Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-97-5122
DCP/NRC0862
Docket No.: STN-52-003

June 26, 1997

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

ATTENTION: T. R. QUAY

SUBJECT: REVISED AP600 DESIGN RELIABILITY ASSURANCE PROGRAM LIST OF RISK SIGNIFICANT STRUCTURES, SYSTEMS, AND COMPONENTS

References:

1. Letter from NRC to Westinghouse (Huffman to Liparulo), "Criteria for Establishing Risk Significant Structures, Systems, and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program," dated January 16, 1997.

2. NUMARC 93-01 Revision 2, "Nuclear Energy Institute (NEI) Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", dated April 1996.

3. Letter from Westinghouse to NRC, NSD-NRC-97-4958 (DCP/NRC0715), "AP600 Reliability Assurance Program Completion," dated February 7, 1997.

Dear Mr. Quay:

The NRC has taken a new position (see Reference 1) for creation of the AP600 Design Reliability Assurance Program (D-RAP) list of risk significant structures, systems, and components (SSCs). It should be noted that these new requirements are more restrictive than the requirements used by the evolutionary ALWRs whose designs were recently approved by the NRC. This position requests that Westinghouse revise AP600 SSAR Section 16.2 to make it consistent with the Reference 2 maintenance rule guidelines for identifying risk significant SSCs.

Given this new requirement, Westinghouse created a list of AP600 PRA internal events which meet the Nuclear Energy Institute (NEI) risk significance determination criteria. These criteria include a risk achievement worth (RAW) greater than or equal to 2.0 or a risk reduction worth (RRW) greater than or equal to 1.005, which is equivalent to a Fussell-Vesely (FV) value of 5%. Note that the only SSC which meets the RRW FV criterion and not the RAW criterion is the hardware failure of residual heat removal system motor-operated valves.

030022

The expert panel then convened and evaluated each of these events/SSCs to determine which should be included in SSAR Table 16.2-1 (SSAR Section 16.2.7.1.4 defines the expert panel referred to in NUMARC 93-01 Section 9). The SSCs which met the NUMARC 93-01 criteria but which the expert panel determined were not appropriate for inclusion in the D-RAP are listed in Table 1, attached to this letter. Generally, the exclusions are based on one of the following justifications:

1. Some SSCs are passive components which do not move and therefore are not considered to be risk significant. (This criteria was not applied to hardware or software or to passive components for which credible failures could be derived from an initiating event).

2. Diversity of hardware and software is not controlled by D-RAP. Rather, it is captured in PRA insights and the ITAACs. This criterion does not apply to common cause failures (CCF).

3. Some systems were conservatively grouped for PRA but are unrelated such that the CCF modelling is overly conservative.

In addition to the events/SSCs which meet the NUMARC 93-01 criteria and the expert panel review, the expert panel judged some additional SSCs should be included in the D-RAP. These are included in the attached markup of SSAR Section 16.2, including Table 16.2-1. This markup is provided for use by the NRC in writing the SSAR Section 16.2 FSER.

The Westinghouse status for DSER open item tracking system (OITS) item 4852 is now Action N for review. In addition, DSER OITS item 3943, for which Westinghouse took the action to evaluate hydrogen ignitors and containment fan coolers for the D-RAP, and provided input to NRC by Reference 3, is statused Closed for Westinghouse since it is superseded by item 4852. NRC should provide Westinghouse with an update to the NRC status for item 3943.

This submittal will be included in Revision 14 of the AP600 SSAR.

Please contact Robin K. Nydes at 412-374-4125 if you have any questions regarding this transmittal.

Brian A. McIntyre

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

jml

Attachments

cc: W. C. Huffman, NRC (w/Attachments)
F. X. Talbot, NRC (w/Attachments)
N. T. Saltos, NRC (w/Attachments)
N. J. Liparulo, Westinghouse (w/o Attachments)

Table 1, Attached to Letter NSD-NRC-97-5122
SSCs Which Meet the NUMARC 93-01 Selection Criteria
but are not Included in the AP600 D-RAP
Based on Expert Panel Review

Basic Event Description	Rationale for not including in the AP600 D-RAP, SSAR Section 16.2
CCF of Core Makeup Tanks (CMTs)	The PRA was overly conservative when making this CCF assumption. The CMTs are physically separated, passive components for which no credible CCF can be derived from a single initiating event. In addition, this is an ASME Class 1 component, subject to regular control and inspection.
CMT Ruptures and Flow Tuning Orifice Plugs and Ruptures	The CMTs are passive components for which the possibility of failure, or rupture, independent of an initiating event is negligible. CMT flow tuning orifice plugging is not expected since this is a nonrestrictive orifice of about 4" ID which carries clean water. The flow through this orifice is tested during the system level inservice tests.
CCF of Accumulator Tanks	The PRA was overly conservative when making this CCF assumption. The accumulator tanks are physically separated, passive components for which no credible CCF can be derived from a single initiating event. In addition, this is an ASME Class 3 component, subject to regular control and inspection.
Accumulator Tank Ruptures and Accumulator Flow Tuning Orifice Plugs and Ruptures	These are passive components for which the possibility of failure, or rupture, independent of an initiating event is negligible. Accumulator flow tuning orifice plugging is not expected since this is a nonrestrictive orifice of about 4" ID which carries clean water. The flow through this orifice is tested during the system level inservice tests.
Leak/Plug of PRHR Heat Exchanger	The PRHR heat exchanger is a passive component for which no credible failure or leak can be derived from a single initiating event. There is a Technical Specification which applies for PRHR leakage. For post-accident (non-Technical Specification) conditions, stresses would decrease from the normal pressurization to full system pressure such that leakage would not develop. In addition, small leaks do not affect the PRHR heat exchanger performance. No plugging of the PRHR heat exchanger is expected since it carries clean water. System level inservice testing demonstrates flow and heat transfer.
Failure of PRHR due to IRWST Failure	The IRWST is a passive component for which no credible failure can be derived from a single initiating event. Failures that would lead to rapid draining of the IRWST and result in failure of the PRHR heat exchanger due to loss of heat sink, would require a significant breach in the IRWST. During PRHR operation, no significant loads are anticipated such that significant margin exists relative to the design loading conditions. The design loading on the IRWST is based on ADS actuation, after which PRHR operation is not important. The design loads were developed from the full-scale sparger tests at the VAPORE facility in Cassaccia, Italy. Because the PRHR is normally pressurized to full system pressure, post-event stresses would decrease pressure such that leakage would not develop.

Basic Event Description	Rationale for not including in the AP600 D-RAP, SSAR Section 16.2
CCF of PMS, PLS, and DAS Indication for Operator Actions	The PRA was overly conservative when making this CCF assumption. This PRA internal event, as an SSC, is captured in the D-RAP as "Main Control Room (MCR) Indication and Control Mechanisms to Support Operator Actions". Diversity is an inherent design requirement such that the PRA is overly conservative in this grouping, which assumes subsequent failure of system indications which have no CCF source.
PLS CCF with PMS	The PRA common cause event is failure of the PLS and PMS. While this event meets the RAW criteria, PMS is the major contributor to the CCF rate and those PMS SSCs are already captured in the DRAP under "PMS Actuation Hardware" and "PMS Actuation Software". In addition, the PLS SSCs are captured in the DRAP under "PLS Actuation Hardware". Because the important SSCs related to PLS CCF with PMS are already captured, this event need not appear separately in the list of SSCs.
CCF of Motor Driven Pumps to Run	The PRA was overly conservative in its grouping of all these motor-driven pumps. The risk-significance of this grouping relates only to the chilled water system (VWS), not component cooling water, TCS, and VWS as grouped in the PRA. This is captured in the D-RAP as "Chilled Water System (VWS) Low Capacity Subsystem for CVS Room Cooling".
CCF of Containment Sump Level Heated RTD Sensors	The PRA was overly conservative in grouping and assuming CCF of CMT and containment sump level heated RTD sensors. The sensors for CMT level, as well as those for IRWST level which initiate containment recirculation, are included in the D-RAP. The containment sump level sensors provide for no automatic action; they provide information to the operator for manual actuation of containment recirculation as a backup to the IRWST level.
Sensors for Component Cooling Water and Service Water Flow and Instrument Air Pressure	The PRA common cause event for feedwater flow is overly conservative in grouping the feedwater flow sensor with low pressure environment sensors for component cooling water, service water, and instrument air. The PRA effect of these sensors on the feedwater flow event, compared to the high pressure/DP sensors provided for in the D-RAP, is negligible.
CCF of BAT Level Transmitters/Sensors	The BAT takes no automatic action based on sensor input. In addition, the BAT has no significance but was grouped with the IRWST level transmitters which are captured in the D-RAP.

AP600 Open Item Tracking System Database: Executive Summary

Date: 5/19/97

Selection: [item no] between 3943 And 3943 Sorted by Item #

Item No	Branch	DSER Section Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
3943	NRR/SPSB	16.2	MTG-OI		RAP/Canton,mike	Closed	Action W	NTD-NRC-96-4830	

Based on an August 16, 1996, meeting with the NRC to resolve their comments on the Reliability Assurnace Program (SSAR Section 16.2), we have placed the hydrogen ignitors and containment fan coolers in the "Risk Significant SSCs under the Scope of RAP" table with TBDs as justification for inclusion. Upon completion of the Focused PRA, there will be an evaluation to determine if these components should be included in the RAP table. A SSAR Section 16.2 markup will be transmitted by DCP/NRC0612 (NSD-NRC-96-4830). This markup will be revised based on the outcome of the PRA evaluation for these components and issued in SSAR Revision 10.

SSAR markup was transmitted. To close, this markup should be revised to reflect replacement or deletion of TBDs. rkn 10/16/96
SSAR confirmatory to ensure the markup provided in NSD-NRC-97-4958 is incorporated into SSAR Rev 12. NRC did not confirm this markup, rather, they revised the criteria for selecting SSCs for the RAP. Suggestion was made 4/15 to NRC that this item be closed with NSD-NRC-97-4958 and the follow-on actions be tracked by OITS item 4852. rkn 4/15/97

AP600 Open Item Tracking System Database: Executive Summary

Date: 6/26/97

Selection: [item no] between 4852 And 4852 Sorted by Item #

Item No.	Branch	DSER Section Question	Type	Title/Description Detail Status	Resp Engineer	(W) Status	NRC Status	Letter No. /	Date
4852	NRR/HQMB	16.2	MTG-COM		RAP/Canton, Mike	~~Action W~~ Action N	Action W		

Evaluate impact of NRC letter (1/16/97), Criteria for Establishing Risk Significant Structures, Systems, and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program

In progress. See NSD-NRC-97-4958, explaining this letter is being evaluated. rkn 2/10/97.
The RAP table of SSCs has been revised based on the maintenance rule criteria and expert panel review and a draft will be sent to NRC on May 2. With NRC concurrence on the draft, the status will be changed to Confirm-W to ensure it gets into the end-May SSAR rev. rkn 5/1/97

This draft was not sent due to extensive mgt review comments. The RAP will go in SSAR Rev 14. A markup is being sent to the NRC (the letter was ready 6/18). rkn 6/25

NTD/NRC0863 issued June 26. NRC to review. Not statused Confirm-W to include in SSAR Rev 14, since I've confirmed its in the print copy. rkn 6/26

 Total Records: 1

SSAR 16.2 Markup

(attachment to
NSD-NRC-97-5122)

16.2 Design Reliability Assurance Program

This subsection presents the AP600 Design Reliability Assurance Program (D-RAP).

16.2.1 Introduction

The AP600 D-RAP is implemented as an integral part of the AP600 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP600 probabilistic risk assessment (PRA) will remain valid throughout plant life. The PRA quantifies plant response to a spectrum of initiating events to demonstrate the low probability of core damage and resultant risk to the public. PRA input includes specific values for the reliability of the various structures, systems, and components (SSCs) in the plant that are used to respond to postulated initiating events.

The D-RAP, as shown in Figure 16.2-1, is implemented in three phases. The first phase, the Design Certification phase, defines the overall structure of the AP600 D-RAP, and implements those aspects of the program which are applicable to the design process. During this phase, risk-significant SSCs are identified for inclusion in the program using probabilistic, deterministic, and other methods. Phase II, the post-design certification process, develops component maintenance recommendations for the plant's operations and maintenance activities for the identified SSCs. The third phase is the site-specific phase, which introduces the plant's site-specific SSCs to the D-RAP process. Phases I and II are performed by the designer. Phase III is the responsibility of the Combined License applicant.

Finally, Figure 16.2-1 shows the Operational Reliability Assurance Process (O-RAP). This phase, which is implemented by the Combined License applicant, provides confidence that the operations and maintenance activities performed by the operating plant support ~~should maintain~~ the reliability assumptions made in the plant PRA.

16.2.2 Scope

The D-RAP includes a design evaluation of the AP600 and identifies the aspects of plant operation, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PRA, deterministic tools, industry sources, and expert opinion are utilized to identify and prioritized those risk-significant SSCs.

16.2.3 Design Considerations

Extensive efforts are involved in optimizing the AP600 design for operational availability as well as safety. The use of consistent reliability information provides confidence that the calculated system availabilities are based on the same data and assumptions as the PRA. When an alternative design is proposed to improve performance in either area, the revised design is first reviewed to provide confidence that the current assumptions in the other areas are not violated. When a potential conflict exists between safety goals and other goals, safety goals take precedence.

As part of the design process, risk-significant components are evaluated to determine their dominant failure modes and the effects associated with those failure modes. For most components, a substantial operating history is available which defines the significant failure modes and their likely causes.

The identification and prioritization of the various possible failure modes for each component lead to suggestions for failure prevention or mitigation. This information is provided as input to the Combined License applicant's ~~operational~~ reliability assurance activities ~~because it defines the means by which component reliability can be maintained~~. O-RAP.

The design reflects the reliability values assumed in the design and PRA as part of procurement specifications.

16.2.4 Relationship to Other Administrative Programs

The D-RAP manifests itself in ~~other~~ administrative and operational programs, ~~in the AP600~~. The technical specifications provide surveillance and testing frequencies for certain risk-significant SSCs, providing confidence that the reliability values assumed for them in the PRA will be maintained during plant operations. ~~In addition, certain~~ Risk-significant systems that provide defense-in-depth or result in significant improvement in the PRA evaluations are included in the scope of the D-RAP~~, to provide a high degree of confidence in their performance.~~

The O-RAP can be implemented through the plant's existing programs for maintenance or quality assurance. For example, the plant's implementation of the Maintenance Rule, 10 CFR 50.65, can provide coverage of the SSCs that would be included in O-RAP. The Combined License applicant will be responsible for the submittal of an O-RAP to the NRC. The NRC will review this process as part of the plant's maintenance program, Quality Assurance program, or other existing program.

16.2.5 The AP600 Design Organization

The AP600 organization described in Section 1.4 formulates and implements the AP600 D-RAP.

The AP600 management staff is responsible for the AP600 design and licensing.

The AP600 staff coordinates the program activities, including those performed within Westinghouse as well as work completed by the architect-engineers and other supporting organizations listed in Section 1.4.

The AP600 staff is responsible for development of Phase I of the D-RAP and the design, analyses, and risk and reliability engineering required to support development of the program. Westinghouse is responsible for the safety analyses, the reliability analyses, and the PRA.

The reliability analyses are performed using common databases from Westinghouse and from industry sources such as INPO and EPRI.

~~Within the engineering organization~~, the Risk and Reliability organization is responsible for ~~managing and integrating~~ the D-RAP and has direct access to the AP600 staff. Risk and Reliability is responsible for keeping the AP600 staff cognizant of the D-RAP risk-significant items, program needs, and status. Risk and Reliability participates in the design change control process for the purpose of providing D-RAP-related inputs to the design process. Additionally, a cognizant representative of Risk and Reliability is present at design reviews, ~~and status meetings~~. Through these interfaces, Risk and Reliability can identify ~~discrepancies~~ between the performance of risk-significant SSCs and the reliability assumptions in the PRA. Meetings between Risk and Reliability and the designer are then held to ~~resolve discrepancies~~.

16.2.6 Objective

The objective of the D-RAP is to design reliability into the plant and to maintain the AP600 reliability consistent with the NRC-established PRA safety goals.

The following goals have been established for the D-RAP:

- Provide reasonable assurance that
  - The AP600 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP600 PRA for these risk-significant SSCs
  - The risk-significant SSCs do not degrade to an unacceptable level during plant operations
  - The frequency of transients that challenge the AP600 risk-significant SSCs are minimized
  - The risk-significant SSCs function reliably when they are challenged
- Provide a mechanism for establishing baseline reliability values for risk-significant SSCs identified by the risk determination methods used to implement the Maintenance Rule (10 CFR 50.65) and consistent with PRA reliability and availability design basis assumptions used for the AP600 design
- Provide a mechanism for establishing baseline reliability values for SSCs consistent with the regulatory treatment of nonsafety systems (RTNSS) process
- Provide a mechanism for establishing baseline reliability values for SSCs consistent with the defense-in-depth functions to minimize challenges to the safety-related systems
- Generate design and operational information to be used by a Combined License

applicant for ongoing plant reliability assurance activities

The site-specific portion of the D-RAP (Phase III) is the responsibility of the Combined License applicant.

The Combined License applicant ~~should submit~~ its D-RAP organization description ~~for~~ NRC ~~review.~~

The goal of the Combined License applicant's O-RAP ~~should be to ensure that~~ reliability ~~is maintained~~ consistent with overall safety goals and ~~that~~ the capability to perform safety-related functions ~~is maintained~~. Individual component reliability values are expected to change throughout the course of plant life because of aging and changes in suppliers and technology. Changes in individual component reliability values are acceptable as long as overall plant safety performance is maintained within the NRC-established PRA safety goals and the deterministic licensing design bases.

16.2.7 D-RAP, Phase I

Phase I, the definition portion of the D-RAP, includes the initial identification of SSCs to be included in the program, implementation of the aspects applicable to design efforts, and definition of the scope, requirements, and implementation options to be included in the later phases.

16.2.7.1 SSCs Identification and Prioritization

The initial task of the D-RAP is identification of risk-significant SSCs to be included within the scope of the program. As shown in Figure 16.2-1, the AP600 PRA ~~and the AP600 implementation of the RTNSS process are sources~~ used to identify those SSCs ~~and their critical failure modes~~. The review of light water reactor industry experience and industry notices (such as licensee event reports) support the process. An expert panel is also employed in the selection process.

PRA-based measurements provide information that contributes to the identification and prioritization of SSCs. A component's ~~risk achievement worth~~ (RAW) is the factor by which the plant's core damage frequency increases if the component reliability is assigned the value 0.0. ~~In selecting a risk-achievement worth threshold for identifying critical components, it was considered that the AP600 has a core damage frequency approximately two orders of magnitude lower than that of currently operating pressurized water reactors. Thus, a threshold risk achievement worth of at least 10 for any given component supports an AP600 core damage frequency that is 10 times better than that of currently operating reactors.~~ Components with risk achievement worth values of 10 or greater ~~will be included~~ in the D-RAP.

~~Risk reduction worth~~ (RRW) is used in the selection process. A component's risk reduction worth is the amount by which the plant's core damage frequency decreases if the component's

reliability is assigned the value 1.0. A threshold measure of ~~1.2~~ or greater is used as the cutoff. ~~Given the low core damage frequency of AP600, this is considered appropriate.~~ Components with ~~risk reduction worth of 1.2~~ or greater will be included in the D-RAP.

~~Fussel-Vesely worth (FVW)~~ is also used in the screening process. This is a measure of an event's contribution to the overall plant core damage frequency. Components with Fussel-Vesely worth of ~~20~~ percent or greater are ~~included~~ in the D-RAP.

~~The RTNSS process is~~ also instrumental in identifying risk-significant SSCs. ~~This process contains both probabilistic and deterministic elements and is described in Reference 1. A PRA sensitivity study (Reference 2) was performed to calculate core damage frequency and large release frequency assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. This sensitivity study is referred to as the focused PRA.~~ The deterministic identification of risk-significant SSCs encompasses the following guidelines and considerations:

- ATWS rule (10 CFR 50.62)
- Loss of all ac power (10 CFR 50.63)
- Post-72-hour actions
- Containment performance
- Adverse interactions with the AP600 safety-related systems
- Seismic considerations

Nonsafety-related systems identified as risk-significant are considered in the scope of the D-RAP:

- Diverse actuation system
- Non-Class 1E dc and uninterruptible power supply system
- Offsite power, main ac power, and onsite standby power systems
- Normal residual heat removal system
- Component cooling water system
- Service water system

Finally, risk-significant SSCs are selected using industry experience, regulations, and engineering judgment.

16.2.7.1.1 Level 1 PRA and Shutdown Analysis

The Level 1 PRA evaluates accident sequences from initiating events and failures of safety functions to core damage events. The probability of core damage and the identification of dominant contributors to that state are also determined in this analysis.

A low-power and shutdown assessment ~~was~~ conducted to address concerns about risk of operations during shutdown conditions. It encompasses operation when the reactor is in a subcritical state or is in a transition between subcriticality and power operation up to 5 percent of rated power. It consists of a Level 1 PRA and an evaluation of release frequencies and

magnitudes.

Included in the D-RAP are events that meet the threshold risk achievement worth, risk reduction worth, or Fussel-Vesely worth values defined in subsection 16.2.7.1.

16.2.7.1.2 Level 2 Analysis

The Level 2 analysis predicts the plant response to severe accidents and offsite fission product releases. Specifically, the analysis includes the following sections:

- Evaluating severe accident phenomena and fission product source terms
- Modeling the containment event tree
- Analyzing hydrogen burn, mixing, and ignitor placement
- Modeling the AP600 utilizing the MAAP4 code

Equipment used in the prevention of severe accidents and severe post-accident boundary conditions is credited in the Level 1 and Level 2 PRA analyses. An example of this preventive equipment is the reactor coolant system automatic depressurization system (ADS). Successful depressurization leads to core cooling, and in the event that injection fails, results in a low pressure core damage sequence that has fewer uncertainties and can be more easily mitigated than high pressure core damage.

The containment event tree used in the AP600 Level 2 PRA examines the operation of equipment which mitigates the threat to the containment from severe accident phenomena. The systems credited for the mitigation of large fission product releases are containment isolation, passive containment cooling water (PCS), and operator action to flood the cavity by opening the recirculation valves and energizing the hydrogen ignitors.

16.2.7.1.3 External Event Analyses

These analyses consider the events whose cause is external to all the systems associated with normal and emergency operations situations. They include the following:

- Internal flood
- Seismic margins analysis
- External events evaluations (such as high winds and tornados, external floods, and transportation accidents)
- Fire

The internal flood analysis identifies, analyzes, and quantifies the core damage risk contribution as a result of internal flooding during at-power and shutdown conditions. The analysis models potential flood vulnerabilities in conjunction with random failures modeled

as part of the internal events PRA.

The seismic margins analysis identifies potential vulnerabilities and demonstrates seismic margin beyond the safe shutdown earthquake. The capacity of those components required to bring the plant to a safe, stable shutdown is evaluated.

16.2.7.1.4 Expert Panel

Meetings were held among Systems Engineering, PRA, and Reliability Engineering to ~~identify additional~~ SSCs that should be included in the D-RAP. As shown in Figure 16.2-1, industry-wide information sources and engineering judgment were employed in considering the addition of SSCs to the D-RAP.

16.2.7.1.5 SSCs to be Included in D-RAP

Table 16.2-1 lists the non-site-specific SSCs included in the D-RAP. In Figure 16.2-1, this list is denoted as "Risk-significant items (non-site-specific)." For each item listed in the "SSC" column, there is a corresponding "Rationale" given. Items whose values exceed the thresholds for ~~risk achievement, risk reduction, or Fussel-Vesely~~ are included and noted as such. Other SSCs are included based upon their significance to ~~RTNSS~~, Level 2 analysis, external event analyses, or seismic margin analysis. Additional items are included based upon an expert panel review. The "~~Remarks~~" column provides additional insights into the selection process.

The use of ~~the risk reduction worth,~~ Fussel-Vesely worth~~, and external event criteria~~ resulted in no SSC selections.

16.2.7.2 D-RAP, Phase II

During Phase II of the D-RAP, maintenance assessments and recommendations are developed ~~by the designer~~ to enhance the reliability of the plant risk-significant components. These activities are shown in Figure 16.2-1 as "Recommended Plant Maintenance Monitoring Activities." The recommendations can take the form of monitoring activities or preventive, predictive or corrective maintenance, and are dependent upon the types of failure modes that a component may experience. These modes are generally determined by a failure modes, effects and criticality analysis. The maintenance recommendations address the most significant failure modes of the component.

16.2.7.2.1 Information Available to Combined License Applicant

To support the Combined License applicant's D-RAP ~~Phase III~~ and O-RAP, the following information is provided ~~at the end of Phase II~~:

- The list of risk-significant SSCs identified during the design phase
- The PRA assumptions for component unavailability and failure data~~, provided in Chapter 32 of the PRA report.~~

- The analyses performed for components identified as major contributors to total risk, with the dominant failure modes identified and prioritized. The suggested means for prevention or mitigation of these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.

- Reference 1 provides recommended short-term availability controls for nonsafety-related SSCs that perform the functions identified as RTNSS-important. These recommendations include the operational modes when the systems are risk significant, the recommended modes for extended maintenance operations on the system, and remedial actions if the system is not available.

16.2.7.3 D-RAP, Phase III

Site-specific activities of the D-RAP are the responsibility of the Combined License applicant. Figure 16.2-1 shows these activities in the Phase III area of the figure. At this stage, the designer's D-RAP package must be modified or appended based on considerations specific to the site. An example of this would be assignment of additional components to the risk-significant list. The Combined License applicant should use the Phase I and II processes as a guide during this phase of the program. The Combined License applicant's Expert Panel should be composed of personnel knowledgeable in the systems, operations, and maintenance of a plant. Furthermore, these personnel should have the breadth of experience necessary to perform the site-specific SSC selections and evaluations for the RAP.

16.2.7.4 D-RAP Implementation

The following is an example of a system that was reviewed and modified under the D-RAP, Phases I and II. The design and analytical results presented here are intended as an example and do not necessarily reflect the current AP600 design.

The automatic depressurization system, which is part of the reactor coolant system, acts in conjunction with the passive core cooling system to mitigate design basis accidents. Its function is to reduce reactor coolant system pressure in a controlled fashion to allow the required flow rates from the lower pressure injection supplies (core makeup tanks, accumulators, and in-containment refueling water storage tank). It is required primarily to mitigate small-break loss-of-coolant accidents (LOCAs). The automatic depressurization system function is discussed in subsection 5.4.6 of the SSAR.

The earlier automatic depressurization system design contained four depressurization stages, with motor-operated valves in all stages. Preliminary PRA analysis established that fourth stage failure, in certain combination with failures of other stages, was a major contributor to core damage frequency. Thus, it was concluded that the fourth stage valves should be diverse in design from the valves in other stages to reduce common cause failure.

As a result of joint meetings among the AP600 PRA, Design, and staff organizations to discuss core melt frequency improvements, the fourth stage automatic depressurization system was changed from a motor-operated valve to a squib (explosively actuated) valve. The new

configuration of the system is shown in the reactor coolant system P&ID (Figure 5.1-5 of the SSAR). An example of the analytical results that reflect this change is provided in Table 16.2-2.

As part of the evaluation of the squib valves, a failure modes and effects ~~criticality~~ analysis (FMECA) was prepared to identify subcomponent failures and critical items that could lead to hazardous or abnormal conditions of the automatic depressurization system and the plant. The identification of failure modes facilitated the development of recommended maintenance and in-service testing activities to maximize valve reliability.

The squib valve is a completely static electromechanical assembly. Prior to activation, there are no moving parts. No powered components are needed to hold a stem seat or globe in place by torque, solenoid coils, or friction. ~~Typically, for a period of two refueling outage cycles, adjustments, switch setting checks, or component replacement are not required; however, due to the inherent nature of an explosive material, the primer chamber assembly must be replaced within 5 years~~. An explosive actuator is a simple, passive device ~~which does not require in-service testing. The integrity of the electrical circuit to the explosive actuator can be continuously verified by a trickle current.~~

Because the automatic depressurization system fourth stage valves perform safety-related functions, they will be subject to in-service testing to verify that they are ready to function in an accident. Subsection 3.9.6 of the SSAR includes in-service testing requirements for these valves.

~~Table 16.2-3 consolidates sample FMECA results from both the fourth stage squib valves and the second and third stage motor-operated valves. These components rank high in risk-significance priority for the automatic depressurization system. The failure modes are provided, along with maintenance/surveillance recommendations and the rationale for the recommendations.~~

16.2.8 Combined License Activities – ●-RAP

These activities are represented in Figure 16.2-1 as "Plant Maintenance Program."

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. Reference 3 contains examples of cost-effective maintenance enhancements, such as condition monitoring and shifting time-directed maintenance to condition-directed maintenance.

The Maintenance Rule (10 CFR 50.65) is relevant to the Combined License applicant's maintenance activities in that it prescribes SSC performance-related goals during plant operation.

~~The~~ objectives of the ●-RAP ~~should be integrated~~ into the ~~Combined License applicant's~~ Quality Assurance Program developed to implement 10 CFR 50, Appendix B.

In addition to performing the specific tasks necessary to maintain SSC reliability at its required level, the activities ~~should~~ include ~~those elements~~:

C-RAP

- Reliability data base – Historical data available on equipment performance. The compilation and reduction of this data provides the plant with ~~an initial key~~ source of component reliability information. ~~After plant operation begins, this data base will grow and become more useful in the Combined~~ License applicant's ~~O-RAP.~~

- Surveillance and testing – In addition to maintaining the performance of the components necessary for plant operation, surveillance and testing provides a high degree of reliability for the safety-related SSCs.

- Maintenance plan – ~~Intended to provide high [illegible]pment reliability by taking into account manufacturer's recommendations and operating experience,~~ This plan describes the nature and frequency of maintenance activities to be performed on plant equipment. The plan includes the selected SSCs identified in the D-RAP~~, that are periodically evaluated~~.

16.2.9 Glossary of Terms

~~ADS~~	~~Automatic depressurization system~~
D-RAP	Design Reliability Assurance Program – performed as part of the AP600 design effort to assure that the reliability assumptions of the PRA remain valid throughout the plant operating lifetime.
FVW	Fussel - Vesely Worth
O-RAP	Operational Reliability Assurance Process
PRA	Probabilistic Risk Assessment
RAW	Risk Achievement Worth
Risk-significant	Any SSC determined in the PRA or by risk-significance analysis (e.g., Level 2 PRA and shutdown risk analysis) to be a major contributor to overall plant risk
RRW	Risk Reduction Worth
RTNSS	Regulatory treatment of Nonsafety-related Systems
SSC	Structures, Systems, and Components

16.2.10 References

1. Brockhoff, C. S., Haag, C. L., More, D. G., Sterdis, A. L., "AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," WCAP-13856, September 1993.

2. AP600 Probabilistic Risk Assessment, ~~1995~~. June 1996.

3. Lofgren, E. V., Cooper, et al, "A Process for Risk-Focused Maintenance," NUREG/CR-5695, March 1991.

4. Letter from NRC to Westinghouse "Criteria for Establishing Risk Significant Structures, Systems and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program," January 16, 1997.

Table 16.2-1 (Sheet 1 of 13)

RISK SIGNIFICANT SSCs UNDER THE SCOPE OF D-RAP

SSC[1]	Rationale[2]	Insights and Assumptions
System: Reactor Coolant System	RAW ≥ 10, EP, Level 2	The RCS removes heat from the reactor core and transfers it to the secondary side of the steam generator for power generation. The RCS also provides for overpressure protection, automatic depressurization to support core cooling following LOCAs, and RCP trip to support CMT operation.
Component: Reactor coolant pump trip breakers	RAW ≥ 10 (CCF)[4]	These breakers open automatically to allow core makeup tank operation.
Component: Pressurizer safety valves	EP	These valves provide overpressure protection of the reactor coolant system.
Component: Automatic depressurization system Stage 1/2/3 motor-operated valves	Level 2, EP	The automatic depressurization system provides a controlled depressurization of the reactor coolant system following loss-of-coolant accidents to allow core cooling from the accumulator, in-containment refueling water storage tank injection, and containment recirculation. The automatic depressurization system provides "bleed" capability for feed/bleed cooling of the core. The automatic depressurization system also provides depressurization of the reactor coolant system to prevent a high-pressure core melt sequence.

Replace entire table with the attached table

Table ~~*~~ 16.2-1 (all pages)

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
System: Component Cooling Water (CCS)		
CCS Pumps	EP	These pumps provide cooling of the normal residual heat removal system (RNS) and the ~~startup feedwater system~~ spent fuel pool heat exchanger. Cooling the RNS heat exchanger is RTNSS-important during shutdown reduced-inventory conditions. CCS valve realignment is not required for reduced-inventory conditions.
System: Containment System (CNS)		
Containment Vessel	EP, L2	The containment vessel provides a barrier to steam and radioactivity released to the atmosphere following accidents.
Hydrogen Ignitors	EP, L2, Regulations	The hydrogen ignitors provide a means to control H_2 concentration in the containment atmosphere, consistent with the hydrogen control requirements of 10 CFR 50.34f.
System: Chemical and Volume Control System (CVS)		
CVS Makeup Pump Suction and Discharge Check Valves	RAW	These CVS check valves are ~~manually~~ normally closed and have to open to allow makeup pump operation.
CVS Makeup Pumps	RAW/CCF	These pumps provide makeup to the RCS to accommodate leaks and to provide negative reactivity for shutdowns, steam line breaks, and ATWS.
System: Diverse Actuation System (DAS)		
Turbine Impulse Pressure Transmitters 001 and 002	RAW	These sensors provide signals used as permissives for the DAS automatic reactor trip function.
Containment Isolation Valves Controlled by DAS	EP, L2	These containment isolation valves are important in limiting offsite releases following core melt accidents.
DAS Actuation Hardware (sensor input through control output and indication)	RAW	The DAS is diverse from the PMS and provides automatic actuation of selected plant features including control rod insertion, turbine trip, passive residual heat removal (PRHR) heat exchanger actuation, core makeup tank actuation, isolation of critical containment lines, and passive containment cooling system (PCS) actuation.
Distribution Panels EDS1-EA-14 and EDS2-EA-14	RAW	These panels distribute power to the DAS equipment.

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
Control Rod MG Set Field Breakers	RAW	These breakers open on a DAS reactor trip signal demand to de-energize the control rod MG sets and allow the rods to drop.
System: Main ac Power System (ECS)		
Ancillary Diesel Generators	EP	For post-72 hour actions, these generators are available to provide power for Class 1E monitoring, MCR lighting and for refilling the PCS water storage tank.
System: Main and Startup Feedwater System (FWS)		
Startup Feedwater Pumps	EP	The startup feedwater system pumps provide feedwater to the steam generator. This capability provides an alternate core cooling mechanism to the PRHR heat exchangers for non-loss-of-coolant-accidents or steam generator tube ruptures.
System: General I&C[4]		
Low Pressure/DP Sensors - IRWST level sensors	RAW/CCF	The in-containment refueling water storage tank (IRWST) level sensors support PMS and DAS functions. They are utilized in automatic actuation and they provide indications to the operator. IRWST level supports IRWST recirculation actions.
High Pressure/DP Sensors list here	RAW/CCF	The following sensors are included in this group: main feedwater flow, startup feedwater flow, pressurizer pressure and level, steam generator wide- and narrow-range level, RCS hot leg level and steamline pressure. These sensors support PMS, DAS and PLS functions. They are utilized in reactor trip and ESF functions, and provide indications to the operator. Main feedwater flow sensors support startup feedwater actuation and startup feedwater flow sensors support PRHR actuation. The hot leg level sensors automatically actuate the IRWST and provide information to the operator for manual actuation of the automatic depressurization system (ADS).
System: Class 1E DC Power and Uninterruptible Power System (IDS)		
125 Vdc Distribution Panels	RAW	These panels distribute power to components in the plant that require 1E dc power support.

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
125 Vdc 24-hour Batteries, Inverters, and Chargers	RAW/CCF	The batteries provide power for the PMS and safety-related valves. The chargers are the preferred source of power for Class 1E dc loads and are the source of charging for the batteries. The inverters provide uninterruptible ac power to the I&C system.
Fused Transfer Switch Box	RAW	The fused disconnect switches connect the different levels of Class 1E distribution panels.
125 Vac Motor Control Centers	EP	These buses provide power for the PMS and safety-related valve operation.
Main Control Room (MCR) Displays and System Level Control Mechanisms to Support Operator Actions	RAW/CCF	The Class 1E QDPS, PLS and DAS displays and system level control mechanisms provide important plant indications and variables to allow the operator to monitor and control the plant during normal conditions and during design basis accidents. insert +
Reactor Coolant Pump Circuit Breakers	RAW/CCF	These breakers open automatically to allow core makeup tank operation.
System: Passive Containment Cooling System (PCS)		
PCS Air-Operated Drain Isolation Valves	EP	These valves open automatically to drain water from a water storage tank onto the outside surface of the containment shell. This water provides evaporative cooling of the containment shell following accidents.
PCS Water Storage Tank Recirculation Pumps	EP	These pumps provide the motive force to refill the PCS water storage tank during post-72 hour support actions.
System: Plant Control System (PLS)		
PLS Actuation Hardware	RAW/CCF	This common cause failure event is assumed to disable all logic outputs from the PLS (insert B)
PLS Logic Cabinet Supporting CVS Functions	RAW/CCF	This is the distributed controller that supports the CVS function.
PLS common cause failure with PMS	RAW/CCF	This common cause failure is assumed to affect both PMS and PLS functions.
System: Protection and Safety Monitoring System (PMS)		
CMT Level Sensors	RAW/CCF	These level sensors ~~are heated RTDs which~~ provide input for automatic actuation of the ADS. They also provide indications to the operator.

This includes the Class 1E PMS (QDPS) and DAS displays and controls. It also includes the PLS displays and controls associated with CVS reactor makeup, RNS reactor injection from the IRWST, spent fuel cooling, component cooling of RNS and SFS heat exchangers, service water cooling of CCS heat exchangers, standby diesel generators, and hydrogen igniters. These displays and system level control mechanisms provide important plant indications and variables to allow the operator to monitor and control the plant during normal conditions and during design basis accidents.

Insert (A)

Insert (B)

associated with CVS reactor makeup, RNS reactor injection from the IRWST, spent fuel cooling, component cooling of RNS and SFS heat exchangers, service water cooling of CCS heat exchangers, standby diesel generators, and hydrogen igniters.

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
PMS Actuation Software	RAW/CCF	The PMS software modules include field input signal processing, control board signal input processing, actuation logic algorithms and output logic functions.
Reactor Trip Switch Gear	RAW/CCF	These breakers open automatically to allow insertion of the control rods.
PMS Actuation Hardware	RAW/CCF	The PMS hardware includes the following: IPC Reactor Trip Subsystems IPC ESF Subsystems ESF Actuation Cabinets Protection Logic Cabinets Manual Input Multiplexers
System: Passive Core Cooling System (PXS)		
Containment Recirculation Isolation MOVs	EP, L2	The containment recirculation lines provide long-term core cooling following a loss-of-coolant accident (LOCA). The motor-operated valves open automatically to allow containment recirculation when the IRWST level is reduced to about the same level as the containment. The motor-operated valves also allow long-term core cooling to be provided by the RNS pumps. These valves together with the IRWST recirculation squib valves can provide a rapid flooding of the containment to support in-vessel retention during a severe accident.
IRWST Check Valves	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. These check valves open when the IRWST level is reduced to approximately the same level as the containment level.
IRWST Injection Squib Valves	RAW/CCF	The IRWST injection lines provide long-term core cooling following a LOCA. These squib valves open automatically to allow injection when the RCS pressure is reduced to below the IRWST injection head.
IRWST Screens	RAW/CCF	The IRWST injection lines provide long-term core cooling following a LOCA. These screens are located inside the IRWST and prevent large particles from being injected into the RCS. They are designed so that they will not become obstructed.

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
Containment Recirculation Squib Valves	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. These squib valves open automatically to allow containment recirculation when the IRWST level is reduced to about the same level as the containment level. These squib valves can also allow long-term core cooling to be provided by the RNS pumps. These squib valves together with the containment recirculation motor-operated valves can provide a rapid flooding of the containment to support in-vessel retention during a severe accident.
Containment Recirculation Screens	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. The screens are located in the containment and prevent large particles from being injected into the RCS. They are designed so that they will not become obstructed.
IRWST Gutter Bypass Isolation Valves	EP	These valves direct water collected in the IRWST gutter to the IRWST. This capability extends PRHR heat exchanger operation.
Accumulator Discharge Check Valves	RAW/CCF	These check valves open when the RCS pressure drops below the accumulator pressure to allow accumulator injection.
CMT Discharge Isolation Valves	RAW/CCF	These air-operated valves automatically open to allow core makeup tank injection.
CMT Discharge Check Valves		These check valves are normally open. They close during rapid accumulator injection.
PRHR Heat Exchanger Control Valves	RAW/CCF	The PRHR heat exchangers provide core cooling following non-LOCAs, steam generator tube ruptures, and anticipated transients without scram. The air-operated valves automatically open to initiate PRHR heat exchanger operation.
System: Reactor Coolant System (RCS)		

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
ADS Stages 1/2/3 Motor-Operated Valves	EP, L2	The ADS provides a controlled depressurization of the RCS following LOCAs to allow core cooling from the accumulator, IRWST injection, and containment recirculation. The ADS provides "bleed" capability for feed/bleed cooling of the core. The ADS also provides depressurization of the RCS to prevent a high-pressure core melt sequence.
ADS 4th Stage Squib Valves	RAW/CCF	The ADS provides a controlled depressurization of the RCS following LOCAs to allow core cooling from the accumulator, IRWST injection, and containment recirculation. The ADS provides "bleed" capability for feed/bleed cooling of the core. The ADS also provides depressurization of the RCS to prevent a high-pressure core melt sequence.
Pressurizer Safety Valves	EP	These valves provide overpressure protection of the RCS.
System: Normal Residual Heat Removal System (RNS)		
RNS Pumps	EP	These pumps provide shutdown cooling of the RCS. They also provide an alternate RCS lower pressure injection capability following actuation of the ADS. The operation of these pumps is RTNSS-important during shutdown reduced-inventory conditions. RNS valve realignment is not required for reduced-inventory conditions.
RNS Motor-Operated Valves	RRW/FVW	These MOVs align a flowpath for nonsafety-related makeup to the RCS following ADS operation.
System: Spent Fuel Cooling System (SFS)		
SFS Pumps	EP	These pumps provide flow to the heat exchangers for removal of the design basis heat load.
System: Steam Generator System (SGS)		
Main Steam Isolation Valves	RAW	The steam generator main steam isolation valves provide isolation of the steam generator following secondary line breaks and steam generator tube rupture.
Main Steam Safety Valves	EP	The steam generator main steam safety valves provide overpressure protection of the steam generator. They also provide core cooling by venting steam from the steam generator.

Table 1

RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC)[1]	Rationale[2]	Insights and Assumptions
System: Service Water System (SWS)		
Service Water Pumps and Cooling Tower Fans	EP	These pumps and fans provide cooling of the CCS heat exchanger which ~~Providing cooling of the CCS heat exchanger~~ is RTNSS-important during shutdown reduced-inventory conditions. Service water system valve realignment is not required for reduced-inventory conditions.
System: Nuclear Island Nonradioactive Ventilation System (VBS)		
VBS MCR and I&C Rooms B/C Ancillary Fans	EP	For post-72 hour actions, these fans are available to provide cooling of the MCR and the two I&C rooms (B/C) that provide post-accident monitoring.
System: Chilled Water System (VWS)		
VWS Low Capacity Subsystem	RAW/CCF	This VWS subsystem provides chilled cooling water to the CVS makeup pump room. The motor-driven pumps, chillers and unit cooler fans are important components of the VWS.
System: Onsite Standby Power System (ZOS)		
Nonsafety-related Standby Diesel Generators	EP	These diesels provide ac power to support operation of nonsafety-related equipment such as the startup feedwater pumps, CVS pumps, RNS pumps, CCS pumps, SWS pumps, and the PLS. Providing ac power to the RNS and the equipment necessary to support its operation is RTNSS-important ~~for~~ for reduced inventory conditions.
Standby Diesels Room Cooling Fans	EP	These fans provide cooling of the rooms containing the standby diesel generators.
Nuclear Fuel	SMA	The nuclear fuel includes the fuel pellets, fuel cladding, and associated support structures. This equipment, which provides a first barrier for release of radioactivity and allows for effective core cooling, had the least margin in the seismic margin analysis.

Notes:

1. Only includes equipment at the **component** level. Other parts of the SSC or support systems are not included unless specifically listed.
2. Definition of Rationale Terms:
   - CCF = Common Cause Failure (for the SSCs whose inclusion rationale is RAW/CCF, the RAW is based on common cause failure of two or more of the specified SSCs.
   - EP = Expert Panel
   - RAW = Risk Achievement Worth

RRW = Risk Reduction Worth
SMA = Seismic Margin Analysis

3. Maintenance/surveillance recommendations for equipments are documented in each appropriate SSAR section.
4. This category captures instrumentation and control equipment common cause failures across systems.

Table 16.2-2

EXAMPLE OF RISK-SIGNIFICANT RANKING OF SSCs FOR THE AUTOMATIC DEPRESSURIZATION SYSTEM

Rank[1]	Event Code	Description
1	ED3MOD07	EDS3 EA1 distribution panel failure or unavailable due to testing and maintenance
2	AD4MOD07, AD4MOD08, AD4MOD09, AD4MOD10	Hardware failure of 2 of 4 automatic depressurization system Stage 4 lines (includes squib valves)
3	EC1BS001TM, ECBS012TM, EC1BS121TM, EC2BS002TM, EC2BS022TM,EC2BS221TM	Unavailability of bus ECS ES due to unscheduled maintenance
4	AD2MOD01, AD2MOD02, AD2MOD03, AD2MOD04	Hardware failure of automatic depressurization system Stages 2 and 3 of lines 1 and 2 (includes motor-operated valves)
5	EC0MOD01	Main generator breaker ES01 fails to open
6	ED3MOD01	Fixed component fails: circuit breaker, inverter or static transfer switch
7	ZO1MOD01, Z02MOD01	Diesel generator fails to start and run or breaker 102 fails to close
8	Z02DG001TM, Z02DG001TM	Standby diesel generator unavailable due to testing and maintenance

Note:
1. The ranking is the order of the decreasing risk achievement component importance.

Table 16.2-3

EXAMPLE OF AUTOMATIC DEPRESSURIZATION SYSTEM FAILURE MODES AND RECOMMENDED O-RAP ACTIVITIES

Component	Failure Mode	Effect on System Operation	Recommended Tests/Maintenance	Remarks
Automatic depressurization system Stage 2 and 3 motor-operated valves	Failure to open on demand	Failure to open blocks reactor coolant system vent flow through one of two parallel branch lines of the affected automatic depressurization system valve stage.	Functional test every 6 months.	Testing represents a risk of reactor coolant system depressurization, and therefore should be minimized.
Automatic depressurization system Stage 4 squib valves	Failure to open on demand	Failure of a Stage 4 automatic depressurization system valve is the most limiting single valve failure from the standpoint of automatic depressurization system performance, based on this stage being the largest valve size. With the limiting Stage 4 automatic depressurization system valve failure, the automatic depressurization system vent flow capacity is reduced, but safety analysis has demonstrated that the automatic depressurization system still meets design basis reactor coolant venting requirements.	Test firing of explosive charge in accordance with ASME Code staggered test guidelines. Continuous trickle current verification of the explosive actuator circuit.	ASME Code guidelines enhanced by results of squib valve failure modes and effects analysis criteria.

Delete

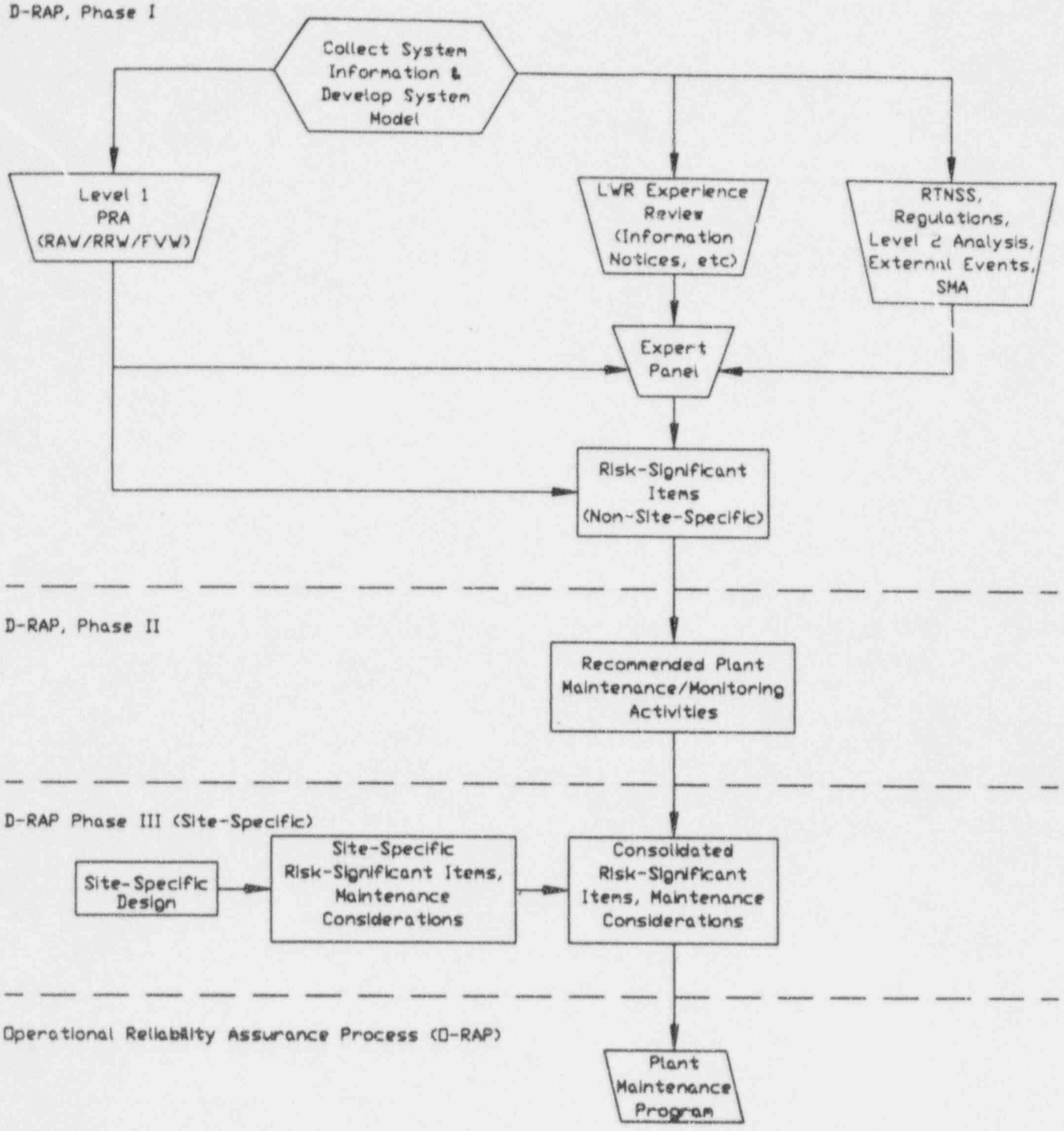

Figure 16.2-1

Design Reliability Assurance Program and O-RAP