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: 724-940-8505
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP_NRC_002772

February 11, 2010

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-SRP7.8-DAS-01
RAI-SRP7.8-DAS-03
RAI-SRP7.8-DAS-04

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

DD63
NRO

cc:	D. Jaffe	-	U.S. NRC	1E
	E. McKenna	-	U.S. NRC	1E
	S. Mitra	-	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-SRP7.8-DAS-01
Revision: 0

Question:

(Formerly Action Item 1 of ML090090187)

Clarify the design descriptions for the diverse actuation system (DAS) circuitry and the anticipated transient without scram (ATWS) mitigation systems actuation circuitry (AMSAC).

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components to be sufficient to permit understanding of the systems designs. Section 15.8 of the AP1000 FSAR-DCD, Revision 17, states that the DAS provides AMSAC functions. It also states that that for Westinghouse plants, the ATWS rule (10 CFR 50.62) requires the installation of ATWS mitigation systems actuation circuitry (AMSAC), which consists of circuitry separate from the reactor protection system, to trip the turbine and initiate decay heat removal. The staff's could not identify a description of the AMSAC circuitry or the relation between the DAS system and the AMSAC system in Section 7.7 of the AP1000 FSAR-DCD, Revision 17. It is not clear to the staff from the design descriptions if the DAS system circuitry and the AMSAC system circuitry are the same system or if they are separate systems. The staff could not identify design figures within the FSAR that would show the relationship between the DAS circuitry and the AMSAC circuitry. The DAS system is credited with providing a diverse backup to the safety-related protection system; however, the AMSAC system has not been credited with providing diverse protection upon a postulated common-cause-failure (CCF) of the safety-related protection system.

Westinghouse Response:
For Westinghouse plants, the ATWS rule (10 CFR 50.62) requires the installation of equipment that is diverse from the reactor protection system to automatically trip the turbine and initiate decay heat removal. This equipment must be designed to perform its function in a reliable manner and be independent from sensor output to final actuation device from the existing reactor protection system.

The AP1000 is equipped with a diverse actuation system, which provides the functions required by the ATWS rule (10 CFR 50.62). The ATWS core damage frequency for the AP1000 is well below the SECY-83-293 goal of 10^{-5} per reactor year. The AP1000 ATWS core damage frequency is discussed in Chapter 33 of the Probabilistic Risk Assessment (PRA). The AP1000 design meets the ATWS rule (10 CFR 50.62) and its ATWS core damage frequency safety goal basis.

The DCD will be revised as described in this response to provide clarity

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

DCD Tier 2, Chapter 15

15.8 Anticipated Transients Without Scram

15.8.1 General Background

An anticipated transient without scram (ATWS) is an anticipated operational occurrence during which an automatic reactor scram is required but fails to occur due to a common mode fault in the reactor protection system. Under certain circumstances, failure to execute a required scram during an anticipated operational occurrence could transform a relatively minor transient into a more severe accident. ATWS events are not considered to be in the design basis for Westinghouse plants.

15.8.2 Anticipated Transients Without Scram in the AP1000

For Westinghouse plants, the ATWS rule (10 CFR 50.62) requires the installation of ~~ATWS mitigation systems actuation circuitry (AMSAC), which consists of circuitry separate from the reactor protection system, to trip the turbine and initiate decay heat removal~~ equipment that is diverse from the reactor protection system to automatically trip the turbine and initiate decay heat removal. This equipment must be designed to perform its function in a reliable manner and be independent from sensor output to final actuation device from the existing reactor protection system.

The basis for the ATWS rule requirements, as outlined in SECY-83-293 (Reference 1), is to reduce the risk of core damage because of ATWS to less than 10^{-5} per reactor year.

The AP1000 includes a diverse actuation system, which provides the ~~AMSAC~~ protection features mandated for Westinghouse plants by 10 CFR 50.62, plus a diverse reactor scram (see Section 7.7). Thus, the ATWS rule is met.

15.8.3 Conclusion

The AP1000 is equipped with a diverse actuation system, which provides the functions ~~of AMSAC~~ required by the ATWS rule (10 CFR 50.62). The ATWS core damage frequency for the AP1000 is well below the SECY-83-293 goal of 10^{-5} per reactor year. The AP1000 ATWS core damage frequency is discussed in Chapter 33 of the Probabilistic Risk Assessment (PRA). The AP1000 design meets the ATWS rule (10 CFR 50.62) and its ATWS core damage frequency safety goal basis.

PRA Revision:

None

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-03
Revision: 0

Question:

(formerly Action Items 3a, 3b and 3c of ML090090187)

Describe how the DAS actuation logic, 2 out of 2 (2oo2), will meet the applicable regulatory criterion.

10CFR part 50, Appendix A, General Design Criteria (GDC) 10, "Reactor design," requires, among other things, that the control, and protection systems shall be designed with appropriate margin to assure that specified fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences." The guidance of BTP 7-19, Point 3 of the Four Point position on D3 states that the diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. The guidance of Revision 2, Digital Instrumentation and Controls, Task Working Group #2: Diversity and Defense-in-Depth Issues (DI&C-ISG-02), Section 4, states that "...spurious trips and actuations are of a lesser safety concern than failures to trip or actuate." It states in Revision 17, FSAR-DCD, Section 16.3-2, that "[w]hen a required channel is unavailable the automatic DAS function is unavailable." The staff could not identify design descriptions that would demonstrate how the 2oo2 DAS actuation logic would meet the applicable regulatory criterion.

Westinghouse Response:

Action Items 3a, 3b, and 3c of ML090090187 were discussed with the NRC Staff during an October 13th 2009 conference call. There are two actuation logic modes, automatic and manual. The automatic actuation logic mode functions to logically combine the automatic signals from the two redundant automatic subsystems in a two-out-of-two basis. The combined signal operates a power switch with an output drive capability that is compatible, in voltage and current capacity, with the requirements of the final actuation devices. The two-out-of-two logic is implemented by connecting the outputs in series. The manual actuation mode operates in parallel to independently actuate the final devices. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual, two out of two redundancy reduces the probability of inadvertent actuation. The details of how the DAS actuation logic of 2 out of 2 meets applicable regulatory requirements is addressed in WCAP-17184, Revision 0 "AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report" submitted via DCP_NRC_002727 dated December 30th, 2009. The WCAP also identifies the DAS architecture and associated licensing basis at the functional design level, and addresses a number of the open items of the Chapter 7 Safety Evaluation Report with Open Items

(Reference: ML092800266), including PSAI 6.1 1 and Section 7.8.1.1 "Diverse Backup Protection System Assessment".

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-SRP7.8-DAS-04
Revision: 0

Question:

(formerly Action Items 4 and 5 of ML090090187)

Describe in detail how DAS equipment (i.e., hardware, software) will be diverse from the safety-related Protection and Safety Monitoring System (PMS).

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22, "Protection System Independence," requires, among other things, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" provide diversity analysis methods to demonstrate that adequate and sufficient diversity are included within the design. The staff could not identify design descriptions that demonstrate adequate and sufficient diversity for the DAS system, in accordance with the guidance listed.

Westinghouse Response:
Under cover of letter DCP_NRC_002683, Westinghouse submitted on the docket, document APP-GW-J1R-004 (WCAP-15775), Rev 3 "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report". This document was discussed during the December 2008 DAS Meeting with the Staff and was submitted to address Action Item #4 and #5 of ML090090l87.

Diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithm, or using different actuation means to provide different ways of responding to postulated plant conditions. NUG/CR-6303 segregates the types of diversity into six different areas: human, design, software, functional, signal, and equipment. NUG/CR-6303 defines echelons of defense as: "...specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the engineered safety features (ESP) actuation system, and the monitoring and indicator system". The submitted report describes the type of diversity that exists among the four echelons of defense for AP1000 and identifies dependencies among the echelons.

Design Control Document (DCD) Revision:
None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

PRA Revision:
None

Technical Report (TR) Revision:
None