U.S. NUCLEAR REGULATORY COMMISSION August 1998

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.176

(Draft was issued as DG-1064)

AN APPROACH FOR PLANT-SPECIFIC, RISK-INFORMED DECISIONMAKING: GRADED QUALITY ASSURANCE

A. INTRODUCTION

Background

The NRC has established deterministic criteria for determining which commercial nuclear power plant equipment is considered safety-related (see Section 50.2, "Definitions," of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities"; Appendix A, "Seismic and Geologic Siting Criteria for Nuclear Power Plants," to 10 CFR Part 100, "Reactor Site Criteria"; Section 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," of 10 CFR Part 50; and Section 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," of 10 CFR Part 50). Because of the importance of the safety-related equipment to protecting public health and safety, the NRC has additionally required that a quality assurance (QA) program (described in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50) be applied to all activities affecting the safety-related functions of that equipment. The overall purpose of the QA program is to establish a set of systematic and planned actions that are necessary to provide adequate confidence that safety-related plant equipment will perform satisfactorily in service. The requirements delineated in Appendix B to 10 CFR Part 50 recognize that QA program controls should be applied in a manner consistent with the importance to safety of the associated plant equipment. In the past, engineering judgment provided the general mechanism to determine the relative importance to safety of plant equipment.

In recognition of advances made in the state of the art in the probabilistic risk assessment (PRA) technology area, the NRC has made the decision to expand the use of PRA in the regulatory process. PRA provides insights that may be utilized by licensees to support the determination of the relative safety significance of plant equipment. The probabilistic insights help identify low safety-significant structures, systems, and components (SSCs) that are candidates for reductions in QA treatment. The end result of this process could be that licensees would have plant equipment that is categorized as safety-related and high safety-significant; safety-related and low safety-significant; non-safety-related and high safety-significant; and non-safety-related and low safety-significant. Grading of QA controls would vary commensurate with these categorizations. This regulatory guide provides guidance that could be used

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the NRC staff in its review of applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance of continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public. Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience.

Written comments may be submitted to the Rules Review and Directives Branch, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust and Financial Review
10. General

Single copies of regulatory guides may be obtained free of charge by writing the Reproduction and Distribution Services Section, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (310)415-2289; or by e-mail to GRW1@NRC.GOV.

Issued guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161.

by licensees both to determine the relative safety significance of plant equipment and to adjust the application of QA controls accordingly.

Requirements related to QA programs for nuclear power plants are set forth in Appendix B to 10 CFR Part 50. The general requirements contained in Appendix B are supplemented by industry standards and NRC regulatory guides that describe specific practices that have been found acceptable by the industry and the NRC staff. Although both Appendix B and the associated industry standards allow a large degree of flexibility, the licensees and the NRC staff have been reluctant to make major changes in established QA practices. Recently, however, changes in the nuclear industry have resulted in numerous proposals to revise QA practices. These changes include the completion of construction projects, establishment of programs related to plant operations and maintenance, maturation of licensee programs and personnel, and increased pressures to control plant operating costs.

The information collections contained in this regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150-0011. The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

B. DISCUSSION

During the last several years, both the NRC and the nuclear industry have recognized that PRA has evolved to the point that it may be used as a tool in regulatory decisionmaking so that the regulations can be implemented more effectively. In 1995, the NRC issued a final policy statement on the use of PRA methods in nuclear regulatory activities (Ref. 1). In its approval of the policy statement, the Commission articulated its expectation that:

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

- PRA and associated analyses (e.g., bounding analyses, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. When appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (backfit rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations will be complied with unless these rules and regulations are revised.

- PRA evaluations in support of regulatory decisions should be as realistic as practicable, and appropriate supporting data should be publicly available for review.

- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

The staff's review of 10 CFR Part 50 indicates that the option of applying QA measures in a manner commensurate with safety significance is clearly available to licensees. That is, no exemptions from current regulations are expected to be needed to implement a graded quality assurance (GQA) program. The implementing industry QA standards (which licensees have committed to implement to fulfill the requirements of Appendix B) also contain general provisions for applying QA using a graded approach. However, when implementing such changes, licensees may need to submit a revised QA program to the staff pursuant to 10 CFR 50.54(a).

Purpose and Scope

In this guide the staff describes an acceptable approach for identifying the safety significance of SSCs and assigning QA controls accordingly to ensure that QA requirements are being graded commensurate with safety. This regulatory guide contains guidance on modifying current QA program controls based on the safety categorization of the SSCs. This regulatory guide also describes acceptable approaches for

monitoring the effectiveness of the GQA program implementation and for determining when it may be necessary to make adjustments in QA practices and safety-significance categorizations to ensure that SSCs remain capable of performing their intended functions. The guide also delineates the principles for risk-informed decisionmaking, or guiding features, of a GQA program that need to be dealt with by a licensee. In some cases, rather than articulating a prescriptive method that must be implemented by a licensee to fulfill these principles (or their subsidiary issues) for GQA, the staff has chosen to identify those issues that must be evaluated, and documented, by licensees when formulating their particular approach to GQA. Thus, the burden would fall on the licensee to be able to inform the staff how the issues were addressed within the site-specific program. This guide has been specifically written for situations when the licensee's GQA program will result in changes to the QA program that do reduce commitments in the program description previously accepted by the NRC.

Graded quality assurance (GQA) is intended to provide a safety benefit by allowing licensees and the NRC to preferentially allocate resources based on the safety significance of the item. The Commission has articulated its expectation that implementation of the policy to expand the use of PRA will improve the regulatory process in three areas: foremost through safety decisionmaking enhanced by the use of PRA insights, through more efficient use of agency resources, and through a reduction in unnecessary burdens on licensees. Background information about initial efforts to implement GQA is in SECY-95-059, "Development of Graded Quality Assurance Methodology" (March 10, 1995) (Ref. 2).

Relationship to Other Guidance Document Applications

Regulatory Guide 1.174 (Ref. 3) describes a general approach to risk-informed, regulatory decisionmaking and includes a discussion of specific topics common to all regulatory applications. This regulatory guide provides guidance specifically for GQA programs, consistent with but more detailed than the generally applicable guidance given in Regulatory Guide 1.174. Licensees may choose to use risk-informed decisionmaking in application areas other than GQA. It is anticipated that certain efficiencies could be realized in that situation.

Licensees developing GQA programs will adjust their QA programs to accommodate their individual needs. The NRC conveyed its goals and expectations for an acceptable graded QA program to Nuclear Energy Institute (NEI) in a letter dated June 15, 1994 (Ref. 4). Irrespective of a licensee's specific approach, the NRC stated a graded QA program should have four essential elements:

(1) A process that determines the safety significance of SSCs in a reasonable and consistent manner, including the use of both traditional engineering and probabilistic evaluations

(2) The implementation of appropriate QA controls for SSCs, or groups of SSCs, according to safety function and safety significance to maintain reasonable confidence in equipment performance and to support the GQA corrective action feedback process

(3) An effective root-cause analysis and corrective action program

(4) A means for reassessing SSC safety significance and QA controls when new information becomes available through operating experience, or based on changes in plant design.

Organization and Content

Limited data are available to define the impact of QA programs on SSC performance. Consequently, this regulatory guide emphasizes the classification of equipment into safety-significance categories as discussed in Section 2.2 and Appendix A of Regulatory Guide 1.174 (Ref. 3). Regulatory Guide 1.174 describes a general four-element process that is elaborated upon in the context of GQA in the Discussion section of this regulatory guide. The Regulatory Positions in this regulatory guide discuss Element 1, a definition of proposed changes to QA applications; Element 2, which addresses engineering evaluations applicable to GQA programs; Element 3, which provides specific guidance for an acceptable approach for implementing GQA controls and for developing performance monitoring strategies; and Element 4, documentation and submittal aspects related to the change.

PROCESS OVERVIEW

As the nuclear industry incorporates risk insights into its QA programs, it is anticipated that the industry will build upon its existing risk-informed activities, including the individual plant examination program. To provide the industry with the NRC's expectations for risk-informed decisionmaking, Regulatory Guide 1.174 (Ref. 3) was developed. This guide establishes five safety principles and describes a four-element

process for evaluating risk-informed regulatory changes consistent with those principles, as illustrated in Figure 1. Regulatory Guide 1.174 provides additional quantitative acceptance guidelines, discussion of defense in depth, and safety margins. The principles are:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change.

2. The proposed change is consistent with the defense-in-depth philosophy.

3. The proposed change maintains sufficient safety margins.

4. When the proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.

5. The impact of the proposed change should be monitored using performance measurement strategies.

The individual elements of this process are described in Regulatory Guide 1.174. Those generally applicable discussions are not repeated here. Instead, this guide describes a method acceptable to the NRC staff for categorizing SSCs at nuclear power plants in a manner commensurate with their safety significance (using an integration of insights from traditional engineering analyses, applicable qualitative considerations, and probabilistic analyses) and for applying appropriate QA programs to each category of SSCs.

The process begins with a set of actions related to proposed changes in the QA categorization of certain SSCs. The following is an overview, with greater detail provided in the Regulatory Positions. The elements are (1) define the proposed change, (2) perform engineering analysis, (3) define implementation and monitoring program, and (4) submit proposed change.

Element 1: Define the Proposed Change

The process for developing the initial proposal for the changes is left to the licensee, but it should derive from an examination of both traditional engineering and probabilistic information, and it should result in categorization of the plant's SSCs based on their safety significance so that an appropriate level of quality controls can be applied. The licensee identifies the candidate SSCs and associated activities for a risk-informed application of QA requirements. A risk-informed GQA submittal includes the QA program change required by 10 CFR 50.54(a)(3)(ii), accompanied by the supplemental information described in Regulatory Position 4.1.2 of this guide, which will be used by the staff to determine the acceptability of the program. A licensee may elect to categorize a limited number of plant systems and apply GQA controls to these selected plant systems. The SSCs included in the bounding analysis discussed in Regulatory Position 2.2 determine which SSCs are candidates for categorization. If all SSCs in the PRA are included in the bounding analysis, all SSCs may be candidates for categorization.

The licensee identifies the systems to be categorized in the supplemental information. The licensee can choose when to categorize each system and may choose not to categorize all the systems identified in the submittal. If categorization of systems not included in the supplemental information proves desirable, the

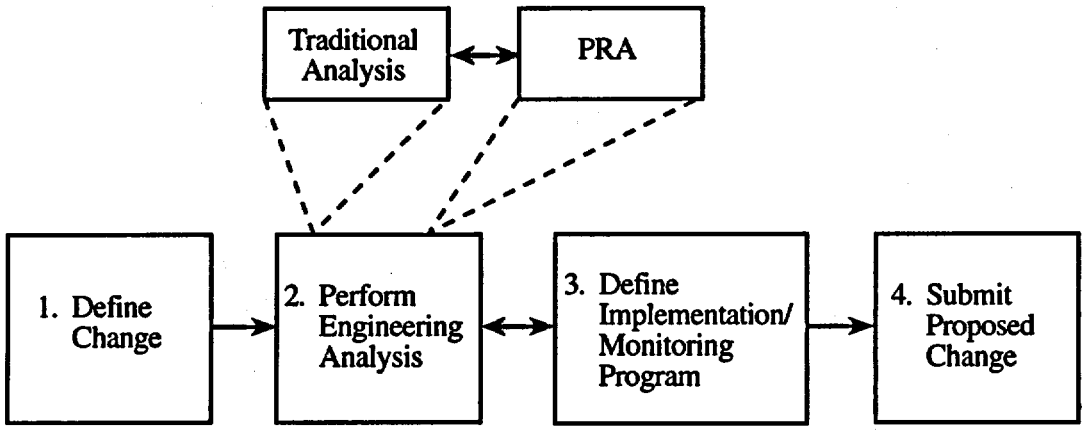

Figure 1. Principle Elements of Risk-Informed, Plant-Specific Decisionmaking

licensee prepares additional supplemental information for NRC approval prior to implementation. SSCs that should be considered as potential candidates include:

- Systems and components that are subject to current QA requirements in Appendix B to 10 CFR Part 50,
- SSCs modeled in the PRA for the plant,
- Non-safety-related SSCs that are within the scope of the Maintenance Rule (10 CFR 50.65), and
- Non-safety-related equipment that has previously received augmented quality treatment (e.g., anticipated transient without scram, station blackout, fire protection).

The licensee should ensure that the QA program commitments and other QA-related information germane to the contemplated changes in QA practices are clearly understood and adhered to, unless modified or amended through the appropriate licensing or regulatory actions. The suitability of the plant-specific PRA should be assessed relative to its use in supporting the GQA decisionmaking process. In addition, available industry and plant-specific operational experience information relative to GQA should be assessed.

Further, the licensee should identify the overall objective and approach of the proposed changes to the QA program for the candidate SSCs. More details are provided in Regulatory Position 1 of this document.

Element 2: Perform Engineering Analysis

In Element 2, the proposed changes in the application of QA controls for SSCs as a function of categorization commensurate with safety are examined and assessed with respect to the relevant risk-informed decisionmaking safety principles. An essential element of the evaluation is the categorization of SSCs into high and low safety-significant categories. The impact of the QA program changes on defense in depth would be determined through the use of both traditional engineering evaluations and PRA techniques. In addition, an assessment would ensure that no more than insignificant risk increases are introduced by the proposed changes, as described in Regulatory Position 2. The engineering evaluation helps to establish the safety significance of systems and components and determines that the effects of the changes in QA controls has a small impact on plant risk. More details concerning Element 2 are contained in Regulatory Position 2.

Element 3: Define Implementation Monitoring Program

The third element involves developing GQA control implementation and monitoring plans. These plans should be formulated to ensure that appropriate system and component performance are maintained. For the safety-related SSCs in the high safety-significant category, no changes in QA controls are expected to be proposed. For the non-safety-related SSCs that are found to be high safety-significant, an evaluation would be performed to determine what augmentation of existing QA controls is appropriate. For low safety-significant SSCs that are safety-related, reductions in QA controls are anticipated. For non-safety-related SSCs that are low safety significant, licensees would continue to define their quality controls. Means should be specified for monitoring the performance of systems and components and of quality-related activities and processes and for applying corrective actions. Specific guidance for Element 3 is provided in Regulatory Position 3.

Element 4: Submit Proposed Change

The final element involves documenting the analyses for NRC staff or independent review or inspection, and submitting the request to change implementation of QA commitments, as required by 10 CFR 50.54(a) if the change involves a reduction in the licensee's QA commitments (for example, a deviation from an NRC regulatory guide or American National Standards Institute (ANSI) standard). If the proposed change does not involve a reduction in the licensee's QA commitments, prior NRC staff review and approval is not required and the change to the QA program is submitted in accordance with 10 CFR 50.71(e). The changes associated with the adoption of GQA proposed by the licensee will be described in the QA Program. In addition, important assumptions that play a key role in supporting the acceptability of the QA program change should be identified by the licensee in the QA program. Documentation necessary to support the GQA effort is listed in Regulatory Position 4 of this regulatory guide.

C. REGULATORY POSITION

1. ELEMENT 1: DEFINE THE PROPOSED CHANGE

The first element in the process of evaluating a change to QA programs involves providing a full definition of the proposed change. The first step is to identify the overall scope of the GQA program in terms of the SSCs that are covered. Additionally, the

licensee's PRA would be evaluated with respect to its adequacy to support the GQA decisionmaking process. To accomplish this the licensee should:

1. Identify, and consider during the GQA process, the set of regulatory requirements and commitments that are directly related to the proposed QA implementation changes as well as those that may be impacted. This information is used to demonstrate that the proposed QA changes do not violate existing regulatory requirements. The major regulatory requirements applicable to GQA programs are set forth in Appendices A and B to 10 CFR Part 50, 10 CFR 50.54(a), and 10 CFR 50.34. Changes to technical requirements are controlled under existing processes such as 10 CFR 50.59, license amendments, relief requests, and exemption requests, which are outside of the scope of this document. Relevant quality commitments that are to be considered reside in a variety of licensing documents such as the QA program description, the Final Safety Analysis Report (FSAR), responses to generic communications, and responses to enforcement actions.

2. Identify the structures, systems, and components (SSCs) and associated activities that are candidates for assessment within the risk-informed application of GQA. The SSCs selected for the risk-informed application of GQA need not include all systems within the scope of this regulatory guide. A licensee may elect to only categorize and apply GQA controls to a limited number of SSCs. For those safety-related SSCs not categorized, the licensee's full Appendix B QA program controls will continue to apply.

3. Identify the expected revisions to existing implementing guidance of QA requirements that will result from the GQA program. Although the NRC staff would consider an application for changes to many areas of a licensee's QA program to support the GQA methodology, such an application is not necessary. A licensee may initially choose to apply GQA controls only to selected portions of its QA programs, such as in the area of procurement. No exemptions from current regulations are expected to be needed to implement a GQA program. However, the commitments of each licensee regarding QA are addressed in a number of documents, including the FSAR, a QA topical report (if applicable), and other docketed correspondence (e.g., responses to generic communications, inspection reports). Licensees are expected to maintain control of their licensing bases. Accordingly, changes in QA program commitments should be identified and the manner in which they are being changed should be documented, reviewed, and approved by the NRC as necessary in accordance with the applicable regulatory requirements (such as 10 CFR 50.54(a)).

4. Evaluate risk studies to determine the extent to which quantitative and qualitative risk insights may be utilized. The quality, level of review, and accuracy of plant representation of the risk studies should also be taken into account when determining the level of support the studies can provide to the development and implementation of the GQA program. The licensee should also consider how it may use risk-study models, computer programs, and personnel to support the long-term performance monitoring program required as part of GQA implementation.

5. The licensee should not make any changes in the application of QA controls and processes prior to the evaluation of the associated system or component to determine its safety significance as discussed in Regulatory Position 2 and before receiving approval of the proposed QA changes by the NRC, if required.

The definition of the change should be completed by categorizing the SSCs identified above according to whether they are high or low safety significant. For those safety-related SSCs that are categorized as high safety significant, current QA practices would apply. For those non-safety-related SSCs that are high safety significant, some increase in QA controls may be warranted and should be implemented as appropriate. For those safety-related SSCs that are low safety significant, relaxation in QA controls should be considered. For non-safety-related SSCs that are low safety significant, licensees would continue to define their quality controls without NRC approval.

2. ELEMENT 2: ENGINEERING EVALUATION

In Regulatory Guide 1.174 (Ref. 3), Element 2 is to perform the engineering evaluation to support decisions to change a plant's licensing basis. Changes in the application of QA controls do not lend themselves to a quantitative assessment because the relationship between QA programs and equipment performance (and, hence, risk contribution) has not been explicitly established. Furthermore, only a small fraction of components that are candidates for application of GQA controls are modeled in PRAs. This small percentage arises from PRA's emphasis on

the control and mitigation of severe accidents; the exclusion of equipment, such as recombiners, useful only for control of design basis accidents; the exclusion of most instrumentation and reactor protection system equipment from the models; the exclusion of emergency preparedness and plant monitoring equipment from the models; the combining of SSCs with identical failure consequences into grouped basic events; and not including some highly reliable SSCs when other less reliable SSCs (of similar impact) or operator actions are modeled.

Categorization of the safety significance of SSCs for utilization in GQA uses quantitative PRA results, supplemented by qualitative engineering evaluations to include SSCs not modeled in the PRA, to develop an initial categorization referred to in this regulatory guide as candidate high or low safety significance. These initial categories should be evaluated, modified as appropriate, and approved during a final traditional engineering decisionmaking process. Such a combined, integrated approach is necessary to utilize the strengths and avoid inherent limitations in both probabilistic and traditional engineering analysis methodologies.

2.1 Safety-Significance Categorization

A minimum of two levels of categorization should be utilized, preferably labeled high and low safety significant. At the prerogative of the licensee, a greater number of safety-significance levels can be defined, such as three levels composed of high, medium, and low safety significance. From a regulatory point of view, it is essential that high safety-significant items are not inappropriately categorized as less than high, since these might then be inappropriate candidates for reduced QA requirements. Therefore, for regulatory purposes, high safety significance may be assumed or assigned. Only assignments of low and medium safety significance must be justified.

Systems have a variety of operating modes and perform a variety of functions, with each function a well-defined task requiring the proper operation of some subset of system equipment. Although certain QA controls are applied at the component or even piece-part level, safety-significance categorization is most appropriately defined at the system function level. Therefore, the guidance in this regulatory guide is based on determining the safety-significance of system functions, identifying the components and component operational modes required to support high safety-significant functions, and determining the categorization of the components based on this information.

The categorization process must also be capable of systematically tracking and documenting system functional boundaries, defined as the point (component) at which a system operating in a particular mode functionally interfaces with a connected system. The categorization of the safety significance of support functions is generally determined by the categorization of the function being supported, augmented by a quantitative or qualitative evaluation of the support system's aggregate safety significance. Interfacing function categorization should be well documented, traceable, and internally consistent. Licensees who chose to implement GQA programs one system at a time must ensure that support system interfaces are sufficiently well defined and documented that the safety significance of interfacing systems will always be explicitly considered as each system is evaluated.

The scope, level of detail, and quality required of the PRA are commensurate with the application for which it is used and commensurate with the role the PRA results play in the integrated decision process. PRAs used to support a GQA application should realistically reflect the actual design, construction, operational practices, and operational experience of the plant and its operator. Furthermore, all calculations using the PRA model should be performed correctly and in a manner that is consistent with accepted practices. The licensee must demonstrate that the PRA and the calculations are of sufficient quality to support a decision on the acceptability of the proposed change.

A well organized and documented safety-significance categorization process, sensitivity and bounding studies performed with the PRA, and implementation of a robust monitoring and feedback program can provide reasonable assurance that implementation of GQA should result in an insignificant change in risk. Consequently, NRC staff evaluation of the quality of the PRA may be directed toward a finding that the quality is sufficient for assigning SSCs into broad safety-significant categories for consideration in an integrated decisionmaking process.

All operational modes and internal and external events should be included in the evaluation of the safety significance of systems, functions, and components. PRA models and results for core damage and large early release frequency for internal initiating events at full power should be used to support the categorization process. Licensees may use qualitative studies of other initiating events and operational modes that identify and characterize scenarios that are believed to be important, but without expending significant resources in quantifying the frequencies of

the scenarios. Seismic margin analysis and fire-induced vulnerability evaluations (FIVE) done to support the individual plant examination of external events (IPEEE) analyses and shutdown risk configuration control evaluations are examples of qualitative studies that have been developed. Evaluations based on quantitative external and shutdown studies may also be used. If importance measures from quantitative studies are combined with measures generated from internal event analyses, the licensee should ensure that the greater uncertainties inherent in the analysis of external events and the modeling of shutdown events are fully considered during the final categorization.

2.1.1 Identification of System Functions

Definition of the proposed change includes identification of all the functions a system must perform. Although many system functions may eventually be categorized as low safety significant, characterization of the proposed change begins with a description of all functions a system must fulfill. System functions should include functions used during normal operation as well as all functions related to the prevention or mitigation of core damage, protection of containment integrity, or reduction in the release probability or consequence to the public from accidents and transients both within and beyond the design basis (e.g., risk analysis).

2.1.2 System Function Safety-Significance Categorization

Determination of the safety significance of system functions is inherently a "top down" process, starting with the front-line systems and system functions directly involved in plant-level safety functions (such as reactivity control, reactor pressure control, and decay heat removal). The delivery of high-pressure primary coolant from the reactor water storage tank to the core may be categorized as a high safety-significant function. The pumps, valves, and other SSCs whose proper operation is required to fulfill this function derive their initial categorization from the significance of the function. Therefore, any determination of an SSC's safety significance requires determination of the safety significance of all functions the SSC supports. Similarly, determination of the safety significance of support system functions (which should be later pursued in the support system's evaluation) is best performed by determining the safety significance of the function being supported.

Licensees may limit their evaluation to the system level and assign all components to the same safety-significance category as the system. This will only reduce the burden on licensees if all the system functions can be categorized as low or medium safety significant. To provide confidence that eventual determination of less than high system safety significance is made with full recognition of each system's contribution to risk, system-level importance should be determined from importance measures developed from the PRA. If the system is not modeled in the PRA, the licensee should determine why the system was not modeled and, guided by this determination, investigate through a traditional engineering review whether any system functional failure will degrade the performance of any human actions or any other systems' high safety-significant functions. A system-level safety significance may be assigned based on the documented results of the review.

2.1.2.1 Quantitative Safety Categorization Insights. Quantitative importance measures from risk studies provide valuable insights about the relative ranking of the safety significance of PRA model elements such as basic events, components, human actions, functions, trains, or systems. At least two quantitative measures of importance are needed, one (such as Fussell-Vesely (FV) or risk reduction worth (RRW)) illustrates the fraction of current risk involving the failure of the model element; the other (such as risk achievement worth (RAW) or Birnbaum) illustrates the margin of safety contributed by the model element's proper operation. Other measures may be used, but at least two measures reflecting current contribution and margin contribution are needed to balance the risk insights.

Importance measures represent the risk sensitivity of an individual model element. Importance measures should be compared to some quantitative guideline values. The specific values chosen as guidelines should be justified by the licensee and should reflect the estimated risk levels at the plant. All model elements characterized by importance measures greater than (or less than, as appropriate) the guidelines are identified as potentially high safety significant. Once one element is varied, the importance measures for the other elements will change. Consequently, while large or small importance measure values identify candidate high or low safety-significant model elements, final categorization is determined by an expert panel during the integrated decisionmaking.

To ensure that the integrated decisionmaking is made with adequate understanding of the sensitivity of the importance results to major PRA modeling assumptions, techniques, and data, the licensee should address the technical issues associated with the use of risk importance measures to categorize SSCs discussed in Regulatory Guide 1.174. For GQA

applications, a minimum of two sensitivity calculations are expected; one in which recovery[1] actions are removed (that is, recovery probabilities set to 0.0) and one in which all common cause failures (CCFs) are removed (that is, failure probabilities set to 0.0). The studies should be performed by modifying and quantifying the original PRA logic model to minimize truncation effects. These sensitivity studies are desirable since human actions and CCF probabilities are derived from models requiring extensive interpretation and manipulation of observable data. When an SSC moves into the high safety-significant category as the result of a sensitivity study, the expert panel should consider the reasonableness of the recovery action or CCF event that caused the low safety significance in the original results and consider assigning the SSC into a higher safety-significant category. If the sensitivity studies are not performed, additional peer and NRC staff review of the human error and CCF probability development may be necessary to develop confidence that the quantitative results provided to the expert panel are sufficiently robust to support the categorization process.

When each SSC is categorized, the safety significance of all the functions that SSC supports must be known. Therefore, the PRA model element most applicable to the SSC grading process described in this regulatory guide is a system function failure. System function importance provides the expert panel clear and documented information referencing individual component functions to plant safety functions. Developing system functional importance will assist in both the risk categorization process and the NRC staff review. If basic event (such as component failure) importance measures, rather than system function importance measures, are used to directly categorize SSCs at the component level, the categorization process becomes more dependent on PRA characteristics such as system success criteria, system modeling detail, and component modeling guidance.

System functions generally require the proper operation of a group of SSCs and are represented in the PRA models as a set of logically linked basic events. Some PRA codes are not well suited to the development and quantification of system level importance measures. One alternative technique uses basic event importance measures (readily calculated by most PRA codes) to identify a set of system functions that are clearly high safety significant. This technique is based on recognition that system function RAW and FV importance measures will always be at least as large as the RAW and FV for basic events whose failure will fail the function. If other importance measures are used with this technique, this property should be validated for the measures used.

When basic events are used to characterize the importance of system functions, the relationship between the failure of the basic events and the system functions they support becomes a critical consideration. For example, the RAW of a CCF basic event that fails a set of nominally identical pumps provides a reasonable estimate of the margin of safety the proper operation of the pumps is contributing. If the pumps fulfill only one system function, the RAW of the CCF provides a reasonable estimate of that function's contribution to margin of safety. Any system function modeled in the PRA that is supported by one or more basic events that have importance measures above the guideline values should be initially categorized as a candidate high safety-significant system function. Since it is possible that the system function's RAW and FV measures are much higher than those of any individual basic event, system functions not categorized as candidate high should, as a minimum, be further evaluated as discussed below, and the licensee should describe technically how each issue was addressed.

- The redundancy and reliability of trains within systems that are available to fulfill a critically important system function can have the result that each individual basic event within the system has very low importance measure values or is even truncated out of the results. A system-based evaluation should be performed to determine the impact of the failure of systems that are modeled in the PRA but that have no single failure event (for example, no CCF) and no basic event importance measure above the guideline values. Discrepancies in the form of high failure consequence for some systems (automatic depressurization system, for example) but low or no basic event importance measures should be identified and the relevant high safety-significant functions defined and properly categorized as high safety significant.

- Initiating events are often not modeled as basic events or, if they are, are modeled as single modularized events. Some examples of such initiating events are the loss of instrument air, the loss of main feedwater, the loss of offsite power (through local switchyard faults), the loss of alternating current (AC) or direct current (DC) buses. If components whose failure contributes to these initiating events are modeled in other initiating events (e.g., loss of an air compressor

[1] Recovery actions include human actions performed to return a failed system or component to operability. Recovery actions may also include using systems in relatively unusual ways. The procedures for recovery actions usually give only general guidance instead of step-by-step procedures and are not part of the standard training routine.

leading to loss of pneumatic valves following a loss of component cooling), the importance of the basic events will not include the contribution of the failure to the initiating event frequency. Thus, the importance of functions whose failure would cause both an initiating event and the partial loss of mitigating function can be severely underestimated by surrogate basic event importance measures.

PRA's integrated models provide an excellent framework to characterize system and system function importance. One area relevant to GQA that PRA modeling does not usually address is cross-system dependencies arising from nominally identical components used in different applications throughout the plant. This occurs because cross-system dependencies are typically not modeled (between nominally identical MOVs in different systems, for example) and because the resolution of the PRA models may not be sufficiently detailed (the PRA analyst may not be able to determine whether the circuit breakers in two different systems are identical models, for example). Cross-system dependencies are not modeled in PRAs yet can have a significant impact on risk. Consequently, licensees must develop a monitoring program capable of timely identification of repetitive failures of nominally identical equipment for further investigation.

2.1.2.2 Qualitative Safety Categorization Insights. PRA results are to be used in conjunction with traditional engineering, and the principles associated with defense in depth and safety margins must also be factored into the safety-significance determination. Consequently, the following qualitative factors should be applied to the quantitative PRA insights developed in the previous section. The licensee is to be able to describe technically how each issue was evaluated and resolved.

- The diversity of systems that are able to fulfill critical high level functions (e.g., reactivity control, decay heat removal) can have the result that each individual system could meet all quantitative guidelines to be categorized in the low safety-significance group. It would be prudent, and the licensee is expected, to designate at least one system associated with critical high-level functions as high safety significant.

- Screening analyses are used to dismiss some functional failures as insignificant. In many cases, credit for the redundancy or reliability of plant systems or structures is taken to bolster the arguments that the functional failure need not be modeled. Thus, the importance of some systems, functions, and structures will not show up in the PRA results since the functional failure is screened out. (For example, screening out certain containment penetrations because of the number of isolation valves involved obscures the importance of the containment isolation function of the system.)

- Risk insights from nonquantitative external event and shutdown risk studies should also be used. All the system functions credited in these studies should initially be categorized as "high safety-significant" candidates. Final categorization into a lower safety-significance category should include consideration of the initiating event's frequency or magnitude and the ability of the SSC to respond to the event.

- Risk insights from the evaluation of the Maintenance Rule (10 CFR 50.65) should be incorporated to ensure the identification of functions that are (1) relied upon to mitigate accidents; (2) used in emergency operating procedures; (3) those whose failure could prevent a safety-related SSC from performing its safety-related function; and (4) those whose failure could cause a reactor scram or actuation of a safety-related system.

- PRA importance measures do not fully address the significance of SSCs that support operator actions for emergency and severe accident management. Such systems can include environmental controls, lighting, alarms, communications, and annunciators. Determination of the categorization of such systems should include consideration of whether the loss of such systems could cause short-term or long-term problems, whether a system failure coincident with an accident is likely, and whether personnel could reasonably compensate for the loss of these support systems.

2.1.3 Identification of Components that Support Functions

QA controls are applied at the component level while PRA basic events often represent groups of components. For example, a diesel failure basic event in the PRA can represent a large number of plant equipment parts, including such items as the diesel motor, oil pump, oil cooling fan, motor generator. Other components are not included in PRA basic events because their reliability is assumed to be high enough that their failure probability would have a negligible impact on the CDF and LERF. Therefore,

once the high safety-significant functions in a system for which GQA is being implemented have been identified, the plant equipment required to support the high safety-significant functions must be identified independently of the PRA basic event definitions.

An efficient format to identify this component versus system function is a matrix that lists and cross-references the high safety-significant system functions to all the components needed to support each function at the level of equipment specificity at which changes in the application of QA controls will be pursued. Although a matrix is not necessary, well-organized information to support the final deliberations and to provide a traceable record for future licensee evaluations and for NRC inspections should cover all high safety-significant system functions, all system components that support the high safety-significant functions, and all external system support functions required by any component. The licensee is to be able to describe technically how each issue was addressed and resolved. Here are some examples that illustrate areas of potential concern regarding the accuracy and completeness of this information.

- One component can directly support another system's function. For example, some containment sump recirculation valves are nominally assigned to the low-pressure injection system but directly support containment spray by providing the recirculation flow path.

- Some instrumentation can belong to one system but provide signals used in other systems, or be used by the operators as a basis for proceduralized or unproceduralized actions. Instrumentation used to actuate and control system and plant functions needs careful attention if grading of instrumentation is contemplated.

- Component failures could lead to an initiating event such as loss of feedwater or loss of component cooling water. Components whose failure could cause an initiating event should be identified in the matrix as being necessary to support the normal operation function (e.g., air-operated feedwater control valves are required to support feedwater at power).

Well organized and detailed information is also needed to systematically propagate safety categorization through successive tiers of support systems not modeled in the PRA. If systems are not graded in a top-down sequence, it is particularly important that the evaluation should include a traceable record of the previously assumed categorization of upper-tiered functions requiring support from other systems. Eventually, the categorization of all support functions should be consistent, e.g., the safety significance of the functions requiring support in the upper-tiered system corresponds to the relevant function in the support system.

2.1.4 Safety-Significance Categorization of Components

The final categorization of system functions and the components that support the high safety-significant system function is selected by an integrated assessment of quantitative and qualitative risk insights as described in Regulatory Position 2.3.

The safety-significance categorization assigned to components (and to support system functions that can be treated as component functions for initial categorization) is based on the safety significance of the function the component supports. Components that support only low safety-significant functions should be classified low safety significant. The safety significance of components supporting high safety-significant functions need not always be high, but each such categorization as low safety significant should be explicitly evaluated and documented and in conformance with licensee-defined guidelines. Justification for categorizing a component's safety significance as low based on high reliability alone will not be acceptable, because the high reliability may be the result of the QA controls applied. If it is not the quality controls that are the cause of the high reliability, the justification should describe the source of the high reliability.

2.2 Demonstration of Conformance with Safety Principles

Once the full set of low safety-significance candidates has been identified, it is necessary to demonstrate that the proposed changes to the QA requirements for these candidates do not violate the safety principles. Guidelines for making that demonstration with due consideration for the scope of the GQA program are summarized below. Other equivalent guidelines are acceptable.

GQA programs need to reflect the multiplicity of current regulations and programs to which some SSCs are subject. For example, some SSCs may need to be excluded from certain reduced QA control categories if those SSCs are also governed by more stringent American Society of Mechanical Engineers (ASME) Code provisions to meet the requirements of 10 CFR 50.55a. In such instances, the ASME Code requirements must be met.

2.2.1 Engineering Evaluation Guidelines

The engineering evaluation should assess whether the impact of the proposed change is consistent with the defense-in-depth philosophy. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent decision guidelines are acceptable.

- A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system and uncertainties (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved and the potential for introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved.
- The intent of the General Design Criteria in Appendix A to 10 CFR 50 is maintained.

The engineering evaluation should also assess whether the impact of the proposed change is consistent with the principle that sufficient safety margins are maintained. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent decision guidelines are acceptable.

- Codes and standards or alternatives approved for use by the NRC are met.
- Safety analysis acceptance criteria in the licensing basis (e.g., Final Safety Analysis Report (FSAR) and supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

2.2.2 Guidelines for Defense in Depth and Safety Margins

Defense in depth and safety margins are expected to be addressed generally by considering the following GQA program aspects.

- The GQA process will not result in changes to the plant configuration. Therefore, no existing plant barriers will be removed. Additionally, existing system redundancy, diversity, and independence will be maintained.
- The GQA process will not result in changes to the technical requirements (e.g., design bases or operational parameters) associated with SSCs.
- The resulting QA provisions will provide the necessary level of assurance that low safety-significant, safety-related and high safety-significant, non-safety-related SSCs remain capable of performing their safety function.

The core damage frequency (CDF) and large early release frequency (LERF) figures of merit do not fully cover long-term containment overpressure protection. Functions credited in the PRA for long-term overpressure protection, but which do not contain any SSCs with CDF or LERF based importance measures above the guideline values, should be identified and the safety significance explicitly assigned. For example, the containment spray systems for PWRs may not contribute to the prevention or mitigation of core damage or large early release.

An important factor to ensure that defense-in-depth and safety margin considerations are not degraded during the implementation of GQA is control of potential common mode failures. As discussed in Regulatory Position 2.1.2.1, groups of nominally identical SSCs, utilized in multiple systems throughout the plant, can as an aggregate have high safety significance.

Principle 4 in Regulatory Guide 1.174 (Ref. 3) states that any proposed increase in CDF and risk are small and are consistent with the intent of the Commission's Policy Statement (Ref. 1). Although the risk impact of GQA changes on individual components is expected to be minimal, reduced QA oversight may be applied to a large number of SSCs. It is recognized that limited data are available to define the impact of QA programs on SSC reliability. Accordingly, the licensee should perform a bounding analysis in which the failure rates or probabilities for basic events representing SSCs that may be subjected to reduced QA controls are set at some increased level (chosen and justified by the licensee). Alternatively, the licensee may choose to address the bounding analyses by modifying the uncertainty distributions in some manner (also chosen and justified by the licensee).

The bounding analysis should include all SSCs modeled in the PRA on which QA controls may be

reduced in all systems that the licensee defines as being within the scope of the GQA program. SSCs not modeled in the PRA must be reviewed to verify that their failure will not impact any functions modeled in the PRA. Any potential impact on systems modeled in the PRA must be qualitatively addressed.

It is recognized that the categorization of SSCs for the bounding analysis will necessarily be an initial categorization, most likely based on an evaluation of basic event importance measures augmented by a limited deterministic review. The purpose of such a study is not to estimate a new plant CDF and LERF, but to understand the potential or bounding impact of the proposed change and to assess the risk impact through bounding evaluations. The results should be compared to the acceptance guidelines in Regulatory Guide 1.174 and contrasted with aspects of the GQA program implementation that are expected to provide an unquantifiable safety benefit. If, during the categorization process, it becomes apparent that the initial categorization is modified to such an extent that the bounding results may be non-conservative (that is, SSCs that were high during the bounding analysis are being placed in lower categories), a new bounding calculation should be performed. If the original results are exceeded, the licensee should adjust the category of selected SSCs categorized or adjust the categorization criteria.

2.3 Integrated Assessment

Generally, the performance of, and integration of, the above described evaluations should be performed by a number of technically knowledgeable personnel. One acceptable approach to accomplish this function is to utilize a multi-disciplinary review group of technically proficient plant personnel, referred to here as an expert panel.

If the integrated assessment function is performed by an expert panel, the expert panel determines safety significance and considers QA program adjustments for SSCs accordingly. The panel would normally include experienced representatives from various disciplines such as operations, maintenance, engineering, safety analysis and licensing, and PRA. The composition of the expert panel should be augmented, if necessary, to support the purpose of the safety-significance ranking and the grading of QA controls. For example, because of the emphasis on QA considerations in the GQA process, QA and procurement engineering personnel may be assigned to the panel.

The expert panel is responsible for determining the safety significance of the system functions and SSCs. The panel should evaluate traditional engineering, probabilistic, and qualitative information available regarding the systems and system functions within the defined scope of the GQA program changes. The evaluation should include either resolving or approving the resolution of the quantitative and qualitative issues addressed in Regulatory Positions 2.1.2.1 and 2.1.2.2.

Safety significance may be determined using guidelines related to prevention and mitigation of core damage, as well as containment integrity and LERF. Factors such as potential common mode failures, human errors, defense in depth, the importance of plant equipment used for emergency preparedness and plant monitoring functions, and the maintenance of safety margins should also be fully considered.

3. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING STRATEGIES

This section addresses the first, second, third and fifth principles for risk-informed decisionmaking. The objective of the GQA effort is to implement a GQA program that provides a reasonable level of confidence that plant SSCs will be capable of performing their intended functions. The extent of QA controls will be determined by the relative safety significance and safety functions performed by the equipment to which those controls are applied. The licensee's revised GQA program should specifically identify how the criterion in Appendix B to 10 CFR Part 50 will be satisfied. The licensee may adjust the elements of the QA program as deemed necessary to provide a reasonable level of confidence that the SSCs will be capable of performing their intended function. The licensee will demonstrate that the proposed program, in total, is sufficient to achieve this objective.

3.1 Grading of Quality Activities

The first step of the evaluation process is for the licensee to identify specific elements of the QA program controls that will be adjusted for the set of plant equipment that is defined to be low safety significant. For example, a licensee may propose a change to its verification practices and perform verifications by sampling. Additionally, the licensee should identify the approach for evaluating the adequacy of QA controls for non-safety-related SSCs determined to be high safety significant. Augmented quality controls will likely be warranted for these items.

3.1.1 Regulations and Commitments

In accordance with the first principle, no exemptions from current regulations are expected to be needed to implement a GQA program.

The licensee's QA program description should be revised to address GQA activities applicable to safety-related SSCs of low safety significance, including a discussion of how the applicable requirements of Appendix B to 10 CFR Part 50 will be satisfied for that part of the program in accordance with 10 CFR 50.34(b)(6)(ii). This may be accomplished by a discussion that identifies exceptions to applicable NRC regulatory guides and associated endorsed industry standards or by including additional text that describes how Appendix B will be satisfied (merely restating the Appendix B provisions will not be acceptable). The submittal should adequately describe the safety-significance determination process and the adjustments made to the QA provisions associated with the 18 criteria of Appendix B to 10 CFR Part 50 to describe how the requirements will be satisfied in a graded manner. While considerable flexibility may be exercised, the GQA program should be based on standards of performance that are clear, definite, and enforceable.

Grading of QA activities will likely result in changes that reduce QA program commitments relating to SSCs of low safety significance. In that event, the NRC would expect the licensee to submit a QA program change to the NRC in accordance with 10 CFR 50.54(a), as discussed further in this section and in Regulatory Position 4.

However, plant SSCs cannot be reclassified as non-safety-related solely on risk considerations. Regulatory requirements in Section VI(a)(1) of Appendix A to 10 CFR Part 100, 10 CFR 50.2, 10 CFR 50.49(b)(1), and 10 CFR 50.65(b)(1) prescribe the criteria for determining which SSCs are safety-related and are subject to the provisions of Appendix B to 10 CFR Part 50. However, GQA does allow for differences in QA controls for safety-related SSCs based upon their safety significance.

GQA programs should not result in either intended or effective changes in the design, configuration, or technical requirements of plant systems. Such design or configuration changes would occur, for example, if QA program reductions result in a loss of confidence of the SSC's ability to perform its safety function. The licensee should ensure that changes to technical requirements are only made in accordance with applicable regulations.

Other regulations, such as the requirements of 10 CFR Part 21, "Reporting of Defects and Noncompliance," including provisions related to basic components and commercial grade item dedication; 10 CFR 50.55(a), "Codes and Standards"; and 10 CFR 50.36, "Technical Specifications," remain in effect and may not be changed by means of the GQA program description.

Licensee commitments regarding QA are addressed in a number of documents, including the FSAR, the QA Topical Report, and other docketed correspondence (e.g., responses to generic communications, inspection reports). Licensees are expected to maintain control of their licensing bases. Accordingly, changes from current commitments to QA regulatory guides that will be revised as part of the GQA program should be identified, and the manner in which they are being changed should be documented, reviewed, and approved as necessary by the NRC in accordance with 10 CFR 50.54(a), as appropriate.

3.1.2 Grading of Quality Elements

After categorizing the system functions and subsequently the SSCs into two or more safety-significance categories as described throughout this regulatory guide, the licensee should apply appropriate QA controls for the various categories. This is a critical factor in achieving the goals of the GQA initiative and is performed by an integrated assessment, for example, by an expert panel, as discussed in Regulatory Position 2.3.

For safety-related SSCs determined to be high safety significant, or for safety-related SSCs that have not yet been evaluated in accordance with the GQA process, the current QA practices contained in the NRC-approved QA program should be retained.

Licensees have the flexibility to define the processes used to achieve reasonable confidence in SSC performance commensurate with their safety significance. Therefore, the licensee may develop reduced, or graded, quality assurance controls for those safety-related SSCs assigned to the low safety-significant category. Examples of areas in which this may be possible are listed in Regulatory Position 3.2 of this regulatory guide. In proposing to reduce controls, two basic objectives should be kept in mind. These are that the GQA program should be sufficient to ensure the SSC's design integrity and ability to successfully perform its safety function and that the GQA program should include processes and documentation that support an effective corrective action program as discussed in Regulatory Position 3.3.2. Accordingly, in reducing or enhancing the QA program for any SSC, the licensee must describe how the proposed changes will achieve the objectives. Also, consideration should be given to issues such as CCF, as discussed in Regulatory Position 2.2.

It should be emphasized that a certain number of SSCs currently categorized as non-safety-related (i.e., that have not previously been subjected to an Appendix B QA program) may fall into the high safety-significant category based on application of the methods described in this regulatory guide. These non-safety SSCs become important because the categorization of safety-related SSCs as either high safety significant or low safety significant is derived either directly or indirectly from the licensee's PRA or from qualitative methods that consider the results of PRA when available. In particular, PRA takes credit systematically for non-safety-related SSCs as (1) providing support to, (2) alternatives to, and (3) back-ups for safety-related SSCs. Thus, the categorization of safety-related SSCs as low safety significant depends upon the proper operation and reliability attributed to non-safety-related SSCs as part of the safety-significance determination process.

Licensees should evaluate whether augmented QA practices are warranted for "high safety-significant, non-safety-related" SSCs. The application of augmented controls provides reasonable confidence that the reliability assumed in the risk analysis, or the associated qualitative decisionmaking process, remains valid. Licensees may voluntarily select certain Appendix B QA program controls as augmented quality provisions. However, a licensee may determine that the amount of QA controls currently being applied to these high safety-significant, non-safety-related SSCs are appropriate. If there is reasonable assurance that the SSC will perform its intended function, there may be no need to apply augmented QA controls. The licensee should be able to provide a documented basis concerning the adequacy of the QA controls applied to these high safety-significant, non-safety-related SSCs. The discussion that QA controls will be applied to high safety-significant, non-safety-related SSCs, and the delineation of the augmented quality controls that will be applied to those SSCs must be documented by the licensee in the QA program. In the above manner, risk insights will be used in an integrated manner to identify areas in which improvements should be implemented.

If the PRA analysis assumed that certain non-safety-related SSCs would perform particular functions under postulated design basis conditions (for example, seismic, harsh environment, or fire), and these SSCs are categorized as high safety-significant, then GQA controls that address the equipment characteristics that support the credited function should be considered.

3.2 Potential Areas for Implementing GQA Program Controls

Low safety-significant SSCs that are safety-related, to which the QA program controls in Appendix B to 10 CFR Part 50 have previously been applied, are candidates for grading subject to the guidance discussed earlier. In addition, for high safety-significant SSCs that are non-safety-related, licensee evaluation should be performed to identify proposed augmented quality controls.

Some areas that may be appropriate for applying GQA program controls for safety-related SSCs of low safety significance are discussed below. The functional areas discussed below are not all-inclusive and licensees may propose graded controls in other areas, provided it can be shown that the objectives discussed in Regulatory Position 3.1.2 are met. The goal is to allow licensees flexibility to define acceptable QA controls that provide reasonable confidence that the SSCs will perform their intended functions. As discussed in Regulatory Position 3.3.2, the assignment of QA controls is dynamic in nature. As part of the GQA process, it is necessary to consider feedback information from the monitoring and corrective action elements that may lead to a need to reinstate controls that had been relaxed. Further details of specific GQA practices that the staff has found acceptable for low safety-significant items are described in SECY-97-229, "Graded Quality Assurance/Probabilistic Risk Assessment Implementation Plan for the South Texas Project Electric Generating Station" (Ref. 5), the associated licensee QA program change, and other documents referenced in the staff safety evaluation attached to SECY-97-229.

When considering the application of GQA controls, the licensee should consider the essential elements of the process (such as the safety-significance determination, identification of GQA controls, associated corrective action methods, and performance monitoring) to be high safety-significant activities that are not subject to grading.

3.2.1 Procurement

Licensees may establish less stringent QA requirements for the procurement of low safety-significant components than for high safety-significant components. In making these changes, licensees must consider requirements in 10 CFR Part 21 and Appendix B to 10 CFR Part 50 and must consider any still-current commitments based on the

use of withdrawn regulatory guides.[2] Within this area, the technical requirements for commercial grade item (CGI) dedication in accordance with 10 CFR Part 21 (critical characteristics of an item for an application) are not subject to grading. However, for safety-related items of low safety significance, the verification of critical characteristics may be graded (e.g, by reduced sampling plans or alternative testing techniques). Other procurement-related activities such as auditing, qualifying suppliers, and receipt inspection may also be graded. Licensees should consider the role its procurement practices play in ensuring the prevention of cross-system common cause failures and implement the procurement activities accordingly.

A licensee may choose to reduce current commitments regarding certificates of conformance that are based upon regulatory guides that have been withdrawn.[2] The licensee would instead follow the guidance in sections 4.2.a, 10.2.a through f, and 10.3.2 in ANSI N45.2.13 (Ref. 6).

A licensee may choose to reduce commitments to ANSI N45.2.13 (Ref. 6) regarding source verifications and procurement program audits described in Sections 7.2.1, 7.3.1, 10.3.1, and 12. The change of practices in this area for low safety-significant items would be appropriate. However, licensee practices for receipt inspections, post-installation testing, and a component-level monitoring program will provide feedback to identify any necessary corrective actions.

A licensee may reduce commitments associated with Regulatory Guide 1.38 (Ref. 7) and other (previously withdrawn) guides[2] and with ANSI N45.2.12 and N45.2.2 (Refs. 8 and 9) regarding the conduct of external supplier audits and supplier evaluations. For low safety-significant items, the external supplier audits could be done as deemed necessary on an unscheduled basis. The associated supplier evaluations could be done on a biennial basis. Overviews of suppliers will be based on performance monitoring and trending of feedback from receipt inspections, post-installation tests and inspections, and plant operational results.

Licensees should also consider the results of the evaluations generated during the categorization process concerning the functions of SSCs, as they may provide useful insights for identifying critical characteristics to be used during the dedication process

3.2.2 Inspections

The licensee may chose to reduce inspection activities related to low safety-significant SSCs and choose to perform monitoring or surveillance oversight to ensure that components can perform their intended functions. Verifications by peer personnel may be implemented for safety-related low safety-significant SSCs provided that the licensee uses individuals who are qualified to do inspections and who are independent from the actual performance of the work activity as discussed above. However, these changes cannot conflict with ASME Code-required inspections and examinations or other inspections and examinations specified in NRC regulations (e.g., use of the Authorized Nuclear Inspector services).

The licensee may choose to reduce commitments to section 5.2.7 of ANS 3.2/ANSI N18.7 (Ref. 10) to perform post-work inspections for maintenance and modification activities depending upon the complexity of the work. Post-work inspections would then be performed for relatively complex maintenance and modifications. Other verifications such as applicable surveillance testing, receiving inspections, and inservice inspections would continue to be performed for the low safety-significant item.

Licensees may propose to reduce their requirements regarding personnel who perform inspections on low safety-significant items. Those inspection personnel will need to be experienced, task-qualified journeymen, or supervisors who did not perform or directly supervise the activity being inspected. These personnel will need to receive training in the quality organization's inspection procedures, processes, and methods in accordance with a training program approved by the quality organization. The quality organization will need to provide periodic oversight of these inspectors. This provision would also not be applicable for staff who perform nondestructive examinations.

3.2.3 Records and Documentation

Documentation, such as procedures and design packages, for low safety-significant SSCs may be less detailed than for high safety-significant items. In assessing the level of detail specified in procedures or actual packages related to low safety-significant items, there should be enough evidentiary detail to maintain plant design and configuration control. Further,

[2] Several QA-related regulatory guides were withdrawn in 1991 because the ANSI standards that they endorsed were incorporated into ANSI/ASME NQA-1-1983, "Quality Assurance Program Requirements for Nuclear Facilities." The withdrawal of a regulatory guide does not alter any prior or existing licensee commitments based on the use of the withdrawn regulatory guides. At their discretion, licensees with prior or existing commitments to withdrawn regulatory guides or standards may continue to implement those provisions, or revise their commitments to adopt the ANSI/ASME NQA-1-1983 standard.

sufficient records need to be maintained to evaluate failures, to perform root cause analyses, and to determine appropriate corrective actions.

3.2.4 Audits

Processes and work associated with low safety-significant SSCs may be audited less deeply and less frequently than high safety-significant activities. Surveillance, performance monitoring, self-assessments, trend data, or other activities may in some cases replace formal audits in low safety-significant areas.

3.2.5 Staff Training and Qualification Requirements

The licensees may establish different training and qualification requirements for personnel performing tasks only on safety-related low safety-significant SSCs, however, those personnel would need to remain sufficiently technically proficient in their assigned area of responsibility to provide reasonable confidence that their tasks were adequately performed to ensure that affected SSCs would be capable of performing their intended functions. The licensee must meet the requirements of the applicable regulations and technical specification requirements pertaining to training programs and staff qualifications.

3.2.6 Corrective Action

The GQA effort will identify a population of low safety-significant, safety-related items. In accordance with Criterion XVI, "Corrective Action," of Appendix B to 10 CFR Part 50, the timeliness of corrective actions for these items can be prioritized commensurately with their safety significance.

3.2.7 Design

The licensee may choose to change selected commitments to previously withdrawn regulatory guides[2] or ANSI Standard N45.2.11 (Ref. 11) for low safety-significant items. These changes could relate to (1) the need to consider *all* design input aspects as stated in Section 3.2 of ANSI N45.2.11, instead replacing this need with the need to prepare a documented checklist for only these items deemed necessary; (2) the need to consider, and document when deemed necessary, the 19 design review items delineated in Section 6.3.1 of ANSI N45.2.11; and (3) the adoption of independent design verification provisions contained in section 6.1 of ANSI N45.2.11 in lieu of the more restrictive position in previously withdrawn regulatory guides.[2] This would not obviate the need for inter-disciplinary design reviews.

3.3 Integrated Performance Monitoring Process

The implementation of an integrated performance monitoring process is necessary to ensure that the observed reliability and availability of SSCs following implementation of GQA remains consistent with the engineering evaluation developed to support the categorization process. The elements of an effective performance monitoring process are generally discussed in Section 2.5 of Regulatory Guide 1.174 (Ref. 3).

As discussed in this regulatory guide, GQA programs do not follow in detail all the steps inherent in other risk-informed regulatory decisionmaking applications as outlined in Regulatory Guide 1.174, because many of the SSCs of interest in GQA programs are not modeled in the PRAs, and it may not be possible to quantify the effects of changed QA programs on the modeled SSCs' performance. For these reasons, a larger portion of the decisionmaking is left to the discretion and judgment of licensee personnel who perform the integrated assessment function (typically an expert panel).

In the GQA program, the "operational feedback" and "corrective action" portions of the program assume considerable importance, and their acceptability must be pivotal in the determination of the overall program's acceptability and effectiveness. The licensee should develop criteria for monitoring the reliability and availability of (1) safety-related, low safety-significant and (2) non-safety-related, high safety-significant SSCs based upon risk insights developed during the safety-significance categorization process. The level of monitoring (e.g., SSC, train, system) should provide the capability to determine whether and when the reliability and availability of safety-related, low safety-significant and non-safety-related, high safety-significant SSCs deteriorates to unacceptably low levels and should include trending aspects intended to identify deteriorating performance. As QA programs address a broad spectrum of plant activities, the monitoring process should address monitoring of both plant hardware (SSCs) and the effectiveness of the process and the organization.

3.3.1 Operational Feedback Process

The GQA program should include a feedback process (which is generally performed by licensees irrespective of GQA) to evaluate plant and industry operational experience and the potential need to revise SSC safety-significance categorizations or QA controls. Sources of information that should be used to provide input to this feedback process include:

- **Operating Experience:** Sources of operating experience data include licensee performance indicators, NRC generic communications, Institute of Nuclear Power Operations (INPO) and Electric Power Research Institute (EPRI) design reliability data, Systematic Assessment of Licensee Performance (SALP) reports, licensee event reports (LERs), NRC inspection reports, equipment maintenance histories, plant performance reviews, reliability and unavailability data, equipment performance or condition trending data, and quality assurance assessments. The industry-wide data should be evaluated for consistency with PRA assumptions, system unavailabilities, and other plant-specific data.

- **Plant Modifications and SSC Replacements:** Plant modifications, as well as SSC replacements and parts thereof, might affect the safety-significance determination or selection of QA controls for low safety-significant SSCs. Accordingly, the GQA program should include provisions to periodically review plant modifications with respect to their potential impact on safety-significance determinations. Alternatively, the design change process may include provisions to verify that changes do not affect SSC safety significance or associated QA controls.

- **Reliability and Availability Monitoring:** The licensee should develop a living PRA or define performance thresholds based on ensuring, to the extent possible, that the equipment performance assumptions used in the PRA and upon which most of the safety categorization is based remain valid. The staff expects that licensees will integrate, or at least coordinate, their monitoring for risk-informed changes with existing programs for monitoring equipment performance and other operating experience on their site and throughout the industry. In particular, monitoring that is performed as part of the Maintenance Rule implementation can be used when the monitoring performed under the Maintenance Rule is sufficient for the SSCs affected by GQA. As GQA requires monitoring of SSCs not included in the Maintenance Rule, or requires a greater resolution of monitoring than the Maintenance Rule (component vs. train- or plant-level monitoring), it may be advantageous for a licensee to adjust the Maintenance Rule monitoring program rather than to develop additional monitoring programs for GQA purposes. Section 2.3, "Element 3: Define Implementation and Monitoring Program," of Regulatory Guide 1.174 provides amplifying guidance in this area.

A program assessment, which could be accomplished in conjunction with similar Maintenance Rule provisions, should be performed to ensure that the overall GQA process (activities associated with safety-significance determination, grading of QA controls, implementation of performance monitoring, and application of corrective actions) is being effectively implemented and provides insights into whether the GQA program needs improvements. As part of the assessment, (1) plant deficiencies should be evaluated, and (2) the bases for (a) the safety-significance categorizations (e.g., the PRA model and assumptions) and (b) the assignment of QA controls to each category should be evaluated to determine whether they continue to reflect plant design and operating practices. This assessment should not be performed in a graded manner and should be considered to be a high safety-significant activity as it serves to confirm the integrity of the GQA process implementation.

3.3.2 Corrective Actions

The licensee's GQA program should include comprehensive and effective corrective action and root cause analysis processes. Failures of safety-related, low safety-significant SSCs and non-safety-related, high safety-significant SSCs should be identified through operational feedback or trending processes so that the licensee can ascertain whether the SSC's unacceptable performance may be attributed to deficient QA controls or practices. Licensee corrective action or trending programs should identify and determine the apparent cause of failures of SSCs to determine whether licensee-established performance criteria or quality elements need to be changed. If the failure is determined to apply generically to other SSCs, or the failure represents a potential common cause concern for similar equipment installed in multiple systems, or if an excessive number of failures occurs that exceed licensee-established thresholds, then further licensee evaluations are warranted. An apparent cause determination is warranted to screen the failures in order to ascertain the necessity to perform more in-depth evaluations.

The SSC risk-categorization methodology could be affected by the SSC reliability and unavailability assumptions. These assumptions also could affect final categorization decisions to the extent that reliability and unavailability were used as a licensee criterion for determining the safety significance of an SSC that fails or exhibits a declining performance trend. Both the probabilistic and non-probabilistic methods previously used should be re-evaluated when there is significant disparity between the analysis assumptions and the observed data. The GQA

program controls should be evaluated to determine whether they need to be strengthened as a result of the failures. Based upon positive performance monitoring results, the licensee may further evaluate both safety-significance categorization and assignment of QA controls to identify situations in which they may be further relaxed. Such changes would be evaluated and reviewed by the staff as necessary, as discussed in other sections of this guide.

When a safety-related SSC has been categorized as low safety significant and, because of events such as plant modifications, reanalysis, or human errors, it is determined that the SSC should now be categorized as high safety significant, the licensee should take appropriate corrective action and evaluate the acceptability of the GQA controls applied to the SSC while categorized as low safety significant. This evaluation should be documented and should address the impact, if any, on the SSC as a result of applying GQA controls and should identify any GQA controls that need to be adjusted in order to provide assurance that the SSC will perform its safety functions. The licensee should maintain documented justification concerning the adequacy of the GQA controls applied to the SSC that is now categorized as high risk significant.

3.4 Change Control for Implementing Procedures

The licensee QA program for GQA will provide a high-level characterization of the GQA program elements as further discussed in Regulatory Position 4.1. As part of the implementation process for GQA, a number of procedures will be developed by the licensee for activities associated with elements of the GQA program. This would include procedures for aspects of the GQA program such as safety-significance determination, monitoring, working group, and expert panel functions, as appropriate. As these procedures will be considering important aspects of the GQA program that the staff will review, it is necessary that the procedures have an appropriate change control applied to them so the staff is informed of significant changes. Any procedure change that impacts on the QA program description must be assessed with respect to 10 CFR 50.54(a) (see Regulatory Positions 1 and 3.1.1 of this guide). The FSAR must incorporate by reference the GQA implementing procedures so that procedure changes will be controlled in accordance with 10 CFR 50.59.

4. ELEMENT 4: DOCUMENTATION

The recommended contents of a plant-specific, risk-informed GQA submittal are presented in this section. The guidance is intended to help ensure the completeness of the information provided and to aid in shortening the time needed for the review process. Additional guidance on style, composition, and specifications of safety analysis reports is provided in the Introduction of Revision 3 of Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)" (Ref. 12).

4.1 Licensee Submittal Documentation

To support the staff's conclusion that the proposed change is consistent with the key principles of risk-informed regulation and NRC staff expectations, the following information is expected to be submitted to the NRC.

4.1.1 GQA Program Change

The licensee's existing QA program description contained in, or referenced by, the FSAR should be revised to describe the GQA program provisions. The submittal containing the proposed GQA provisions should contain the following.

(1) A discussion of the essential implementation elements of the GQA program, the scope of potential SSCs that may be in the GQA program, and the basis for concluding that the overall GQA program provides reasonable confidence that SSCs remain capable of performing their intended function.

(2) An overview discussion of the process and guidelines developed by the licensee to determine the safety-significance categorization of all SSCs within the GQA program scope as defined in this regulatory guide.

(3) A statement of the role of the staff who perform the integrated assessment function (expert panel).

(4) The process for determining the QA controls being applied to each safety-significance category of SSCs.

(5) A description of the adjustments proposed as part of the GQA program and how the requirements of each of the criterion of Appendix B to 10 CFR Part 50 will be satisfied in a graded manner. The description should identify any exceptions to existing QA program commitments (such as regulatory guides).

(6) A discussion of how augmented QA controls for non-safety-related SSCs categorized as high safety significant will be determined.

(7) A discussion of the operational feedback and enhanced corrective action mechanisms and processes to adjust both safety-significance categorization of SSCs and the associated QA controls.

(8) A discussion of the performance monitoring process, along with the SSC functional performance and availability attributes that form the basis of the proposed change.

4.1.2 Supplemental Information

In addition to the submittal of the QA program change, the licensee should submit documentation that, although not incorporated into the QA program itself, will be needed by the staff to help determine the acceptability of the program. These documents should include:

(1) A full set of the records and analyses related to the categorization of one system. This documentation should include all supporting information developed and used during the process, all documented deliberations and justifications developed by the relevant panels, and the results of the categorization for all SSCs in the system. The submitted information should only include documentation that the licensee intends to maintain in support of future program changes and NRC inspections.

(2) Plant procedures and instructions that provide the programmatic guidance to the utility staff on the SSC categorization, monitoring, and feedback that will be implemented in support of the GQA program.

(3) The methodology, PRA change summary, and results of the bounding analysis, augmented by a discussion of the nonquantified aspects of the GQA program that are expected to provide a safety benefit. The scope, in terms of systems included in the bounding analysis, should be discussed. If the bounding analysis was performed on a limited number of systems, the systems should be clearly identified.

(4) A description of the licensee process to ensure PRA quality, a discussion as to why the PRA is of sufficient quality to support the categorization process, and the results of all peer or industry reviews of the PRA.

(5) Applicable documentation discussed in Section 3.3, "Cumulative Risk," of Regulatory Guide 1.174 (Ref. 3).

(6) A description of how the proposed change impacts any licensee commitments.

4.2 Plant Data and Engineering Evaluation

Licensees may submit the following information as a separate document to support the proposed GQA submittal. This information should be available for staff review at the licensee's offices.

4.2.1 Systems Pertinent to GQA

Summarize design and operating features of systems in which changes to the QA program are planned, as well as systems supported by the systems in which changes to the QA program are planned. For each system, include a table summarizing the key design and operating data. Values that are used in the analysis should be identified and justified. Refer to appendices or other documents (e.g., specific sections of the FSAR or design basis documents) as necessary for more details. Systems to be considered should include the pertinent portions of all systems modeled in the plant-specific probabilistic analysis.

4.2.2 Status of SSCs

All SSCs whose QA program control is proposed to be changed should be listed and should include (at a minimum) the plant's SSC label, the current QA categorization (by default all safety-related SSCs will initially have a "high" QA categorization), the proposed QA categorization, associated correlation with system functions, and a brief explanation of the justification for the proposed change.

4.2.3 Plant Operating Experience

Summarize any major events involving failures if the occurrence was attributable to inadequate or improperly applied QA controls at this plant. Include in this summary any lessons learned from these events and indicate actions taken to prevent or minimize recurrence of the events.

4.2.4 Engineering Evaluation

The categorization process is considered an engineering analysis, and as such, the completed analysis should be considered a quality record. In addition to the submittal documentation discussed in Regulatory Position 4.1, Regulatory Guide 1.174 (Ref. 3) provides guidance on documentation that may

be required to support a risk-informed application. The licensee should review the guidance in Regulatory Guide 1.174 and either develop the documentation or ensure that sufficient material is available that the documentation can be developed if requested. Additional documentation that should be available if requested includes:

- Documentation describing the methods and techniques used for developing quantitative and qualitative risk insights used to support the safety-significance categorization of SSCs.

- Documentation corresponding to the sample document submitted (described in (1) in Regulatory Position 4.1.2) for all systems that have been categorized.

- A description of how the importance measures were calculated and used (including the guidelines to categorize if applicable). This information should be augmented by technical description on how the limitations associated with the use of importance measures were communicated to the expert panel and resolved.

- Important assumptions, including SSC functional capabilities and performance attributes, that play a key role in supporting the acceptability of the QA program change and that are used in the monitoring and feedback program.

REFERENCES

1. USNRC, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register,* Vol. 60, p. 42622 (60 FR 42622), August 16, 1995.

2. "Development of Graded Quality Assurance Methodology," SECY-95-059, March 10, 1995.[1]

3. USNRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, July 1998.[2]

4. Letter from James L.Milhoan (NRC) to William Rasin (Nuclear Energy Institute), June 15, 1994.[1]

5. "Graded Quality Assurance/Probabilistic Risk Assessment Implementation Plan for the South Texas Project Electric Generating Station," SECY-97-229, October 6, 1997.[1]

6. American National Standards Institute (ANSI), "Quality Assurance Requirements for Control of Procurement of Items and Services for Nuclear Power Plants," N45.2.13, published by the American Society of Mechanical Engineers, 1976.

7. USNRC, "Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage, and Handling of Items for Water-Cooled Nuclear Power Plants," Regulatory Guide 1.38, Revision 2, May 1977.[1]

8. ANSI, "Requirements for Auditing of Quality Assurance Programs for Nuclear Power Plants," ANSI N45.2.12, 1977.

9. ANSI, "Packaging, Shipping, Receiving, Storage and Handling of Items for Nuclear Power Plants (During the Construction Phase)," ANSI N45.2.2, 1972.

10. American Nuclear Society (ANS), "Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants," ANS 3.2/ANSI 18.7, American Nuclear Society, 1976.

11. ANSI, "Quality Assurance Requirements for the Design of Nuclear Power Plants," ANSI N45.2.11, 1974.

12. USNRC, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.70, Revision 2, November 1978.[2]

[1] Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

[2] Single copies of regulatory guides, both active and draft, and draft NUREG documents may be obtained free of charge by writing the Reproduction and Distribution Services Section, OCIO, USNRC, Washington, DC 20555-0001, or by fax to (301)415-2289, or by email to GRW1@NRC.GOV. Active guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161. Copies of active and draft guides are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

REGULATORY ANALYSIS

A draft regulatory analysis was published with the draft of this guide, DG-1064, when it was issued for public comment in June 1997. No significant changes were necessary from the original draft, so a separate value/impact statement for this final Regulatory Guide 1.176 has not been prepared. A copy of the draft regulatory analysis is available for inspection or copying for a fee in the Commission's Public Document Room at 2120 L Street NW, Washington, DC, under Task DG-1064.

Printed on recycled paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67