



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/NRC2405

March 27, 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:

RAI-SRP7.3-ICE-02 R2

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,

A handwritten signature in black ink, appearing to read 'Robert Sisk'.

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

/Enclosure

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

DO63
NRO

cc:	D. Jaffe	- U.S. NRC	1E
	E. McKenna	- U.S. NRC	1E
	S. K. 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
	D. Peck	- 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-SRP7.3-ICE-02

Revision: 2

Question (Revision 0):

Provide additional detail of the manual control scheme of the PMS Engineered Safety Features Actuation System (ESFAS) function as described in WCAP 16675-P.

Per WCAP 16675-P, the manual system level actuation uses all automatic PMS components with the exception of the Bistable Processor Logic device. Regulatory Position Point 4 in Regulatory Guide 1.62, "Manual Initiation of Protective Actions," reads, "*The amount of equipment common to both manual and automatic initiation should be kept to a minimum.*" Furthermore, Section 6.2.1 of IEEE Standard 603-1991 reads, "*The means provided [for manual initiation of a safety system] shall... **depend on the operation of a minimum of equipment consistent with the constraints of [Section] 5.6.1 [Independence].***" It is currently difficult for the NRC staff to see how the manual actuation of the ESFAS functions meets this criteria.

Westinghouse Response (Revision 0):

Within a division of the PMS, the only parts involved in manual ESF system level actuation are the switch itself, the Local Coincidence Logic (LCL), Integrated Logic Processor (ILP) and Component Interface Module (CIM).

Manual ESF system level actuation is initiated by the operator from the Main Control Room (MCR) via dedicated switches located on the Primary Dedicated Safety Panel (PDSP) and Secondary Dedicated Safety Panel (SDSP), or from the Remote Shutdown Room (RSR) via dedicated switches located on the RSR panel. In each PMS division, the signal from the switch is connected to the LCL subrack where it is converted into a redundant ESF system level actuation command. In the LCL, the manual ESF system level actuation command is "ORed" with the automatic determination of ESF system level actuation from the ESF coincidence logic. The ESF system level actuation command from the OR function is sent to the ILP via a High Speed Link (HSL). The ILP performs the component fan-out function which converts the ESF system level command into individual actuation signals to the various Component Interface Modules (CIMs). The CIM outputs are directly connected to the actuated component.

The approach for AP1000 PMS is analogous to the manual ESF system level actuation in a conventional Westinghouse plant. In a conventional Westinghouse plant, the manual ESF system-level actuation is initiated by the operator from the MCR via dedicated switches located on the Main Control Board. The signal from each switch is connected to the Solid State Protection System (SSPS). The signal enters the SSPS downstream of the 2oo4 coincidence logic and block control, and upstream of the Master Relay. The Master Relays within the SSPS latch the system-level actuations. The output contacts of the Master Relays perform the fan-out of the system-level actuations to the individual component-level Slave Relays. Comparing

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

AP1000 PMS to a conventional Westinghouse manual ESF system level actuation scheme, the LCL is equivalent to the SSPS 2oo4 coincidence logic, block control, and the latch function of the Master Relay; the fan-out of the High Speed Links to the ILPs and the fan-out from the ILPs to the CIMs are equivalent to the fan-out function of the Master Relay; and the CIM is equivalent to the Slave Relay interface to the field component.

In summary, the "minimum of equipment" criterion in IEEE-603-1991, Sections 5.6.1 and 6.2.1 involves two areas: (1) minimum signal path from manual switch to actuated component, and (2) minimum amount of actuated equipment. The information above describes how the manual ESF actuation function is implemented in the AP1000 PMS. Compliance with the minimum signal path criterion is achieved because the design involves the minimum signal path for manual actuation of ESF functions from the MCR. If the manual ESF system level command from the MCR enters the ILP downstream of the LCL, then it would have to be hardwired to every ILP chassis in each division (2 to 8 ILP chassis). This approach would result in undue wiring complexity and cable separation issues.

Compliance with the minimum amount of actuated equipment is achieved because only the fluid system components (valves, breakers, etc) necessary to achieve the desired ESF result are actuated. No additional ESF components are actuated.

The AP1000 PMS combines the manual system actuations with the automatic system actuations in a manner analogous to that used in the operating fleet.

Question (Revision 1):

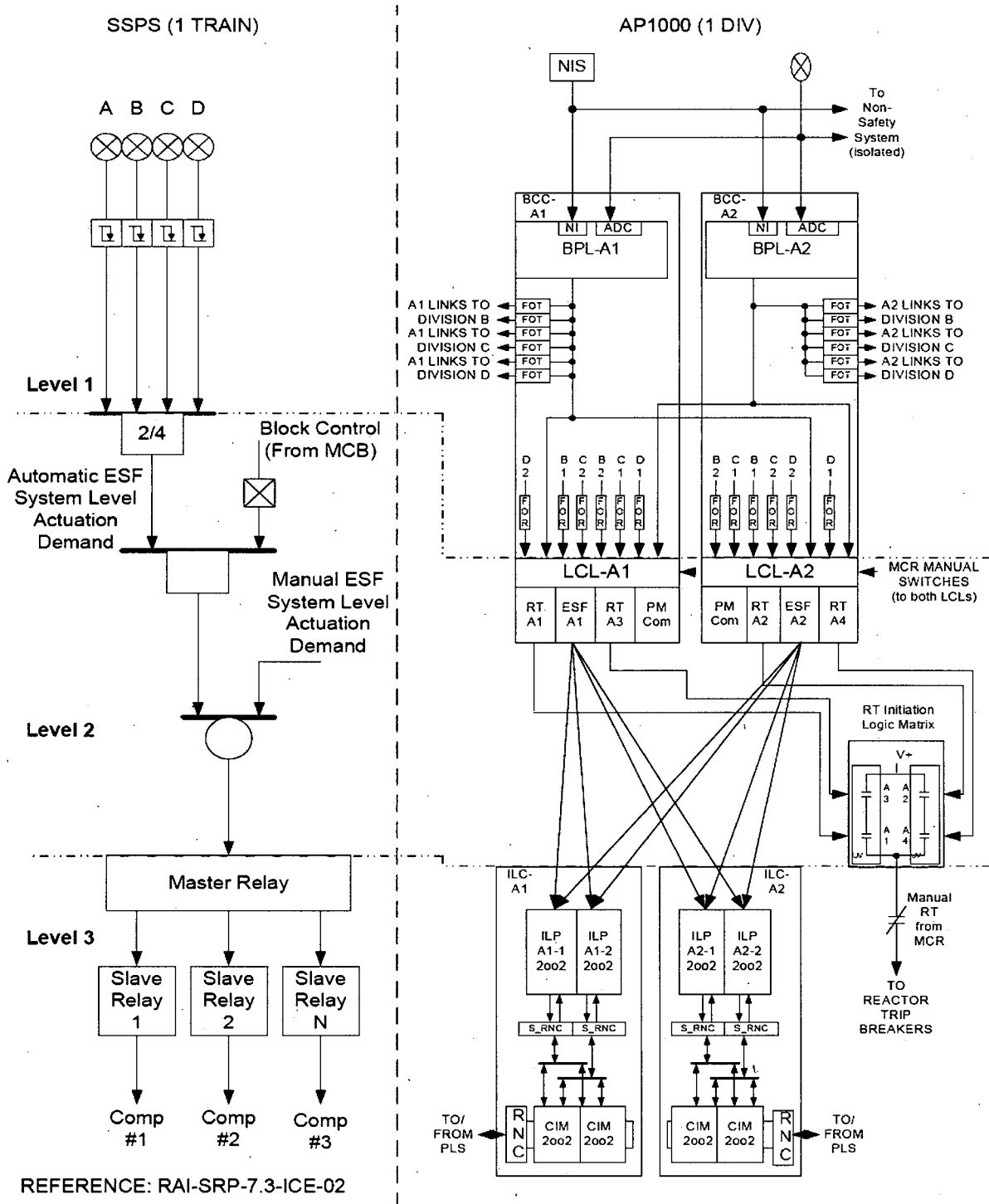
NRC requested additional information to depict the correlation between the conventional solid state protection system (SSPS) and the protection and safety monitoring system (PMS).

Westinghouse Response (Revision 1):

Added attached sketch depicting the ESF actuation path and the correlation between a conventional SSPS system and the PMS. The attached sketch depicts the correlation, showing the Level 1, 2, and 3 functionality.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Question from Terry Jackson e-mail dated December 29, 2008 (Revision 2):

In WES proposed I&C architecture, the only part of the automatic protection system line of operation they are not using is the bistable processor logic. The local coincidence logic, integrated logic processor, and component interface module are digital components in the automatic protection line of operation that are common to the proposed system-level manual ESF actuation line of operation. The staff does not find this approach acceptable. We do find their manual reactor trip proposal acceptable because it is a hardwired actuation from the operator to the reactor trip breaker. For WES to have an acceptable design, they would need a system-level ESF manual actuation that bypasses the digital components of the automatic protection system line of operation. They may be able to use the action-sequencing functions and interlocks of the automatic protection system if such functions and interlocks are not susceptible to a software-common cause failure.

Westinghouse Response (Revision 2):

AP1000 meets the requirements of IEEE Standard 603-1991. The single-failure requirement is met through the use of divisional redundancy.

In addition to the single-failure criterion, Paragraph 6.2.1 in IEEE 603-1991 requires manual means to actuate, at the division level, the automatically-initiated protective actions. The manual means "shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment..." The requirement for "minimum of equipment" does not specify whether or not the equipment can be common to the automatic initiation.

Regulatory Guide 1.62 (October 1973) states that "the amount of equipment common to both manual and automatic initiation should be kept to a minimum."

For AP1000, manual engineered safeguard feature (ESF) system actuation is accomplished through dedicated manual actuation switches in the control room. These switches are processed by high quality, Class 1E software. Manual actuation logic includes permissives, resets, and sequencing logic that are a function of the plant conditions as shown in Figure 7.2-1 in the Design Control Document (DCD). The implementation of the manual actuation depends on a relatively small number of digital components. If no digital circuitry was included in the manual actuation circuitry, there would be a significant amount of additional circuitry, relays, timers, and wiring, thus, utilizing more than a "minimum of equipment."

ESF component actuation is accomplished from the following sources:

- Automatic system-level actuation by the safety system
- Manual system-level actuation from the main control room
- Manual component-level actuation from the main control room
- Manual system-level actuation from the remote shutdown room
- Manual component-level actuation from the remote shutdown room

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

- Automatic system-level actuation from the diverse actuation system (DAS)
- Manual system-level actuation from the DAS

These sources need to be combined with a method for prioritization and the DAS actuation is required to be diverse. If signals from all of these sources were combined at the final actuation device, and if no digital circuitry was included, there would be a significant amount of additional circuitry needed for each component, further exceeding the “minimum of equipment” requirement.

The AP1000 design minimizes the use of common equipment by using common digital circuits in Level 2 local coincidence logic (LCL) and Level 3 integrated logic processor (ILP) and component interface module (CIM) to arbitrate the prioritization (permissives, blocks, resets, etc.) and actuation of ESF components from the sources identified above.

Implementation of this functionality at the component-level (below Level 3) would require hundreds of individual component control switches, latching relays, fan-out relays, prioritization relays, timers, discrete circuits, and wiring. Implementation of this functionality at Level 3 would also require fan-out relays, prioritization relays, timers, discrete circuits, and wiring. The use of relays instead of digital circuits would be very complicated and difficult to maintain. Periodic testing of relays is costly, difficult, and contributes to the potential for human error.

Many of the manual controls must interact with signals generated within the PMS. Some of the manual actuations are interlocked with signals generated automatically within the Level 1 BPL logic (e.g., Manual Stage 4 ADS actuation that is interlocked with either the 3rd stage ADS actuation signal or low RCS wide range pressure signals – see DCD Figure 7.2-1, Sheet 15 of 20).

Implementation of this functionality at Level 2 provides a much simpler design. Digital circuits have higher reliability than relays. For the AP1000 design, the functions performed in the LCL and ILP are redundant within each division. The internal redundancy is provided in the design to facilitate the following:

- Continuous monitoring of processor performance
- Use of signal quality assignments
- Online testability with half of a division in test while the other half remains operational
- Self-revealing diagnostics
- Reduces the potential for LCO because the minimum number of operable channels can be maintained under many failure scenarios

In AP1000, the ESF system-level actuation enters the process at the same point as in a conventional Westinghouse plant (i.e., where the prioritization logic is performed). The correlation between AP1000 and a conventional plant is provided in the diagram provided in the Revision 1 response to this RAI.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Regulatory Guide 1.62 further states that "action-sequencing functions and interlocks... associated with the final actuation devices and actuated equipment may be common if individual manual initiation at the component or channel level is provided in the control room." The Regulatory Guide does not specify that the manual initiation at the component-level is required to be safety grade.

In AP1000, component-level actuation in the control room is accomplished via soft control for each component. Safety component control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary
- Component actuation could cause an over pressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed

Component control of the other safety components is accomplished through non-safety controls.

To address the software common cause failure concern identified in the NRC e-mail from Terry Jackson dated December 29, 2008, Westinghouse provides the following:

The 1998 revision of IEEE Standard 603 added Paragraph 5.16 to address software common-mode failures. This paragraph allows the use of manual actuation and non-safety related systems, components, or both as a means to accomplish the function that would otherwise be defeated by a software common cause failure. IEEE Standard 603 (1998) points to IEEE Standard 7-4.3.2 to determine if diversity is necessary.

Branch Technical Position (BTP) 7-19 provides guidance for diversity that applies to AP1000 at the plant level. The AP1000 DAS provides a combination of automatic and manual controls to address software common cause failures in accordance with BTP 7-19.

The AP1000 DAS provides manual initiation of reactor trip and selected functions. The manual actuation function of the DAS is implemented by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the PMS path and the DAS automatic logic. These DAS manual actuation circuits are a non-safety equivalent to the hard-wired manual reactor trip circuitry and meet the requirements of IEEE 603-1998 Paragraph 5.16 and BTP 7-19 described in the previous two paragraphs.

Based on these points, AP1000 meets IEEE 603 and is a good, reliable, sound design based on the technology available today.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

None