U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

June 1997
Division 1
Draft DG-1064

DRAFT REGULATORY GUIDE

Contact: J. Guttmann (301)415-7732

DRAFT REGULATORY GUIDE DG-1064

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

DFD2 0/1

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules and Directives Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by **September 30, 1997.**

Requests for single copies of draft or active regulatory guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, Attention: Printing, Graphics and Distribution Branch, or by fax to (301)415-5272.

1. INTRODUCTION

1.1 Background

The NRC has promulgated deterministic criteria for determining which commercial nuclear power plant equipment is considered safety-related (see 10 CFR 50.2, Appendix A to 10 CFR Part 100, 10 CFR 50.65, and 10 CFR 50.49). Because of the importance of the safety-related equipment to protect public health and safety, the NRC has additionally required that a quality assurance (QA) program (described in Appendix B 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 judgement 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 will provide new insights that may be utilized by licensees to determine the relative safety-significance of plant equipment. The probabilistic insights could then be utilized to 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 typically categorized as follows: 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 document provides guidance that could be used 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 Part 50 of Title 10 of the Code of Federal Regulations (10 CFR 50). The general statements contained in Appendix B are supplemented by industry standards and NRC regulatory guides which describe specific practices that have been found acceptable by the industry and NRC staff. Although both Appendix B and the associated industry standards allow a large degree of flexibility, the licensees and the Nuclear Regulatory Commission (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, maturing of licensee programs and personnel, and increased pressures to control plant operating costs.

Graded quality assurance (GQA) is intended to provide a safety benefit by allowing licensees and 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 decision making 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 given in SECY-95-059, "Development of Graded Quality Assurance Methodology" (March 10, 1995) (Ref. 1).

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) on June 15, 1994. 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 structures, systems, and components (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

Also, during the last several years, both the NRC and the nuclear industry have recognized that PRA has evolved to the point where it may be used as a tool in regulatory decision making 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. 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. Where 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 shall 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 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).

1.2 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 an acceptable approach for monitoring the effectiveness of the GQA program implementation, and for determining when it may be necessary to make adjustments in quality assurance 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 decision making, 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 which must be evaluated, and documented, by a licensee 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 their site specific program.

1.3 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 two or more safety significance categories as discussed in Draft Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Ref. 2). Chapter 2 provides an overview of the four-element process used for implementing risk-informed GQA. Chapter 3 provides a discussion of Element 1, a definition of proposed changes to QA applications; Chapter 4 discusses element 2 and addresses engineering evaluations applicable to GQA programs; Chapter 5 discusses element 3 and provides specific guidance for an acceptable approach for implementing graded quality assurance controls and for developing performance monitoring strategies; The documentation and submittal aspects related to the change (element 4) is specified in Chapter 6.

1.4 Relationship to Other Guidance Document Applications

Draft Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Ref. 2) describes a general approach to risk-informed, regulatory decision making 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 the "overall" guide.

Licensees may choose to use risk-informed decisionmaking in application areas other than Graded QA. It is anticipated that certain efficiencies could be realized in that situation. It is possible that a single list of SSCs could be defined as safety significant for multiple risk-informed applications if a sufficiently robust process were utilized.

Regulatory guides are issued to describe to the public methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques used by the staff in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations; and compliance with regulatory guides is not required. Regulatory guides are issued in draft form for public comment to involve the public in developing the regulatory positions. Draft regulatory guides have not received complete staff review; and they therefore do not represent official NRC staff positions.

The information collections contained in this draft 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.

2. 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 decision making, a regulatory guidance document, DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Ref. 2), is being developed that establishes five safety principles and describes a 4-element process for evaluating risk-informed regulatory changes consistent with addressing those principles, as illustrated in Figure 2.1. DG-1061 provides additional description of quantitative acceptance guidelines, discussion on defense-in-depth aspects, and addresses safety margins. The principles are:

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

2. Defense-in-depth is maintained.

3. Sufficient safety margins are maintained.

4. Proposed increases in risk, and their cumulative effect are small and do not cause the NRC Safety Goals to be exceeded.

5. Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.

The individual elements of this process are described in the general guidance document. Those generally applicable discussions are not repeated here. Instead, an acceptable method and issues to be addressed by the licensee to fulfill the guiding principles is described for categorizing SSCs at nuclear power plants in a manner commensurate with their safety significance (using integrated traditional engineering, qualitative, and probabilistic insights) and for applying appropriate QA programs to each category of SSCs.

The process described below begins with a set of actions related to proposed changes in the QA categorization of certain SSCs. The process for developing the initial proposal for the changes is left to the utility, 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 (see further discussion under "Element 1" below).

Element 1: Define the Proposed QA Program Change

In this element, the licensee identifies the scope of candidate SSCs, and associated activities, for a risk-informed application of QA requirements including:

a) systems and components that are subject to current Appendix B QA requirements,

b) SSCs modeled in the PRA for the plant,

c) non-safety related SSCs that are within the Maintenance Rule scope, and

d) 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 on the docket, 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 decision-making process. And, available industry and plant-specific operational experience information relative to GQA should be assessed.

Further, the licensee should also identify the overall objective and approach of the proposed changes to the QA program for the candidate SSCs. More details are provided in Chapter 3 of this document.

Element 2: Engineering Evaluations

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 decision making 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 probabilistic risk assessment techniques. In addition, an assessment is required to ensure that no more than small risk increases are introduced by the proposed changes, as described in Chapter 4. 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 Chapter 4.

Element 3: Develop Implementation and Performance Monitoring Strategies

The third element involves developing graded QA control implementation and monitoring plans. These plans should be formulated to assure 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 which are found to be 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. 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 Chapter 5.

Element 4: Document Evaluations and Submit Request

The final element involves documenting the analyses for staff or independent review, audit 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. If the proposed change does not involve a reduction in the licensee's QA commitments, then prior staff review and approval is not required and the change to the QA program is submitted in accordance with 50.71(e). The changes associated with the adoption of graded QA proposed by the licensee will be described in the QA Program. In addition, important assumptions including SSC functional capabilities, impact of failure on safety significant functions, and performance attributes, which 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 graded QA effort is listed in Chapter 6 of this regulatory guide.

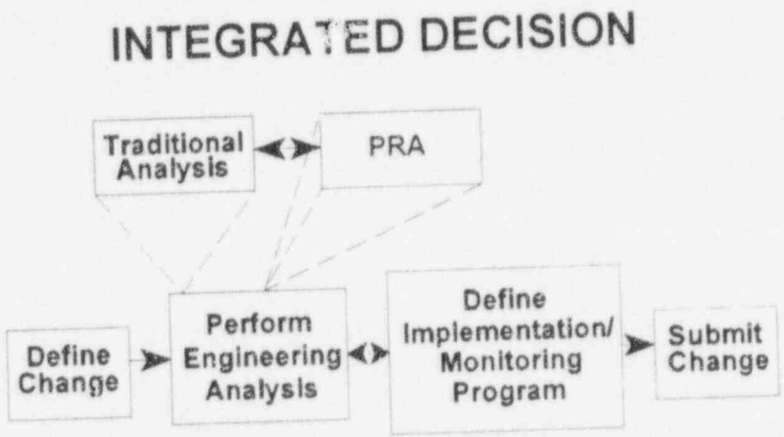

Figure 2.1 General Description of an Acceptable Approach to Risk-Informed Applications

3. ELEMENT 1: DEFINE THE PROPOSED CHANGES

The first element in the process of evaluating a change to GQA programs involves providing a full definition of the change. The first step is to identify the overall scope of the QA 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 decision making process. To accomplish this the licensee should:

1. Identify 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 10 CFR Part 50, Appendices A and B, 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 documentation such as the QA program description, the final safety analysis report, 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 graded QA requirements. Candidate SSCs include those that are (a) subject to current Appendix B QA requirements, (b) SSCs modeled in the licensee's PRA for the plant, and (c) non-safety related SSCs that are within the Maintenance Rule scope (which includes the non-safety-related SSCs that are (i) relied upon to mitigate accidents; ii) that are used in emergency operating procedures; iii) those whose failure could prevent a safety-related SSC from performing its safety-related function; and iv) those whose failure could cause a reactor scram or actuation of a safety-related system). In addition, non-safety related equipment that has previously received augmented quality treatment (e.g., Anticipated Transient Without Scram, Station Blackout, Fire Protection) should be considered in the GQA application scope.

3. Identify the expected revisions to existing implementing guidance of QA requirements that will result from the graded QA program. 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 Final Safety Analysis Report (FSAR), a QA topical report (if applicable), and other docketed correspondence (e.g., responses to generic communications, inspection reports, etc). 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 in accordance with 10 CFR 50.54(a).

4. The licensee should evaluate its risk studies to determine the extent to which quantitative and qualitative risk insights may be utilized. The quality, level of review of, 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 graded QA 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 graded QA 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 Chapter 4 and receive subsequent approval of the 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 where appropriate. For those safety-related SSCs that are low-safety-significant, relaxation in QA controls may be proposed. For non-safety-related SSCs that are low-safety-significant, licensees would continue to define their quality controls.

4. ELEMENT 2: ENGINEERING EVALUATION

In Draft Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis " (Ref. 2), Element 2 is the engineering evaluation conducted to support decisions to change a plant's licensing bases. 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 graded QA controls are explicitly modeled in PRAs. This small percentage arises from PRA's emphasis on the control and mitigation of severe accidents and 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 monitoring equipment from the models, 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 components for utilization in Graded QA should be accomplished through the use of traditional engineering evaluations in combination with quantitative risk importance measures and qualitative risk insights. Such a combined, "integrated" approach is necessary to utilize the strengths and avoid inherent limitations in each method. Draft Regulatory Guide DG-1061 discusses applications where risk insights are characterized by calculated risk importance measures or bounding estimates, or a qualitative assessment where the anticipated risk impact is minimal.

4.1 Safety-Significance Categorization

A minimum of two levels of categorization are needed, 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 comprised of high/medium/low safety significance. From a regulatory point of view, it is essential to assure 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 (medium, etc.) safety significance must be justified.

Systems have a variety of operating modes and perform a variety of functions, where each function is a well defined task requiring the proper operation of some sub-set 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 document 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 linkage between the functions a system performs and the components required to support each function is most clearly established in a matrix format as described in Section 4.1.3.

The categorization process must also systematically identify and track 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.

The quality, scope, and level of detail of the PRA should be commensurate with the extent that the PRA is used in the categorization process. As discussed in Draft Regulatory Guide DG-1061, the baseline risk profile and the magnitude of the anticipated change in risk are important considerations in the determination of the acceptability of risk informed applications. The licensee must demonstrate that the PRA is of sufficient quality to support a decision on the acceptability of the proposed change.

All operational modes and internal and external events should be included in the evaluation of the safety significance of systems, functions, and components. At a minimum, models and results for core damage and large early release frequency for internal initiating events at full power are needed. If quantitative risk analyses for shutdown conditions and "external" initiators such as fire, seismic, and winds are not available, qualitative assessments should be used to ensure the functions' safety significance categorization fully considers all relevant operational demands. Qualitative studies identify and characterize scenarios that are believed to be important, but without expending significant resources in quantifying the scenarios' frequencies. Seismic margin analysis and FIVE evaluations done to support IPEEE analyses are examples of qualitative studies which should be used.

4.1.1 Identification of System Functions

Definition of the proposed change includes the 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).

4.1.2 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 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 conservatively judge all components in a high-safety-significant system to be high-safety-significant, or they may further categorize components within systems based on the safety significance of the functions each component supports. To provide confidence that eventual determination of less than high-safety-significance is made with full recognition of each system's contribution to CDF and LERF, system-level importance should be determined even when function- or component-level importance measures are available.

PRA's integrated models provide an excellent framework to characterize system and system function importance. One area where PRA modeling is not fully adequate for graded QA applications is, however, cross-system dependencies arising from nominally identical components used in different applications throughout the plant (a type of circuit breaker, for example). Cross-system dependencies are not modeled in PRAs yet can have a significant impact on risk. Consequently, special consideration must be given to these sets of components as discussed in 4.2.

4.1.2.1 Quantitative Safety Categorization Insights

Quantitative importance measures from risk studies provide valuable insights about the relative ranking of the safety significance of well defined model elements in the PRA model such as basic events, components, human actions, functions, trains, or systems. Each measure represents the risk sensitivity of an individual model element. 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 during the integrated decision making.

At least two quantitative measures of importance are needed, one (such as Fussell-Vesely (FV) or risk reduction worth (RRW)) illustrating the fraction of current risk involving the failure of the model element, the other (such as risk achievement worth (RAW) or Birnbaum) illustrating the margin of safety contributed by the model element's proper operation. Other measures than those suggested may be used, but at least two measures reflecting current contribution and margin contribution are needed to balance the risk insights. A number of issues associated with the calculation and interpretation of importance measures are discussed in Appendix A of DG-1061 (Ref. 2). The licensee needs to be able to describe technically how each issue discussed in Appendix A was addressed and resolved.

System and system function level measures are difficult to define and calculate and alternative techniques for categorizing the safety significance of functions may be more practical. One alternative technique uses basic event importance measures (readily calculated by most PRA codes) to identify a set of system functions which are clearly high-safety-significance. This technique is based on recognition that the system and 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 and this technique are used, this property should be validated for the measures used).

The basic event importance measures should be calculated and compared to some quantitative guideline values (e.g., RAW > 2 or FV > 0.005; the specific values chosen should be justified by the licensee). All basic events with importance measure greater than (or less than, as appropriate) the guidelines are identified as potentially high-safety-significance basic events. Any system function modeled in the PRA which is supported by one or more potentially high-safety-significant basic events is categorized as a candidate high-safety-significant system function. Since it is possible that the system's and system function's RAW and FV measures are much higher than any individual basic event's, systems and 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 function-based analysis should be performed to determine the impact of the failure of candidate low-safety-significant systems. 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.

- Initiating events are usually 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 (i.e., loss of an air compressor 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 both cause an initiating event as well as the partial loss of mitigating function can be severely underestimated by surrogate basic event importance measures.

4.1.2.2 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 needs 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 (i.e., reactivity control, decay heat removal, etc.) 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 of 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 non-quantitative risk studies should also be used. Transients initiated during shutdown or initiated by external events such as earthquakes, high winds, and fires are often evaluated without developing and quantifying full probabilistic models. Nevertheless, these studies include information on the systems, functions, and components whose proper operation is credited in the defense against such transients. In particular, it is shown how the plant is intended to respond to such events, and, further, what alternative strategies are available if the preferred strategy fails. When such studies are not included in the quantitative safety significance categorization, all the systems and functions credited in these studies should be categorized as candidate "high-safety significant."

- 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.

4.1.3 Identification of Components Which Support Functions

Systems components where QA controls are applied and PRA basic events are different. 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, etc. 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 graded QA 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 for this component versus system function identification is a matrix as illustrated in Table 4.1 where the high-safety-significant system functions are listed and cross referenced to all the components needed to support each function at the level of equipment

specificity where changes in the application of QA controls will be pursued. The matrix should include all high-safety-significant system functions, all system components which support the high-safety-significant functions, and all external system support functions required by any component. Some examples illustrating areas of potential concern regarding the accuracy and completeness of the matrix are detailed below. The licensee needs to be able to describe technically how each issue was addressed and resolved.

- A 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.

- Instrumentation used to actuate and control system and plant functions needs careful attention if grading of instrumentation is contemplated. 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 un-proceduralized actions.

- Each system should be reviewed for the possibility of component failures that lead to an initiating event such as loss of feedwater, loss of component cooling water, etc. Components whose failure could cause an initiating event should be identified in the matrix as being required to support the normal operation function (e.g., AOV feedwater control valves are required to support feedwater at power).

The matrix 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, the matrix provides a traceable record of the previously assumed categorization of upper tiered functions requiring support from other systems. Eventually, all support function categorization 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.

4.1.4 Component Safety Significance Categorization

Selection of the final categorization of system functions and the components which support the high-safety-significant system function is done by integrated assessment of quantitative and qualitative risk insights as described in section 4.3.

The safety significance categorization assigned to components (and to support system functions which can be treated as component functions for initial categorization) is based on the safety significance of the function(s) the component supports. Components which 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 generally done 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 of the component could be a result of the QA program.

Table 4.1: Sample Emergency Service Water System Function Versus Component Function Matrix

COMPONENT	SYSTEM FUNCTIONS			REQUIRED COMPONENT SUPPORT
	Cool DG1A	Cool DG1B	Cool Charging Pump	
P-SCC-10A	X	X	X	E.Bus 13 DC Bus 23 ESAF x.x
CV-7	X	X	X	
MOV-SCC-165				E.Bus 13 DC.Bus 23 ESAF x.x
MV-63			X	
HX-14B			X	
MV-65			X	
CV-291	X			
HX-E-82A	X			
AOV-296	X			IA Fun. 5 DC.Bus 33 ESAF x.x

4.2 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 does not violate the safety principles. Guidelines for making that demonstration with due consideration for the scope of the QA program are summarized below. Other equivalent guidelines are acceptable.

The 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 ASME Code provisions to meet the requirements of 10 CFR 50.55a. In such instances, the ASME Code requirements need to be met.

The engineering evaluation conducted should assess whether the impact of the proposed change is consistent with the principle that sufficient defense-in-depth is maintained. 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 (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 engineering evaluation conducted 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 current licensing basis (e.g., FSAR and supporting analysis) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

The aspects of 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 reduced QA controls will be applied only to safety-related SSCs that are determined to be low-safety-significant, and these controls will continue to provide an adequate basis for concluding that the SSCs are expected to perform satisfactorily when called upon to operate .

- The resulting QA provisions will provide the necessary level of assurance that low-safety-significant, safety-related SSCs remain capable of performing their design functions.

The CDF and 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 PWR's 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 graded QA is control of potential common mode failures. As discussed in 4.1.2, groups of nominally identical SSCS, utilized in multiple systems throughout the plant, can as an aggregate have high safety significance. The reduction or loss of independence among components that could be introduced by a reduction of QA controls is not modeled in PRA. Consequently, the licensee should demonstrate that the potential for cross system common mode failures to substantially increase risk is minimized. This assessment is necessary since an underlying assumption in the PRA functional safety-significance determination is that cross system independence exists. Attributes of the QA program that would reduce the likelihood of such vulnerability should be discussed . For example, the graded QA program compensatory measures might include features such as receipt inspection and testing coupled with an appropriate performance monitoring and feedback program. Alternatively, quantitative analyses can be performed to demonstrate that substantial risk increases are minimal.

Principle four in Draft Regulatory Guide DG-1061 states that any proposed increase in risk is small and does not cause the NRC safety goals to be exceeded. The draft regulatory guide subsequently defines "small" quantitatively in the form of acceptance guidelines (see section 2.4.2.1 of DG-1061). Although the risk impact of graded QA 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 is available to define the impact of quality assurance programs on SSC reliability. Accordingly, licensees may chose to provide a qualitative evaluation addressing principle four directly, e.g., that any increase in risk will be small and the safety goals will not be exceeded. Such evaluations should explicitly address the monitoring and corrective action program. Alternatively, the licensee may use a quantitative evaluation based on, for example, sensitivity studies to demonstrate that the change in CDF and LERF as a result of the implementation of the graded QA program is not expected to exceed the acceptable changes in risk as defined by DG-1061.

4.3 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 categorized as low-safety-significant. The panel would nominally 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 both traditional engineering, probabilistic, and qualitative information available regarding the systems and system functions within the defined scope of the graded QA program changes. The evaluation should include either resolving or approving the resolution of the quantitative and qualitative issues addressed in sections 4.1.2.1 and 4.1.2.2.

Safety significance may be determined using guidelines related to prevention and mitigation of core damage, as well as containment integrity and large early release frequency. 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.

5. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING STRATEGIES

This section addresses the first, second, third and the fifth principles for risk-informed decisionmaking. The objective of the graded QA effort is to implement a QA 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 revised licensee's graded QA program will need to specifically identify how the 10 CFR 50, Appendix B criterion will be satisfied. The licensee may adjust the elements of the QA program as it deems 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.

5.1 Grading of Quality Activities

The first step of the evaluation process is for the licensee to identify specific elements of the quality assurance 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 on a sampling basis. 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.

5.1.1 Regulations and Commitments

In accordance with the first principle, no exemptions from current regulations are expected to be needed to implement a graded QA 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 re-stating 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 eighteen 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 QA 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 section 6.

However, plant SSCs cannot be re-classified as non-safety-related solely based on risk considerations. Regulatory requirements in Appendix A, Section VI(a)(1) of 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, when QA program reductions result in a loss of confidence of the SSC's ability to perform its design 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 relating 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 Final Safety Analysis Report (FSAR), the QA Topical Report, and other docketed correspondence (e.g., responses to generic communications, inspection reports, etc). 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 graded QA program should be identified and the manner in which they are being changed should be documented, reviewed, and approved where necessary by the NRC in accordance with 10 CFR 50.54(a), as appropriate.

5.1.2 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 section 4.3.

For safety-related SSCs determined to be high-safety-significant, the current QA practices contained in the NRC approved QA program should be retained.

Licensees have 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 SSCs assigned to the low-safety-significant category. Example areas where this may be possible are listed in Section 5.2 of this regulatory guide. In proposing to reduce controls, two basic objectives should be kept in mind. These are: the GQA program should be sufficient to assure the SSC's design integrity and ability to successfully perform its safety function, and the GQA program should include processes and documentation that support an effective corrective action program as discussed in section 5.3.2. Accordingly, in reducing or enhancing the QA program for any SSC the licensee needs to describe how the proposed changes will achieve the objectives. Also, consideration should be given to issues such as common cause failure issues, as discussed in section 4.2.

A QA program which will identify certain SSCs of low safety-significance and apply reduced QA requirements to those SSCs should, as a minimum, encompass the four essential elements [as identified in SECY 95-059, "Development of Graded Quality Assurance Methodology" (Ref. 1)], described in section 1.

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. Licensees should evaluate whether augmented quality assurance practices are warranted for these "high-safety-significant, non-safety-related" SSCs to achieve the above objectives and to fulfill the regulatory requirements of General Design Criterion 1 of Appendix A to 10 CFR Part 50,which requires that quality programs are to be applied commensurate with the relative importance of SSCs to plant safety. Licensees may voluntarily select certain Appendix B QA program controls as these augmented quality provisions. The use of risk insights should be performed in an integrated manner to identify areas where improvements should be implemented.

The categorization of SSCs as either high-safety or low-safety-significant is either derived directly or indirectly from the licensee's PRA, or from qualitative methods that consider the results of PRA where available. In particular, PRA takes credit systematically for non-safety-related SSCs as: 1) providing support to, or 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. The application of the augmented controls discussed above provides reasonable confidence that the reliability assumed in the risk analysis, or the associated qualitative decision making process, remains valid. The commitment to apply QA controls 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 QAP.

5.2 Potential Areas for Implementing Graded QA Program Controls

All QA program controls in Appendix B to 10 CFR Part 50 previously applied to low-safety-significant SSCs that are safety-related 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 which may be appropriate for applying graded quality assurance program controls for safety-related SSCs of low-safety-significance are discussed below. The list is not exhaustive and licensees may propose graded controls in other areas provided it can be shown the objectives discussed in section 5.1.2 above are met. The goal is to allow licensees flexibility to define acceptable QA controls which provide reasonable confidence that the SSCs will perform their intended functions.

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

5.2.1 Procurement

Licensees may establish less stringent quality assurance requirements for the procurement of low-safety-significant components than for high-safety-significant components. In making these changes, licensees should consider 10 CFR Part 21 and Appendix B to 10 CFR Part 50 requirements, as implemented by Regulatory Guides 1.44 and 1.123. Within this area, the technical requirements for CGI dedication in accordance with 10 CFR Part 21 (critical characteristics of an item for an application) are not subject to grading. However, for items of low-safety-significance, the verification of critical characteristics may be graded (e.g, by reduced sampling plans, or alternate 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.

5.2.2 Frequency of Inspections

The licensee may chose to reduce inspection activities related to low-safety-significant SSCs and choose to perform monitoring or surveillance oversight to assure that components can perform their intended functions. Verifications by peer personnel in-lieu of certified inspectors may be implemented for the low-safety-significant SSCs provided that the licensee uses individuals 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).

5.2.3 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, sufficient records need to be maintained to evaluate failures, perform root cause analyses, and to determine appropriate corrective actions. In all cases and regardless of the risk ranking, a licensee should be able to show that it has sufficient documentation to show that the current facility configuration is consistent with its design bases.

5.2.4 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.

5.2.5 Staff Training and Qualification Requirements

The licensees may establish different training and qualification requirements for personnel performing tasks on 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 affected SSCs would be capable of performing their intended functions. The licensee would need to meet the requirements of the applicable regulations and technical specification requirements pertaining to training programs and staff qualifications.

5.2.6 Corrective Action

Corrective actions are important for all safety-related SSCs and the staff has therefore not identified any portions of the Appendix B corrective action controls which appear to be candidates for grading.

5.3 Performance Monitoring

The implementation of a performance monitoring program is necessary so that the GQA program continues to ensure that component performance is consistent with that assumed in the categorization process. The conduct of performance monitoring is generally addressed in section 2.5 of DG-1061.

As discussed in this regulatory guide, GQA programs do not follow in detail all of the steps inherent in other risk-informed regulatory decision-making applications as outlined in DG-1061, 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 SSC's performance. For these reasons, a larger portion of the decision-making is left to the discretion and judgement 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 in the programs, and their acceptability must be pivotal in the determination of the overall program's acceptability. The licensee should develop criteria for monitoring the performance of the low-safety-significant SSCs based upon risk insights developed during the safety-significance categorization process. The level of the monitoring program (SSC, train, system, etc.) should provide the capability to determine if, and when, the performance of the low-safety-significant SSCs deteriorates to unacceptably low levels. As QA programs address a broad spectrum of plant activities, the monitoring program should address both plant hardware (SSCs) monitoring as well as process and organizational effectiveness monitoring.

5.3.1 Operational Feedback

The GQA program should include a 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. Operating experience and plant modifications are two sources of information that could give insights about the effectiveness of a licensee's GQA program and feedback mechanisms.

- 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, Nuclear Plant Reliability Data System (NPRDS), 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, and 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 periodically review plant modifications with respect to their potential impact on safety significance determinations. Alternately, 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 define performance thresholds based on ensuring, to the extent possible, that the equipment unavailabilities used in the PRA and upon which most of the safety categorization is based remain valid.

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 provide insights into whether the GQA program needs improvements. As part of the assessment, plant deficiencies should be evaluated and the bases for whether the safety significance categorizations (e.g., the PRA model and assumptions) and assignment of QA controls 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.

5.3.2 Corrective Actions

The licensee's graded QA program should include strong and effective corrective action and root-cause analysis, and one of the potential root causes considered should be whether the graded quality assurance treatments of SSCs are sufficient. That is, failures of low-safety-significant SSCs should be identified in accordance with corrective action programs or

trending programs so that the licensee can ascertain whether the reduction of the QA controls may have resulted in an unacceptable decrease in an SSC's performance.

Licensee corrective action or trending programs should identify, and determine the apparent cause of failures of SSCs, that meet licensee established thresholds, under the less stringent QA controls to determine if licensee established performance criteria and/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 occur, then further licensee evaluations are warranted. An apparent cause determination is still warranted to screen the failures in order to ascertain the necessity to perform more in-depth evaluations. The licensee's response to negative performance trends may need to include an assessment of the SSC's safety significance categorization, since the reduction in performance could affect the basis for assigning the SSC to the low-safety-significant category.

The SSC risk-categorization methodology could be potentially affected by the SSC reliability assumptions. This could also potentially affect final categorization decisions to the extent that reliability was used as a licensee criterion for determining the safety significance of the SSC that failed. Both the probabilistic and non-probabilistic methods previously used should be re-evaluated in those instances where there is significant disparity between the analysis assumptions and the observed data. The GQA program controls should be evaluated to determine if they need to be strengthened as a result of the failures. Additionally, based upon performance monitoring results, the licensee may further evaluate both safety-significance categorization and assignment of QA controls to identify situations where they may be relaxed. Such changes would be evaluated as discussed in other sections of this guide.

6. ELEMENT 4: DOCUMENTATION

The recommended format of a plant-specific, risk-informed GQA submittal is presented in this chapter. Use of this format by licensees will help ensure the completeness of the information provided, will assist the NRC staff in locating the information, and will 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)."

6.1 GQA Program Submittal

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) The description of the graded QA program implementation scope and the basis for concluding the overall QA program provides reasonable confidence that SSCs remain capable of performing their intended function.

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

(3) 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 50 will be satisfied in a graded manner.

(6) Augmented QA controls for non-safety-related SSCs categorized as high-safety-significant.

(7) Important assumptions including SSC functional capabilities and performance attributes, which play a key role in supporting the acceptability of the QA program change. Since continued satisfaction of these assumptions is necessary to maintain the validity of the categorization process, these licensee commitments will need to be reflected in the QAP description of the change.

(8) The operational feedback and enhanced corrective action mechanisms and processes to adjust both safety significance categorization of SSCs and the associated QA controls.

(9) The performance monitoring process, and SSC functional performance and availability attributes which form the basis of the proposed change.

6.2 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.

6.2.1 Systems Pertinent to GQA

Summarize design and operating features of systems where changes to the QA program are planned, and systems supported by the systems where changes to the QA program are planned. For each system, include a table summarizing 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 bases 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.

6.2.2 Status of SSCs

All SSCs whose QA program control is proposed to be changed should be listed in a table which 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.

6.2.3 Plant Operating Experience

Summarize any major events involving failures whose 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.

6.2.4 Engineering Evaluation

In addition to the general documentation requirements identified in DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Ref. 2), provide justification of the plant's continued compliance with applicable rules and regulations, and provide a complete description of each issue considered for the engineering evaluation and a discussion of how the resolution of each issue impacts the categorization of SSCs. All information should be provided in the main report.

Documentation should also be available describing the methods and techniques used for developing quantitative and qualitative risk insights used to support the categorization the safety significance of SSCs. All risk studies used should be clearly identified, including the date and the version of the studies as applicable. Other documentation should include a description of;

(1) The review process whereby the risk studies, the findings of the review process, and the licensees response to any questions or comments raised by the reviewers.

(2) 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 discussed in Chapter 4.1.2.1 were resolved.

General guidance on acceptable documentation for the content and quality of risk studies used to support a risk informed application can be found in DG-1061, "An approach for using probabilistic risk assessment in Risk-informed decisions on plant-specific changes to the current licensing basis."

REFERENCES

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

2. USNRC,"An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Draft Regulatory Guide DG-1061, June 1997.[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]Requests for single copies of draft or active regulatory guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, Attention: Printing, Graphics and Distribution Branch, or by fax to (301)415-5272.

Regulatory Analysis

1. Statement of the problem

During the past several years, both the Commission and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point that it can be used increasingly as a tool in regulatory decisionmaking. In August 1995 the Commission published a policy statement that articulated the view that increased use of PRA technology would 1) enhance regulatory decisionmaking, 2) allow for a more efficient use of agency resources, and 3) allow a reduction in unnecessary burdens on licensees. In order for this change in regulatory approach to occur, guidance must be developed describing acceptable means for increasing the use of PRA information in the regulation of nuclear power reactors.

2. Objective

To provide guidance to power reactor licensees and NRC staff reviewers on acceptable approaches for utilizing risk information (PRA) to support requests for changes in a plant's current licensing basis (CLB). It is intended that the regulatory changes addressed by this guidance should allow a focussing of both industry and NRC staff resources on the most important regulatory areas while providing for a reduction in burden on the resources of licensees. Specifically, guidance is to be provided in several areas that have been identified as having potential for this application. These applications include risk-informed inservice testing, technical specifications, and graded quality assurance.

3. Alternatives

The increased use of PRA information as described in the draft regulatory guides being developed for this purpose is voluntary. Licensees can continue to operate their plants under the existing procedures defined in their CLB. It is expected that licensees will choose to make changes in their current licensing bases to use the new approaches described in the draft regulatory guides only if it is perceived to be to their benefit to do so.

4. Consequences

Acceptance guidelines included in the draft regulatory guides state that only small increases in overall risk are to be allowed under the risk-informed program. Reducing the test frequency of valves identified to represent low risk as provided for under this program is an example of a potential contributor to a small increase in plant risk. However, an improved prioritization of industry and NRC staff resources, such that the most important areas associated with plant safety receive increased attention, should result in a corresponding contributor to a reduction in risk. Some of the possible impacts on plant risk cannot be readily quantified using present PRA techniques and must be evaluated qualitatively. The staff believes that the net effect of the risk changes associated with the risk-informed programs, as allowed using the guidelines in the draft regulatory guides, should result in a very small increase in risk, maintain a risk-neutral condition, or result in a net risk reduction in some cases.

5. Decision Rationale

It is believed that the changes in regulatory approach provided for in the draft regulatory guides being developed will result in a significant improvement in the allocation of resources both for the NRC and for the industry. At the same time, it is believed that this program can be implemented while maintaining an adequate level of safety at the plants that choose to implement risk-informed programs.

6. Implementation

It is intended that the set of risk-informed regulatory guides be published by the end of CY 1997.

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