APP-GW-GLR-018
Revision 0

June 2006

AP1000 Standard Combined License Technical Report

Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System

Revision 0

Westinghouse Electric Company LLC
Nuclear Power Plants
Post Office Box 355
Pittsburgh, PA 15230-0355

INTRODUCTION:

This technical report addresses AP1000 Design Control Document (Reference 1) Combined Operating License (COL) Information Item 7.2-1 and NRC FSER (Reference 2) Combined License Action Items 7.2.3-2 and 7.2.6-1 on Failure Modes and Effects Analysis (FMEA) for the AP1000 protection system. WCAP-16438-P (Reference 3) and WCAP-16592-P (Reference 4) provide information to close this COL Information Item.

> *DCD Paragraph 7.2.3, Combined License Information:*
> Combined License applicants referencing the AP1000 certified design will provide an FMEA for the protection and safety monitoring system. The FMEA will include a Software Hazards Analysis. This FMEA will provide the basis for those Technical Specification Completion Times that rely on an FMEA for their basis."

Based on this report, including WCAP-16438-P and WCAP-16592-P, the NRC should consider the COL Information Item closure to be acceptable and generically applicable to COL applications referencing the AP1000 design certification.

TECHNICAL BACKGROUND:

The FMEA was performed using the approach previously accepted by the NRC for AP600 in DCD (Reference 5) Section 7.2.2.1 and documented in WCAP-13594 (Reference 6).

WCAP-16438-P (Reference 3) provides the results of an FMEA of the AP1000 Protection and Safety Monitoring System. WCAP-16592-P (Reference 4) provides the results of a software hazards analysis of the AP1000 Protection and Safety Monitoring System (PMS).

WCAP-16438-P reached the following conclusions:

a. Due to the high degree of redundancy within the reactor trip interface, a single failure of the electronics does not prevent a division from responding to a valid actuation signal for reactor trip.
b. Single failures may prevent the actuation of an individual ESF component, or may lead to its spurious actuation; however, plant safety is retained through the redundancy of redundant ESF components actuated from other divisions.
c. Failures affecting protective functions are detectable by either diagnostics or planned periodic surveillance tests.
d. Several failures have been identified that depend on the periodic surveillance test for their detection. The design of the test facilities and sequence and the interval at which the testing is performed, take these failures into account.

The software hazards analysis described in WCAP-16592-P demonstrates that the PMS software continues to provide a low probability of creating hazards even when it fails. It also shows that a single failure in the plant will not create software hazards. The PMS design is capable of performing its protective functions with high reliability.

There are no changes to the AP1000 design or design functions required to support generic application of WCAP-16438-P or WCAP-16592-P.

REGULATORY IMPACT:

The AP1000 FSER (Reference 2) in Subsection 7.2.6 discusses the need for an FMEA. Using WCAP-16438-P and WCAP-16592-P for generic closure of COL Information Item 7.2-1 does not alter the conclusions in FSER Subsection 7.2.6.

This report does not include any change to:

- a System, Structure, or Component (SSC)
- a procedure
- a DCD-described evaluation methodology
- a test or experiment not described in the DCD where an SSC is utilized or controlled in a manner that is outside the reference bounds of the design for that SSC or is inconsistent with analyses or descriptions in the DCD

As a result, the changes to the DCD presented in this report do not represent an adverse change to the design function or to how design functions are performed or controlled. The changes to the DCD do not involve revising or replacing a DCD-described evaluation methodology nor involve a test or experiment not described in the DCD. The DCD change does not require a license amendment per the criteria of VIII. B. 5.b. of Appendix D to 10 CFR Part 52.

SEVERE ACCIDENT CHANGE CRITERIA

The DCD change does not affect resolution of a severe accident issue and does not require a license amendment based on the criteria of VIII. B. 5.c of Appendix D to 10 CFR Part 52. Mitigation features are not impacted.

SECURITY

The subject changes will not alter barriers or alarms that control access to protected areas of the plant, and will not alter requirements for security personnel. Therefore, the proposed change does not have an adverse impact on the security assessment of the AP1000.

REFERENCES:

1. APP-GW-GL-700, AP1000 Design Control Document, Revision 15.
2. NUREG-1793, Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design, September 2004.
3. WCAP-16438-P, "FMEA of AP1000 Protection and Safety Monitoring System", Revision 1, June 2006.
4. WCAP-16592-P, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System", Revision 0, June 2006.
5. GW-GL-700, AP600 Design Control Document, Revision 4.
6. WCAP-13594(P), WCAP-13662 (NP), "FMEA of Advanced Passive Plant Protection System," Revision 1, June 1998.

DCD MARK-UP

The following DCD markups identify how COL application FSARs should be prepared to incorporate the subject change.

Revise Table 1.6-1 as follows:

Table 1.6-1 (Sheet 11 of 20)

MATERIAL REFERENCED

DCD Section Number	Westinghouse Topical Report Number	Title
6.3	~~WCAP-13594 (P)~~WCAP-16438-P ~~WCAP-13662~~WCAP-16438-NP	FMEA of AP1000 Protection and Safety Monitoring System, Revision 1, June 2006~~FMEA of Advanced Passive Plant Protection System, Revision 1, June 1998~~
7.2	~~WCAP-13594 (P)~~WCAP-16438-P ~~WCAP-13662~~WCAP-16438-NP	FMEA of AP1000 Protection and Safety Monitoring System, Revision 1, June 2006~~FMEA of Advanced Passive Plant Protection System, Revision 1, June 1998~~
	WCAP-16592-P WCAP-16592-NP	Software Hazards Analysis of AP1000 Protection and Safety Monitoring System, Revision 0, June 2006

Revise subsection 6.3.9 as follows:

6.3.9 References

1. WCAP-8966, "Evaluation of Mispositioned ECCS Valves," September 1977.
2. WCAP-16438-P, WCAP-16438-NP, "FMEA of AP1000 Protection and Safety Monitoring System", Revision 1, June 2006~~WCAP-13594 (P), WCAP-13662 (NP), "FMEA of Advanced Passive Plant Protection System," Revision 1, June 1998~~.

Revise subsection 7.2.2.1 as follows:

7.2.2.1 Failure Modes and Effects Analysis (FMEA)

~~The AP1000 protection system is similar to the AP600 protection system.~~ A failure modes and effects analysis was performed on the ~~AP600~~ AP1000 protection and safety monitoring system. Through the process of examining the feasible failure modes, it was concluded that the ~~AP600~~ AP1000 protection system maintains safety functions during single point failures. The ~~AP600~~ AP1000 failure modes and effects analysis is documented in Reference 1. The Common Q failure modes and effects analysis is documented in Reference 3 and also concludes that the protection system maintains safety functions during single point failures.

Revise subsection 7.2.3 as follows:

7.2.3 Combined License Information

Complete. ~~Combined License applicants referencing the AP1000 certified design will provide a~~An FMEA ~~for the protection and safety monitoring system. The FMEA will include~~and a Software Hazards Analysis for the protection and safety monitoring system have been performed. See References 1 and 4 for details. This FMEA ~~will~~ provides the basis for those Technical Specification Completion Times that rely on an FMEA for their basis.

Revise subsection 7.2.4 as follows:

7.2.4 References

1. WCAP-16438-P, WCAP-16438-NP, "FMEA of AP1000 Protection and Safety Monitoring System", Revision 1, June 2006~~WCAP-13594(P), WCAP-13662 (NP), "FMEA of Advanced Passive Plant Protection System," Revision 1, June 1998~~.
2. WCAP-15776, "Safety Criteria for the AP1000 Instrument and Control Systems," April 2002.
3. CENPD-396-P, Appendix 3, Rev. 1, "Common Qualified Platform, Digital Plant Protection System," May 2000.
4. WCAP-16592-P, WCAP-16592-NP, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System", Revision 0, June 2006.

Revise subsection 7.3.2.1 as follows:

7.3.2.1 Failure Modes and Effects Analyses

The ~~AP600~~ AP1000 failure modes and effects analysis (Reference 1 of Section 7.2) examines failures of the protection and safety monitoring system. ~~The AP1000 instrumentation and control systems are similar to the AP600. The Common Q failure modes and effects analysis is documented in Reference 3 of Section 7.2. Both of these analyses~~This analysis concludes that the protection system maintains safety functions during single point failures.