WESTINGHOUSE AP600 ADVANCED NUCLEAR PLANT DESIGN

W. GANGLOFF
Westinghouse Energy Systems,
Pittsburgh, Pennsylvania,
United States of America

XA0053563

Abstract

As part of the cooperative U.S. Department of Energy (DOE) Advanced Light Water Reactor (ALWR) Program and the Electric Power Research Institute (EPRI), the Westinghouse AP600 team has developed a simplified, safe, and economic 600-megawatt plant to enter into a new era of nuclear power generation. Designed to satisfy the standards set by DOE and defined in the ALWR Utility Requirements Document (URD), the Westinghouse AP600 is an elegant combination of innovative safety systems that rely on dependable natural forces and proven technologies. The Westinghouse AP600 design simplifies plant systems and significant operation, inspections, maintenance, and quality assurance requirements by greatly reducing the amount of valves, pumps, piping, HVAC ducting, and other complex components. The AP600 safety systems are predominantly passive, depending on the reliable natural forces of gravity, circulation, convection, evaporation, and condensation, instead of AC power supplies and motor-driven components. The AP600 provides a high degree of public safety and licensing certainty. It draws upon 40 years of experience in light water reactor components and technology, so no demonstration plant is required. During the AP600 design program, a comprehensive test program was carried out to verify plant components, passive safety systems components, and containment behavior. When the test program was completed at the end of 1994, the AP600 became the most thoroughly tested advanced reactor design ever reviewed by the U.S. Nuclear Regulatory Commission (NRC). The test *results confirmed the exceptional behavior of the passive systems and have been instrumental in facilitating code* validations. Westinghouse received Final Design Approval from the NRC in September 1998.

1. INTRODUCTION

The Westinghouse AP600 reactor has been designed as part of the Advanced Light Water Reactor (ALWR) Program sponsored by the U.S. DOE and EPRI. The AP600 has been reviewed by the U.S. NRC and received Final Design Approval in 1998. It is scheduled to receive NRC certification in 1999. A detailed design program (FOAKE-First-of-a-Kind-Engineering) is proceeding in parallel with the NRC certification under the sponsorship of DOE, the Advanced Reactor Corporation (ARC), and EPRI.

The AP600 is a 600 MWe reactor which utilizes passive safety features that, once actuated, depend only on natural forces such as gravity and natural circulation to perform all required safety functions. These passive safety systems result in increased plant safety and can also significantly simplify plant systems, equipment, and operation.

2. DESIGN OBJECTIVES

The primary design objective of the AP600 plant was to provide a greatly simplified plant design that meets the NRC regulatory requirements, meets or exceeds the NRC safety goals and ALWR Utility Requirements and addresses past safety issues while being economically competitive with other power generation systems over the full operating cycle. The objective is to be met using experience-based components so that plant prototype or demonstration models are not required. Simplification of plant systems, combined with increased plant operating margins, reduces the actions required by the operator in the event of an accident. As a result, the AP600 design requires no operator actions following a design basis accident to maintain a safe configuration. The design target for the AP600 is to technically support elimination of the emergency planning zone beyond the site boundary. The simpler systems, combined with the licensing reforms of 10CFR52, increase the licensing certainty of the AP600.

Implementation of the passive safety features greatly reduces the operation, maintenance and testing requirements of the AP600. The AP600 has been designed to have a shorter construction schedule through the use of modular construction techniques that are similar to those applied in ship construction. The construction design objective is a 36-month schedule from first concrete pour to the fuel load. An added benefit of this approach is that a significant portion of the quality assurance inspections can be completed in the factory before the modules are delivered to the construction site.

3. PASSIVE SAFETY FEATURES

The AP600 uses passive safety systems to enhance the safety of the plant and to satisfy NRC safety criteria. The systems use only natural forces, such as gravity, natural circulation, and compressed gas to make the system work. No pumps, fans, diesels, chillers, or other rotating machinery are used. A few simple valves are used to align the passive safety systems when they are automatically actuated. In most cases these valves are "fail safe" (i.e., they require power to stay in their normal, closed position; loss of that power causes them to open to their safety alignment. This power is normally supplied by class 1E uninterruptible power supplies). The passive safety systems are significantly simpler than typical PWR safety systems.

In addition to being simpler, the passive safety systems do not require the large network of safety support systems needed in typical nuclear plants, such as AC power, HVAC, and cooling water systems and seismic buildings to house these components. This simplification includes eliminating the safety-grade emergency diesel generators and their network of support systems, air start, fuel storage tanks and transfer pumps, and the air intake/exhaust system. As a result, the support systems no longer need to be safety grade and can be simplified or eliminated.

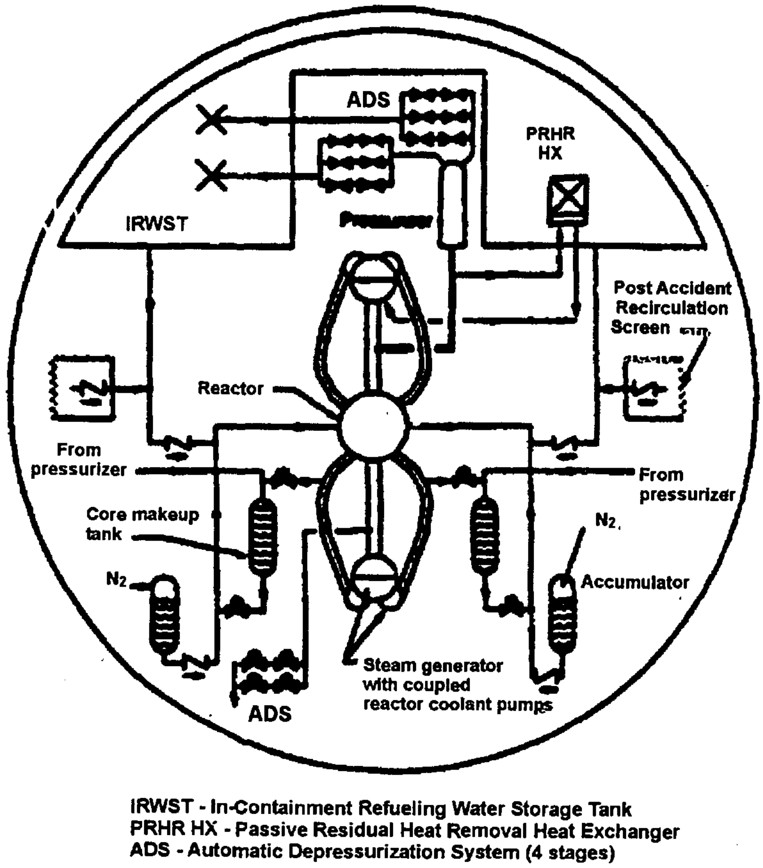

FIG. 1. Schematic Representation of the In-Containment Passive Safety Injection System

The features of the AP600 passive safety systems include passive safety injection, passive residual heat removal, and passive containment cooling. All these passive systems have been designed to meet the NRC single-failure criteria and its recent criteria including TMI lessons learned and unresolved and generic safety issues. PRAs have also been used to quantify the safety of the design.

3.1. Passive safety injection system

The passive safety injection system (PSIS), Figure 1, performs three major functions: residual heat removal, reactor coolant makeup for inventory control, and safety injection. Computer analyses demonstrate that the PSIS provides effective core cooling for various break sizes and locations. These calculations show that the PSIS prevents core damage for breaks as large as the 0.2m (8 inch) vessel injection lines and provides about 260°C (500°F) margin to the maximum peak clad temperature limit for the double-ended rupture of a main reactor coolant pipe.

The passive residual heat removal heat exchanger (PRHR HX) protects the plant against transients that upset the normal steam generator feedwater and steam systems. The analysis results, using NRC-approved codes, has shown the PRHR HX to satisfy the NRC safety criteria for loss of feedwater, feedwater line breaks, and steam line breaks with a single failure. Anticipated transients without reactor trip have also been analyzed and shown to result in peak RCS pressures of about 20 MPa (2900 psig), well within NRC criteria. The PRHR HX consists of a 100 percent capacity bank of tubes connected to the RCS in a natural circulation loop. The loop is normally isolated from the RCS by valves that are normally closed, but fail open if power is lost. The heat exchanger tubes are located in the in-containment refueling water storage tank (IRWST). This location places the PRHR HX above the RCS loop so that hot water leaving the RCS hot leg will rise to the top of the PRHR HX where it is cooled. The difference in temperature between the hot inlet water and the cold outlet water drives the natural circulation loop. If the reactor coolant pumps are running, they boost the PRHR HX flow.

The IRWST provides the heat sink for the PRHR HX. The IRWST water volume is sufficient to absorb decay heat for about 2 hours before the water would start to boil. After that, steam would be generated and enter the containment. This steam would condense on the steel containment vessel and then drain back into the IRWST.

The PSIS uses three sources of water to maintain core cooling, including core makeup tanks (CMTs), accumulators and the IRWST. All of these injection sources are connected directly to two nozzles on the reactor vessel. These connections, which have been used on existing two-loop plants, reduce the possibility of spilling part of the injection flow.

Passive reactor coolant makeup is provided to accommodate small leaks following transients or whenever the normal makeup system is unavailable. Two CMTs, filled with borated water, are designed to provide this function at any RCS pressure using only gravity as a motivating force. These tanks are designed for full RCS pressure and are located above the RCS loop piping. If the water level in the pressurizer reaches a low-low level, the reactor is tripped, the reactor coolant pumps are tripped, and the CMT discharge isolation valves open automatically.

The relative elevations of the CMTs and the pressurizer are such that if RCS level continued to decrease, the water in the CMTs would drain into the reactor vessel.

As with current pressurized water reactors (PWRs), high pressure accumulators are required for large loss-of-coolant accidents (LOCAs) to meet the need for higher initial makeup flows to refill the reactor vessel lower plenum and downcomer following RCS blowdown. The gas pressure forces open check valves that normally isolate the accumulators from the RCS. The accumulators are sized to respond to the complete severance of the largest RCS pipe by rapidly refilling the vessel downcomer and lower plenum. The accumulators continue delivery to assist the CMTs in rapidly reflooding the core.

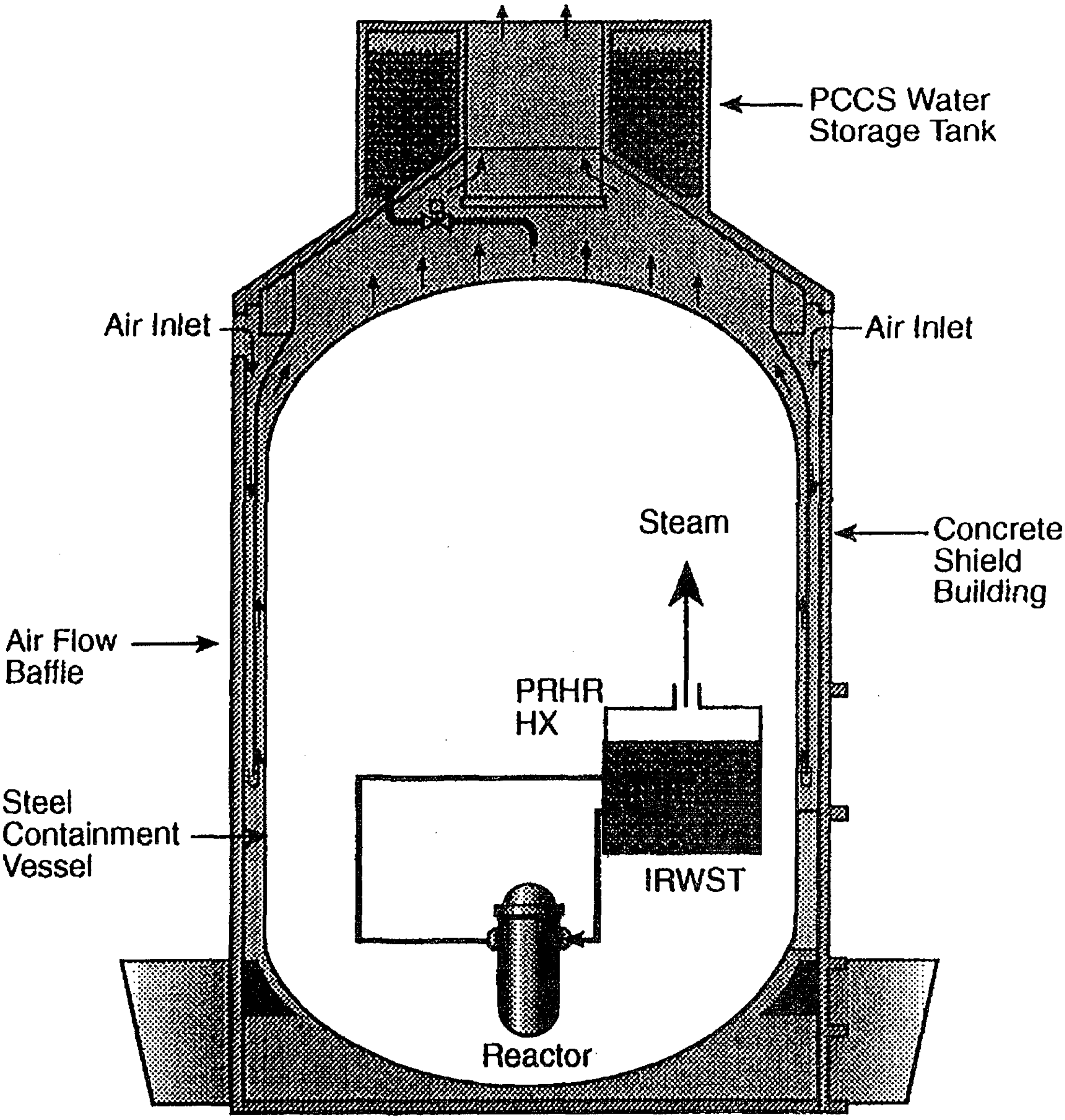

FIG. 2. AP600 Plant Heat Sink

Long-term injection water is provided by gravity from the IRWST, which is located in the containment just above the RCS loops. Normally, the IRWST is isolated from the RCS by self-actuating check valves. This tank is designed for atmospheric pressure. As a result, the RCS must be depressurized before injection can occur. The AP600 automatically controls depressurization of the RCS to reduce its pressure to about 6.89 x 10^4 Pa (10 psig), at which point the head of water in the IRWST is sufficient to overcome the small RCS pressure and the pressure loss in the injection lines. The automatic depressurization system (ADS) is made up of four stages of valves to permit a relatively slow, controlled RCS pressure reduction. The first three stages are connected to the pressurizer and discharge through spargers into the IRWST. The fourth stage is connected to a hot leg and discharges through redundant isolation valves to the containment. The ADS stages are actuated by CMT level.

3.2. Passive containment cooling system

The passive containment cooling system (PCCS) provides the safety-related ultimate heat sink for the plant, as shown in Figure 2. As demonstrated in the computer analysis and tests, the PCCS is able to effectively cool the containment following an accident such that the design pressure is not

TABLE I. AP600 PRA RESULTS

Event	AP600	Current Plants
Transients	5.0E-9	1.3E-5
Loop/Blackout	1.0E-9	6.6E-6
SG Tube Rupture	6.1E-9	1.7E-6
LOCA - Small	1.0E-8	8.0E-6
LOCA - Medium	7.6E-8	5.0E-6
LOCA - Large	5.0E-8	8.0E-7
ATWT	1.0E-8	2.2E-6
Loss of Cooling	<E-9	1.1E-5
Interfacing LOCA	<E-9	1.0E-6
Vessel Rupture	1.0E-8	3.0E-7
Total - Safety and Nonsafety Systems	1.7E-7/Yr	5.0E-5/Yr
Safety Systems Only	7.7E-6/Yr	

exceeded and the pressure is rapidly reduced. The steel containment vessel itself provides the heat transfer surface that removes heat from inside the containment and rejects it to the atmosphere. Heat is removed from the containment vessel by a natural circulation flow of air that cannot be isolated. During an accident, the air cooling is supplemented by water evaporation on the outside of the containment shell. The water is drained by gravity from a tank located on top of the containment shield building. Two normally closed, fail-open valves are opened to initiate the water drain. The water tank is sized for three days of operation, after which time the tank is expected to be refilled to maintain the low containment pressure achieved after the accident. If the water is not resupplied after three days, the containment pressure will increase, but the peak is calculated to reach only 90 percent of design pressure after about two weeks.

3.3. Severe accident considerations

PRA has been an integral part of the AP600 design process. The AP600 PRA report was a joint effort between Westinghouse and Ente Nazionale per l'Energia Elettrica of Italy. Numerous design changes were made as a result of examination of the PRA results, for example, the diversity in the fourth stage ADS valves, logic in the startup feedwater system and active valves in parallel with several of the key check valves. The resulting core damage frequency for the AP600 is 1.7 E-7/yr. This compares well to the NRC safety goal of 1.0 E-4/yr and the ALWR goal of 1.0 E-5/yr. Typical numbers for current plant designs are 5.0 E-5/yr.

The PRA also illustrates that the AP600 containment design is robust in its ability to prevent releases following a severe accident and that the risk to the public due to severe accidents for AP600 is very low. The overall release frequency for AP600 is 1.8E-8/yr. This meets the NRC safety goal and the ALWR goal of 1.0E-6/yr. Typical numbers of current plant designs are 5E-6/yr.

The PRA analysis shows that the capability to flood the reactor cavity prevents the failure of the reactor vessel given a severe accident without water in the cavity. The vessel and its insulation are designed so that the water in the cavity is able to cool the vessel and prevent it from failing (termed in-vessel retention of molted core debris). Maintaining the vessel integrity eliminates the potential of a large release due to ex-vessel phenomena and its potential to fail the containment.

By reducing the reactor system pressure, the ADS eliminates the possibility of high pressure core melt ejection and the resultant direct containment heating. The AP600 also has an igniter system to mitigate the effects of hydrogen released during a severe accident.

4. TEST PROGRAM

The AP600 is, of course, designed to the last function and flow rate with computers. According to the computer codes, each of the AP600's systems works even better than required. The primary burden of the extensive testing program has been to supply hard data to verify those computer codes.

To perform the testing, some of for the best facilities in the world were selected. Work was performed at Oregon State University; at a thermal-hydraulic test complex and a steam testing facility in Italy; in Ontario, Canada, at the University of Western Ontario; and at two of Westinghouse's technology development centers in Pittsburgh.

The Oregon State work was the "crown jewel" of the testing program. The work was conducted in a new facility. The tests went so well that the work planned for several months was performed in just six weeks, completing the last test on August 3, 1994. The Oregon State testing focused on 30 small-break loss-of-coolant accidents (LOCAs). Using a one-quarter scale model that replicates the AP600, the transition from LOCA events into long-term cooling were simulated, relying on coolant injected from the passive safety systems. The tests validated the codes, proving that the AP600 core will be adequately cooled at all times during all LOCAs.

Other LOCA tests were conducted in Piacenza, Italy, at the SPES-2 facility. These were full-height, full-pressure simulations of both the primary cooling and passive core cooling systems. Thirteen small-break LOCAs were conducted, as well as simulations of ruptures in steam generator tubes and steam lines. Again, the results validated the safety analysis computer codes and models.

In Casaccia, Italy, full-scale, full-flow tests were done on the automatic depressurization system. These tests went through two major phases -- first, 21 steam blowdowns, and second, 24 steam and water blowdowns. And again, the results matched the computer modeling.

In London, Ontario, Canada's University of Western Ontario used its wind tunnel to be sure that winds -- especially high winds -- would not diminish cooling in the annulus of the containment while the natural convection and evaporative forces were doing their job. A detailed scale model of the AP600 was placed in the tunnel. The Ontario tests shows that wind was not a safety factor. The natural circulation of air occurs over the surface of the reactor shield under all wind conditions.

At the Westinghouse Science and Technology Center in Pittsburgh, containment cooling work was performed. First, a flat plate was built ... 0.91 m (3 feet) wide and 1.82 m (6 feet) high ... that met the specifications for the containment. It was used it to examine basic thermodynamics. Water was run across its surface to acquire hard data on the heat transfer to be expected under varying circumstances. The data took us a step forward in the containment code safety analysis.

A much larger test device was built -- a 7.3 m (24-foot) high, 0.91 m (three-foot)-diameter model of the containment. This time, steam was put inside, and air moved over the outside as water ran across the surface. This larger scale, more detailed testing gave us even more data for the computer codes. Then an even larger model was used: a one-eighth scale model of the containment. Again, the entire range of passive safety actions were tested -- using various internal conditions and external air and humidity values. Tests were conducted with water applied to the top of the external surface, and with a dry surface. This exhaustive, real-world testing shows that the theory of passive containment cooling is valid. Even the toughest internal and external conditions -- and combinations of both -- did an adequate job of cooling. While water applied to the top of the vessel helped, it was determined that it was not absolutely needed, even from the first moment of an event. This is a cooling concept that just sits there and does the job perfectly, relying on nature.

At another Westinghouse test facility, a scaled version of the core makeup tank was constructed. It was used to investigate the thermal-hydraulic behavior of the tank under a wide range of conditions. The data from this series of tests was a major source for the refinement of the computer model codes.

Those are just the highlights of the testing. Along the way at these sites, the reactor coolant pumps, check valves and incore instrumentation were tested as well as a wide variety of flow and heat transfer tests. Every aspect of the passive safety system was simulated -- from safety-grade components to the containment cooling and core cooling systems.

The testing was thorough and exhaustive, but the results were well worth the cost and effort. The AP600 is now the most thoroughly tested reactor design ever reviewed by the NRC. The very sophisticated, detailed, conservative computer codes were validated which are used to analyze the AP600. In some cases, the data was used to refine the codes. The data and codes predict safety under a long list of scenarios, both normal and abnormal. The AP600 is safe under all predicted accident conditions. These tests met the very demanding requirements defined at the start by the DOE, the NRC, and the supporting utilities.

5. LICENSING STATUS

One of the most challenging aspects of the testing was the initial agreement on the scope and nature of the tests. All of this work has been monitored very closely by both the DOE and the NRC through a series of milestones. This steady advance in testing has now brought the AP600 to the equally painstaking process of licensing.

In June of 1992, the safety analysis report and probabilistic risk assessment report was submitted to the NRC. The Commission replied with a draft safety evaluation report, listing its questions. Westinghouse responded to them. In some cases, the response created open issues that we have resolved. In May of 1996, the NRC issued a supplement to the Draft Safety Evaluation Report on the AP600 computer codes and testing program. This report identified the final questions the staff had concerning the computer codes and testing program. Westinghouse has responded to the last of these questions.

This highly technical iteration continued through 1997. Westinghouse has now resolved all the issues to the NRC's satisfaction. In May 1998, the NRC's technical staff approved the Final Safety Evaluation Report for the AP600. Final Design Approval (FDA) was received in September 1998, following review by both the Advisory Committee on Reactor Safety (ACRS) and the NRC Commissioners. The FDA documented NRC acceptance of AP600 safety and at this point, the AP600 is a saleable plant on international markets. In the United States, there will be an additional year for a public rule-making, after which the NRC will be able to issue a final design certification. This final design certification is relevant only in the United States and is not needed in other countries.

Westinghouse now has what no other advanced passive plant has: the numbers on performance, on safety, on costs, and on schedule. Westinghouse has told the utility supporters that it can meet their goals.

Financially, the AP600 will do better than the original cost goals established by America's utilities for a 600-megawatt advanced passive plant. A twin-unit site can meet the tougher cents-per-kilowatt-hour goals established for a 1200-megawatt plant. The AP600 can compete with the largest plants now being designed -- whether nuclear or coal.

The AP600 defies assumptions about economies of scale because its initial costs are well down that scale. That is the value of safety through simplicity. It is the value of the 600-megawatt size and three-year timetable for construction. The challenge of financing an AP600 is relatively simple. This is a plant that can be built ... starting now.