



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: 412-374-6206
Direct fax: 412-374-5005
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP/NRC2292

November 20, 2008

Subject: AP1000 Responses to Requests for Additional Information (SRP7)

Westinghouse is submitting responses to the NRC requests for additional information (RAIs) on SRP Section 7. These RAI responses are submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in the responses is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application.

Enclosure 1 provides the response for the following RAIs:

RAI-SRP7.1-ICE-08 Rev 1
RAI-SRP7.1-ICE-21 Rev 0
RAI-SRP7.1-ICE-28 Rev 0
RAI-SRP7.9-ICE-02 Rev 0

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.

Very truly yours,

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Enclosure

1. Response to Request for Additional Information on SRP Section 7

cc: D. Jaffe - U.S. NRC 1E
E. McKenna - U.S. NRC 1E
S. K. Mitra - U.S. NRC 1E
P. Ray - TVA 1E
P. Hastings - Duke Power 1E
R. Kitchen - Progress Energy 1E
A. Monroe - SCANA 1E
J. Wilkinson - Florida Power & Light 1E
C. Pierce - Southern Company 1E
E. Schmiech - Westinghouse 1E
G. Zinke - NuStart/Entergy 1E
R. Grumbir - NuStart 1E
R. Seelman - Westinghouse 1E

ENCLOSURE 1

Response to Request for Additional Information on SRP Section 7

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.1-ICE-08
Revision: 1

Question:

In Table 3.3-1, Risk Identification Checklist, of the AP1000 NuStart Protection and Safety Monitoring System Software Project Plan (WNA-PJ-00071-GEN), the risk for superfluous features being added to the software was given a probability, impact, and exposure of "zero".

Provide the basis for establishing this risk identification. Specifically, provide a definition of superfluous. Verify that the probability and exposure of superfluous features would be high. In addition, since the risk of having an inexperienced personnel/software developer was identified as "high" in the table, describe the processes that Westinghouse has in place to prevent superfluous features from being added by inexperienced personnel?

Westinghouse Response:

Using the standard definition of the word superfluous as being: exceeding what is sufficient or necessary; not needed; or unnecessary, the use of "0" for the probability and exposure to superfluous code, means minimal probability and exposure as explained in the below paragraph. The impact would be high if the code resident on the safety system is superfluous and therefore may not be verified or tested.

The Common Q Design Process is a requirements driven process. Experienced engineers are generating the requirements. All software documentation is peer-reviewed by experienced engineers. All software documentation is linked to higher level requirements as part of the requirements management process. The software documentation and requirements analyses are reviewed by experienced engineers and the V&V team. All software code is subject to a formal code review process by the V&V team. Any features in the code not driven by requirements will have to be justified or else removed from the code.

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-SRP7.1-ICE-21
Revision: 0

Question:

Provide a detailed description of the functions, architecture, construction, and implementation of the CIM.

Section 4 of IEEE 603-1991 requires, in part, that the design basis be available as needed to facilitate the determination of the adequacy of the safety system. The description of the CIM provided in Section 5.1.5 of WCAP-16675-P, "Protection System Architecture," Rev. 0, was not sufficient to determine how the CIM meets the various requirements of IEEE 603-1991 and its associated guidance, including IEEE 7-4.3.2-2003. Provide sufficient information describing the CIM such that a determination of adequacy could be made. At a minimum, the following aspects of the CIM should be addressed in detail:

1. Priority scheme and logic implemented in the CIM
2. Actuators that the CIM can control and how the configuration for those actuators is implemented with the CIM
3. Incoming and outgoing signals to the CIM
4. Major hardware and logic components within the CIM
5. Communication protocols with safety and non-safety systems; including mechanisms to prevent the interference of safety functions by non-safety communications
6. Physical and electrical isolation between the safety and non-safety components
7. CIM operation for various plant/equipment modes (i.e., normal, abnormal, accident conditions and manual, testing, and maintenance modes)
8. Identification of how automatic (if applicable) and periodic testing is performed on the CIM, including the ability of the CIM to perform its safety function during testing
9. Time response
10. Power supplies
11. Control of the CIM from locations other than the main control room
12. Cyber-security for the CIM
13. How maintenance is performed on the CIM
14. Reliability of the CIM

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

15. Description of how the state of the CIM following power-up and initialization will correspond to the current plant state
16. Operating history
17. Applicable regulations, guidance, testing measures and standards used in CIM design

Westinghouse Response:

The design requirements for the CIM design are completed. The detailed design is ongoing.

Additional details on the CIM are included in WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components". Revision 1 of the WCAP is being prepared and is expected to be submitted to the NRC in September 2008. The WCAP will include the following technical information:

1. Data communication between the functional systems that comprise the AP1000™ Instrumentation and Control (I&C) system and between the AP1000 I&C system and external systems
2. The Component Interface Module (CIM) that is used to interface the I&C system to safety system components
3. The manual control of the safety system at the system level and the component level.

The following provides a more detailed response to the bulleted items of the Question of this RAI:

1. Priority scheme and logic implemented in the CIM

The algorithm used by the CIM to resolve conflicting demands from the Safety and non-Safety System is State-based Priority.

2. Actuators that the CIM can control and how the configuration for those actuators is implemented with the CIM

The CIM interfaces with components of the following types: motor-operated valves, air-operated valves, circuit breakers, and squib valves. No configuration of the CIM is required to interface to any of these plant component types. The same priority logic and component control logic is applied for each CIM.

3. Incoming and outgoing signals to the CIM

The CIM module typically arbitrates the component command signals received on two different ports: Port X and Port Y. Port X connects the PMS (via the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Safety Remote Node Controller), and Port Y connects to the PLS via the Ovation® remote I/O bus. The CIM also interfaces to the motor control centers in the plant. Command outputs (i.e. Open or Close) are output from the CIM, and feedback (i.e. valve position, torque limits, etc) are inputs to the CIM.

4. Major hardware and logic components within the CIM

The logic that interfaces to the PLS is located in the Ovation® Remote Node Controller, and the logic that interfaces to the PMS is located in the Safety Remote Node Controller. Within the CIM, there is interface logic that translates the information from remote node controllers to local buffers. These buffers provide the input signals to the priority logic and component control logic in the CIM.

5. Communication protocols with safety and non-safety systems; including mechanisms to prevent the interference of safety functions by non-safety communications

The communication protocol that is used with the non-safety system is the Ovation® remote I/O bus, and the protocol to the safety system is the Common-Q High Speed Serial Link.

There are three mechanisms used to prevent the interference of safety functions by non-safety communications. First, electrical isolation is provided by using a fiber optic link to the PLS. Second, communication isolation is provided by the interface logic in the CIM. This logic will only accept a command signal if the it is transmitted from PLS using the proper protocol. The third protection is the functional isolation that is provided by the priority logic in the CIM.

6. Physical and electrical isolation between the safety and non-safety components

The non-safety system (PLS) is contained in a separate cabinet from the PMS cabinets, and the interface to the PLS system uses a fiber optic connection. For the non-safety loads that are controlled by the PMS system, a qualified isolator is used for all signals between the CIM and the plant component.

7. CIM operation for various plant/equipment modes (i.e., normal, abnormal, accident conditions and manual, testing, and maintenance modes)

The CIM operation does not change based on plant/equipment modes. The inputs that are presented to the CIM are applied to the same priority logic and component control logic under all conditions.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

8. Identification of how automatic (if applicable) and periodic testing is performed on the CIM, including the ability of the CIM to perform its safety function during testing

The CIM supports continuous on-line diagnostics. These features are discussed in WCAP-16674-P.

9. Time response

The Requirements for the CIM design are completed, and the detailed design is ongoing. The time response of the CIM will be included in the time response budget for the PMS.

10. Power supplies

The CIM is powered from the standard 24 V power supply in the PMS cabinet.

11. Control of the CIM from locations other than the main control room

The CIM receives inputs from the PMS and PLS systems. These systems provide the normal control (automatic and manual) for the components that are controlled through the CIM. A local manual interface is also provided on the CIM for maintenance and test purposes.

12. Cyber-security for the CIM

The CIM can not be reconfigured from either the Safety or Non-Safety Ports. The features that are provided to prevent unauthorized or incorrect reconfiguration of the Ovation Remote Node Controller via the Ovation network are provided in the response to RAI-TR88-017 (WCAP-16767). The response contains Emerson Proprietary information therefore the details are not repeated in this answer.

13. How maintenance is performed on the CIM

The CIM supports continuous on-line diagnostics. These features are discussed in WCAP-16674-P.

14. Reliability of the CIM

The Requirements for the CIM design are completed, and the detailed design is ongoing. Based on the requirements, Mean Time Between Failure for the CIM and SRNC are 100,000 hours.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

15. Description of how the state of the CIM following power-up and initialization will correspond to the current plant state

The Requirements for the CIM design are completed, and the detailed design is ongoing. Based on the requirements, the CIM will be initialized to a state that does not output any command to the component, and the outputs will remain in this state until a valid command is received on the input to the CIM. With this approach, no plant components will change state following power-up and initialization of the CIM.

16. Operating history

The Requirements for the CIM design are complete, and the detailed design is ongoing. Since the design has not been completed, there is no operating history for this version of the CIM.

17. Applicable regulations, guidance, testing measures and standards used in CIM design

The CIM design is being done to comply with all AP1000 standards and is being accomplished under the standard Westinghouse process for development of Safety Grade components.

Reference(s):

None

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

1. WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components" (APP-GW-GLR-065)
2. WCAP-16767, "Response to Request for Additional Information on Westinghouse AP1000 Combined License (COL) Pre-Application Technical Reports Number 42 and Number 88" (APP-PMS-GL-042)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.1-ICE-28

Revision: 0

Question:

Demonstrate how the PMS System meets 10 CFR Part 50, Appendix A, GDC 21, "Protection System Reliability and Testability," and Clause 5.1 of IEEE-603-1991.

Although the Westinghouse report WCAP-16438-P - FMEA of AP1000 Protection and Safety Monitoring System, provides a good starting point detailing failure modes from a fully operational system, it lacks detailed analysis from a less than fully operational system (i.e., a division in maintenance). Additionally, the FMEA does not detail all possible initial system states which are required for a comprehensive and complete single failure analysis.

Westinghouse Response:

Westinghouse submitted Revision 2 of WCAP-16438-P (APP-GW-JJ-002) to the Westinghouse Rockville office on October 9, 2008 for NRC review. This revision of the document provides the detail requested in this RAI. This document and related information was also discussed at the Technical Review meetings held between Westinghouse and the NRC on October 15th and 16th 2008. Revision 2 of this document also incorporates the information referenced in the WEC submittal to the NRC, DCP/NRC1884, dated May 11, 2007, and entitled "AP1000 COL Response to Requests for Additional Information (TR #43).

Reference(s):

1. DCP/NRC1884 dated 5/11/2007 "AP1000 COL Response to Requests for Additional Information
2. APP-GW-GLR-018, Rev 0

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

1. APP-GW-JJ-002 (WCAP-16438-P), Rev 2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.9-ICE-02
Revision: 0

Question:

Provide further design information of the communication network within the AP1000 PMS. Specifically, in the AP1000 PMS design, what types of network segregation exist between message transfer and process data transfer to prevent the two processes from interfering with each other?

Section 7.9 of the Standard Review Plan, "Data Communication Systems," defines performance criteria for data communication systems; specifically on system capacity, data rates, and bandwidth requirements. Section 3.1 of WCAP-16675-P states that process data transfers will be of a certain percentage of the maximum capacity of the network and message transfers will use the remainder of the capacity. What mechanisms within the network design prevent interference of process data transfers with message transfers when there is excess network traffic?

Westinghouse Response:

The AF100 process data transfer is a deterministic protocol which has priority over the non-deterministic message transfers. Message transfers are used for such off-line functions as interrogating the PLC internal error buffer, or loading an application program into the PLC. Such message transfers are non-deterministic such that their interruption by process data transfers has no significant impact on the system. The process data transfers are protected from such interruption because they have pre-allocated bandwidth segments for each cyclic data packet on the AF100. The message transfers use any bandwidth left over for their non-deterministic data.

Reference(s):

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

None