used in the Evaluation

The following assumptions are used in the evaluation. TS

TS

### 5.1.2. Initial Conditions

The initial condition of Failure Type 1 events is same as that of DCD Chapter 15 events.

### 5.1.3. Acceptance Criteria

Acceptance criteria for Failure Type 1 events are the same as those of DCD Chapter 15 AOO.

- Maximum RCS pressure: less than 110% of design value
- Maximum SG pressure: less than 110% of design value
- Fuel failure: transient departure from nucleate boiling ratio (DNBR) does not violate specified acceptable fuel design limit (SAFDL)

### 5.1.4. Evaluation Results

When a single failure of shared signals occurs, multiple failures of two or more than two control groups can be happened. The following shared signals are evaluated during high and low fail.

- Reactor power
- PZR pressure
- RCS average temperature
- Turbine load index
- PZR level
- SG steam flow
- Steam header pressure

- 13.8kV Lo-Lo

The evaluation results are shown in Tables 5.1-2.

#### 5.1.4.1. Reactor power signal fails low

TS

[ ]

TS

[ This evaluation is summarized in Table 5.1-2 (Sh. 1 of 18). Therefore, this failure is bounded by DCD Chapter 15.2.3 (Loss of condenser vacuum, LOCV). ]

TS

[ ]

#### 5.1.4.2. Reactor power signal fails high

TS

[ ]

TS

[ This evaluation is summarized in Table 5.1-2 (Sh. 2 of 18). This failure is bounded by DCD Chapter 15.1.2 (Increase in feedwater flow). ]

TS

[ ]

#### 5.1.4.3. PZR pressure fails low

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 3 of 18).

This failure is bounded by DCD Chapter 15.2.3 (Loss of condenser vacuum).

#### 5.1.4.4. PZR pressure fails high

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 4 and 5 of 18).

The CPCS is based on the results of pressurizer spray malfunction event to prevent fuel failure. There is no fuel failure because the low DNBR signal is generated by CPCS before transient DNB reaches the SAFDL.

#### 5.1.4.5. RCS temperature fails low

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 6 of 18).

Therefore, this failure is bounded by DCD Chapter 15.4.2 (Uncontrolled Control Element Assembly Withdrawal at Power).

TS

#### 5.1.4.6. RCS temperature fails high

TS

This evaluation is summarized in Table 5.1-2 (Sh. 7 of 18).

TS

This failure is bounded by DCD Chapter 15.4.3 (Control Element Assembly Misoperation).

TS

#### 5.1.4.7. TLI fails low

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 8 of 18).

This failure is bounded by DCD Chapter 15.4.3 (Control Element Assembly Misoperation). This failure is not more severe than the dropped CEA event of DCD Chapter 15.4.3 in terms of the CEA insertion time.

#### 5.1.4.8. TLI fails high

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 9 of 18).

This failure is bounded by DCD Chapters 15.4.1 and 15.4.2 (uncontrolled CEA withdrawal at low power and power).

#### 5.1.4.9. PZR level fails low

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 10 of 18).

This failure is bounded by DCD Chapter 15.5.2 (CVCS malfunction that increases the reactor coolant inventory).

#### 5.1.4.10. PZR level fails high

TS

TS

This evaluation is summarized in Table 5.1-2 (Sh. 11 of 18).

Therefore, this failure is bounded by DCD Chapter 15.6.2 (Failure of small lines carrying primary coolant outside the containment).

#### 5.1.4.11. SG 1 steam flow fails low

TS

Therefore, a reactor trip does not occur during this failure and normal operation is maintained continuously. The evaluation result is shown in Table 5.1-2 (Sh. 12 of 18).

#### 5.1.4.12. SG 2 steam flow fails low

TS

This evaluation is summarized in Table 5.1-2 (Sh. 13 of 18).

Therefore, reactor trip does not occur during this failure and normal operation is maintained continuously.

#### 5.1.4.13. SG 1 steam flow fails high

TS

TS

This evaluation result is shown in Table 5.1-2 (Sh. 14 of 18).

This failure is bounded by DCD 15.1.4 (Inadvertent opening of a steam generator relief or safety valve).

TS

#### 5.1.4.14. SG 2 steam flow fails high

TS

The evaluation result is shown in Table 5.1-2 (Sh. 15 of 18).

Therefore, reactor trip does not occur during the failure and normal operation is maintained continuously.

#### 5.1.4.15. Steam header pressure fails low

TS

The evaluation result is shown in Table 5.1-2 (Sh. 16 of 18).

Therefore, this failure is bounded by DCD Chapter 15.2.3 (Loss of condenser vacuum).

#### 5.1.4.16. Steam header pressure fails high

TS

This evaluation result is shown in Table 5.1-2 (Sh. 17 of 18).

This failure is bounded by DCD Chapter 15.1.2 (Increase in feedwater flow).

#### 5.1.4.17. Non-Class 1E 13.8kV Lo-Lo

TS

TS

Therefore, this failure is bounded by DCD Chapter 15.2.6 (Loss of Nonemergency AC Power).

Therefore, this failure is bounded by DCD Chapter 15.2.6 (Loss of Nonemergency AC Power).

The failure is bounded by DCD Chapter 15.2.6 (Loss of nonemergency AC power).

This evaluation result is shown in Table 5.1-2 (Sh. 18 of 18).

## 5.2. Failure Type 2: Multiple Failure due to Single Control group

### 5.2.1. Selection of Initiating Events

The input failure and a CSCCF of the control group cause spurious outputs of the each control group as fail high, fail low or fail as-is. Multiple failures of a single control group are assumed as initiating events with respect to fuel cladding integrity and primary system integrity. Two worst combinations of multiple failures are separately selected in view of fuel cladding integrity and primary system integrity respectively. The control group segmentation are presented in Table 5.2-1 and the eighteen cases of spurious component actuation due to a single control group failure are evaluated as shown in Tables 5.2-2 through 5.2-18.

### 5.2.2. Assumptions Used in the Evaluation

The following assumptions are used in the evaluation.

TS

### 5.2.3. Acceptance Criteria

TS

### 5.2.4. Evaluation Results

#### 5.2.4.1. Turbine Bypass Control (SBCS Main)

TS

Based on the above evaluation, it is concluded that multiple failure of the SBCS main control group has no effect on the plant and does not cause plant conditions more severe than the analysis of DCD Chapter

15 AOOs. The evaluation result is shown in Table 5.2-2.

#### 5.2.4.2. Turbine Bypass Control (SBCS Permissive)

This failure is the same as multiple failures of SBCS main control group described in Subsection 5.2.4.1. Therefore, it is concluded that multiple failure of the SBCS permissive control group has no effect on the plant and does not cause plant conditions more severe than the analysis of DCD Chapter 15 AOOs. The evaluation result is shown in Table 5.2-3.

#### 5.2.4.3. SG #1 Feedwater Control (FWCS 1)

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of the FWCS 1 control group are bounded by DCD Chapters 15.1.2 and 15.2.7. The evaluation result is shown in Table 5.2-4.

#### 5.2.4.4. SG #2 Feedwater Control (FWCS 2)

The failure of the FWCS 2 control group results in the same erroneous control outputs for SG #2 and

causes same plant transients as the failure of FWCS 1 control group described in Subsection 5.2.4.3. Therefore, the event consequences for multiple failures of the FWCS 2 control group are bounded by DCD Chapters 15.1.2 and 15.2.7 events. The evaluation result is shown in Table 5.2-5.

#### 5.2.4.5. Pressurizer Pressure Control (PPCS)

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of PPCS control group with respect to fuel integrity and primary pressure integrity meet the AOOs acceptance criteria because the RPS and CPCS are designed to ensure primary pressure and fuel integrity. The evaluation result is shown in Table 5.2-6.

#### 5.2.4.6. Pressurizer Level Control (PLCS)

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of PLCS control group are bounded by DCD Chapters 15.5.2 and 15.6.2. The evaluation result is shown in Table 5.2-7.

#### 5.2.4.7. Reactor Makeup Control (CVCS)

TS

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of CVCS control group are bounded by DCD Chapter 15.4.6 and 15.5.2 events. This evaluation result is shown in Table 5.2-8.

TS

#### 5.2.4.8. Control Rod Control (RRS/RPCS)

TS

TS

TS

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of RRS/RPCS control group are bounded by the event presented in DCD Chapter 15.4.1 and 15.4.2 and meet the fuel and system pressure design limits. This evaluation result is shown in Table 5.2-9 (sh. 2 of 2).

#### 5.2.4.9. Control Rod Control (DRCS)

TS

#### 5.2.4.10. Reactor Coolant Pump Control

TS

Therefore, it is concluded that the event consequences for multiple failures of RCP control group are bounded by the event presented in DCD Chapter 15.3.1. This evaluation result is shown in Table 5.2-11.

#### 5.2.4.11. HP Feedwater Heater Train A

TS

TS

Therefore, it is concluded that the event consequences for multiple failures of HP feedwater heater train A control group are bounded by the event presented in DCD Chapter 15.1.1 and 15.2.7 with respect to fuel cladding integrity and primary system integrity. This evaluation result is shown in Table 5.2-12.

#### 5.2.4.12. HP Feedwater Heater Train B

This failure causes the same effect as multiple failures of HP feedwater heater train A control group described in Subsection 5.2.4.11. Therefore, the event consequences for multiple failures of HP feedwater heater train A control group are bounded by the event presented in DCD Chapter 15.1.1 and 15.2.7 with respect to fuel cladding integrity and primary system integrity. This evaluation result is shown in Table 5.2-12.

#### 5.2.4.13. HP Feedwater Heater Bypass Line

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of HP feedwater heater bypass line control group are bounded by the event presented in DCD Chapter 15.1.2 with respect to fuel cladding integrity. This evaluation result is shown in Table 5.2-13.

#### 5.2.4.14. Feedwater Pumps On/Off

TS

Based on the above evaluation, it is concluded that the event consequences for multiple failures of feedwater pumps on/off control group are bounded by the event presented in DCD Chapter 15.1.2 and

15.2.7. This evaluation result is shown in Table 5.2-14.

#### 5.2.4.15. Non-1E AC Power to the Station Auxiliaries (13.8kv Non-Class 1E System)

TS

The loss of flow (LOF) event discussed in the DCD Chapter 15.3.1 leads to the most conservative predictions of the fuel cladding integrity. Therefore, the event consequences for multiple failures of non-Class 1E AC power to the station auxiliaries (13.8kV) control group are bounded by the event presented in DCD Chapter 15.3.1. This evaluation result is shown in Table 5.2-15.

#### 5.2.4.16. Condenser Vacuum and LP Feedwater Heater Control

TS

TS

Therefore, it is concluded that the event consequences for the failure of condenser vacuum and LP heater control group are bounded by the event presented in DCD Chapter 15.1.1, 15.2.3 and 15.2.7 with respect to fuel cladding integrity and primary system integrity. This evaluation result is shown in Table 5.2-16.

#### 5.2.4.17. Turbine Control System (TCS)

TS

Therefore, it is concluded that the event consequences for multiple failures of turbine control group are bounded by the DCD Chapter 15.2.2 event. This evaluation result is shown in Table 5.2-17.

#### 5.2.4.18. Miscellaneous BOP control

TS

Therefore, it is concluded that the event consequences for the failure of miscellaneous BOP control group are bounded by the event presented in DCD Chapter 15.1.1, 15.2.3 and 15.2.7 with respect to fuel cladding integrity and primary system integrity. This evaluation result is shown in Table 5.2-18.

### 5.2.5. Conclusion

For Failure Types 2, the qualitative evaluations are performed to verify and demonstrate that the results of initiating events caused by all possible multiple failures of a single control group are bounded by the acceptance criteria of the AOOs presented in the DCD Chapter 15.

### 5.3. Failure Type 3: Multiple Failures of more than One Control Group

#### 5.3.1. Selection of Initiating Events

The multiple failures of more than one control group due to a software design defect or a CSCCF cause spurious output signals of the multiple control groups as high, low or as-is. Multiple failures of more than one control group are assumed as initiating events with respect to fuel cladding integrity and primary system integrity. Two worst combinations of multiple failures are separately selected in view of fuel cladding integrity and primary system integrity respectively. These combinations include the normal operation of some control group if the normal operation causes the worst event results.

#### 5.3.2. Assumptions Used in the Evaluation

TS

TS

### 5.3.3. Initial Conditions

TS

### 5.3.4. Acceptance Criteria

TS

### 5.3.5. Evaluation Results

#### 5.3.5.1. Fuel cladding integrity (Event 1)

TS

#### 5.3.5.2. Primary system integrity

TS

TS

### 5.3.6. Conclusion

The worst combinations of multiple control group failures with respects to fuel cladding integrity and primary system integrity are evaluated.

TS

In conclusion, the worst case scenarios in terms of fuel cladding and primary system integrity have been verified to be bounded by the consequences of DCD Chapter15 PA by performing quantitative analysis.

## 5.4. Failure Type 4: Multiple Failures of IFPD Control Commands

Multiple failures of IFPD control commands due to a software design defect are assumed as initiating events with respects to fuel cladding integrity and primary system integrity. TS

, it is concluded that the worst case scenarios for the multiple failures of IFPD commands are bounded by the consequences of DCD Chapter 15 PA. Refer to Tables 5.4-1 and 5.4-2.

Table 5.1-1 Shared Signals (Sh. 1 of 2)

TS

Table 5.1-1 Shared Signals (Sh. 2 of 2)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 1 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 2 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 3 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 4 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 5 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 6 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 7 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 8 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 9 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 10 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 11 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 12 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 13 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 14 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 15 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 16 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 17 of 18)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (Sh. 18 of 18)

TS

Table 5.2-1 Control Group Segmentation (Sh. 1 of 3)

TS

Table 5.2-1 Control Group Segmentation (Sh. 2 of 3)

TS

Table 5.2-1 Control Group Segmentation (Sh. 3 of 3)

TS

Table 5.2-2 Multiple Failures of Single Control Group (SBCS Main)

TS

Table 5.2-3 Multiple Failures of Single Control Group (SBCS Permissive)

TS

Table 5.2-4 Multiple Failures of Single Control Group (FWCS1)

TS

Table 5.2-5 Multiple Failures of Single Control Group (FWCS2)

TS

Table 5.2-6 Multiple Failures of Single Control Group (PPCS)

TS

Table 5.2-7 Multiple Failures of Single Control Group (PLCS)

TS

Table 5.2-8 Multiple Failures of Single Control Group (CVCS)

TS

Table 5.2-9 Multiple Failures of Single Control Group (RRS/RPCS) (Sh. 1 of 2)

TS

Table 5.2-9 Multiple Failures of Single Control Group (RRS/RPCS) (Sh. 2 of 2)

TS

Table 5.2-10 Multiple Failures of Single Control Group (DRCS)

TS

Table 5.2-11 Multiple Failures of Single Control Group (RCP)

TS

Table 5.2-12 Multiple Failures of Single Control Group (HP FW Heater)

TS

Table 5.2-13 Multiple Failures of Single Control Group (HP FW Heater Bypass Line)

TS

Table 5.2-14 Multiple Failures of Single Control Group (FW Pump On/Off)

TS

Table 5.2-15 Multiple Failures of Single Control Group (Non-1E AC Power to the Station Auxiliaries – 13.8kv)

TS

Table 5.2-16 Multiple Failures of Single Control Group (Condenser Vacuum Control)

TS

Table 5.2-17 Multiple Failures of Single Control Group (Turbine Control System)

TS

Table 5.2-18 Multiple Failures of Single Control Group (Miscellaneous BOP control)

TS

Table 5.3-1 Assumptions for Event 1

TS

Table 5.3-2 Assumptions for Event 2

TS

Table 5.3-3 Initialization of RELAP5 for Nominal Initial Condition

TS

Table 5.3-4 Sequence of Major Events for Event 1

TS

Table 5.3-5 Sequence of Major Events for Event 2

TS

Table 5.4-1 Multiple Failures of IFPD control commands - Fuel Cladding Integrity

TS

Table 5.4-2 Multiple Failures of IFPD control commands - Primary System Integrity

TS


Figure 5.3-1 Core Power (Event 1)


Figure 5.3-2 Pressurizer Pressure (Event 1)


Figure 5.3-3 Safety Injection Flow (Event 1)


Figure 5.3-4 SG Pressure (Event 1)


Figure 5.3-5 DNBR (Event 1)


Figure 5.3-6 Core Power (Event 2)


Figure 5.3-7 RCP Discharge Pressure – Short Term (Event 2)


Figure 5.3-8 RCP Discharge Pressure – Long Term (Event 2)


Figure 5.3-9 POSRV Flow (Event 2)


Figure 5.3-10 SG Pressure (Event 2)

# 6. CONCLUSIONS

The following Failure Types caused by a shared signal failure and a CSCCF are evaluated to confirm that the event consequences of DCD Chapter 15 are still effective and the analysis acceptance criteria are met.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to a CSCCF
- Failure Type 3 : multiple failures of more than one control group due to a CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to a CSCCF

For Failure Types 1 and 2, the qualitative evaluations are performed to verify and demonstrate that the results of initiating events caused by all possible multiple failures are bounded by the acceptance criteria of the AOOs presented in the DCD Chapter 15.

For Failure Types 3 and 4, the worst combinations of multiple failures of control groups with respect to fuel cladding integrity and primary system integrity are quantitatively evaluated by using the RELAP5 code. Analysis results show that the worst case scenarios in terms of fuel cladding and primary system integrity are verified to be bounded by the acceptance criteria of the PAs presented in the DCD Chapter 15.

The evaluation concludes that all multiple failures caused by a shared signal or a CSCCF do not cause plant conditions more severe than the acceptance criteria of the DCD Chapter 15 AOOs and PAs.

## 7. REFERENCES

1. NUREG-0800, USNRC Standard Review Plan, Revision 3, 15.0 Introduction - Transient and Accident Analyses, March 2007.

2. DI&C-ISG-04, “Highly Integrated Control Rooms – Communications Issues,” Rev. 1, 2009

3. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

4. APR1400-Z-J-NR-14013-P, “Response Time Analysis of Safety I&C System,” January 2018.

5. APR1400-Z-J-NR -14002-P, “Diversity and Defense-in-Depth,” January 2018.

## 8. DEFINITIONS

1. Acceptance Criteria — Practical and reasonable objective pass/fail tests that identify approved requirements. Criterion is qualitative or quantitative, and defines sufficiency, not optimality.

2. Penalty factor — A multiplicative number necessary to ensure that the CPCS calculate DNBR and LPD conservatively