



Westinghouse  
Electric Corporation

Energy Systems

Box 355  
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-96-4796  
DCP/NRC0576  
Docket No.: STN-52-003

August 9, 1996

Document Control Desk  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555

ATTENTION: T. R. QUAY

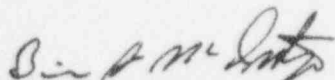
SUBJECT: AP600 PASSIVE SYSTEM RELIABILITY ROADMAP

Dear Mr. Quay:

Enclosed with this letter is a copy of the AP600 Passive System Reliability Roadmap. The roadmap provides an overview of the types of design and design certification activities that contribute to passive system reliability and references the associated documents related to the activity.

During past Westinghouse/NRC Senior Management meetings, the staff has asked questions related to different passive system reliability activities (i.e., how ensure passive system reliability for scenarios such as if a tool is left in piping following test or maintenance activities) and wanted to know where a discussion of the AP600 information could be found. This roadmap is in response to that request.

Please contact Cynthia L. Haag on (412) 374-4277 if you have any questions concerning this transmittal.

  
Brian A. McIntyre, Manager  
Advanced Plant Safety and Licensing

/nja

Enclosure

cc: W. Huffman, NRC (enclosure)  
N. J. Liparulo, Westinghouse (without enclosure)

9608150128 960809  
PDR ADOCK 05200003  
A PDR

1/1  
Eddy

150038

Enclosure to Westinghouse  
Letter NSD-NRC-96-4796  
August 9, 1996

## AP600 PASSIVE SYSTEM RELIABILITY ROADMAP

### Introduction

The AP600 design incorporates passive engineered safety features that perform safety-related functions to mitigate the consequences of design basis accidents and to establish and maintain safe shutdown conditions following an event.

During the design certification process, the United States Nuclear Regulatory Commission (U.S. NRC) has identified concerns related to passive system reliability.

An extensive range of activities have been completed as part of both the AP600 design and design certification processes to provide confidence in the design capabilities and reliability of the safety-related, passive systems and components, and the associated passive processes. Figure 1 provides an overview of the types of design and certification activities that contribute to passive system reliability.

### Purpose

This report provides a summary of the various activities, completed in support of the AP600 design and certification processes, that help to demonstrate the reliability of the various passive systems and components.

This document functions as a roadmap for passive system reliability by providing a concise overview of each activity and the associated reference documents related to the activity. Table 1 provides this roadmap to reference documents for each design activity.

### Scope

The scope of this document includes the following safety-related passive AP600 systems, structures, and components that provide design basis protection and that differ from those safety-related passive systems or components provided in currently licensed Westinghouse pressurized water reactors (PWRs):

- Passive core cooling system
  - Passive residual heat removal (PRHR) heat exchanger heat removal
  - Core makeup tank (CMT) injection
  - In-containment refueling water storage tank (IRWST) injection
  - Containment recirculation
  - Automatic depressurization system (ADS) depressurization
- Passive containment cooling system
  - Containment water drain
  - Containment air circulation
  - Containment heat removal

## Background

Various questions have been raised during the design and design certification processes concerning the design, operation, and analysis of the passive safety-related systems and components. Due to the large number of activities implemented as part of both the design and design certification processes that help to demonstrate the reliability of the passive systems, it was decided to compile a high-level overview of these many activities and provide this roadmap document.

The following broad design and design certification activities contribute to the reliability of the passive safety-related systems:

- Incorporation of operational experience
- Conservative system design and analyses
- Conservative design basis safety (thermal/hydraulic) analyses
- Probabilistic Risk Assessment (PRA) success criteria analyses
- PRA evaluation and sensitivity studies
- Conservative equipment and component design
- AP600 testing program
- Emergency response guidelines thermal/hydraulic analyses
- Design activities for plant operation

The AP600 design and design certification processes have produced highly reliable designs for the safety-related passive systems and components through careful integration of numerous activities. The conceptual design was based on incorporating design features with successful plant operating experience. Development of the passive safety-related system and component designs evolved through multiple iterations of the activities listed above and described in this report.

### **1.0 INCORPORATION OF OPERATING EXPERIENCE**

Implementation of proven design features and incorporation of lessons learned from operational experience are important initial steps in ensuring the reliability of the AP600 safety-related, passive systems. The various safety-related passive systems, structures, and components incorporate design applications and approaches that have been successfully implemented both in currently licensed commercial PWRs and boiling water reactors (BWRs).

The operational experience incorporated in the AP600 safety-related and nonsafety-related systems has been reflected in the various design certification documents. For example, section 1.9 of the AP600 Standard Safety Analysis Report (SSAR) discusses AP600 compliance with various regulatory design requirements and the approach for resolution of the advanced light water reactor (ALWR) design certification issues. Many of the system and component descriptions in the AP600 SSAR identify specific design characteristics or capabilities that are based on operating plant experience. In addition, the various regulatory, industry, and Westinghouse design requirements, and in particular, the regulatory design certification issues, significantly reflect operational experience with currently licensed plants. Other design certification documents clarify lessons learned from operating experience in specific areas, such as WCAP-14645, "Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant."

### Features Previously Implemented in Westinghouse PWRs

Some of the passive safety-related features that have been used in licensed and operating plants and that are also incorporated in the AP600 include the following:

- Control rod insertion
- Accumulator injection
- Main control room pressurization
- Safety valve operation to prevent system overpressurization
- Battery power supplies for vital dc electrical buses

These passive safety-related components that are part of AP600 passive safety-related systems are not specifically addressed in other sections of this document since their reliability has been demonstrated through extensive successful operational experience in currently licensed commercial Westinghouse PWRs and precludes the need for additional focus.

The AP600 passive core cooling system uses direct vessel injection lines that are fundamentally identical to the application in some two-loop Westinghouse PWRs. This arrangement enhances the reliability of AP600 safety injection for many potential loss-of-coolant accident (LOCA) events when compared to other licensed designs where the injection lines are connected to the reactor coolant system primary loops. The accident performance of the direct vessel injection arrangement has been enhanced by installing a flow nozzle and a deflector at the reactor vessel interface. The flow nozzle reduces break flow for an injection line break, but has no significant impact on injection flow for the various design basis events. The deflector helps to properly direct post-accident injection flow into the reactor vessel downcomer annulus, reducing the potential for injection flow bypass of the core. The sloping of the direct vessel injection lines improves maintenance capabilities during shutdown with reduced reactor coolant system inventory conditions.

The AP600 main control room pressurization design approach is another passive design feature that is essentially identical to a design currently licensed on operating Westinghouse PWRs. Some three-loop Westinghouse PWRs have main control room air pressurization design capability (for the first hour following an accident) that has been licensed. The implementation of the AP600 main control room pressurization approach is fundamentally identical to the current application, except that the duration of main control room pressurization is longer for the AP600, requiring a greater pressurization air volume.

### Features Previously Implemented in Other Plant Designs

Some AP600 passive design features have not been implemented in currently licensed Westinghouse PWRs, but have very extensive and successful operational histories in BWRs.

An ADS, functionally similar to the system currently licensed in BWRs, is included in the AP600 design to facilitate transition between the various passive core cooling system injection sources. However, unlike the BWR system that actuates using fast-opening actuation valves, the AP600 ADS sequentially opens stages of power-actuated depressurization valves that operate relatively slowly. This design provides a more controlled depressurization and minimizes air-clearing loads in depressurization discharge piping and the resulting hydrodynamic tank loads.

The ADS incorporates dc-powered, motor-operated valves. These valves have been successfully licensed and used in many BWR designs. The design process for the AP600 included extensive discussions with both BWR utilities and valve and operator vendors early in the design process to identify potential operational concerns. Therefore, appropriate design improvements were made in the AP600 applications of these valves, based on consideration of power cable length, the impact of different valve operator maintenance requirements, differences in motor-operator sizing, and other factors.

The containment water recirculation design has considered operational experience from a variety of different plants in the design of containment recirculation flowpaths, including the recirculation screen configuration. Some important concerns related to recirculation screen clogging have been identified in currently operating plants and the AP600 design includes features to reduce the potential for screen clogging. The AP600 design inherently reduces the likelihood of screen clogging in several ways. First, AP600 recirculation occurs much later -- in about 6 to 9 hours for the AP600 versus within 1 hour for the limiting cases for current plants -- which allows significant additional settling time for any suspended debris. In addition, the AP600 recirculation screens are much taller than screens in current plants, due to the extended floodup elevation and increased loop compartment floodup water depths inherent in the AP600 design. This provides considerable distance between screen surface areas and floor areas during recirculation, where debris settling tends to occur, reducing the potential for clogging that has been identified in some current plants. In addition, the insulation for the AP600 loop piping and other piping and components that may be exposed to flooding and potentially increase the likelihood of clogging, is constructed of materials or uses designs, such as using stainless steel insulation or enclosing insulation material in stainless steel cans, that will prevent or minimize the potential for recirculation screen clogging.

The passive residual heat removal heat exchanger is a primary-loop heat exchanger that is an equivalent design approach to the isolation condenser design used in BWRs for direct reactor core decay heat removal. The fundamental difference is that the BWR heat exchanger functions in the steam condensation mode while the AP600 passive residual heat exchanger can operate with both single-phase forced flow and natural circulation of reactor coolant, in addition to functioning as a natural-circulation steam condenser for events where reactor coolant system voiding occurs. However, passive residual heat removal is not required following design basis LOCA events with excessive voiding since the break flow provides adequate decay heat removal. The AP600 design also incorporates lessons learned from BWR operating experience to prevent destructive water hammer following actuation by keeping the system connected to the reactor coolant system and pressurized during standby operation by keeping at least one isolation valve open.

The passive core cooling system includes explosively actuated isolation (squib) valves in both the IRWST injection and fourth-stage ADS lines of the passive core cooling system. This type of valve has a successful performance history and is currently licensed for use in the standby liquid control system for BWRs, which provides passive emergency shutdown boron injection following an accident. This valve design provides positive isolation and reduced potential for leakage for the passive safety-related systems during standby operation, while providing reliable actuation.

The CMT safety injection discharge flowpath in the passive safety injection system contains bias-opened, tilt-disc check valves using a proven valve design with an extensive operational history in the Shippingport nuclear power plant. This application is another example of borrowing a proven valve design to perform an equivalent safety-related valve function -- to passively transfer open and remain



open under static or low driving head conditions. In the Shippingport application, these valves were used in the reactor coolant pump discharge with multiple pumps per reactor coolant loop to prevent reverse flow through the standby pumps during plant power operation. The discharge valves for the standby pump were required to remain closed during plant operation and to open to provide natural-circulation flow through the core if all reactor coolant pumps were lost. In the AP600 application, these valves are subjected to significantly less challenging conditions (static conditions in a standby component flowpath) than in the Shippingport application, where they are continuously closed and required to open with relatively low driving heads.

## 2.0 CONSERVATIVE SYSTEM DESIGN AND ANALYSIS

The AP600 system design process includes a wide variety of activities that help ensure that the plant systems, including the safety-related passive systems, are capable of performing their design basis functions, that their availability and reliability are sufficient to satisfy their design basis requirements, and that there is sufficient conservatism incorporated in the design to satisfy the licensing design basis.

The AP600 design process must provide an effective method to integrate both the technical and administrative aspects of the design process. The AP600 design engineering group has overall responsibility for the individual system design activities and is responsible for a design approach based on conservative system design and analysis that supports the licensing design basis for the AP600.

The system design engineers are responsible for meeting the various regulatory and industry design requirements for each plant system. Therefore, a comprehensive assessment of the plant design against these design requirements must be completed and documented. These assessments are maintained in a plant design data base and reported in various design certification documents. The results of the conformance assessment against the various regulatory design requirements is provided in the AP600 SSAR. Examples of the types of criteria that the AP600 design is assessed against include the following:

### Regulatory

- 10 CFR, Part 50, and the associated General Design Criteria
- 10 CFR, Part 52
- Standard Review Plan (NUREG-0800)
- Regulatory Guides
- Unresolved Safety Issues and Generic Safety Issues
- Three Mile Island Issues
- ALWR Certification Issues

### Industry

- American National Standards Institute (ANSI) Standards
- American Society of Mechanical Engineers (ASME) Codes
- International Electrical and Electronics Engineers (IEEE) Standards
- Electric Power Research Institute (EPRI) ALWR Utility Requirements Document

The AP600 design process also includes coordination, integration, and review of the various supporting design activities discussed in this report. These activities include the following:

- Confirmation that the correct design information is used in these activities
- Reviewing preliminary and final results of these design support activities
- Confirmation or modification of the design, as appropriate
- Review and confirmation of final design performance

In addition, there are many other supplemental design tasks and supporting design activities that must be integrated, coordinated, and followed by the system design engineers that are not directly discussed in this review. These other design support activities are performed by groups that are separate from the AP600 design organization to ensure independence from the design effort and provide broader design review and input to the design organization. For example, the design engineers must complete supplemental evaluations of systems capabilities in performing their safety-related functions. These supplemental evaluations may be either completely performed by or extensively supported by the various independent engineering groups, such as reliability engineering, but the overall systems support for these activities, and integration of the results of these evaluations into the AP600 design, is the responsibility of the AP600 system design engineering group.

Examples of these supplemental or supporting evaluations include the following:

- A failure modes and effects analysis (FMEA) to assess the capabilities of each safety-related system in response to postulated credible single failures
- An evaluation of potentially adverse systems interactions to determine the impact of other safety-related and nonsafety-related systems on the operation of each safety-related system
- An evaluation of the shutdown performance of the plant and safety-related systems and equipment and an assessment against regulatory shutdown design requirements
- An evaluation of the reliability, availability, and maintainability for each system, including identification of potential system failures that could prevent each system from meeting specific reliability and availability goals

The system design process provides the primary vehicle to coordinate the range of design activities and to integrate the results of these activities into the specific system design. The effectiveness of the overall design process and the supporting design activities contributes significantly to the reliability of the passive safety-related systems in performing their design basis safety-related functions.

The results of the individual system design activities are presented in the appropriate system design discussions in the AP600 SSAR. These system design discussions also reference the associated design information in other sections of the SSAR.



### 3.0 CONSERVATIVE DESIGN BASIS SAFETY (THERMAL/HYDRAULIC) ANALYSES

One of the fundamental steps in the design certification process is to perform suitably conservative, licensing basis thermal/hydraulic analyses of anticipated operational occurrences and postulated accidents to evaluate the capability of the plant to mitigate effects of these accidents and to establish and maintain safe shutdown conditions following these events. Safety analyses provide assurance that the plant will be adequately protected for the range of analyzed events. The regulatory requirements for the safety analyses are provided in the Standard Review Plan (NUREG-0800). The safety analyses include a range of LOCAs and various non-LOCA events such as loss of electrical power, loss of load (load rejection), and steam generator tube rupture. These safety analyses confirm the design basis performance and design margins by providing an independent verification that the plant design as implemented by the system designers satisfies the functional requirements specified by the analysis engineers. The AP600 safety analyses are performed by safety analysis engineering groups that are independent of the AP600 design engineering group.

The reliability of the passive safety-related systems is demonstrated through the use of licensing basis analysis codes that accurately model the AP600 and represent the various passive processes and phenomena that can occur in the plant. A phenomena importance ranking table (PIRT) has been developed to identify important phenomena for the various plant events that are analyzed. The AP600 tests have been compared to the PIRTs to help ensure that tests capture the phenomena of interest for the plant design calculations. The AP600 analysis codes have been benchmarked, verified, and validated against the results of the AP600 and other testing programs as part of the design process. Specific AP600 component models have been implemented and validated to better model specific AP600 design features in these codes.

The codes used to perform the safety analyses include the following:

- NOTRUMP for small-break LOCA events
- LOFTRAN for non-LOCA events
- W COBRA-TRAC for large-break LOCA events and long-term post-LOCA cooling

The details of the safety analyses and information related to analysis methodologies are presented in Chapter 15 of the AP600 SSAR. In addition, various analysis code validation reports have been submitted to the NRC as part of the AP600 design certification application.

### 4.0 PRA SUCCESS CRITERIA ANALYSES

To support the PRA, analyses were performed to justify some of the PRA success criteria. These success criteria represent combinations of passive components used to perform specific safety-related functions to mitigate the consequences of various accidents and to establish and maintain safe shutdown following an event. The AP600 PRA success criteria analyses are performed by a risk assessment engineering group that is independent of the AP600 design and nuclear safety analysis engineering groups.

Success criteria activities consist of performing thermal/hydraulic analyses using different performance codes than the codes used to perform conservative licensing basis safety analyses in Chapter 15 of the AP600 SSAR. This analysis work represents another analytical evaluation of the AP600 passive safety-related systems using different analysis codes, such as MAAP4. The success criteria work has

addressed the plant performance for a very large number of additional accident scenarios beyond those in the licensing design basis. The success criteria analysis work and the associated NRC interface activities are focused on two continuing efforts to complete this task -- benchmarking of the MAAP4 code and evaluating the potential impact of thermal/hydraulic uncertainties on the PRA.

The MAAP4 code is being benchmarked against the NOTRUMP safety analysis code to gain confidence in the MAAP4 analysis results. There are also continuing activities to address questions related to thermal/hydraulic uncertainties. The focus of these efforts is on events that have low margin and higher frequencies of occurrence.

Appendix A of the AP600 PRA provides information on the PRA success criteria analyses. Additional information related to the MAAP4 benchmarking and resolution of the thermal/hydraulic uncertainties will be provided in separate submittals.

## 5.0 PROBABILISTIC RISK ASSESSMENT

Part 52 of Section 10, Code of Federal Regulations, requires that a PRA be submitted as a part of an application for design certification. The PRA provides a detailed evaluation of the design, including plant, containment, and typical site analyses that consider both internal and external events. The AP600 PRA is performed by a risk assessment engineering group that is independent of the AP600 design engineering group.

Multiple PRA evaluations of the AP600 have been completed throughout the AP600 design evaluation. The AP600 PRA program comprises three distinct phases. A scoping study on the AP600 conceptual design, which was performed prior to 1989, provided preliminary information to support the conceptual design work. The Phase 1 effort performed in support of the initial intermediate design engineering included completion of preliminary level 1 studies, analysis of preliminary severe accidents, and preparation of a preliminary model of the containment event tree required to complete the level 2 PRA analysis. The objectives of current PRA activities, including the recent revisions to the PRA, are to evaluate and enhance the AP600 design and to complete the PRA for the design certification process. The last phase of PRA activities includes a number of sensitivity evaluations, including studies of the effects of operator actions, nonsafety-related systems, common-cause failures, and system importance. The PRA evaluations have required extensive interaction between the PRA analysts and design engineers for a variety of tasks including the following:

- Confirm the system designs as modeled in the PRA
- Confirm the appropriate component failure data used in the PRA calculations
- Confirm the appropriate system and component unavailabilities due to maintenance and testing
- Confirm the appropriate component testing frequencies
- Review the PRA results and cutsets
- Make appropriate system design modifications and improvements based on the results of the PRA quantification and associated PRA insights

The PRA evaluations have provided a comprehensive, detailed assessment of passive safety-related system performance, as well as that of nonsafety-related systems. The PRA has evaluated a broad range of areas and contributes significantly to understanding the operation of these safety-related systems. The PRA evaluations provide more realistic, best-estimate predictions of plant post-accident performance. The equipment and component failures are based on more realistic component failure

data available from data bases that reflect industry component data and performance history.

The technical tasks for the AP600 PRA include the following:

- Level 1 analysis for internal events
- Level 2 analysis for internal events
- Level 3 analysis for internal events
- Sensitivity, importance, and uncertainty analyses for internal events
- Shutdown risk assessment
- External events analysis
- Focused PRA sensitivity study to support resolution of the regulatory treatment of nonsafety-related systems

Many of the activities completed as part of the PRA evaluation provide information related to passive safety-related system performance and capabilities, as well as interactions and interdependencies with other safety-related and nonsafety-related systems and components. Therefore, the PRA helps to improve the understanding of passive safety-related systems and resolve various issues identified during the design and certification processes.

The results of the current PRA activities are provided in the latest update to the AP600 PRA Report. The results of the PRA demonstrate the benefits of passive safety-related systems in reducing dependence on active systems and indicate a core damage frequency for the AP600 that is lower than for current plants.

## **6.0 CONSERVATIVE EQUIPMENT AND COMPONENT DESIGN**

The selection of appropriately conservative AP600 equipment and component designs that can perform the required safety-related functions is another important part of the AP600 design process that increases the reliability of passive safety-related systems. This is accomplished through a variety of activities in the AP600 design process.

First, the system design engineers develop conservative functional specifications for the various systems components. These functional requirements identify bounding process flows, pressures, and differential pressures that are verified through extensive sensitivity studies that make use of computer-based design calculations. The AP600 design process also includes the development of more comprehensive and detailed component design performance requirements than were typically prepared for predecessor plants at equivalent phases of the design process.

As discussed in section 1.0, the use of experience-based selection for many of the specific equipment and components greatly enhances passive safety-related system reliability since the selected components have proven operating histories from a wide variety of plant designs. The component design and selection process also makes extensive use of many other sources of industry experience from various programs. For example, a large information base was developed through the industry power-operated valve testing program, performed to address regulatory concerns initially identified in Generic Letter 89-10 for motor-operated valves. This information was used appropriately in the AP600 system design. The formal and informal design reviews for the various plant systems include utility and industry representatives who helped to confirm that the most appropriate component applications were incorporated in the AP600 design, that lessons learned were considered in

component design and selection, and that state-of-the-art technology was considered, if it demonstrated a satisfactory performance history in equivalent applications.

The component design and selection process includes increased focus on component and equipment qualification testing and analysis. The availability of more detailed design information and more complete functional design requirements helps to better define and clarify the required environmental qualification for plant components and associated performance characteristics and conditions. This information is used to interface with the component design groups and equipment vendors to develop the appropriate inservice testing for safety-related valves. Increased interaction with manufacturers early in the design process helps to confirm that the specified qualification testing and analyses and identified inservice tests accurately assess component adequacy in performing design basis function(s). This is particularly important, considering concerns related to assessing power-operated valve performance, including motor-operated valves, and the industry goal to identify and periodically confirm component performance at test conditions that are as close as practical to design basis conditions.

The AP600 equipment design, and the coordination of interfaces with the various component manufacturers, are performed by an equipment design engineering group that is independent of the AP600 system design engineering group. The equipment design group is responsible to confirm that the component design is satisfactory to meet functional requirements for the system application(s) specified, and confirm the adequacy of component manufacturer design and associated equipment qualification and testing programs. The advanced plant design process has greatly increased the focus on improving the integration of activities between the system design engineering groups, the component design engineering groups, and the various equipment and component manufacturers.

Information related to the functional and design basis capabilities of various plant components is provided in the associated sections of the AP600 SSAR. Chapter 3 of the AP600 SSAR provides information related to seismic, environmental, and dynamic design and testing requirements of the various plant components, and overall design of mechanical systems and components.

## **7.0 AP600 TESTING PROGRAM**

The AP600 design process includes a comprehensive design testing program that is used primarily to provide experimental input data to verify the safety analysis codes used to evaluate and confirm AP600 accident response performance. The testing program also provides important insights into the design and operation of the passive safety-related systems and components. In addition, some specific equipment engineering performance tests, such as reactor coolant pump and check valve tests, were completed to gain information on a specific component or system to remove design and performance uncertainties. The development of the AP600 testing program uses analytical approaches to design tests for proper simulation. The test implementation incorporates component design experience to select proper design applications for test facilities. The AP600 testing program is performed by a design testing engineering group that is part of the AP600 project organization, but independent of the AP600 design engineering group.

The development of the design test and analysis program includes a number of considerations such as:

- Systems that are different in the AP600 versus standard Westinghouse plants

- Thermal/hydraulic phenomena important for AP600 passive safety-related systems
- Data needed to capture the phenomena for modeling AP600 passive safety-related systems
- Applicable data already in existence for code validation, such as existing Westinghouse data or data in the public domain (e.g., NUREG-1230)
- Codes or models used (existing 10 CFR 50, Appendix K codes or best-estimate models) to best represent the passive system behavior

The four classifications of experiments used to develop the AP600 and provide the data needed for design certification are the following:

- Basic research experiments used to provide data on particular thermal/hydraulic phenomena, to provide engineering guidance, or to verify a proof of principle used in the design
  - Condensation experiments performed at the University of Wisconsin used to support the heat transfer models and correlations in the WGOTHIC containment computer code
  - Cold water film flow tests used to verify exterior containment surface wetting
  - One-ninth scale reactor vessel flow tests performed at the University of Tennessee examined core inlet velocity distribution that provided results for use in the safety analysis codes
  - Small-scale wind tunnel tests on the containment used to establish the air inlet location
- Engineering tests developed to gain specific information on a particular component or system to remove design and performance uncertainty so that the final engineering design can proceed with confidence
  - High-inertia rotor bearing tests helped characterize design, horsepower losses, and cooling requirements of the main reactor coolant pumps (RCPs) so that increased pump inertia could be obtained for loss-of-flow accidents.
  - Reactor vessel instrumentation tests used to verify that instrumentation located at the top of the reactor vessel would operate as planned so that no reactor vessel bottom penetrations were necessary.



Separate effects component experiments, specifically designed to provide data on AP600 component geometries on a large scale, and develop and verify models and correlations used in the AP600 safety analysis computer codes

- The CMT test (a 1/6th-diameter, 1/2-height simulation of the AP600 CMT) covers the full range of thermal/hydraulic conditions, pressures, and temperatures the AP600 CMT could experience under postulated conditions. Data from these tests will be used to develop and verify the condensation heat transfer models for the WCOBRA/TRAC and NOTRUMP loss-of-coolant codes and the LOFTRAN-AP transient systems analysis code. The tests will also be used to verify the design performance of CMT recirculation behavior, draining behavior, and mixing performance of the CMT steam diffuser.
- The ADS test examines the critical flow and two-phase pressure drop for the ADS flowpath and sparger. This test is full-scale and simulates the flow, pressure, and temperature conditions calculated from the AP600 safety analysis. The test verifies the critical-flow models used in the WCOBRA/TRAC and NOTRUMP loss-of-coolant computer codes, and will provide design information of the sparger and piping support loads, and IRWST behavior.
- The full-length, low-flow departure from nucleate boiling (DNB) tests are conducted to extend the Westinghouse critical heat flux correlations to cover the lower flow conditions for the AP600 plant. The revised correlations will be used in the LOFTRAN-AP transient analysis code.
- Heated plate tests are used to develop the evaporative film cooling correlations for the exterior of the containment. These tests provide the models and correlations for the WGOTHIC containment computer code.
- Full-height PRHR heat exchanger experiments are conducted using three vertical tubes. Test conditions cover the full range of forced flow and natural-circulation flow calculated for the loss-of-heat-sink transients. A heat transfer correlation is developed from the data and used in the LOFTRAN-AP transient analysis code.

- Integral systems tests that examine the integration and interaction of the different thermal-hydraulic phenomena that occurred during postulated accidents
  - Two systems tests
    - SPES full-height, full-pressure integral tests
    - Oregon State University (OSU) 1/4-height, reduced-pressure integral tests
  - Two integral containment tests
    - Passive containment cooling system (PCS) test of a 3-foot-diameter, 25-foot-high model of the AP600 containment
    - Large-scale containment tests (LSTs) of a 1/8-linear scale model of the AP600 containment

The AP600 test program contributes significantly to the overall understanding of operation of passive safety-related plant systems and components, and supports validation of the analysis codes. Numerous design testing documents have been developed as part of this program. Section 1.5 of the AP600 SSAR describes the tests that were conducted during the AP600 conceptual design program (from 1986 through 1989).

## **8.0 EMERGENCY RESPONSE GUIDELINES THERMAL/HYDRAULIC ANALYSES**

Additional thermal/hydraulic analyses were completed as part of the effort to develop the AP600 emergency response guidelines. These additional analyses were made to confirm the adequacy of the guidelines in mitigating accidents. These analyses provide an additional tool to evaluate accident response using both passive safety-related systems and various nonsafety-related systems. Many of these analyses were performed using the TREAT-AN code, an interactive simulation computer program that models many of the automatic and manual operation actions available following an accident. This code includes some important differences from the analysis codes used for both the safety analyses described in section 3.0 and the PRA success criteria analyses described in section 4.0. This analysis work represents another analytical evaluation of AP600 passive safety-related systems beyond the safety analysis and PRA analysis work completed and discussed previously. The emergency response guideline development and associated thermal/hydraulic analyses are performed by engineering groups that are independent of the AP600 design, nuclear safety analysis, and PRA success criteria analysis engineering groups.

For example, these analyses are focused on providing more realistic analysis assumptions to provide best-estimate evaluations of plant response for the various events. The TREAT-AN analysis scenarios were designed to take credit for the equipment realistically expected to be available following an accident and for anticipated operator actions to mitigate the event in conjunction with the emergency response guidelines. In addition, these analyses provide more detailed and extensive modeling of control system interactions.

Although the intent of these additional analyses is to confirm the adequacy of the emergency response guidelines, the analyses provide additional supporting information related to the operation of specific plant systems, and response of passive safety-related systems and components.

The detailed results of these analyses are provided in the AP600 emergency response guidelines and the associated background documents.

## **9.0 DESIGN ACTIVITIES FOR PLANT OPERATIONS**

As part of the plant construction and startup activities, a plant initial test program has been developed that consists of a series of tests categorized as construction and installation, preoperational, and startup tests. The overall objective of the test program is to demonstrate that the plant has been constructed as designed, that the systems perform as required by the plant design, and that activities culminating in operation at full licensed power, including initial fuel load, initial criticality, and power ascension, are performed in a controlled and safe manner. This testing program includes the passive safety-related systems and components. Information related to the plant initial test program is provided in Chapter 14 of the AP600 SSAR.

As required by 10 CFR 52.47 (a)(1)(vi), following completion of the construction phase, the required inspections, tests, analyses, and acceptance criteria (ITAACs) relating to the AP600 design will provide reasonable assurance that, if the inspections, tests and analyses are performed and acceptance criteria met, a future plant that references the design will operate in accordance with the design certification for the AP600. The ITAACs provide Tier 1 design descriptions for each of the plant systems that perform either safety-related or nonsafety-related defense-in-depth functions. ITAACs have been developed for the passive safety-related systems to confirm the design capability as described in the design description and supporting Tier 2 documents, such as the AP600 SSAR. Information related to ITAACs may be found in the AP600 ITAAC document.

The AP600 will also have to meet regulatory and industry requirements to confirm the design basis for the passive safety-related systems on a continuing basis during the plant operation. Initial operation of the AP600 requires system and component operability in conformance with the AP600 technical specifications, contained in Chapter 16 of the AP600 SSAR. The technical specifications become part of the operating license for the plant and identify specific safety-related passive component operability

requirements for all plant conditions and operating modes, including power operation and shutdown. The technical specifications identify periodic surveillance requirements that must be performed to confirm operability, as well as limiting conditions for operation and the associated actions to be taken if these limiting conditions are not satisfied.

The ASME Code requires performance of periodic tasks to verify the integrity and functionality of the various plant systems, structures, and components that perform safety-related functions to mitigate the consequences of an accident or to establish and maintain safe shutdown conditions.

The AP600 inservice testing program is based on the requirements of ASME Code, Section III, where testing of Class 1, 2, and 3 pumps and valves is performed in accordance with Section XI of the ASME Code and applicable addenda, as required by 10 CFR 50.55a(f), except where specific relief has been granted by the NRC in accordance with 10 CFR 50.55a(f). The Code includes requirements for leak tests and functional tests for active components. The AP600 inservice testing program is described in subsection 3.9.6 of the AP600 SSAR.

The AP600 inservice inspection program identifies preservice and inservice inspection and testing of ASME Code Class 1 pressure-retaining components (including vessels, piping, pumps, valves, bolting, and supports) within the reactor coolant pressure boundary and similar Class 2 and 3 components that are performed in accordance with Section XI of the ASME Code, including addenda according to 10 CFR 50.55a(g). This includes all ASME Code, Section XI mandatory appendices. The AP600 inservice inspection program is described in sections 5.24 and 6.6 of the AP600 SSAR.

These post-design activities help to provide continuing assurance that the passive safety-related components will continue to perform their safety functions following plant construction and operation.

## **10.0 CONCLUSION**

The reliability of the AP600 passive safety-related systems is demonstrated through a broad range of design and design certification activities that have been described in this roadmap document.

One of the design goals for the AP600 is to use proven technologies with extensive operational experience. The passive safety-related systems and components incorporated in the AP600 design include many that have been successfully licensed by the NRC in other plant designs.

A formal design process is being followed in developing the AP600 design and in the integration and completion of the various design and design certification activities. The design process includes formal design procedures to satisfy the quality assurance requirements for nuclear design activities.

The design and operation of the passive safety-related systems are evaluated using at least four independent analysis activities. These analysis activities, which consider a wide range of conservatisms in the analysis inputs and assumptions, and which use a variety of analysis codes and calculational methodologies, include the following:

- System design engineering calculations
- Design basis safety (thermal/hydraulic) analyses
- PRA success criteria analyses
- Emergency response guideline thermal/hydraulic analyses

The design activities also include a number of independent support activities and evaluations to support the design and design certification. The design process provides independence from a variety of perspectives, but primarily through the use of a large number of engineering groups that are independent from the AP600 project and associated AP600 design engineering groups.

The performance of the passive safety-related systems is also evaluated extensively through the completion of a number of PRA evaluations throughout the design process. The PRA has successively included more detailed system and component modeling and provided a number of useful sensitivity studies that have consistently demonstrated the reliability of the passive safety-related systems.

The design process also includes incorporation of equipment and component designs that will meet the design requirements, including qualification testing to ensure that the components are capable of performing their required safety-related functions.

An extensive testing program has been implemented to support the AP600 design certification. Extensive regulatory input and review aid development of a comprehensive testing program and provide design information required to validate the design and licensing codes used to analyze plant performance. In addition, the testing program provides valuable insights into passive safety-related system operation.

The design process also identifies a number of post-design activities to confirm that the final construction meets the original design basis and that the design basis continues to be satisfied during plant operation.

Overall, there are a large number of activities that have been completed as part of the design process that help to demonstrate the reliability of the passive safety-related systems, structures, and components.



**TABLE 1 -- PASSIVE SYSTEM RELIABILITY ROADMAP**

Design/Certification Activity	Associated Design Documents
Operating Experience	AP600 SSAR - Appropriate system design features that reflect operational experience as discussed in individual system design sections - Sections 1.9 and 3.1 (compliance with regulatory requirements, such as discussions such as mid-loop operation in section 1.9.5 under ALWR Certification Issues) - Appendix 1A (compliance with regulatory guides) WCAP-14645 (Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant)
Conservative System Design and Analyses	AP600 SSAR - Appropriate system design sections - Section 6.2 (containment systems) - Section 6.3 (passive core cooling) - Section 6.4 (habitability systems) - Chapter 7 (instrumentation and control) - Chapter 8 (electric power) - FMEA for each safety-related system WCAP- 14476 (AP600 Adverse Systems Interactions) WCAP-[to be provided LATER] (AP600 Shutdown Report)
Conservative Design Basis Safety (thermal/hydraulic) Analyses	AP600 SSAR, Chapter 15
PRA Success Criteria Analyses	AP600 PRA - Chapter 6 (Success Criteria Analyses) - Appendix A (Analyses to Support Success Criteria) Other supporting documents [to be provided LATER] - MAAP4 benchmarking - Thermal/hydraulic uncertainty
Probabilistic Risk Assessment	AP600 PRA
Conservative Equipment and Component Design/ Equipment Qualification Analysis and Testing	AP600 SSAR - Chapter 3 and appendices (protection against seismic, dynamic, and external effects, mechanical and electrical component design, etc.) - Section 3.11 (environmental qualification) - ASME codes - ANS standards
AP600 Testing Program	AP600 SSAR, section 1.5

**TABLE 1 -- PASSIVE SYSTEM RELIABILITY ROADMAP**

Emergency Response Guideline Procedures Thermal/Hydraulic Analyses	AP600 Emergency Response Guidelines, AP600 Emergency Response Guidelines Background Information (Books 1 and 2)
Design Activities for Plant Operations	AP600 SSAR - Section 3.9.6 (inservice testing) - Section 5.2 and 6.6 (inservice inspection) - Chapter 14 (initial test program) - Section 16.1 (technical specifications) - Section 16.2 (reliability assurance program) WCAP-1386 (AP600 RTNSS process implementation, including designer recommendations for nonsafety- related system short-term availability controls) ITAACs and Tier 1 design descriptions

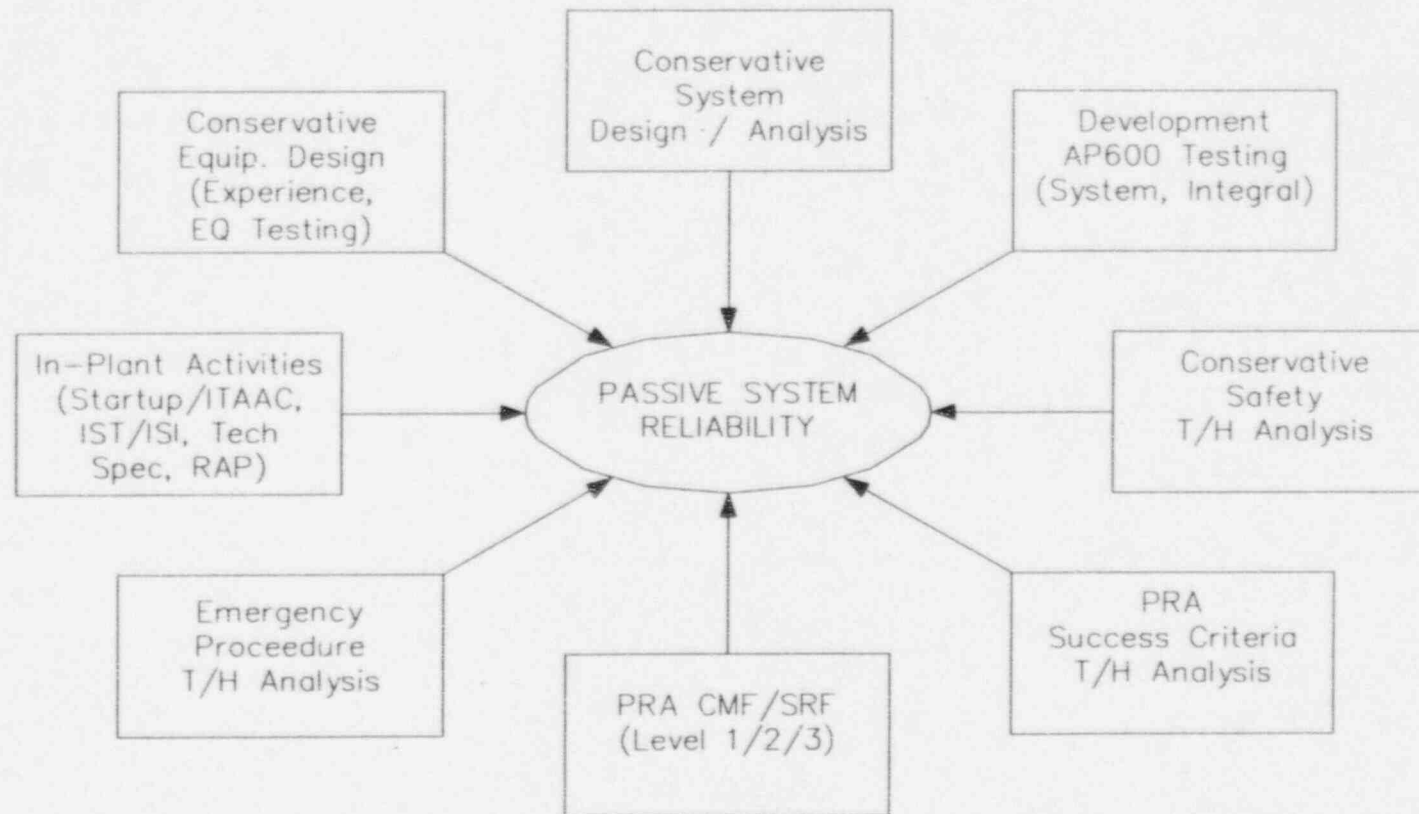


Figure 1 -- Passive System Reliability Overview