Westinghouse

Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-6306
Direct fax: 412-374-5005
e-mail: sterdia@westinghouse.com

Your ref: Project Number 740
Our ref: DCP/NRC1913

May 30, 2007

Subject: AP1000 COL Response to Requests for Additional Information (TR #43) Non-Proprietary Responses

In support of Combined License application pre-application activities, Westinghouse is submitting responses to NRC requests for additional information (RAIs) on AP1000 Standard Combined License Technical Report 43, APP-GW-GLR-018, Rev. 0, Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System. These RAI responses are submitted as part of the NuStart Bellefonte COL Project (NRC Project Number 740). The information included in the responses is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification.

Responses are provided for requests TR43-1 through TR43-17, transmitted in NRC letter dated March 11, 2007 from Steven D. Bloom to Andrea Sterdis, Subject: Westinghouse AP1000 Combined License (COL) Pre-application Technical Report 43 – Request for Additional Information (TAC No. MD2496).

Pursuant to 10 CFR 50.30(b), the responses to requests for additional information on Technical Report 43 is submitted as Enclosure 1 under the attached Oath of Affirmation.

It is expected that when the RAIs on Technical Report 43 are complete, the technical report will be revised as indicated in the responses and submitted to the NRC. The RAI responses will be included in the document.

These RAI responses are Westinghouse Non-Proprietary Class 3. The Westinghouse Proprietary Class 2 responses were already transmitted via DCP/NRC1884 on May 11, 2007.

Questions or requests for additional information related to the content and preparation of this response should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.



D079

Very truly yours,

D. F. Hutchings for

A. Sterdis, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Attachment

1. "Oath of Affirmation," dated May 30, 2007

/Enclosure

1. Response to Requests for Additional Information on Technical Report No. 43, RAI-TR43-001 through RAI-TR43-017

| | | | | | |
|---|---|---|---|---|---|
| cc: | D. Jaffe | - | U.S. NRC | 1E | 1A |
| | E. McKenna | - | U.S. NRC | 1E | 1A |
| | G. Curtis | - | TVA | 1E | 1A |
| | P. Grendys | - | Westinghouse | 1E | 1A |
| | P. Hastings | - | Duke Power | 1E | 1A |
| | C. Ionescu | - | Progress Energy | 1E | 1A |
| | D. Lindgren | - | Westinghouse | 1E | 1A |
| | A. Monroe | - | SCANA | 1E | 1A |
| | M. Moran | - | Florida Power & Light | 1E | 1A |
| | C. Pierce | - | Southern Company | 1E | 1A |
| | E. Schmiech | - | Westinghouse | 1E | 1A |
| | G. Zinke | - | NuStart/Entergy | 1E | 1A |
| | T. Hayes | | Westinghouse | 1E | 1A |

ATTACHMENT 1

"Oath of Affirmation"

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

| | |
|---|---|
| In the Matter of: | ) |
| NuStart Bellefonte COL Project | ) |
| NRC Project Number 740 | ) |

APPLICATION FOR REVIEW OF
"AP1000 GENERAL COMBINED LICENSE INFORMATION"
FOR COL APPLICATION PRE-APPLICATION REVIEW

James W. Winters, being duly sworn, states that he is Manager, Standardization and Configuration Management, for Westinghouse Electric Company; that he is authorized on the part of said company to sign and file with the Nuclear Regulatory Commission this document; that all statements made and matters set forth therein are true and correct to the best of his knowledge, information and belief.

James W. Winters
Manager
Standardization and Configuration Management

Subscribed and sworn to
before me this 30th day
of May 2007.

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Debra McCarthy, Notary Public
Monroeville Boro, Allegheny County
My Commission Expires Aug. 31, 2009
Member, Pennsylvania Association of Notaries

Notary

ENCLOSURE 1

Response to Requests for Additional Information on Technical Report No. 43

RAI-TR43-001 through RAI-TR43-017

(Non-Proprietary)

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-001
Revision: 0

***Question:***

The Failure Mode and Effect Analysis (FMEA) assumes a perfectly operating system as the starting point. Discuss the effect on analysis conclusions if the starting point is a system: 1) with one division bypassed; 2) one division bypassed and one division tripped; and 3) with the system operating on batteries.

**Westinghouse Response:**

The PMS has no feature that would allow an entire division to be bypassed. Instead, maintenance bypasses are applied at the individual channel bistable output level in the BPL through action taken by the operator at the MTP flat panel display. Bypasses may be applied to a single BPL in a division or to both BPLs. The latter case is used in the event of a sensor failure since a single sensor feeds both of the BPL process stations. The effect of a maintenance bypass on the protection logic is the same as a failed sensor. The two-out-of-four coincidence logic becomes two-out-of-three for that bistable function. Other functions are not affected. If the bypass were to be applied to only a single BPL, the LCL processor logic would use the data from the un-bypassed BPL and the logic would remain two-out-of-four. With a maintenance bypass applied to a bistable function (in both BPLs) in one division and with two-out-of-three logic, the single failure criterion is still met. Therefore, continued operation under this condition is permitted.

If a second sensor failure leads to the need to bypass a second channel, the resulting logic would become two-out-of-two. Since this does not meet the single failure criterion, the operator instead trips the bistables of the second channel. This effectively causes the logic to become one-out-of-two of the remaining good channels. This configuration also meets the single failure criterion thus plant safety is ensured. However, a further failure could cause spurious plant trip or actuation of ESF functions.

Whether an operator chooses to bypass or trip a channel, or to bypass multiple functions in a division is under control of plant administrative procedures. In addition, the coincidence logic voting gates enforce the rule that the single failure criterion must continue to be met under the condition of multiple bypasses. The same administrative procedures govern which of the bistable functions are to be bypassed when a given sensor channel fails.

Maintenance bypasses are not automatically applied for periodic testing or for restorative maintenance within the PMS cabinets. If they are used by manual actuation under administrative control, they will be applied to only to the bistable outputs of one of the BPL

process stations, that being the one under test. The redundancy of the processors within a given division provides the required fault tolerance to prevent spurious actions as a result of the test signal generation. The processors are tested, through operator action at the MTP, one at a time. Since coincidence of action is required at each level of the system, no spurious actions result from the temporary signal states created during testing. If a BPL is taken out of service for repair, the LCL processors in all division will ignore the data from that BPL, choosing instead the data from the redundant partner BPL in the same division. If an LCL is taken out of service for repair, its watchdog timer relays drop out allowing the outputs of its partner to control the opening of the trip breakers. The HSL link to the ILC cabinets from the un-affected LCL will continue to provide safety actuation of the division's ESF equipment if needed. If an ILC processor is taken out of service for repair, all valves operated by that cabinet will become inoperable from a safety point of view. However, many valves (those without onerous consequences of operation) will continue to be operable for manual actuations through the soft controls of the PLS since the CIMs remain powered. Redundancy of the PMS divisions allows safety functions to be accomplished through actuation of other safety equipment. The time required to conduct any repairs of ILC processors will be less than the action times for the controlled equipment in the plant Technical Specifications. Taking any other processor in a division (ITP, MTP, etc.) out of service for repair will not affect PMS actuations.

As for PMS operation on battery power, there is no effect. In the event of loss of normal AC power, the uninterruptible power supply (UPS) inverters will take their source power from the battery banks rather than the AC busses. Their AC output to the PMS cabinets remains unchanged. The PMS cabinets do not experience any difference in this mode of operation. The battery banks are sized to provide power to divisions A and D for 24 hours and to B and C for 72 hours. The longer time for divisions B and C provides extended plant monitoring on the safety displays. At the point of battery discharge when an inverter in a division can no longer produce AC power within specified tolerances, the inverter will shut off its output. The PMS cabinets in that division will become de-energized. Plant monitoring and ESF actuation through that division is no longer possible, including manual actuation of the equipment from the PLS. Since the entire division is fed from the same inverter, the de-energization will affect all cabinets at the same time, though the timing of the power off condition will be different in the four divisions.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

A discussion of abnormal operating conditions will be added to the next revision of the Technical Report, WCAP-16438, APP-GW-JJ-002, "FMEA of AP1000 Protection and Safety Monitoring System.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-002
Revision: 0

***Question:***

Discuss how failures of maintenance bypass and operation bypass functions are considered in the FMEA.

**Westinghouse Response:**

Maintenance bypass and operation bypass functions are performed through soft controls on flat panel displays. They are "software only" functions and do not depend on dedicated hardware components. Because software itself does not fail, these functions are not specifically treated in the Failure Modes and Effects Analysis (FMEA). Safety system Common Mode Failure (CMF) due to software design defect is dealt with in the AP1000 Instrumentation and Control Defense-in-depth and Diversity Report (WCAP-15775).

Operation bypasses, such as the Source Range Nuclear Instrumentation System (NIS) Trip Block function, are actuated through soft controls on the flat panel display of the Primary Dedicated Safety Panel. Operation bypasses are applied individually to the four Protection and Safety Monitoring System (PMS) divisions. These bypasses are used by the plant operator to allow transition into plant states where a protective function is no longer required and which would otherwise prevent putting the plant into the desired state. In accordance with the requirements of IEEE Std 603, if the plant state is such that a particular operation bypass is not permitted, the PMS automatically blocks the application of that bypass. If an operation bypass has been established and the plant state subsequently changes such that the bypass is not permitted, it is automatically removed by the PMS. If, through some non-specific failure mode, an operation bypass is not applied when needed, and the operator does not recognize the condition and proceeds to change the plant state, then the safety function that was to be bypassed will be actuated in the affected division(s). This could lead, for instance, to an un-intended plant trip if multiple divisions are affected. If the non-specific failure mode of the operation bypass leads to it becoming active when not commanded by the operator, the automatic features of the PMS to establish permissive conditions for operation bypasses will ensure plant safety.

Maintenance bypasses are applied through soft controls on the flat panel displays in the Maintenance and Test Panel (MTP) in each division. Bypasses can only be applied in the division in which the technician has accessed the MTP. The current state of the bypasses is displayed locally on the MTP, on the safety displays located on the Primary Dedicated Safety Panel in the Main Control Room (MCR), and on the displays of the Data Display and Processing System. Maintenance bypasses are applied at the channel level to individual bistable outputs.

They are separately applied to the two BPL process stations within the division. Therefore, it would take multiple faults to inadvertently defeat any portion of the safety system, and then only one division would be affected. The safety of the plant is ensured through the redundancy of the PMS.

In the event that some non-specific fault would cause a maintenance bypass to not be applied when the technician calls for it at the MTP, the effect would be that partial trip signals from the affected channel would propagate through the PMS divisions and would be included in the majority voting for the safety function rather than being blocked by the Local Coincidence Logic (LCL). With no other faults or partial trip conditions, there would be no net effect on the plant. One additional channel (of the same function) going to the trip state would cause a reactor trip (or other safety action). These are multiple failure scenarios that end in a safe plant state.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-003
Revision: 0

***Question:***

Discuss how corruption of message traffic between processors, between divisions, and between safety and non-safety systems have been considered in the FMEA.

**Westinghouse Response:**

Communication between processors within the same process station (e.g., Bistable Processor Logic [BPL] or Local Coincidence Logic [LCL]) is conducted by means of shared memory contained on the Communications Interface (CI) communication module. This communication is not done as messages; rather, the source processor deposits data values in the memory where the destination processor accesses these values for use in its functional algorithms. Shared memory failure is a line item included in the Failure Modes and Effects Analysis (FMEA) table for each process station.

Communications between divisions are conducted by means of High Speed Datalinks (HSL) from the BPL process stations to the LCL process stations in all divisions. Discussions of failures of these communications are found in the FMEA as transmission failures in Section 4.1 and as reception failures in Section 4.2. Communication failures can have many causes including broken media, component failures in the transmitter or receiver, processor failure on either end or corruption of the message by noise. The net effect of any of these causes is the same, valid data is not passed from the source processor to the destination processor. The destination processor takes note of the lack of data if the failure is persistent and takes a default action as described in the FMEA. Message corruption is detected by Cycle Redundancy Check (CRC) codes contained within the message. If the receiving processor detects that bit errors have occurred within a given message, the entire message is rejected. Processing continues with the previously received "good" quality data. Generally, the next message will be received without problem and no special action needs to be taken. If the lack of data due to message corruption (or for other reasons) persists, the communication channel will be marked as having "bad" quality. All data points conveyed by that channel will be marked as "bad" quality. In the case of the LCL processor, the alternate link from the same division will be used as input to the voting process.

The HSL communication links from the LCL to the Integrated Logic Processors (ILPs) within each division have the same type of protection against message corruption described above. The HSL from each of the two LCL processors perform Engineered Safeguards Features (ESF) actuation functions is sent to both of the ILPs in each of the Integrated Logic Cabinets (ILCs), thus allow selection of an alternate communications path should one become invalid.

Communications between the safety and non-safety systems occur through the gateways provided for each division. The MTP assembles data to be sent and passes messages to the gateway by means of a dedicated Fast Ethernet link. While these messages do provide protection against corruption using similar error detection means, the actions taken by the non-safety system upon receipt of corrupted data are beyond the scope of the FMEA.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

The above explanations will be added to the next revision of the Technical Report WCAP-16438, APP-GW-JJ-002, "FMEA of the AP1000 Protection and Safety Monitoring System," to enhance reader understanding of the analysis.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-004
Revision: 0

***Question:***

Discuss the effect of the Component Interface Module (CIM) module sending conflicting component status information via the different ports.

**Westinghouse Response:**

A potential failure mode of the CIM is that the equipment status that is reported to the Protection and Safety Monitoring System (PMS) via the Port X signals and to the Plant Control System (PLS) via the Port Y serial bus signals is inconsistent. It is also possible that the signals sent through one port are inconsistent (e.g., indicating that a valve is both open and closed). This type of inconsistency could affect one or both ports.

The PMS does not use the component status information in the actuation logic for the components. Therefore, any errors in these signals caused by CIM failures will not prevent the proper safety actuation of the equipment if necessary. The only consequence of conflicting component status information via the different ports will be that the status display on the flat panel displays on the Dedicated Safety Panel will be different from that on the displays of the Data Display and Processing System. As a general rule, there is no automatic checking done between the two measurements of the equipment status. It will only be evident if the operator notices the difference.

To determine which of the displays is correct, the operator will first determine whether either can be ruled out due to self inconsistency (e.g., a valve that is both open and closed). If this does not resolve the ambiguity, then other process information such as measured fluid flow through a valve can be used to resolve the true equipment state.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-005
Revision: 0

***Question:***

Discuss the failure path which leads to, and the plant consequences which result from, the CIM failures in fault classification I.

**Westinghouse Response:**

Component Interface Module (CIM) failures can be placed into three types: 1) those which prevent the component actuation, 2) those which issue spurious output commands, and 3) those which do not affect the component actuation paths. Within these types are failures that affect the safety actuation input (Port X), failures that affect the non-safety actuation input (Port Y), and failures that affect both actuation paths. Of these failure types, only the second one leads to fault classification I in the Failure Modes and Effects Analysis (FMEA). This is due to the fact that failure to actuate equipment in one division does not lead to loss of capability to perform the safety function, because redundant equipment in other divisions is not affected by the failure.

Spurious actuation commands could result from failures in the CIM itself or from failures in the host systems providing inputs to the CIM. For the majority of components, coincidence of two actuation signals from redundant Integrated Logic Processors (ILPs) is required to actuate equipment. A few components will be actuated on a signal from either of the ILPs. In these cases, the consequences of spurious actuation are deemed to be acceptable. Thus, the CIM will prevent spurious actuations from the ILPs from causing an adverse plant transient. For non-safety actuations from the Plant Control System (PLS), the commands are received as coded messages with bit error detection via a serial bus. Failures in this path are much more likely to prevent action rather than cause spurious actuation.

There are several components within the CIM whose failure could cause one of the output relays to inadvertently turn off. These components include the Field Programmable Gate Array (FPGA) device and the relay drive transistors. Such failures are detected by the self-diagnostic features of the CIM, in addition to being revealed by the consequent actions that would result from issuing a spurious command to plant equipment.

Generally, the consequence of spurious valve actuations on the plant is beyond the scope of the FMEA. However, some broad statements can be made in this regard. First, under a condition of normal plant operation, any spurious movement of many of the Class 1E valves will be towards the defined "safe" direction of that valve. This motion may cause a plant transient (for instance, by isolating an important fluid system line) that will subsequently lead to a trip;

however, plant safety is maintained. For the cases where spurious motion of the valve is towards the "un-safe" direction, the valve position is independently monitored. The operator will take action to restore the safe configuration within the Tech Spec allowed action time. The likelihood of a plant accident in the interim before that safe configuration is restored is extremely low.

A subset of the actuated equipment has been designated as components whose operation poses onerous consequences on the plant. These components include the 12 squib-operated valves, 12 Motor-Operated Valves (MOV) in the Automatic Depressurization System (ADS), and the 4 head vent valves.

The squib valves are each actuated by two separate CIMs located in different ILCs. One of the CIMs charges the squib firing circuit, while the other discharges the energy into the squib igniter. These CIMs must be operated within precise sequence and timing parameters in order to fire the squib and open the valve. This sequence includes the removal of the charging command before the firing command is issued. Therefore, it is not credible that a single random failure, or even multiple random failures, of the CIMs could cause spurious opening of a squib valve.

For the MOVs in the ADS and the head vent valves, there are two normally closed valves in series in each depressurization path. These valves are controlled by different divisions of the Protection and Safety Monitoring System (PMS). Therefore, spurious opening of a single valve will not have a direct impact on the plant. The opening of the valve will be detected by its position status indication as well as by the self-diagnostic features of the CIM. Corrective action (i.e., replacing the failed CIM) will be possible in a short time period without impact to plant operations.

Therefore, a single failure of a CIM may lead to a plant trip, but it cannot cause an unsafe plant condition. The frequency of these spurious trips will be shown to be acceptably low compared to other causes of forced outage.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

The above explanation of the effects of fault classification I CIM failures will be added to the next revision of the Technical Report WCAP-16438, APP-GW-JJ-002, "FMEA of the AP1000 Protection and Safety Monitoring System.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-006
Revision: 0

***Question:***

Of the failure modes in detectability class C, which should be considered as undetected failures for the purposes of single failure analysis?

**Westinghouse Response:**

IEEE Std. 379-2000 defines detectable failures as, "Failures that can be identified by periodic testing by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures."

Dectectability class C denotes those failures that are not immediately revealed by self supervision of the system equipment or by the consequent impact of the failure on the process, but that are revealed during the execution of planned surveillance testing. Since, by definition of the class, these failures are revealed by surveillance testing, they are all considered to be detected failures for the purposes of single failure analysis. Failure modes that should be considered as undetected failures for the purposes of single failure analysis are assigned to detectability class D.

The specific test sequences to be performed for Protection and Safety Monitoring System (PMS) surveillance and the interval at which these tests will be performed have not been determined as of yet for the PMS. When the surveillance testing is designed, the failure modes in detectability class C shall be included in the test coverage.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-007
Revision: 0

***Question:***

How is the CIM Field Programmable Gate Array start-up issue addressed in the FMEA?

**Westinghouse Response:**

The type of Field Programmable Gate Array (FPGA) used in the Component Interface Module (CIM) uses the Actel Anti-fuse™ technology to permanently program the linkage between the logic gates in the device. The programming process makes permanent, low resistance electrical connections between the signal pathways in the device. There is no initialization process or program loading performed at device start-up.

A power monitor on the CIM holds the FPGA in the reset state until the power supply voltages are within specified bounds. This prevents spurious signals on the device outputs from occurring before the appropriate combinatorial logic can be performed.

Because the nature of the FPGA is the same as hardwired solid state logic, it is not given any special treatment in the Failure Modes and Effects Analysis (FMEA). FPGA failures are included in the potential failure causes of the CIM. Safety system Common Mode Failure (CMF) due to design errors (such as errors in the FPGA) is dealt with in the AP 1000 Instrumentation and Control Defense-in-Depth and Diversity Report (WCAP-15775).

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-008
Revision: 0

***Question:***

Discuss how possible Maintenance and Test Processor (MTP) failure that could corrupt system parameter data (e.g., setpoints, scaling constants, bus address assignments) or bypass status are addressed in the FMEA.

**Westinghouse Response:** a,c

a,c

[ ]

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-009
Revision: 0

***Question:***

Discuss the process for identifying failure modes and how vendor insights or field experience were considered.

**Westinghouse Response:**

For digital Instrumentation and Control (I&C) technology it is not practical to do a Failure Modes and Effects Analysis (FMEA) to the level that identifies individual components and their specific failure modes (short, open, value change, etc.). Instead, the analysis is done at a more abstract level. In the case of the FMEA done for the Protection and Safety Monitoring System (PMS), the "components" selected were at a level of replaceable modules (CPU boards, I/O modules, Component Interface Module [CIM], etc.). Failures of the module are then listed in a way that describes a specific function that is not performed or a behavior that is exhibited. This list represents insight of the analyst into the ways that module failure could impact the safety functions to which the module contributes. In determining the functions and behaviors to be included, the module interfaces are examined. Previous FMEA studies, such as those done for the AP600 Design Certification and the Common Q topical report, are used as guidance for the appropriate level of abstraction.

In some cases, further illustration of the module failure modes is provided by dividing the module into sub-modules. Such is the case in the Technical Report (WCAP-16438, FMEA of the AP1000 Protection and Safety Monitoring System) where the CPU module is divided into the functional processor portion and the communications processor portion. Another example of this sub-division is the analog input module where the individual channel behaviors are considered in addition to the common portion that controls communication with the host processor over the I/O bus. Such sub-division requires insight as to the potential failure modes of the module to know which portions can function independently and where interactions between the sub-modules may affect their performance.

Vendor insight is also used in determining the response of various modules to abnormal signals and the means by which faults will be detected. This insight is provided through a study of product specifications and other background material beyond that which is formally part of the PMS design documentation.

While no specific attempt is made to capture field experience into the definition of failure modes, the understanding of basic operation of digital systems and how these circuits interact is the result of years of experience in the application of this technology.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-010
Revision: 0

***Question:***

Discuss the possible modes and consequences of momentary power interruption or over / under voltage conditions. This might occur at the division, cabinet, bin, or module level.

**Westinghouse Response:**

Power to the Protection and Safety Monitoring System (PMS) cabinets is provided from battery backed inverters. In the event of inverter failure, automatic switchover of the output to an AC bus will occur. During this switchover, power may be momentarily interrupted. The inverters and supply busses (AC and DC) are not in the scope of the PMS and have not been included in detail in the PMS Failure Modes and Effects Analysis (FMEA). An FMEA of the Class 1E 125V DC and Class 1E Uninterruptible Power Supplies is contained in Chapter 8 of the AP1000 Design Control Document. The inverters are separate for each safety division, so that any effects of the switchover will be limited to a single division.

The AC power feed to each PMS cabinet is processed by redundant power supply modules. Internal to each of these modules is a capacitor bank that provides the capability to ride through momentary power interruptions. While the length of the "hold up" period is a function of the loading on the supply, the specification of the power supply guarantee a minimum of 48 milliseconds when fully loaded. When the holding charge of the capacitor bank is depleted (after the "hold up" time) the power supply will no longer be able to provide output voltage within its specified range. A monitor circuit internal to the supply detects this as an under-voltage condition, turns off the voltage outputs to the cabinet equipment and asserts a status alarm. This action is latched and will persist until the power is turned completely off and is subsequently restored. It is conceivable that the momentary power loss on the input could be long enough to cause this reset to occur. Over-voltage conditions on the input are also detected and dealt with in a similar fashion.

The PMS cabinet power supplies are redundant; their outputs are auctioneered by diodes such that the higher of the two voltage outputs is passed on to the assemblies within the cabinet. In normal conditions with both supplies operating, the load is shared between the two supplies such that each supply carries a nominal load of approximately 50 percent of the total load. Thus, if the momentary power interruption or over/under voltage condition only affects one of the two power feeds to the cabinet, the downstream equipment will not see any effect. If power is removed from both power supplies, the cabinet processors will be put into a reset state. Outputs of the processor will go to their default state. When power is restored, the processors will go through their initialization sequence, which takes several minutes to complete. After

initialization, the processor outputs are put into the state corresponding to the logic algorithms being applied to the sensor inputs.

If the momentary power disturbance affects only one of the two cabinets holding Bistable Processor Logic (BPL) and Local Coincidence Logic (LCL) process stations, then the net effect on the PMS function will be negligible since the safety functions of reactor trip and Engineered Safeguards Features (ESF) can be carried out through the un-affected cabinet. If the power disturbance affects both cabinets (i.e., originated in the inverter source), then the reactor trip breakers for that division will open and ESF actuations will be blocked until the restart sequence is completed. ESF actuations for a subset of plant equipment will also be blocked if the power disturbance affects both feeds to an Integrated Logic Cabinet (ILC).

Downstream of the redundant power supply auctioneering diodes, there are no credible faults that could cause momentary interruption or over/under voltage conditions to a module. Any fault that causes an over-current condition will either blow the fuse on the module, thus protection in the supply to other modules in the cabinet, or will cause the over-current protection in both of the redundant power supplies to shut off their outputs until the fault condition is cleared and the power is cycled off and then on.

The Component Interface Module (CIM) module has a power supply monitor circuit that holds the Field Programmable Gate Array (FPGA) in a reset state and holds the outputs as "off" until the internal logic supply voltage is within specification. The reset state is held for a minimum of 30 milliseconds. If the supply voltage to the module deviates from specification at some time after power up, this monitor circuit will reset the device until the power supply returns to being within specification. This circuit prevents anomalous actuation outputs from occurring during initialization of the module.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

A discussion of the effects of power transients will be added to the next revision of the Technical Report WCAP-16438, APP-GW-JJ-002, "FMEA of the AP1000 Protection and Safety Monitoring System."

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-011
Revision: 0

***Question:***

Discuss how field components are assigned to different Interposing Logic Cabinet and CIM and the implication of the assignment on failure consequences.

**Westinghouse Response:**

a,c

[ ]

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

a,c

[ ]

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-013
Revision: 0

***Question:***

Section 2.2, [Local Coincidence Logic] LCL PROCESS STATION, discusses how the logic within a division handles the situations where: 1) if one of the two Bistable Processor Logic (BPL) signals has "bad" quality or if its receive channel has "bad" quality, 2) if both BPL signals have "good" quality, and 3) if both BPL signals have "bad" quality. How does the logic handle the situation where the signal quality are both "good" for each BPL signal, but one BPL signal indicates its bistable is "tripped" and the other BPL signal indicates its bistable is "not tripped"?

**Westinghouse Response:**

Section 2.2 of the TR states: "In the condition that signals of GOOD quality are available from both BPLs of a division, a logical OR of the FORCE PARTIAL TRIP OR SIGNAL VALUE AND NOT BYPASS is used." The logic combination of the signal value with the forced partial trip and bypass signals is performed for the signals from each of the BPLs in each division; the two results are then combined with a logical OR. Thus, if both BPLs issue GOOD quality signals, one "tripped" and the other "not tripped" the result that is sent to the two out of four (2/4) voting logic is TRUE ("tripped").

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

The above explanation will be added in Section 2.2 of the next Technical Report revision.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-014
Revision: 0

***Question:***

Section 2.5, [Nuclear Instrumentation System] NIS SUBSYSTEM, discusses the Nuclear Instrumentation Modules (NIMOD). Do the signals to the divisional BPL modules from NIMOD Source Range, NIMOD Intermediate Range/Wide Range and NIMOD Power Range carry a quality tag? If not, then how is the quality of the signal determined?

**Westinghouse Response:**

The signals from the NIMOD drawers to the Bistable Processor Logic (BPL) are analog signals, thus there is no quality tag. After signal processing and analog-to-digital conversion (ADC), a quality tag is assigned. A range check is performed, and if the signal is within the pre-determined engineering unit range (e.g., percent power), a quality of "good" is assigned to the value.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-015
Revision: 0

***Question:***

Section 2.2 states that the logic signals received by the High Speed Link(s) can be substituted by test injection signals, received via the AF100 bus, under the control of the status of the "Test Enable keyswitch (digital) input" and a test enable software signal both of which are received via the AF100 bus. Is this "Test Enable keyswitch" the same as the "Key-lock switches, located in the cabinet housing the ITP station"? If not please provide a more detailed description of their location and function.

**Westinghouse Response:**

The "Test Enable keyswitch" mentioned in Section 2.2 is one of the "Key-lock switches, located in the cabinet housing the ITP station" described in Section 2.7. The Interface and Test Processor (ITP) and Maintenance and Test Panel (MTP) are in the same cabinet in each division. Separate key-lock switches are provided to enable testing and to allow software maintenance.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-016
Revision: 0

***Question:***

Figure 2-2, Typical PMS Division Configuration (Division B Shown), shows a block labeled "DISABLE TUs" above a switch labeled "Main Control Room Remote Shutdown Room (RSR) TRANSFER" that is not marked as being in the Main Control Room. Where is this switch located? Also, what are the Termination Unit "TU" labeled boxes and their purpose?

**Westinghouse Response:**

The Main Control Room/Remote Shutdown Room (MCR/RSR) Transfer Switch is located outside the MCR, on the way from the MCR to the RSR, so that the personnel can activate the switch on the way from the MCR to the RSR.

a,c

[ ]

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

Technical Report WCAP-16438, "Failure Modes and Effects Analysis of the AP1000 Protection and Safety Monitoring System," will be revised accordingly.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

RAI Response Number: RAI-TR43-017
Revision: 0

***Question:***

Figure 2-2 shows the input to module LCL-B1X from RSR going to the fifth "DI" rack module counting, the input to module LCL-B2X from RSR goes to the first "DI" rack module making two inputs to that "DI" module. Is this a drawing error? Explain which input goes to the "DI" module?

**Westinghouse Response:**

This is not a drawing error. There are six Digital Input modules located in the Local Coincidence Logic (LCL) subrack to accommodate all of the various switch inputs. The intent of the drawing is to depict the inputs to the LCL subrack, not the exact electrical connections.

**Design Control Document (DCD) Revision:**

None.

**PRA Revision:**

None.

**Technical Report (TR) Revision:**

None.