WO 89

Response to Digital I&C Questions

1.0 Request

NRC RAI 271-8290, Question 19-15 presented the following request:

Regulation 10 CFR 52.47(a)(27) requires that a standard design certification applicant provide a description of the design specific PRA. SRP Chapter 19, Revision 3 (Draft), Section I. "Areas of Review, Review Interfaces" states that the staff should "…confirm that: All common-cause failure (CCF) mechanisms for digital instrumentation and control (DI&C) systems have been accounted for in the PRA." The staff reviewed APR1400 DCD Section 19.1, "Probabilistic Risk Assessment," and did not find sufficient information describing the modeling of the DI&C system, including the hardware and software common-cause failures, to be able to make this conclusion. Therefore, in order for the staff to reach a reasonable assurance finding that the description of the PRA is adequate, please provide the following details of DI&C modeling in the PRA and include it in the DCD:

- *System description (e.g., describe the functions, subsystem interfaces, operator actions, etc.)*
- *Key assumptions (e.g., modeling, uncertainties)*
- *CCF analysis of both the hardware and software, including the basis and/or justification of this information*
- *Failure effects, if modeled at the system/subsystem level*
- *Description of basic event followings:*

  No. 8: CCF of ESF actuation logic software

  No.9: CCF of PMS ESF output logic software

  No.11: Software CCF of all Cards

Also, including event boundaries, and characteristics, failure mode description, parametric uncertainty parameters (e.g., error factors):

- *Description difference of AP1000 and APR1400's architecture*

In support of responding to this information request, Westinghouse has agreed to provide the following information as it relates to the AP1000 DI&C information for the ESF CCF PRA information used by KHNP and referenced in their APR1400 DCD.

- System description (e.g., describe the functions, subsystem interfaces, operator actions, etc.)
- Key assumptions (e.g., modeling, uncertainties)
- CCF analysis of both the hardware and software, including the basis and/or justification of this information
- Failure effects, if modeled at the system/subsystem level
- Description of basic event followings:

  No. 8: CCF of ESF actuation logic software

  No. 9: CCF of PMS ESF output logic software

No. 11: Software CCF of all Cards

Also, includes event boundaries, and characteristics, failure mode description, parametric uncertainty parameters (e.g., error factors).

- Description difference of AP1000 and APR1400's architecture

2.0 Background

As stated in Section 1.0 of the purpose, this letter is pulling information from several references to make a comparison. The AP1000 plant information in Sections 4.0 through 8.0 summarizes the AP1000 DCD (Reference 1). The protection and monitoring system (PMS) which houses the safety-related ESF functions is summarized in Chapter 7. The modeling of the PRA and common cause of software is discussed in Chapter 19.

The AP1000 PRA model has followed regulatory feedback in this area of software common cause. The AP1000 PRA UK design acceptance of the AP1000 reactor was archived in March 2017. During the generic design assessment (GDA), the AP1000 PRA model supported this initiative and included updates to the design and methods as part of this licensing effort. GDA responses including PRA are available to the public on the ONR website (http://www.onr.org.uk/new-reactors.htm).

3.0 References

1. Westinghouse AP1000 Design Control Document, Revision 19, https://www.nrc.gov/docs/ML1117/ML11171A500.html.
2. UK Office of Nuclear Regulation, Nuclear Safety Technical Assessment Guide, NS-TAST-GD-046, Revision 4, “COMPUTER BASED SAFETY SYSTEMS,” February 2017.
3. International Electrotechnical Commission Standard IEC 61508, Edition 2.0, “Functional safety of electrical/electronic/programmable electronic safety-related systems.”

4.0 Description of the AP1000 I&C Systems

The AP1000 I&C system include some safety system protection and safety monitoring system (PMS) which performs the primary automatic safety functions of reactor trip and engineered safety features (ESF) actuation. It has four independent sensors and logic divisions.

The diverse actuation system (DAS) is separate, independent, and diverse from the PMS and performs limited safety functions.

In addition, there are four non-safety systems, plant control system (PLS), data display and processing system (DDS), and a special monitoring system (SMS); and two systems that perform both safety and non-safety functions, incore instrumentation system (IIS) and the operations and control centers system (OCS).

The focus of this paper is on PMS as the primary safety actuation system. The PMS provides detection of off-normal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The PMS controls safety-related components in the plant that are operated from the main control room. In addition, the PMS provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by NRC Regulatory Guide 1.97.

The AP1000 PMS implements its functions by software logic installed in programmable digital devices (data processors). Plant data and other signals are exchanged between data processors by means of isolated data links and data highways. The functions of the PMS are implemented in separate processor-based subsystems. Each subsystem is located on an independent computer bus to prevent propagation of failures and to enhance availability. [

]^{a,c,e}

The PMS includes four independent divisions, [ ]^{a,c,e}
The system in general uses traditional 2oo4 logic to process trip and safety actuation which reverts to 2/3 if one channel must be bypassed. To enhance reliability, the PMS includes built in continuous self-testing capability along with periodic manual testing.

5.0 Description of difference between AP1000 and APR1400's architecture

The AP1000 PMS and APR1400 plant protection system (PPS) architectures (see Figure 5-1 and Figure 5-2) have very similar BPL (Bistable Processor Logic) and LCL (Local Coincidence Logic) configurations. Both the AP1000 PMS and APR 1400 PPS use the safety qualified Common Q platform. APR1400 refers to this as the qualified safety related programmable logic controller (PLC) platform. The AP1000 PMS has two BPL processors in each rack with one processor module handling the excore nuclear instrumentation logic and the other handling the reactor protection system (RPS) and ESF safety functions.

The APR1400 PPS has one BPL processor module (PM) as it only handles the RPS and ESF functions. External to the APR1400 PPS there are separate testable cabinets/systems consisting of a four channel core protection calculator system (CPCS), and four channels of NIS electronics (excore neutron flux monitoring system [ENFMS]) that handle those functions. A digital input is received by the PPS BPL from these systems and processed for the reactor trip functions. The NIS electronics performs the same functionality as the AP1000 NIS. The CPCS is separate functionality for the APR1400 only. The BPLs communicate to the LCLs via RS422 High Speed Links (HSLs) (Serial Data Links [SDLs] in APR1400 DCD terminology). Whenever HSLs (SDLs) are used between channels, fiber optic modems are employed to maintain separation between the divisions. The figures of the architectures do not include this detail to simplify the drawings.

The LCLs in the APR1400 receives two BPL status inputs from each channel for each trip function. The LCL performs a 1oo2 on the BPL inputs for each channel and then performs 2oo4 voting on the Channel A, B, C, and D signals as the APR1400 has four nearly identical sensor channels that are processed in the

LCL. The AP1000 LCLs perform the same logic, where possible, [

] [a,c,e] Both the AP1000 and APR1400 have redundant LCL processor racks [
] [a,c,e]

The AP1000 and APR1400 differ in the way they handle the ESF component actuations. The APR1400 uses group controllers (GCs) to handle system actuations and loop controllers to send hardwired digital signals to component interface modules (CIMs) that handle the component actuations and feedback. CIMs receive the signals from ESF-CCS (ESF component control system) loop controllers, diverse protection system (DPS), and diverse manual actuation (DMA) switches. The DPS and diverse indication system (DIS) use a non-software based field programmable gate array (FPGA) platform which is diverse from the safety related programmable logic controller (PLC) platform. The CIMs are hardwired to the loop controller, the DPS, and the DMA switches. The CIM contains digital logic that performs a priority logic scheme on the signals that are received. The diverse manual actuation overrides the DPS signals which override ESF safety signals. Group Controller 1 receives system level actuation signals from LCL1 in each division via SDL. Group Controller 2 receives system level actuation signals from LCL2 in each division. The GCs perform a selective 2oo4 on the signals from each division and send the resultant actuation signal to the Loop controllers. GC-1 sends the resultant ESF-CCS actuation signal to the LCC primary PM. GC-2 sends the resultant ESF-CCS actuation signal to the LCC hot standby PM. The LCC's only respond to GC-1 under normal operating conditions where GC-1 has good SDL quality. If GC-1 SDL communications indicate bad quality, the LCC switches to using GC-2 data for component actuation.

The AP1000 sends the component actuations to Integrated Logic Cabinets [

] [a,c,e] The CIM modules are intelligent modules that provide priority logic based on receiving signals from the control system (Ovation) and from the safety system. [
] [a,c,e]

The diverse actuation system (DAS) interface on the AP1000 is connected directly to the ESF actuator on the ESF component. The DAS (DMA switches) on the APR1400 is connected at the high priority port on the CIM modules.

The normal operator interfaces are all flat panel displays for both AP1000 and APR1400. Both AP1000 and APR1400 have a minimum subset of manual controls on the main control board for ESF system level actuations. The AP1000 manual switches are hardwired from the Dedicated Safety Panels to the Local Coincidence Logic (LCL) rack in the PMS cabinet which performs logic and sends signals to the ILPs and SRNCs. The APR1400 ESFAS manual switches are hardwired from the MCR to the MCR-CPM (Main Control Room Control Panel Multiplexer) which sends the signals to the GCCs which perform logic and then pass on the manual actuations to the LCCs.

The APR 1400 CIM receives the signals from ESF-CCS LC, DPS, DMA switches. The LC also receives the manual control signal from the ESF-CCS soft control module (ESCM) through the control channel gateway (CCG) safety system data network (SDN) and from minimum inventory switches hard wired to

the Control Panel Multiplexers and sent via SDL to the CCGs then via SDL to the GCCs and via SDL to the LCCs.

The other difference is that the AP1000 is a highly integrated safety system. The PMS cabinets contain the nuclear instrumentation system (NIS) electronics, reactor protection functions, ESF functions, and post accident monitoring functions. The APR1400 has separate testable cabinets/systems consisting of four channel core protection calculator system (CPCS), two channel post accident monitoring system (QIAS-P), four channels of NIS electronics (excore neutron flux monitoring system [ENFMS]) and four channels of plant protection system and ESF-CCS functions.

a,c,e

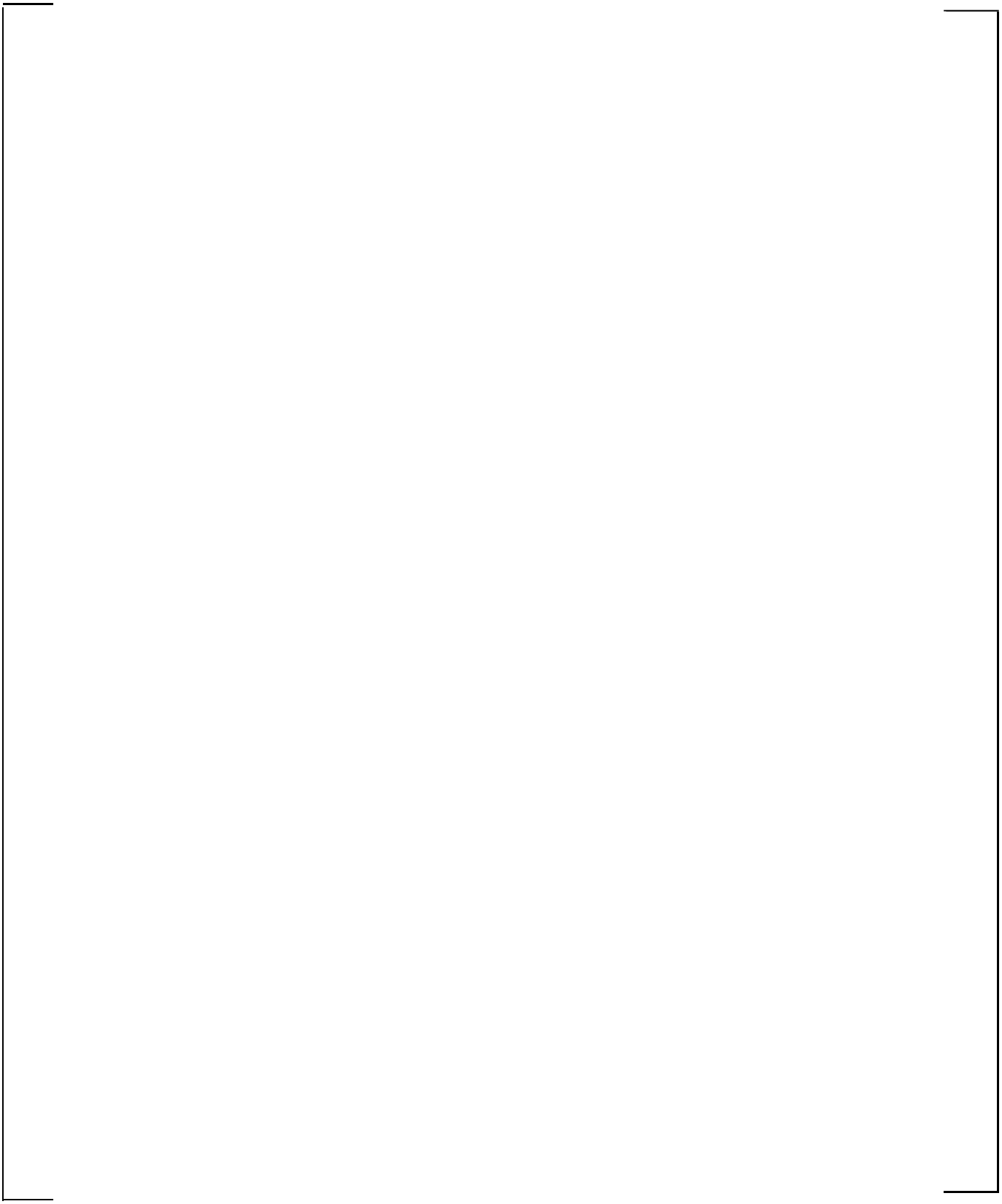

Figure 5-1: AP1000 Simplified PMS Architecture

a,c,e

6.0 Common Cause Failure Analysis of CCF Hardware and Software

Common cause failure evaluation of the AP1000 digital instrumentation and control systems in the AP1000 DCD are based on analyses performed to support AP600. Table 6-1 provides a qualitative discussion of potential logic and instrumentation common cause failures that may occur across divisions. Table 6-2 provides a summary of the potential CCFs within one division of the I&C system.

Table 6-1: Potential Logic and Instrumentation Common Cause Failure Modes for AP1000		
Common Cause	**Assessment of Failure Mode**	**Conclusion/Impact**
Sensors/transmitters Miscalibration	Assessment of potential miscalibration errors requires consideration of the plant-specific organizational environment. At many nuclear plants, including the AP1000 plant, a very high degree of redundancy *is* built into the calibration practices and procedures. This means that the practice for calibration of standards and (the double checking of the calibration protocols are specifically verified to prevent human errors to pass undetected. Furthermore, during normal plant operation, there is essentially a continuous checking by the main control room crew that calibration errors do not exist. The calibration of sensors/transmitters is carried out during the refueling outage. If a gross miscalibration were to pass undetected through the elaborate verification, then it would most likely be recognized during plant startup by operation personnel (by checking the parameter values in the main control room or because the miscalibration leads to the reactor trip).	[ ]a,c,e
Manufacturing/installation errors	Manufacturing is an automated process that is subjected to multiple tests both in factory as well as after the in situ installation. Furthermore many errors are detected by self-testing (including memory checks) and channel checking, performed every 24 hours. Therefore, it is highly improbable that these failures would remain undetected for a long period or that they would occur at the same time unless caused by an environment stress	[ ]a,c,e
Analog input boards NIMOD miscalibration	The analog input board configuration for field inputs includes [ ]a,c,e Each subsystem functional processor uses these values to calculate the compensation factors for each input. Gross mis-calibrations are immediately detected by the self-diagnostic features and the	[

Table 6-1: Potential Logic and Instrumentation Common Cause Failure Modes for AP1000		
Common Cause	**Assessment of Failure Mode**	**Conclusion/Impact**
	functional processor takes appropriate actions to prevent the occurrence of an unsafe state. In addition to the channel check required by the Technical Specification, calibration by personnel only involves only the setting of the high and low reference voltage. Choosing the reference values in a proper manner allows detection of the failure to reconnect to the sensor input signal after auto-calibration period, and allows detection of failures that drive the input signal beyond the normal input range. The reference voltage calibration is performed only during plant outage and is administratively controlled.	]a,c,e
Loss of 120 VAC Distribution Panel	The loss of power is explicitly considered in the fault tree construction, except for fail-safe components (e.g., containment isolation AOVs) where the loss of both 120 vac sources is towards the safety.	[ ]a,c,e
Earthquake	All cards are designed and tested to support the intensity and frequency of the vibration due to the highest OBE and SSE seismic level for the plant site.	[ ]a,c,e
Setpoint drift/setpoint initially incorrectly set	[ ]a,c,e There is a chance that the setpoint could be incorrectly set initially, but the continuous software verification, the nuclear test and the calibration of the sensors with trip of logic every refueling, will drastically reduce the probability 'hat the error, if it occurs, can remain undetected for a long period. This error can affect the trip of the same parameter for the same setpoint in all four PMS channels.	[ ]a,c,e
Maintenance/test errors	Tests by the operator are generally performed only during refueling outage. If test or maintenance conditions have to be performed during normal plant operation, plant personnel place the system or component into a bypass condition using the bypass controls located at the local cabinet. Test selection may be optionally performed using portable terminal which interface to the	[

Table 6-1: Potential Logic and Instrumentation Common Cause Failure Modes for AP1000		
Common Cause	**Assessment of Failure Mode**	**Conclusion/Impact**
	automatic tester subsystem. The number of bypasses that may be established at the same time are limited. If plant personnel try to bypass more channels or functions than is permitted, the IP&CS (Integrated protection and Control System) automatically initiates a trip of the channels or ESF actuation. The initiation of system bypasses are administratively controlled with bypass and system status information being provided to the plant operator in the control room. Once the portable terminal is removed, the IP&CS subsystems automatically go through an initialization and self-check sequence of system components and software. Once these checks are successfully completed, each main processor automatically starts its loop cycle. This allows the subsystem to return to operation immediately. After successful completion of initialization sequence, the plant personnel must manually initiate the automatic tester to perform the functional test of the system. Therefore, all potential failure due to maintenance/test errors can be immediately detected.	]a,c,e
Electromagnetic interference (EMI)	*The IP&CS* through design practices and protection provided via shielding is capable of withstanding electromagnetic radiation without deviating from the stated performance limits of the system. Testing of the system must confirm the adequacy of the cables and connectors used once the system is completely installed m the plant. Each channel is tested by means of an injection line laid parallel to the signal cable along its outline route. EMI can enter a circuit through any of several paths: power supplies adjacent equipment, adjacent cabling or output signals. The use of fiber optic is able to reduce the susceptibility to EMI as well as radio frequency interference (RFl). The design provides protection against EMI between different channels. Protection against lightning effects is achieved by adopting a special connection during rebar junction (so that a Faraday cage provides protection for the inside equipment). This prevents EMI from altering the voltages in all channels which might cause potential damage to the memory. Protection from internal EMI sources is a combination of shielding requirement (e.g., cabinet assembly affords the first line of protection against susceptibility of equipment to radiated EMI), physical separation, and administrative controls (e.g., avoid the use of walkie talkies inside the buildings). Potential areas affected by EMI, in	[ ]a,c,e

Table 6-1: Potential Logic and Instrumentation Common Cause Failure Modes for AP1000		
Common Cause	**Assessment of Failure Mode**	**Conclusion/Impact**
	areas without proper protection, are the local areas where transmitters are located and the auxiliary building compartments containing the cabinet assemblies. No more than one channel at the same time can be affected by the consequence of EMI radiation from PLC to CLC to the components. The potential common cause failure due to EMI could eventually affect only the hard-wired from PLC or CLC to the components. Only the components of the "energize to operator" type can be affected by this common cause failure.	
Software error	The software provided for the equipment operation is subjected to extensive "debugging" procedures and strict quality control and test requirements. Nevertheless, it is not credible that an undetected “bug" could remain and affect some of the programmed functions. Software errors that affect self-testing and calibration functions are easily detected during normal operation. Preoperational and nuclear tests should produce a situation similar to real accidents and lead to the discovery of any remaining errors. In addition, the automatic tester subsystem tests the software monthly. However these tests could not cover all possible input combinations and, therefore, some trip functions could be affected by software error. Therefore potential software common cause failures for undesigned input data strings is accounted among all cards that manage relatively important software.	[ ]a,c,e
Fire	The areas where IP&CS equipment are located have a very low probability of fire. Furthermore, physical separation within the plant is accomplished to prevent single credible events from preventing the operation of required safety system function.	[ ]a,c,e

Table 6-2: Summary of Common Cause Failure within Instrumentation and Control	
Common Cause	**Microprocessor Based Logic**
Setpoint initially incorrect	Very low (accounted for within other common cause failures)
Manufacturing/installation errors	Low [ ]^{a,c,e}
EMI	Very low within one division
Software errors	Low

7.0 Failure Modes and Effects Assessment

A qualitative summary of DI&C system common cause failure modes is provided in Table 6-1.

8.0 Description of CCF Basic Event Parameters

Table 8-1 provides a summary of the software related CCF values used for AP1000. Basis for the mean failure probabilities are provided in Section 8.3. Error factors are set based on the large uncertainties in the mean values.

Table 8-1: CCF Basic Events for Digital I&C Software Failures

ID	AP1000 Basic Event	Description	[ ]^{a,c,e}	[ ]^{a,c,e}
8	CCX-PMXMOD2-SW	CCF of PMS ESF actuation logic software (single subsystem due to dedicated software)	[ ]^{a,c,e}	[ ]^{a,c,e}
9	CCX-PMXMOD1-SW	CCF of PMS ESF OUTPUT LOGIC SOFTWARE (single subsystem due to dedicated software)	[ ]^{a,c,e}	[ ]^{a,c,e}
11	CCX- SFTW	SOFTWARE CCF OF ALL CARDS	[ ]^{a,c,e}	[ ]^{a,c,e}

8.1 Basic Event Boundaries

The PMS system boundary is defined by the sensors on the input side and the CIMs on the output side of the system. The PMS has limited dependencies, including no AC power dependencies. Operation of the PMS is supported by independent DC battery supply to each of the four safety divisions. Batteries are design to provide actuation functions for 24 hours. Additional batteries support monitoring capability for 72 hours. Room heat-up models indicate HVAC cooling of the PMS is not required for a 72 hour duration. The PMS accepts signals from plant sensors and generates actuation signals to the RTS the ESF functions. The PMS requires no manual actuation but functions may be accessed via a software interface in the main control room

8.2 Key Assumptions

These key assumptions used in the CCF assessment include:

[

]a,c,e

A discussion of the development of system unreliabilities are provided below.

8.3 Evaluation of Common Cause Failure Modes

Table 6-1 presents a qualitative assessment of the probability of the different causes of common cause failure is given. This assessment is based on the possibility of occurrence of the initiating causes, and it takes into account protective measures. Table 6-2 summarizes common cause failures within instrumentation and control. Basically, three possible common cause failures are found to be credible:

1. Software common cause failures
2. Manufacturing/installation common cause failure
3. Electromagnetic interference (EMI) common cause failure

These failure modes are discussed below.

8.3.1 Evaluation of Common Cause Software Failure for Digital I&C

Several software errors could occur, the first of which are requirement errors. Requirement errors are of two types:

Errors at Functional Level: The requirements do not specify the correct input that occurs during a design event. This would be independent of the instrumentation and control technology. This probability is considered negligible.

Error in software design specification: The interfaces between plant situation and software are not wrong but they are not completely defined. For example, external inputs that are strictly needed for automatic logic are not considered in the specification (such as simultaneous manual operations). These additional inputs could potentially cause malfunction (such as microprocessor overloaded). In the AP1000 plant this error is considered negligible mainly because the level system manual actuations are performed directly to the final components for essential systems such as passive residual heat removal, core makeup tank, automatic depressurization system containment isolation, and reactor trip.

These error types would potentially be detected during the validation test, system test, or nuclear test in the plant. The error which led to microprocessor overload due to excessive inputs coming from the specified external inputs and from the functions controlled by microprocessors (such as the self-test) are considered as program errors because the software developers should know that.

The program is generally written, in a high language, and then passes the verification and validation program. After that, a compiler is used to obtain a running program in a machine language (such as assembler). The compiled program is validated again.

The software error to produce a common cause failure of instrumentation and controls during events should:

- Be undetected during the verification and validation task and during the factory, installation, and surveillance testing
- Show up during a unique event situation which should challenge many divisions and many systems

Software errors that are activated or caused by internal hardware failure are discussed in Section 8.3.2.

[ ]^{a,c,e}

[

]^{a,c,e}

[

]a,c,e

8.3.2 Manufacturing / Installation errors

There is a potential for a manufacturing error to remain undetected because it was not activated during the multiple tests in factory and in situ after installation and during some surveillance tests. This potential error activated in multiple components, causes a cause failure as a result of one of the following processes:

- Aging - The common cause failure is a concern only if the failure is not detectable during the self-test.

  The probability to be considered is causing multiple failures between two subsequent surveillance tests (the aging effect has a time distribution).

- Abnormal conditions during normal operation that might activate the manufacturing error.
- Abnormal conditions during the event which might activate the manufacturing errors.
- Vulnerability to heavily ionized particles (such as alpha particles issuing from minute levels of radioactive impurities present in the materials used in the chips). This failure can impact the software error as it may lead to charge or discharge of a cell that can change its state from "zero" to "one" or vice versa, impacting the stored code instructions

These failure mechanisms for microprocessors are similar to the failure mechanism for common cause failure of mechanical components. Therefore, they are treated in the same way:

[ ]^{a,c,e}

where:

U is the unavailability of the microprocessor due to common cause manufacturing/installation issue UR is the random failure unavailability probability of one component (which already accounts for the possibility of self detection).

CCF is taken based on the taking [ ]^{a,c,e} This value is judged to be a conservative representation for this failure mode given the automatic manufacturing processes and the multiple testing performed in the factory and "in situ".

Manufacturing/Installation UR values are dependent on the card type and surveillance frequency.

8.3.3 Electromagnetic Interference (EMI)

The electromagnetic interference can affect only one division at the same time and can induce only a spurious actuation on "energize to trip" components. Common cause failure is related to the length of wires to transmitters to the cabinets and from output device (EPO) to the components. The components within the cabinets are supposed to be shielded by the cabinet assembly. Therefore, only rare probability human errors could induce electromagnetic interference into the components located in the cabinets. Therefore, because electromagnetic interference affects only one of four divisions at a time and at least a signal from two divisions is needed to produce an actuation signal, its effect on core damage frequency is assessed to be negligible.