



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/NRC2460

May 6, 2009

Subject: AP1000 Response to Request for Additional Information (SRP 7)

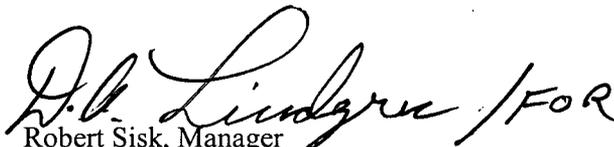
Westinghouse is submitting a response to the NRC request for additional information (RAI) on SRP Section 7. This RAI response is submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in this response is generic and is expected to apply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

Enclosure 1 provides the response for the following RAI(s):

RAI-SRP7.7-ICE-01 R1  
RAI-SRP7.9-ICE-02 R1

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. Mitra	- U.S. NRC	1E
	C. Proctor	- U.S. NRC	1E
	T. Spink	- TVA	1E
	P. Hastings	- Duke Power	1E
	R. Kitchen	- Progress Energy	1E
	A. Monroe	- SCANA	1E
	P. Jacobs	- Florida Power & Light	1E
	C. Pierce	- Southern Company	1E
	E. Schmiech	- Westinghouse	1E
	G. Zinke	- NuStart/Entergy	1E
	R. Grumbir	- NuStart	1E
	B. 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-SRP7.7-ICE-01

Revision: 1

### **Question:**

Demonstrate what actions, or outputs, are generated when one or more signals disagree or fall outside a defined parameter field for a given set of inputs (e.g. temperature, pressure, flux) to the Signal Selector Algorithms within the Plant Control System. For example, what alarm, control or indication outputs are processed based upon the logic contained within the Signal Selector Algorithms once a signal originating from the PMS is flagged as "bad" quality?

### **Westinghouse Response:**

This RAI was discussed with the NRC at the January 30, 2009 technical review meeting at the WEC Rockville office. The following response (Rev 1) has been revised to include the discussions at the January meeting.

Signal selector algorithms are utilized as a functional means to perform signal validation and increase fault tolerance within the Plant Control System (PLS). The nature of the signal validation is contingent on the redundancy available in the various process measurements. The signal selection algorithms are able to identify invalid inputs on the basis of the deviation between the redundant measurements. The signal selection algorithms provide at least two levels of warning. The first level shall alert the operator to a measurement deviation that is approaching the point at which the signal would be identified as invalid. A final level of warning shall alert the operator to the failure of the signal selection process.

A first stage operator notification is provided to alert operators that there are input channel deviations or quality issues, but the output value is still valid. A second stage operator notification is provided to alert operators that there are more significant input deviations or quality issues and the output value is no longer considered valid. The Plant Control Systems' identification of first stage operator notification or second stage operator notification does not result in any feedback to the PMS or DAS from PLS.

Coincident with the second level alert the analog output value is flagged as having "bad quality." Control functions shall monitor the quality of the output value and appropriate control action shall be taken. In the case of "closed loop controls" the affected modulating valve controller shall automatically be switched into the manual mode of operation. This automatic action prevents plant transients or upsets from occurring in response to a failed input sensor, and the PLS control action does not impact PMS or DAS from performing their safety functions. The operator is able to control the outputs manually and can return to the automatic mode once the fault condition has been repaired and returned to normal. An alarm is provided to indicate that a controller is switched to manual as a result of a "bad quality" input.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

---

Anywhere the output value of the signal selector algorithms is used for indication on a graphical display, the signal quality will also be indicated. When the value is "flagged" as having bad quality, the output value which is shown on the graphical display will also indicate the bad quality, through the usage of a single quality character made available to the operator in the form of a color change. This quality character is located immediately to the right of the displayed analog output 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-SRP7.7-ICE-01

Revision: 1

### **Question:**

Demonstrate what actions, or outputs, are generated when one or more signals disagree or fall outside a defined parameter field for a given set of inputs (e.g. temperature, pressure, flux) to the Signal Selector Algorithms within the Plant Control System. For example, what alarm, control or indication outputs are processed based upon the logic contained within the Signal Selector Algorithms once a signal originating from the PMS is flagged as "bad" quality?

### **Westinghouse Response:**

This RAI was discussed with the NRC at the January 30, 2009 technical review meeting at the WEC Rockville office. The following response (Rev 1) has been revised to include the discussions at the January meeting.

Signal selector algorithms are utilized as a functional means to perform signal validation and increase fault tolerance within the Plant Control System (PLS). The nature of the signal validation is contingent on the redundancy available in the various process measurements. The signal selection algorithms are able to identify invalid inputs on the basis of the deviation between the redundant measurements. The signal selection algorithms provide at least two levels of warning. The first level shall alert the operator to a measurement deviation that is approaching the point at which the signal would be identified as invalid. A final level of warning shall alert the operator to the failure of the signal selection process.

A first stage operator notification is provided to alert operators that there are input channel deviations or quality issues, but the output value is still valid. A second stage operator notification is provided to alert operators that there are more significant input deviations or quality issues and the output value is no longer considered valid. The Plant Control Systems' identification of first stage operator notification or second stage operator notification does not result in any feedback to the PMS or DAS from PLS.

Coincident with the second level alert the analog output value is flagged as having "bad quality." Control functions shall monitor the quality of the output value and appropriate control action shall be taken. In the case of "closed loop controls" the affected modulating valve controller shall automatically be switched into the manual mode of operation. This automatic action prevents plant transients or upsets from occurring in response to a failed input sensor, and the PLS control action does not impact PMS or DAS from performing their safety functions. The operator is able to control the outputs manually and can return to the automatic mode once the fault condition has been repaired and returned to normal. An alarm is provided to indicate that a controller is switched to manual as a result of a "bad quality" input.

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

---

Anywhere the output value of the signal selector algorithms is used for indication on a graphical display, the signal quality will also be indicated. When the value is "flagged" as having bad quality, the output value which is shown on the graphical display will also indicate the bad quality, through the usage of a single quality character made available to the operator in the form of a color change. This quality character is located immediately to the right of the displayed analog output 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-SRP7.9-ICE-02

Revision: 1

### **Question (Revision 0):**

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 (Revision 0):**

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.

### **Westinghouse REVISED response based on NRC comments from the January 29-30 meeting (Revision 1):**

At the January 2009 NRC meeting with Westinghouse, the NRC requested more information about process data transfer and how it works. Westinghouse committed to identifying the docketed references that describe this. The Common Q Safety Evaluation Report (SER) (ML003740165, August 11, 2000), Section 4.1.3.1 on pages 31-32 describe this. It is also discussed in the Common Q Topical Report (WCAP-16097-P-A) Section 6.3.1.4.

What is not described in the SER or Topical Report is the fact that the AMPL Control Configuration (ACC) tool limits the number cyclic data packets (CDPs) that can be configured. A CDP, as described in WCAP-16097-P-A, contains 8 process data values. By limiting the number of CDPs, the ACC tool protects the engineer from configuring too many CDPs that may

# AP1000 TECHNICAL REPORT REVIEW

## Response to Request For Additional Information (RAI)

---

overload the Advant Fieldbus 100 (AF100). Another limitation check is when the AC160 controller starts up. If the multiprocessors in the AC160 attempt to configure more than 400 CDPs, then an error will occur. When this error occurs, the processor module will not start up and this will cause a fault condition in the safety division. The operator will then be alerted of this fault condition.

**Reference(s):**

1. ML003740165, "Common Q Safety Evaluation Report," August 11, 2000.
2. WCAP-16097-P-A, Rev. 0, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.

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

None

**PRA Revision:**

None

**Technical Report (TR) Revision:**

None