# Component Interface Module

## Revision 1

## Non-Proprietary

## March 2017

# REVISION HISTORY

| Revision | Date | Page | Description |
|---|---|---|---|
| 0 | November 2014 | All | First Issue |
| 1 | March 2017 | 2<br>(2) | "fully tested" → "tested"<br>R_342-8291(6R) |
| | | 3<br>(3) | The qualification criteria of the isolation devices added.<br>R_45-7883(1) |
| | | 3<br>(3) | "isolator" → "isolation devices" for consistency<br>R_45-7883(1) |
| | | 4<br>(4.1) | "qualified isolation devices" → "qualified interposing relays" to provide more information R_45-7883(1) |
| | | 4<br>(4.1) | Description for isolation device of CIM added.<br>R_45-7883(1) |
| | | 5-6<br>(4.2) | Description of output signals from the CIM added to provide more information.<br>R_37-7882(1), R_323-8281(13R) |
| | | 5<br>(4.2) | "soft" → "software" editorial correction.<br>R_37-7882(1) |
| | | 10<br>(5.3) | Description of modulating control signal added.<br>R_323-8281(14) |
| | | 11<br>(5.4) | Description of priority logic development testing added.<br>R_342-8291(6R) |
| | | 39<br>(14) | Reference 21 added.<br>R_45-7883(1) |

# ABSTRACT

The document describes the component interface module (CIM) of the Advanced Power Reactor 1400 (APR1400). The CIM is used to interface the output signals from the engineering safety features-component control system (ESF-CCS) digital controllers to the plant's safety components (e.g., pumps, valves, dampers) to allow control of each component based on automatic safety actuation signals and manual safety actuation signals from plant operators. For most applications, a single CIM controls a single engineered safety features (ESF) plant component.

The CIM is also used to interface with signals from the diverse systems of the APR1400 to control a subset of the plant components that are also controlled by the ESF-CCS digital controllers. The diverse systems also provide automatic and/or manual control of these same ESF components to facilitate coping with anticipated operational occurrences (AOOs) and postulated accidents (PAs) with a concurrent common-cause failure (CCF) in the redundant digital safety systems. The safety systems and diverse systems have no common digital components; therefore, a software or hardware defect that could result in a CCF of the redundant safety systems will not impact the diverse systems (or vice versa), and therefore will not result in a concurrent CCF of both main and diverse systems.

The CIM combines the signals from the ESF-CCS digital controllers and diverse systems to establish the final output control signal to each safety plant component (e.g., energize or de-energize). Pre-defined priority logic within the CIM resolves any control signal conflicts between the two sets of inputs to ensure plant safety is maintained. Since the CIM, including its priority logic, is relied on for both component control from the ESF-CCS digital controller and component control from the diverse systems, the CIM is implemented with conventional (non-programmable) technology, whose simple design can be demonstrated to be free of any design defects. Therefore, the CIM is not a potential source of CCF that could adversely affect the functions of both the ESF-CCS and the diverse systems.

This document describes the CIM design and its interfaces. It also describes the CIM design process including the thoroughness of validation testing and equipment qualification testing, which supports the conclusion that the CIM is free of hardware or software design defects and not subject to failure from external events, either of which could otherwise cause a CCF. This document also describes the periodic surveillance testing methods, which provide full coverage of all CIM interfaces and internal devices, to ensure that there are no undetectable random hardware failures that could accumulate over time in multiple CIMs to become a CCF.

# TABLE OF CONTENTS

# LIST OF TABLES



# LIST OF FIGURES

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AOO | anticipated operational occurrence |
| APR1400 | Advanced Power Reactor 1400 |
| BISI | bypassed and inoperable status indication |
| BTP | Branch Technical Position |
| CCF | common-cause failure |
| CFR | Code of Federal Regulations |
| CIM | component interface module |
| CMOS | complementary metal-oxide semiconductor |
| DI&C | digital instrumentation and control |
| DMA | diverse manual ESF actuation |
| DPS | diverse protection system |
| EMC | electromagnetic compatibility |
| EMI/RFI | electromagnetic interference/radio-frequency interference |
| EPRI | Electric Power Research Institute |
| ESF | engineered safety features |
| ESFAS | engineered safety features actuation system |
| ESF-CCS | engineered safety features-component control system |
| FMEA | failure modes and effects analysis |
| FPC | front panel control |
| FPGA | field-programmable gate array |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISG | Interim Staff Guidance |
| I&C | instrumentation and control |
| I/O | input/output |
| LC | loop controller |
| LED | light-emitting diode |
| MCC | motor control center |
| MCR | main control room |
| MSS | mode select switch |
| NRC | U.S. Nuclear Regulatory Commission |
| PA | postulated accident |
| PLC | programmable logic controller |
| RG | Regulatory Guide |
| RSR | remote shutdown room |

| | |
|---|---|
| SDOE | secure development and operational environment |
| Std. | Standard |
| TTL | transistor-transistor logic |

# DEFINITIONS

| | |
|---|---|
| Diverse systems | Diverse systems provide back-up functions for failure of the ESF-CCS. Diverse systems contain diverse digital components from the ESF-CCS, so that there is no potential for a common software defect or hardware that could lead to a CCF of both the ESF-CCS and the diverse systems.<br><br>"Diverse systems" refers collectively to the diverse protection system (DPS) and the diverse manual ESF actuation (DMA) switches. The CIM receives inputs from both the ESF-CCS and diverse systems for actuation of a plant component (e.g., pump, valve, and damper). |
| Hardware device | A device implemented by complementary metal-oxide semiconductor (CMOS) or transistor-transistor logic (TTL) devices that are configured using hardwired connections not software |
| State-based priority | One of two methods for determining the CIM output when the CIM receives conflicting input signals; the other is system-based priority defined below. When state-based priority is applied, the CIM prioritizes signals so that one direction of signals (e.g., energize or de-energize, open or close) always has higher priority over the opposite direction, regardless of the system generating the input signal.<br><br>Therefore, inputs demanding the non-priority state are blocked by the CIM when the CIM receives an input for the state-based priority. The specific state having priority is determined on a component-by-component basis for each CIM. For most components this is the state corresponding to the demand of the engineered safety features actuation system (ESFAS); exceptions are explained in the CCF Coping Analysis Technical Report (Reference 5). The logic to establish the desired state-based priority is configured on each CIM using conventional hardwired techniques. |
| System-based priority | One of two methods for determining the CIM output when the CIM receives conflicting input signals; the other is state-based priority defined above. When system-based priority is applied, the CIM prioritizes signals so that the signal of the specific system input (e.g., DMA switches) has priority over signals from other systems, regardless of the state demanded by that signal.<br><br>Therefore, inputs from other systems that have a lower priority than the system defined to have a higher priority are blocked by the CIM. The specific system having priority is determined on a component-by-component basis for each CIM; however, the systems defined to have priority are applied for all CIMs for the entire project. The logic to establish the desired state-based priority is configured on each CIM using conventional hardwired techniques. |

# 1. PURPOSE

This document describes the design features of the Advanced Power Reactor 1400 (APR1400) CIM that are critical for compliance with Branch Technical Position (BTP) 7-19 (Reference 1) and Digital Instrumentation and Control (DI&C) - Interim Staff Guidance (ISG)-04 (Reference 2) to cope with a common-cause failure (CCF) of the safety instrumentation and control (I&C) systems. A CCF of the safety I&C systems is considered because the safety I&C systems are digital; therefore, in accordance with BTP 7-19 a CCF of those systems is assumed to exist coincident with plant accidents. In addition, since the CIM is part of the safety I&C system, this document also describes the design features and design processes pertinent to compliance with the Institute of Electrical and Electronics Engineers (IEEE) Std. 603 (Reference 3) and the 10 Code of Federal Regulations (CFR) Part 50, Appendix A, General Design Criteria (Reference 4).

For the APR1400, the CIM manages the priority of different actuation signals, resulting from different I&C systems within various layers of defense-in-depth, which can be sent to a given plant component. Accordingly, the CIM receives component control signals from the engineered safety features-component control system (ESF-CCS), diverse protection system (DPS), and diverse manual ESF actuation (DMA) switches. In addition, each CIM has its own conventional hardwired front panel control (FPC) switch. The CIM prioritizes these component control signals using priority logic and then sends the signal with the highest priority to a controlled component such as a motor operated valve, pump motor, or solenoid operated valve.

One function of the CIM is to provide prioritization between component control signals from the ESF-CCS and DPS to provide assurance that the credited automatic safety function can be accomplished by either system. Therefore, the CIM accommodates a CCF of either system using state-based priority logic. This state-based priority logic ensures that if either system fails in a manner that sends an incorrect spurious signal for the non-safe state, the other system can reposition the component to its safe state, when required for accident mitigation.

A second function of the CIM is to interface manual system-level actuation signals to comply with Point 4 of BTP 7-19 and to accommodate manual operator actions that are credited in the CCF Coping Analysis Technical Report (Reference 5). The DMA switches are provided in the main control room (MCR) for manual system-level ESF actuation, and manual operator actions that are credited in the CCF Coping Analysis Technical Report within the first 30 minutes of an accident. The FPC switch, which is provided for each CIM, accommodates manual operator actions that are needed after hot shutdown and that cannot be accommodated using the DMA switches. The CIMs along with their FPC switches are located in the four I&C equipment rooms for each safety division and the corresponding mux rooms for each safety division.

The CIM is implemented using conventional hardware technology; the resulting simplicity ensures there is no potential for a software or hardware design defect that could result in a CCF of the CIM.

# 2. OVERVIEW DESCRIPTION

The CIM is a hardware-based qualified safety device for safety component control. Each CIM is used to control one plant component.

TS

## 3. SYSTEM QUALIFICATION

TS

## 4. DESIGN DESCRIPTION

TS

TS

### 4.1. General Design Features

TS

TS

**Figure 4.1-1 Block Diagram of the CIM Interface**

### 4.2. CIM Configuration

The overview diagram of the CIM is shown in Figure 4.2-1. As discussed earlier, the CIM consists of the priority logic section, base section, and diagnosis section. The purpose of each section is as follows:

TS

TS

TS

**Figure 4.2-1 Overview Diagram of the CIM**

## 5. PRIORITY LOGIC SECTION

TS

### 5.1. Component Control Signal Sources

TS

TS

### 5.2. Priority Logic

TS

TS

TS

**Figure 5.2-1 Priority Logic Section**

## 5.3. Priority Logic Configuration

TS

TS

TS

**Table 5.3-1 Priority Mode Configurations**

TS

TS

**Figure 5.3-1 Priority Logic Configuration in the CIM for the APR1400**

## 5.4. Priority Logic Development Testing

TS

# 6. FAILURE MODE FEATURES

TS

## 6.1. Failure Modes and Effects Analysis

The FMEA of the CIM is shown in Table 6.1-1.

**Table 6.1-1 FMEA for the CIM (1 of 8)**

TS

**Table 6.1 1 FMEA for the CIM (2 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (3 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (4 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (5 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (6 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (7 of 8)**

TS

**Table 6.1-1 FMEA for the CIM (8 of 8)**

TS

# 7. TESTING AND MAINTENANCE FEATURES

TS

## 7.1. General Design Features

TS

## 7.2. CIM INPUT Interface Test

TS

### 7.2.1. INPUT A Interface Test

Figure 7.2-1 shows the test signal flow of the INPUT A interface. The following steps are to test the integrity of the energize signal path from INPUT A to the output result of the CIM.

TS

TS

TS

**Figure 7.2-1 Test Signal Flow for INPUT A Interface**

### 7.2.2. INPUT B Interface Test

Figure 7.2-2 shows the test signal flow of the INPUT B interface. The following steps are to test the integrity of the energize signal path from INPUT B to the output result of the CIM.

TS

TS

TS

**Figure 7.2-2 Test Signal Flow for INPUT B Interface**

### 7.2.3. INPUT C Interface Test

Figure 7.2-3 shows the test signal flow of the INPUT C interface. The following steps are to test the integrity of the energize signal path from INPUT C to the output result of the CIM.

TS

TS

TS

**Figure 7.2-3 Test Signal Flow for INPUT C Interface**

### 7.2.4. Front Panel Control Switch Interface Test

Figure 7.2-4 shows the test signal flow of the FPC switch interface. The following steps are to test the integrity of the energize signal path from the FPC switch to the output result of the CIM.

TS

TS

TS

**Figure 7.2-4 Test Signal Flow for the FPC Switch Interface**

### 7.2.5. Input Select Switch Interface Test

Figure 7.2-5 shows the test signal flow of the input select switch interface. The following steps are to test the integrity of the signal path from the input select switch to the output result of the CIM.

TS

TS

TS

**Figure 7.2-5 Test Signal Flow for the Input Select Switch Interface**

### 7.3. Diagnosis Section

TS

TS

TS

**Figure 7.3-1 Block Diagram of CIM Diagnosis Section**

### 7.4. Test Points

TS

TS

**Figure 7.4-1 Connection Diagram of Test Points**

## 8. ELECTRICAL CHARACTERISTICS

The CIM electrical characteristics are as follows:

TS

TS

## 9. LOCAL INDICATION FEATURES

The CIM has LEDs that indicate status and error conditions. The following status and error indications are provided:

TS

## 10. DESCRIPTION OF MANUAL CONTROL SWITCH ON THE CIM

TS

TS

## 11. INTERFACE PROPERTIES

The interface properties are as follows:

TS

TS

## 12. DESIGN QUALITY AND VALIDATION

TS

## 13. PACKAGING

TS

## 14. REFERENCES

1. NUREG-0800, Standard Review Plan, BTP 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” Rev. 6, U.S. Nuclear Regulatory Commission, July 2012.

2. DI&C-ISG-04, “Highly-Integrated Control Rooms – Communications Issues (HICRc),” Rev. 1, U.S. Nuclear Regulatory Commission, 2009.

3. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1991.

4. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission.

5. APR1400-Z-A-NR-14019-P, “CCF Coping Analysis,” Rev.1, KHNP, March 2017.

6. APR1400-Z-J-EC-14002-P, “Diversity and Defense-in-Depth,” Rev.1, KHNP, March 2017.

7. Regulatory Guide 1.100, “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants,” Rev. 3, U.S. Nuclear Regulatory Commission, September 2009.

8. IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2004.

9. Regulatory Guide 1.89, “Qualification for Class 1E Equipment for Nuclear Power Plants,” Rev.1, U.S. Nuclear Regulatory Commission, June 1984.

10. IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2003.

11. WCAP-16097-P-A, “Common Qualified Platform Topical Report”, Rev. 3, Westinghouse Electric Corporation, February 2013.

12. Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related instrumentation and Control Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.

13. EPRI TR-102323, “Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants,” Electric Power Research Institute, 1997.

14. Regulatory Guide 1.75, “Criteria for Independence of Electrical Safety Systems,” Rev. 3, U.S. Nuclear Regulatory Commission, February 2005.

15. IEEE Std. 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” Institute of Electrical and Electronics Engineers, 1992.

16. APR1400-Z-J-NR-14003-P, “Software Program Manual,” Rev.1, KHNP, March 2017.

17. 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” U.S. Nuclear Regulatory Commission.

18. Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.

19. NUREG-0800, Standard Review Plan, BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.

20. IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” Institute of Electrical and Electronics Engineers, 2004.

21. NUREG-0800, Standard Review Plan, BTP 7-11, “Guidance on Application and Qualification of Isolation Devices,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.