Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

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

Direct tel: 412-374-6306
Direct fax: 412-374-5005
e-mail: sterdia@westinghouse.com

Your ref: Project Number 740
Our ref: DCP/NRC2075

52-06
52-14
52-15

January 29, 2008

Subject: AP1000 COL Standard Technical Report Submittal of APP-GW-GLR-117, Revision 1 (TR 117)

In support of Combined License application pre-application activities, Westinghouse is submitting Revision 1 of AP1000 Standard Combined License Technical Report Number 117. This report identifies and justifies standard changes to Chapter 17 in the AP1000 Design Control Document (DCD). The purpose of this revision to TR117 is to clarify the association between the new Maintenance Rule Program and the previously used Operational Reliability Assurance Program (ORAP). This revision is in response to NRC concerns raised and discussed in a teleconference between Billy Gleaves and Sam Adams on December 12, 2007. The changes to the DCD that are identified in this report consist of both changes that are included in Revision 16 of the DCD as well as changes to Revision 16 of the DCD. This report is submitted as part of the NuStart Bellefonte COL Project (NRC Project Number 740). The information included in this report is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification.

The purpose for submittal of this report was explained in a March 8, 2006 letter from NuStart to the NRC.

Pursuant to 10 CFR 50.30(b), APP-GW-GLR-117, Revision 1, "Incorporation of the Maintenance Rule," Technical Report Number 117, is submitted as Enclosure 1 under the attached Oath of Affirmation. Revision 0 of Technical Report Number 117 was submitted to the NRC under Westinghouse letter DCP/NRC1898 dated May 24, 2007.

It is expected that when the NRC review of Technical Report Number 117 is complete, the changes to the DCD proposed in the report will be considered approved for all COL applicants referencing the AP1000 Design Certification.

Questions or requests for additional information related to content and preparation of this report should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Westinghouse requests the NRC to provide a schedule for review of the technical report within two weeks of its submittal.



D085
D063

NRO

Very truly yours,

A. Sterdis, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Attachment

1. "Oath of Affirmation," dated January 29, 2008

/Enclosure

1. APP-GW-GLR-117, Revision 1, "Incorporation of the Maintenance Rule," Technical Report Number 117

| | | | | | |
|---|---|---|---|---|---|
| cc: | D. Jaffe | - | U.S. NRC | 1E | 1A |
| | E. McKenna | - | U.S. NRC | 1E | 1A |
| | P. Ray | - | TVA | 1E | 1A |
| | P. Hastings | - | Duke Power | 1E | 1A |
| | R. Kitchen | - | Progress Energy | 1E | 1A |
| | A. Monroe | - | SCANA | 1E | 1A |
| | J. Wilkinson | - | Florida Power & Light | 1E | 1A |
| | C. Pierce | - | Southern Company | 1E | 1A |
| | E. Schmiech | - | Westinghouse | 1E | 1A |
| | G. Zinke | - | NuStart/Entergy | 1E | 1A |
| | R. Grumbir | - | NuStart | 1E | 1A |
| | C. Steuck | - | Westinghouse | 1E | 1A |

ATTACHMENT 1

"Oath of Affirmation"

ATTACHMENT 1

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

| | |
|---|---|
| In the Matter of: | ) |
| NuStart Bellefonte COL Project | ) |
| NRC Project Number 740 | ) |

APPLICATION FOR REVIEW OF
"AP1000 GENERAL COMBINED LICENSE INFORMATION"
FOR COL APPLICATION PRE-APPLICATION REVIEW

W. E. Cummins, being duly sworn, states that he is Vice President, Regulatory Affairs and Standardization, for Westinghouse Electric Company; that he is authorized on the part of said company to sign and file with the Nuclear Regulatory Commission this document; that all statements made and matters set forth therein are true and correct to the best of his knowledge, information and belief.

W. E. Cummins
Vice President
Regulatory Affairs and Standardization

Subscribed and sworn to
before me this 29th day
of January 2008.

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Patricia S. Aston, Notary Public
Murrysville Boro, Westmoreland County
My Commission Expires July 11, 2011
Member, Pennsylvania Association of Notaries

Patricia S. Aston
Notary Public

ENCLOSURE 1

APP-GW-GLR-117, Revision 1

"Incorporation of the Maintenance Rule"

Technical Report 117

# AP1000 DOCUMENT COVER SHEET

TDC:_____ Permanent File:_____

| AP1000 DOCUMENT NO. | REVISION | PAGE | ASSIGNED TO | OPEN ITEMS (Y/N) |
|---|---|---|---|---|
| APP-GW-GLR-117 | 1 | 1 of 24 | W-MCGINNIS | N |

ALTERNATE DOCUMENT NUMBER: TR 117 WORK BREAKDOWN #: NA

ORIGINATING ORGANIZATION: Westinghouse Electric Company

TITLE: **Incorporation of the Maintenance Rule**

| ATTACHMENTS: | DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: |
|---|---|
| NA | NA |
| CALCULATION/ANALYSIS REFERENCE: NA | |

| ELECTRONIC FILENAME | ELECTRONIC FILE FORMAT | ELECTRONIC FILE DESCRIPTION |
|---|---|---|
| APP-GW-GLR-117 R1.doc | Word Document | .doc |



☒ WESTINGHOUSE NON PROPRIETARY CLASS 3

Class 3 Documents being transmitted to the NRC require the following two review signatures in lieu of a Form 36.

| | |
|---|---|
| LEGAL REVIEW T. WHITE | SIGNATURE / DATE T. J. White 1-23-08 |
| PATENT REVIEW William R Rice | SIGNATURE / DATE William R Rice 1/23/08 |

☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

| | | |
|---|---|---|
| ORIGINATOR(S) Steuck, C.M. | SIGNATURE / DATE 1/23/08 | |
| REVIEWER(S) Schulz, T.L. | SIGNATURE / DATE 1/23/08 | |
| | SIGNATURE / DATE | |
| | SIGNATURE / DATE | |
| VERIFIER(S) Evans, M.C. | SIGNATURE / DATE 1/23/08 | Verification Method PAGE BY PAGE |

**__Plant Applicability__: ☒ All AP1000 plants except: No exceptions

☐ Only the following plants:

| | |
|---|---|
| APPLICABILITY REVIEWER** J. A. Speer | SIGNATURE / DATE 1/23/08 |
| RESPONSIBLE MANAGER* McGinnis, C.A. | SIGNATURE / DATE 1/23/08 |

* Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to the EDMS, and the document is released for use.

*** ***Electronically approved records were authenticated in the electronic document management system.***

APP-GW-GLR-117
Revision 1

January 2008

# AP1000 Standard Combined License Technical Report

## Incorporation of the Maintenance Rule

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

## INTRODUCTION

Chapter 17 of the AP1000 Design Control Document (DCD) is being restructured to incorporate the industry's write-up of the Maintenance Rule (MR) Program, NEI 07-02, which is replacing the AP1000 O-RAP. All changes made to the DCD in this document are related to NEI 07-02. The D-RAP will now be an input to the MR Program and will no longer reference O-RAP. The incorporation of the MR Program has closed the COL information items shown below.

17.5-3 The COL applicant or holder will establish PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP.

17.5-5 The following activities are represented in Figure 17.4-1 as "Plant Maintenance Program."

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. Reference 8 contains examples of cost-effective maintenance enhancements, such as condition monitoring and shifting time-directed maintenance to condition-directed maintenance.

17.5-6 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.

17.5-7 In addition to performing the specific tasks necessary to maintain SSC reliability at its required level, the O-RAP activities include:

- Reliability data base – Historical data available on equipment performance. The compilation and reduction of this data provides the plant with source of component reliability information.
- 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 – 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.

Based on this report the NRC should consider the COL information item closure to be acceptable and generically applicable to COL applications referencing the AP1000 design certification.

## TECHNICAL BACKGROUND

Per industry guidance the MR Program is replacing the O-RAP description in the DCD. These changes are referencing the letters submitted by NEI to the NRC for the "Generic FSAR Template Guidance for Maintenance Rule Program Description for Plants Licensed under 10 CFR Part 52" (NEI 07-02).

Sections 17.4.7.2, 17.4.7.2.1, and 17.4.7.3 of the DCD have been deleted as a result of the incorporation of the Maintenance Rule (MR). Section 17.4.7.2 has been deleted as it is will be detailed in the MR Program Sections "Monitoring and corrective action per 10 CFR 50.56(a)(1)," "Preventive maintenance per 10 CFR 50.65(a)(2)," and "Periodic evaluation of monitoring and preventive maintenance per 10 CFR 50.65(a)(3)." Section 17.4.7.2.1 has been deleted as it will be detailed in the MR Program Section "Maintenance Rule scoping per 10 CFR 50.65(b)(1), 10 CFR 50.65 (b)(2) and Risk Significance." Section 17.4.7.3 has been deleted as it will be detailed in the MR Program Section "Maintenance Rule scoping per 10 CFR 50.65(b)(1), 10 CFR 50.65 (b)(2) and Risk Significance."

Discussions with the NRC have led to the need for revising this document. Originally, ORAP was replaced in the DCD with MR Program. This is incorrect as the MR Program is just one of the programs that would be encompassed by what was referred to as ORAP and therefore it is not a one to one replacement. Text has been added to clarify this association.

DCD Revision 15 mark-ups begin on Page 5 and DCD Revision 16 mark-ups begin on Page 18.

## REGULATORY IMPACT

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

Severe accident change criteria

The severe accident change criteria are not applicable because mitigation features are not impacted.

Security

The closure of the COL Information Item will not alter barriers or alarms that control access to protected areas of the plant. The closure of the COL Information Item will not alter requirements for security personnel. Therefore, the closure of the COL Information Item does not have an adverse impact on the security assessment of the AP1000.

**DCD Rev 15 MARK-UP**

# CHAPTER 16
# 16.3 Investment Protection

## 16.3.1 Investment Protection Short-Term Availability Controls

The importance of nonsafety-related systems, structures and components in the AP1000 has been evaluated. The evaluation uses PRA insights to identify systems, structures and components that are important in protecting the utilities investment and for preventing and mitigating severe accidents. To provide reasonable assurance that these systems, structures and components are operable during anticipated events short-term availability controls are provided. These investment protection systems, structures and components are also included in the D-RAP/~~O-RAP~~ MR Program (refer to Subsection 17.4), which provides confidence that availability and reliability are designed into the plant and that availability and reliability are maintained throughout plant life through the maintenance rule. Technical Specifications are not required for these systems, structures and components because they do not meet the selection criteria applied to the AP1000 (refer to subsection 16.1.1).

CHAPTER 17

QUALITY ASSURANCE

## 17.4 Design Reliability Assurance Program

This subsection presents the AP1000 Design Reliability Assurance Program (D-RAP).

### 17.4.1 Introduction

The AP1000 D-RAP is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 probabilistic risk assessment (PRA) (Reference 5) 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 17.4-1, is implemented during ~~in three phases. The first phase, the~~ Design Certification ~~phase, defines the overall structure of the AP1000 D-RAP, and implements those aspects of the program which are applicable to the design process. During this phase.~~, The D-RAP identifies risk-significant SSCs ~~are identified~~ for inclusion in the Maintenance Rule (MR) Program (Reference 10) using probabilistic, deterministic, and other methods.

~~Finally, Figure 17.4-1 shows~~ The MR Program ~~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.

### 17.4.2 Scope

The D-RAP includes a design evaluation of the AP1000 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 used to identify and prioritize those risk-significant SSCs.

### 17.4.3 Design Considerations

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 O-RAP~~ MR Program.

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

### 17.4.4 Relationship to Other Administrative Programs

The D-RAP manifests itself in other administrative and operational programs. 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. 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. Implementation of the Maintenance Rule, 10 CFR 50.65, will provide coverage of the SSC's that would have been included in the O-RAP.

~~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.~~

### 17.4.5 The AP1000 Design Organization

The AP1000 organization of Section 1.4 formulates and implements the AP1000 D-RAP.

The AP1000 management staff is responsible for the AP1000 design and licensing.

The AP1000 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 AP1000 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.

The Risk and Reliability organization is responsible for developing the D-RAP and has direct access to the AP1000 staff. Risk and Reliability is responsible for keeping the AP1000 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. Through these interfaces, Risk and Reliability can identify interfaces 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 manage interface issues.

### 17.4.6 Objective

The objective of the D-RAP is to design reliability into the plant and to maintain the AP1000 reliability consistent with the NRC-established PRA safety goals.

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

- Provide reasonable assurance that
  - The AP1000 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP1000 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 AP1000 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 AP1000 design

- 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

Development of maintenance assessments and recommendations ~~for the D-RAP (Phase II)~~ and the site-specific portion of the program ~~D-RAP (Phase III)~~ is the responsibility of the Combined License applicant under the MR program.

~~The Combined License applicant is responsible for submitting its maintenance recommendations (Phase II) and site specific (Phase III) D-RAP organization description to the NRC.~~

~~The goal of the Combined License applicant's O-RAP is to maintain reliability consistent with overall safety goals and to maintain the capability to perform safety related functions. 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.~~

## 17.4.7 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.

### 17.4.7.1 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 17.4-1, the AP1000 PRA is used to identify those SSCs, consistent with the criteria of Reference 7 for risk achievement worth (RAW), risk reduction worth (RRW), and Fussel-Vesely Worth (FVW). Note that, although Reference 7 was developed for AP600, it is directly applicable to AP1000. The review of light water reactor industry experience and industry notices (such as licensee event reports) supports 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 RAW is the factor by which the plant's core damage frequency increases if the component reliability is assigned the value 0.0. Components with risk achievement worth values of 2 or greater are considered for inclusion in the D-RAP.

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 1.005 or greater is used as the cutoff. Components with RRW of 1.005 or greater are considered for inclusion in the D-RAP.

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 0.5 percent or greater are considered for inclusion in the D-RAP.

Deterministic considerations are also instrumental in identifying risk-significant SSCs. 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 AP1000 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.

#### 17.4.7.1.1 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 is 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 17.4.7.1.

#### 17.4.7.1.2 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 igniter placement
- Modeling the AP1000 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 AP1000 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 igniters.

#### 17.4.7.1.3 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.

#### 17.4.7.1.4 Expert Panel

Meetings were held among Systems Engineering, PRA, and Reliability Engineering to perform the final selection of SSCs that should be included in the D-RAP. As shown in Figure 17.4-1, industry-wide information sources and engineering judgment were employed in considering the addition of SSCs to the D-RAP.

#### 17.4.7.1.5 SSCs to be Included in D-RAP

Table 17.4-1 lists the non-site-specific SSCs included in the D-RAP. In Figure 17.4-1, 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 RAW or RRW are included and noted as such. Other SSCs are included based upon their significance to Level 2 analysis, external event analyses, or seismic margin analysis. Additional items are included based upon an expert panel review. The "Insights and Assumptions" column provides additional insights into the selection process.

The use of Fussel-Vesely worth resulted in no SSC selections.

### 17.4.7.2 Deleted ~~D-RAP, Phase II~~

~~During Phase II of the D-RAP, maintenance assessments and recommendations are developed to enhance the reliability of the plant risk-significant components. These activities are shown in Figure 17.4-1 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.~~

#### 17.4.7.2.1 Deleted ~~Information Available to Combined License Applicant~~

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

~~The list of risk-significant SSCs identified during the design phase (Table 17.4-1)~~

~~The PRA assumptions for component unavailability and failure data (Chapter 32 of the AP1000 PRA [Reference 5])~~

~~The analyses performed for components identified as major contributors to total risk, with the dominant failure modes identified and prioritized. (Chapter 50 of the AP1000 PRA [Reference 5] identifies major contributors to total risk, and Chapters 8 to 28 of the AP1000 PRA describes the analyses of the respective systems and associated components in Table 17.4-1.) The suggested means for prevention or mitigation of these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.~~

### 17.4.7.3 Deleted

~~D-RAP, Phase III~~

~~Site-specific activities of the D-RAP are the responsibility of the Combined License applicant. Figure 17.4-1 shows these activities in the Phase III area of the figure. At this stage, the D-RAP package is modified or appended based on considerations specific to the site.~~

~~The COL applicant will need to establish PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP.~~

~~The Combined License applicant would benefit from using the Phase I and II processes as a guide during this phase of the program. It is the responsibility of the Combined License applicant to ensure its Expert Panel is composed of personnel knowledgeable in the systems, operations, and maintenance of a plant, and that these personnel should have the breadth of experience necessary to perform the site-specific SSC selections and evaluations for the RAP.~~

**17.4.7.4 D-RAP Implementation**

The following is an example of a system that was reviewed and modified under the D-RAP~~, Phase I~~. The design and analytical results presented here are intended as an example.

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. The automatic depressurization system valves are discussed in subsection 5.4.6 of the DCD.

An earlier AP600 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 DCD). An example of the analytical results that reflect this change is provided in Table 17.4-2. This design feature is included in the AP1000 design to maintain the core melt frequency improvements included in the AP600 design.

As part of the evaluation of the squib valves, a failure modes and effects analysis (FMEA) 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. The explosive actuator is a simple, passive device that is triggered by an applied voltage.

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 DCD includes in-service testing requirements for these valves.

Example FMEA results for the fourth stage squib valves and the second and third stage motor-operated valves are included in DCD Table 6.3-3. DCD subsection 3.9.6.3.1 provides testing recommendations for the second and third stage valves.

### 17.4.8 Glossary of Terms

| | |
|---|---|
| D-RAP | Design Reliability Assurance Program – performed as part of the AP1000 design effort to assure that the reliability assumptions of the PRA remain valid throughout the plant operating lifetime. |
| FVW | Fussel-Vesely Worth |
| MR | Maintenance Rule |
| ~~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 Systems |
| SSC | Structures, Systems, and Components |

## 17.5 Combined License Information Items

17.5.1 The Combined License applicant or holder will address its design phase Quality Assurance program.

17.5.2 The Combined License applicant will address its Quality Assurance program for procurement, fabrication, installation, construction and testing of structures, systems and components in the facility. The quality assurance program will include provisions for seismic Category II structures, systems, and components.

17.5.3 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

The COL applicant or holder will establish PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP.

17.5.4 The Combined License applicant or holder will address its Quality Assurance program for operations.

17.5.5 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

The following activities are represented in Figure 17.4-1 as "Plant Maintenance Program."

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. Reference 8 contains examples of cost-effective maintenance enhancements, such as condition monitoring and shifting time-directed maintenance to condition-directed maintenance.

17.5.6 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

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.

17.5.7 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

In addition to performing the specific tasks necessary to maintain SSC reliability at its required level, the O-RAP activities include:

- Reliability data base – Historical data available on equipment performance. The compilation and reduction of this data provides the plant with source of component

reliability information.

- 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 – 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.

17.5.8 The Combined License applicant is responsible for integrating the objectives of the MR Program ~~O-RAP~~ into the Quality Assurance Program developed to implement 10 CFR 50, Appendix B. This program will address failures of non-safety-related, risk-significant SSCs that result from design and operational errors in accordance with SECY-95-132, Item E.

## 17.6 References

1. "Energy Systems Business Unit – Quality Management System," Revision 2.

2. WCAP-8370 Revision 12a, "Energy Systems Business Unit - Power Generation Business Unit Quality Assurance Plan."

3. WCAP-8370/7800, Revision 11A/7A, "Energy Systems Business Unit - Nuclear Fuel Business Unit Quality Assurance Plan."

4. WCAP-12600 Revision 4, "AP600 Advanced Light Water Reactor Design Quality Assurance Program Plan," January 1998.

5. APP-GW-GL-022 Revision 0, AP1000 Probabilistic Risk Assessment.

6. Deleted.

7. ~~Letter from NRC to Westinghouse~~NRC/DCP0669, "Criteria for Establishing Risk Significant Structures, Systems, and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program," January 16, 1997.

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

9. Westinghouse Electric Company Quality Management System (QMS), Revision 5, dated October 1, 2002.

10. NEI 07-02, "Generic FSAR Template Guidance for Maintenance Rule Program Description for Plants Licensed Under 10 CFR Part 52."

11. APP-GW-GLR-117, Rev. 0, "Incorporation of the Maintenance Rule."

D-RAP ~~Phase I~~

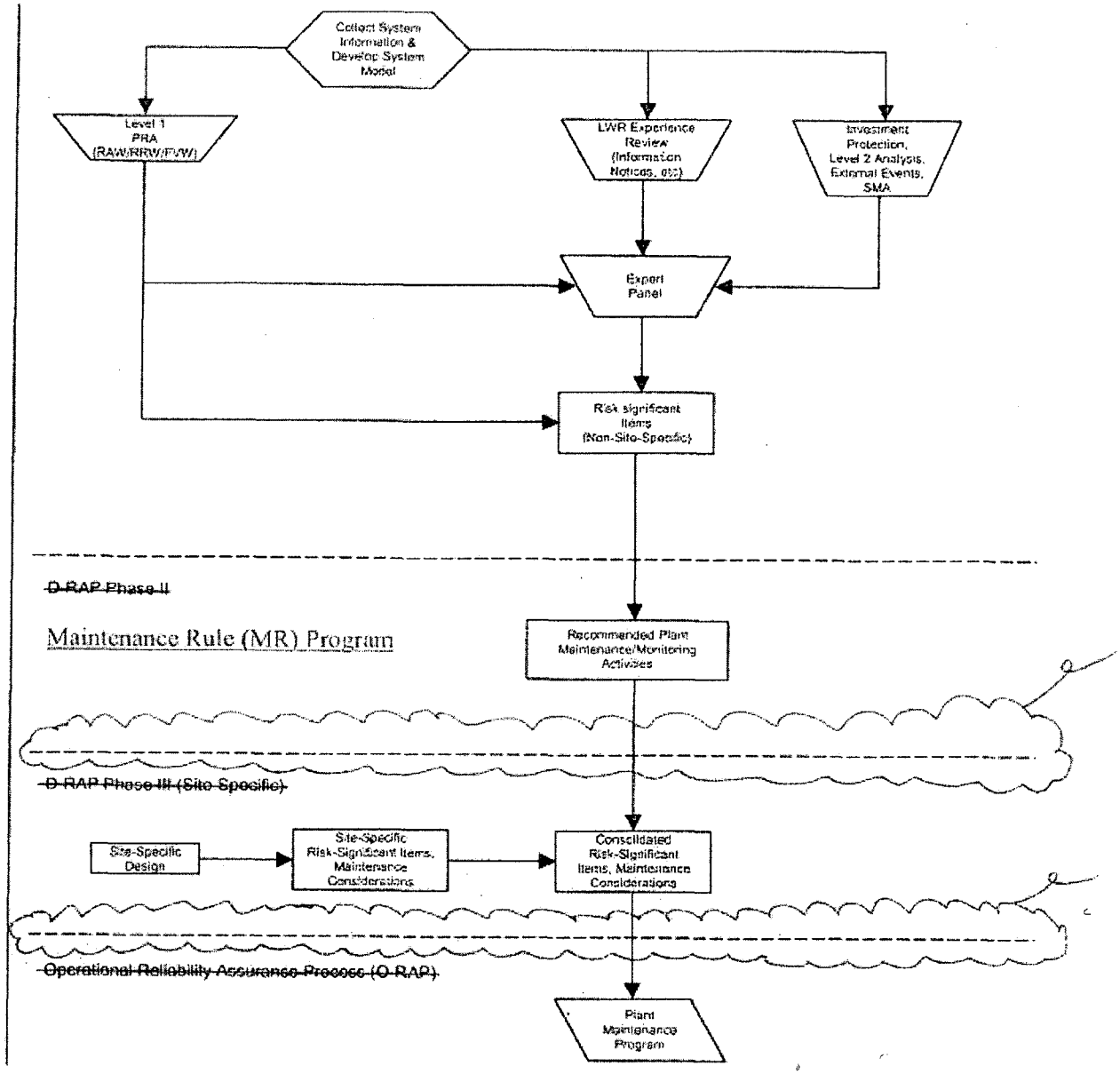


Figure 17.4-1

**Design Reliability Assurance Program and ~~O-RAP~~ MR Program**

**DCD Rev 16 MARK-UP**

**CHAPTER 16**

**16.3 Investment Protection**

**16.3.1 Investment Protection Short-Term Availability Controls**

The importance of nonsafety-related systems, structures and components in the AP1000 has been evaluated. The evaluation uses PRA insights to identify systems, structures and components that are important in protecting the utilities investment and for preventing and mitigating severe accidents. To provide reasonable assurance that these systems, structures and components are operable during anticipated events short-term availability controls are provided. These investment protection systems, structures and components are also included in the D-RAP/~~MR Program~~ OPRAAs (refer to Subsection 17.4), which provides confidence that availability and reliability are designed into the plant and that availability and reliability are maintained throughout plant life through the maintenance rule. Technical Specifications are not required for these systems, structures and components because they do not meet the selection criteria applied to the AP1000 (refer to subsection 16.1.1).

**CHAPTER 17**

**QUALITY ASSURANCE**

**17.4 Design Reliability Assurance Program**

This subsection presents the AP1000 Design Reliability Assurance Program (D-RAP).

**17.4.1 Introduction**

The AP1000 D-RAP is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 probabilistic risk assessment (PRA) (Reference 5) 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, shown in Figure 17.4-1, is implemented during Design Certification. The D-RAP identifies risk-significant SSCs for inclusion into the site Operational Phase Reliability Assurance Activities (OPRAAs)~~Maintenance Rule (MR) Program (Reference 10)~~ using probabilistic, deterministic, and other methods.

The OPRAAs ~~MR Program~~ provides confidence that the operations and maintenance activities performed by the operating plant support should maintain the reliability assumptions made in the plant PRA.

### 17.4.3 Design Considerations

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 OPRAAs~~MR Program~~.

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

### 17.4.4 Relationship to Other Administrative Programs

The D-RAP manifests itself in other administrative and operational programs. 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. 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. ~~Implementation of the Maintenance Rule, 10 CFR 50.65, will provide coverage of the SSC's that would have been included in the O-RAP.~~

The OPRAAs are comprised of site administrative, maintenance, operational, and testing programs to enhance operational phase reliability throughout the designed plant life. As documented in Reference 10 and Reference 12, the following reliability assurance programs are credited as OPRAAs:

- Maintenance Rule Program (Reference 10)
- Quality Assurance Program (Subsection 17.2)
- Inservice Testing Program (Subsection 3.9)
- Inservice Inspection Program (Subsection 5.2 and Subsection 6.6)
- Technical Specifications Surveillance Test Program (Subsection 16.1)
- AP1000 Investment Protection Short Term Availability Controls Program (Subsection 16.3)
- Site Maintenance Program

## 17.4.6 Objective

The objective of the D-RAP is to design reliability into the plant and to maintain the AP1000 reliability consistent with the NRC-established PRA safety goals.

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

- Provide reasonable assurance that
  - The AP1000 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP1000 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 AP1000 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 AP1000 design
- 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

Development of maintenance assessments and recommendations and the site-specific portion of the program is the responsibility of the Combined License applicant ~~under the MR program~~.

## 17.4.8 Glossary of Terms

| | |
|---|---|
| D-RAP | Design Reliability Assurance Program – performed as part of the AP1000 design effort to assure that the reliability assumptions of the PRA remain valid throughout the plant operating lifetime. |
| FVW | Fussel-Vesely Worth |
| MR | Maintenance Rule |
| OPRAAs | Operational Phase Reliability Assurance Activities |

| | |
|---|---|
| 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 Systems |
| SSC | Structures, Systems, and Components |

## 17.5 Combined License Information Items

17.5.1 The Combined License applicant or holder will address its design phase Quality Assurance program.

17.5.2 The Combined License applicant will address its Quality Assurance program for procurement, fabrication, installation, construction and testing of structures, systems and components in the facility. The quality assurance program will include provisions for seismic Category II structures, systems, and components.

17.5.3 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

The COL applicant or holder will establish PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP.

17.5.4 The Combined License applicant or holder will address its Quality Assurance program for operations.

17.5.5 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

The following activities are represented in Figure 17.4-1 as "Plant Maintenance Program."

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. Reference 8 contains examples of cost-effective maintenance enhancements, such as condition monitoring and shifting time-directed maintenance to condition-directed maintenance.

17.5.6 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

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.

17.5.7 The Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-117 (Reference 11), and the applicable changes are incorporated in the DCD. No additional work is required by the Combined Operating License Applicant to address the aspects of the Combined License information requested in this subsection.

The following words represent the original Combined Operating License Information Item commitment, which has been addressed as discussed above.

In addition to performing the specific tasks necessary to maintain SSC reliability at its required level, the O-RAP activities include:

- Reliability data base – Historical data available on equipment performance. The compilation and reduction of this data provides the plant with source of component reliability information.
- 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 – 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.

17.5.8 The Combined License applicant is responsible for integrating the objectives of the OPRAAs ~~MR Program~~ into the Quality Assurance Program developed to implement 10 CFR 50, Appendix B. This program will address failures of non-safety-related, risk-significant SSCs that result from design and operational errors in accordance with SECY-95-132, Item E.

## 17.6 References

1. "Energy Systems Business Unit – Quality Management System," Revision 2.

2. WCAP-8370 Revision 12a, "Energy Systems Business Unit - Power Generation Business Unit Quality Assurance Plan."

3. WCAP-8370/7800, Revision 11A/7A, "Energy Systems Business Unit - Nuclear Fuel Business Unit Quality Assurance Plan."

4. WCAP-12600 Revision 4, "AP600 Advanced Light Water Reactor Design Quality Assurance Program Plan," January 1998.

5. APP-GW-GL-022 Revision 0, AP1000 Probabilistic Risk Assessment.

6. Deleted.

7. NRC/DCP0669, "Criteria for Establishing Risk Significant Structures, Systems, and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program," January 16, 1997.

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

9. Westinghouse Electric Company Quality Management System (QMS), Revision 5, dated October 1, 2002.

10. NEI 07-02, "Generic FSAR Template Guidance for Maintenance Rule Program Description for Plants Licensed Under 10 CFR Part 52."

11. APP-GW-GLR-117, Revision ~~0~~1, "Incorporation of the Maintenance Rule."

12. SECY 95-132, "Policy And Technical Issues With The Regulatory Treatment Of Non-Safety Systems (RTNSS) In Passive Plant Designs (SECY 94-084)"

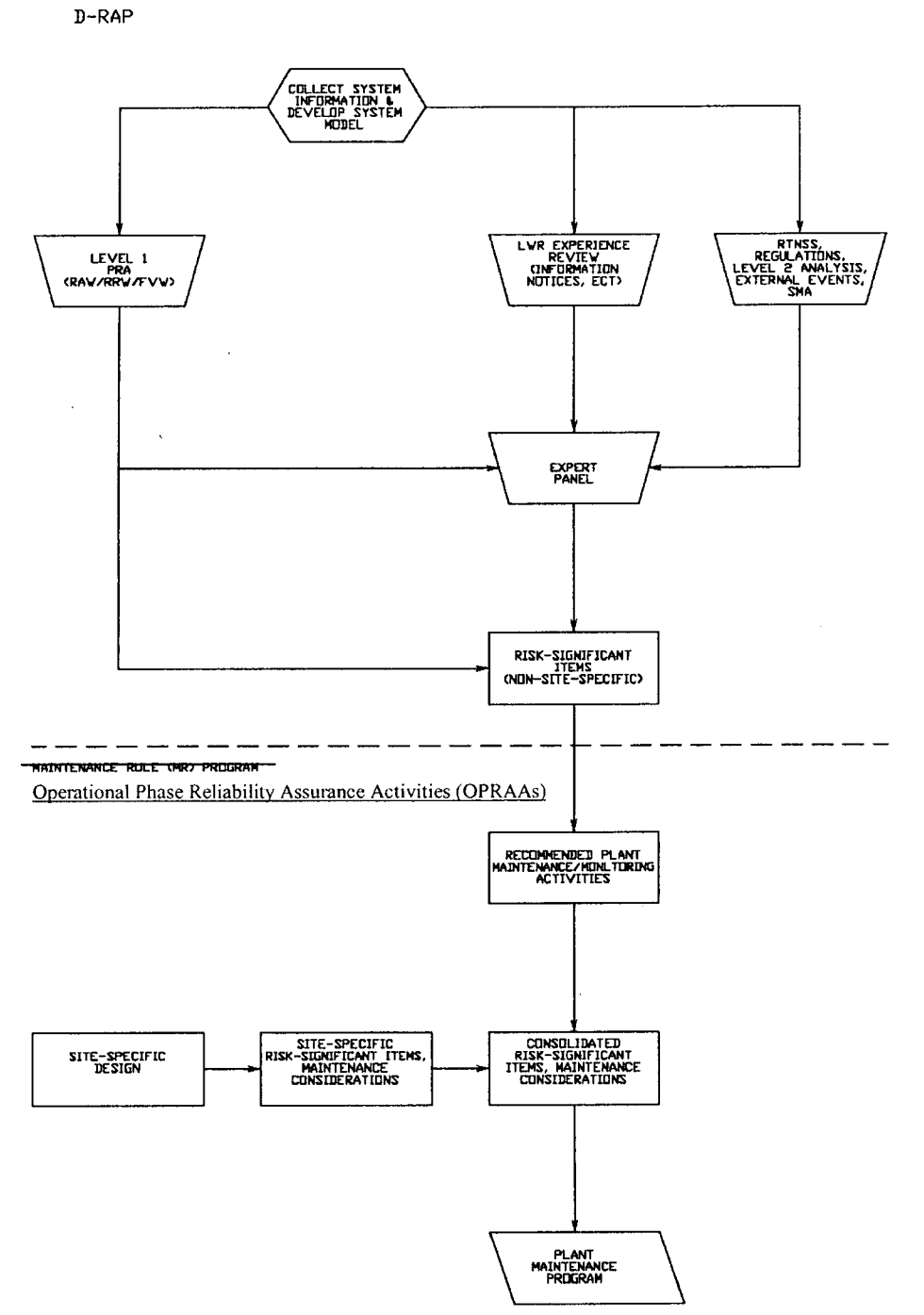


Figure 17.4-1

Design Reliability Assurance Program and ~~MR Program~~ Operational Phase Reliability Assurance Activities