Inspection Procedure 62709

# CONFIGURATION RISK ASSESSMENT AND RISK MANAGEMENT PROCESS

PROGRAM APPLICABILITY: 2515, APPENDIX B

## 62709-01 INSPECTION OBJECTIVE

01.01 The objective of this procedure is to independently assess the extent of conditions of a licensee's implementation of Maintenance Rule (a)(4) requirements after significant problems associated with the licensee's configuration risk assessment and risk management process have been identified. This procedure can also be used to independently assess the licensee's use of probabilistic safety assessment (PSA) and risk assessment tools for implementing the Maintenance Rule 10 CFR 50.65(a)(4) requirements.

## 62709-02 INSPECTION REQUIREMENTS

The scope of the inspection is focused on those specific requirements listed below that are necessary to assess the adequacy of the licensee's implementation of the Maintenance Rule (a)(4) requirements. The inspection may involve an in-depth review of the licensee's use of PSA and risk assessment tools for the configuration risk assessment and risk management process. Due to the variation of PSA methodologies and analytical tools used by licensees, this inspection shall be performed by Regional Senior Reactor Analysts (SRAs), or Headquarters risk analysts supported by personnel who are qualified inspectors and have Maintenance Rule training. This procedure is to be used in conjunction with Supplemental Inspection Procedure 95002, "Inspection for One Degraded Cornerstone or Any Three White Inputs in a Strategic Performance Area."

02.01 Scope of SSCs for (a)(4) Assessments. Determine if the licensee has established an adequate scope of structures, systems, or components (SSCs) required for 10 CFR 50.65 (a)(4) assessments. Select a sample of 10 to 12 SSCs covered by the Maintenance Rule that the licensee's expert panel has excluded from (a)(4) assessments. The sample shall include high safety-significant SSCs that are not explicitly modeled in the licensee's PSA, and SSCs which have been removed from the (a)(4) list of SSCs modeled in the PSA as a result of decisions made by the licensee's expert panel.

02.02 Configuration Risk Assessments. Determine if the licensee has adequately assessed the overall effect on the performance of safety functions when SSCs are removed from service for surveillance or maintenance activities. Obtain plant operating/maintenance records for at least two or three monthly periods of high maintenance activities during power operation with a particular focus on periods when trains of components were removed from service or when components from different trains were

out of service simultaneously for surveillance or maintenance. In the case of plant shutdown conditions, select two or three weekly periods of plant outage surveillance or maintenance activities with a particular focus on periods of reduced reactor coolant system inventory, reduced shutdown cooling availability, or reduced electric power availability. Evaluate the results of the licensee's safety assessments of those selected time periods, and verify the licensee's safety assessments encompassed all the SSCs that have significant impact on public health and safety. If the licensee had not kept records of prior assessment results, the SRA/risk analyst shall consider performing independent assessments of current maintenance activities.

02.03 Risk Management. Determine if a licensee is using a reasonable approach to manage the risk of planned configurations when SSCs are removed from service for surveillance or maintenance activities. On the basis of licensee's safety assessments of those selected maintenance configurations, either during power operation or shutdown conditions, verify that the licensee has process controls in place that ensure risk management actions would be implemented for plant maintenance configurations with risk increases that exceed risk management action thresholds. Section 11.3.7 of NUMARC 93-01 provides a detailed discussion of establishing risk management action thresholds based on quantitative and qualitative considerations.

## 62709-03 INSPECTION GUIDANCE

### General Guidance

This inspection procedure is to be used to assess the adequacy of the licensee's implementation of Maintenance Rule (a)(4) requirements after significant problems associated with the licensee's configuration risk assessment and control process have been identified by NRC resident inspectors. Typical significant problems are failure to consider SSCs that have potentially significant impact on public health and safety in the scope of (a)(4) assessments, chronic failures to perform (a)(4) assessments, inadequate safety assessments, and inadequate compensatory measures when risk management action thresholds are exceeded. Except when the licensee proposes an alternate method for complying with specified portions of 10 CFR 50.65 (a)(4), the methods described in Regulatory Guide (RG) 1.182 will be used to evaluate the activities of licensees who are required to comply with the Maintenance Rule (a)(4) provisions. This regulatory guide endorses NUMARC 93-01, Section 11, and provides methods acceptable to the NRC for complying with the Maintenance Rule (a)(4) requirements. The SRA/risk analyst should become familiar with RG 1.182, and Section 11 of NUMARC 93-01 before initiating this inspection. The SRA/risk analyst should also be aware that licensees may use methods other than those described in RG 1.182 and NUMARC 93-01 to satisfy the Maintenance Rule (a)(4) requirements. Where other methods are used, the licensee must demonstrate that those methods satisfy the (a)(4) requirements of the rule. Where a licensee implements (a)(4) partly in accordance with RG 1.182 and Section 11 of NUMARC 93-01 and partly in accordance with other methods, the licensee must demonstrate that those other methods comply with the applicable parts of the Maintenance Rule (a)(4) statement.

With very few exceptions, licensees would be using the guidance in Section 11 of NUMARC 93-01. Before inspecting the implementation of (a)(4), the SRA/risk analyst should be familiar with the methods used by other plants that the NRC staff has found acceptable.

A. SSC Scoping Process

10 CFR 50.65(a)(4) states in part: "The scope of the assessment may be limited to structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety." This statement provides an option for determining the scope of SSCs subject to the (a)(4) assessment that may not include all SSCs which meet the scoping criteria of 10 CFR 50.65(b)(1) and (b)(2). If the licensee elects to use a risk-informed evaluation process to determine the scope of SSCs for the (a)(4) assessment, the plant's PSA could be used as an appropriate mechanism to define the assessment scope. Typically, the PSA scope is developed with consideration of dependencies and support systems. Through definition of top events, cutsets, and operator recovery actions, the PSA scope includes those SSCs that could, in combination with other SSCs, result in significant risk impacts. Thus, the SSCs subject to an (a)(4) assessment may be limited to the following scope:

(1) SSCs modeled in the plant's Level 1, internal events PSA, and

(2) SSCs determined to be high safety-significant by the Maintenance Rule expert panel based on engineering judgment and operating experience.

The licensee's PSA model must be of sufficient detail to support decisions regarding SSC scope determinations. At the minimum, the PSA model should have visible and accurate treatment of dependencies and interfaces among the plant safety functions, system responses, and operator actions needed for accident mitigation. For (a)(4) assessments, the PSA model should include both front-line/support system dependencies and support system/support system dependencies, to the extent that these inter-system dependencies would have a significant effect on the key plant safety functions. Typically, the licensee's PSA documentation would provide dependency matrices which show the systematic evaluation of inter-system dependencies. Furthermore, the Initiator and System Dependency Table (i.e., Table 2) of the plant Risk-Informed Inspection Notebook (also called the SDP Notebook) would provide information on the major dependencies between front-line and support systems. The SRA/risk analyst could utilize the information provided in this Table to verify the adequacy of the scope of SSCs subject to (a)(4) assessments. If the modeling of inter-system dependencies is determined to be inadequate, the licensee should either revise the PSA to address the inter-system dependencies or add the SSCs to the scope of (a)(4) assessments.

The SRA/risk analyst should be aware of limitations in the licensee's PSA. The SRA/inspector should verify that the Maintenance Rule expert panel compensates for known limitations in the PSA by using the Maintenance Rule expert panel's experience-based perspective during the SSC scoping process. Significant PSA limitations and how the Maintenance Rule expert panel addresses the limitations should be documented in the inspection report.

The SRA/risk analyst should be aware that the results obtained from any PSA can be highly dependent on the plant configuration and the system reliability and availability data used to perform the calculations. Therefore, licensees should reconsider SSC scope determinations periodically whenever the plant design is modified, the PSA is updated, new insights become available from configuration management reviews, or new reliability and availability data become available.

B. Configuration Risk Assessments

10 CFR 50.65(a)(4) requires that licensees assess and manage risk that may result from maintenance activities during all modes of plant operation (i.e., including low power and shutdown conditions). An appropriate assessment would include a review of the current configuration of the plant and the plant configuration expected during the planned maintenance activity. Assessing the current plant configuration as well as expected changes to plant configuration due to the planned maintenance activities is intended to ensure that the plant is not inadvertently placed in risk-significant configurations. These assessments do not necessarily require that a quantitative assessment of probabilistic risk be performed. The level of sophistication with which such assessments are performed is expected to vary, based on circumstances involved. It should be understood that the contribution to risk of a specific plant configuration depends on both the degree of degradation of the safety functions and the duration for which the plant is in that configuration. However, the majority of available shutdown risk assessment tools do not allow the effects of duration on maintenance configurations during plant shutdown conditions to be easily assessed. Therefore, the risk impact of shutdown configurations may be assessed, at the present time, by considering only the effects of degradation of key safety functions. Furthermore, assessing the degree of safety function degradation requires that there be an understanding of the impact of maintenance activities on the capability of the plant to prevent or mitigate accidents and transients, as well as the potential impact of external conditions (e.g., inclement weather, electrical grid instability, flooding or seismic events) on plant maintenance configurations. The assessments may range from deterministic judgments to the use of an on-line PSA tool.

An assessment should be initiated following the discovery of emergent failures or changes in plant conditions to determine the safety impact of the failure or change in plant conditions. However, the reevaluation of prior assessment(s) should not interfere with, or delay, operator and maintenance crew from taking timely actions to restore the appropriate SSC to service or taking compensatory actions before the end of a work shift. If the SSC is expeditiously restored to service prior to the performance of the assessment, the evaluation need not be conducted.

The process for performing these safety assessments should be scrutable and repeatable. Known limitations in the assessment process should be described in the licensee’s Maintenance Rule program documentation. The licensee’s process should be sufficiently robust and comprehensive to assess maintenance activities during power operating conditions and low power and shutdown conditions. The sophistication of the assessment(s) for evaluating the risk of a maintenance configuration should be commensurate with the complexity of the configuration.

Two methods commonly used to evaluate the risk impact of plant maintenance configurations are (1) using a plant "risk monitor" and (2) using a matrix of preanalyzed plant configurations. Most plant "risk monitors" are customized to evaluate the risk impact of maintenance activities on SSCs used to mitigate events and SSCs which may initiate events (e.g., switchyard maintenance). The adequacy and quality of this assessment tool depends on the fidelity of the PSA model and the accuracy of input assumptions. It is expected that the scope of the PSA model in a plant "risk monitor" should reflect the "as-built, as-operated" plant configuration to ensure a valid estimate of risk associated with maintenance configurations. Since fast-computing PSA models have sometimes been simplified or optimized, the SRA/inspectors should review the licensee's process to validate the adequacy of the optimized model. In particular, attention should be directed to situations in which the proposed maintenance activities affect SSCs with differing safety functions. For example, maintenance on

emergency core cooling systems (ECCS) concurrently with containment systems would reduce plant protection at two different levels (i.e., both accident mitigation and containment performance). If the underlying analytical tool does not accurately model containment performance, then the output of such an analysis may significantly underestimate the total plant risk.

Additionally, full requantification (rather than cutset editing) of the PSA model for the assessment of each maintenance configuration is desirable to assure a greater fidelity of results when multiple components are involved. Some versions of "risk monitors" may use presolved cutsets for the quantification process. The SRA/risk analyst should be aware that the fidelity of the results from these types of "risk monitors" decreases when multiple SSCs are out of service at the same time and that the risk impact may be significantly understated. If a licensee uses this type of "risk monitor" and the licensee is removing several SSCs from service at the same time for maintenance activities, then the SRA/risk analyst needs to assess how the licensee compensates for this loss of result fidelity. Vendor or licensee sensitivity studies may suggest that there is a limit on the number of SSCs which a cutset editor can reasonably handle.

If a matrix of preanalyzed plant configurations is used for the assessment, the limitations of the risk matrix should be clearly identified and the users of this tool should have sufficient knowledge and familiarity with the tool's limitations. The adequacy of the safety assessment tool(s) should be evaluated by the licensee's Maintenance Rule expert panel to determine the possible limitations. The known limitations of the assessment tool should be described in the licensee's Maintenance Rule program documentation, and training on the limitations should be provided. The SRA/risk analyst should assess the technical adequacy of the matrix, including how the licensee determined the risk associated with the equipment outage combinations and how the licensee may have categorized that risk. Some high safety-significant SSCs may not be included in the matrix due to size limitations. It should be noted that this approach is limited due to the number of allowable configurations which can be considered. It is possible that situations will arise whereby unexpected failures of other SSCs will occur within the scope of the rule after the licensee has entered an allowed configuration as specified by the matrix approach. This new configuration would then be outside of the scope of the preanalyzed condition. The SRA/risk analyst should determine what methods the licensee employs to determine the acceptability of the emergent condition and what contingency measures are in place to maintain plant risk at an acceptable level during such situations. At a minimum, the SRA/risk analyst should verify that the licensee has a program in place to ensure that key plant safety functions are maintained even when the resultant configurations exceed the boundaries of the preanalyzed configurations.

The specific format of the quantitative assessments used by licensees may vary. However, the end result of the assessment should provide information about the effects of individual maintenance configurations on plant risk. The specific measure of plant risk being considered should be clearly defined (e.g., core damage frequency, large early release frequency, or time to boiling). In this respect, certain approaches have been shown to exhibit unique strengths and weaknesses which are specific to the approach which has been used. The assessment should consider the risk impact associated with the proposed maintenance activities for SSCs used to mitigate events as well as the risk impact for SSCs that are considered to be event initiators (i.e., scheduling switchyard maintenance during an emergency diesel outage).

C. Managing Risk

The safety assessments provide insights on the risk-significance of maintenance activities. The process for managing risk involves using results of the assessment(s) in plant decision-making to control the overall risk impact. This is accomplished through careful planning, scheduling, coordinating, monitoring, and adjusting of maintenance activities.

One objective of risk management is to control the temporary and cumulative risk increases from maintenance activities so that the increases in plant's average baseline risk are maintained within a minimal range. This is accomplished by using the result of the (a)(4) assessment to plan and schedule maintenance so that the risk increases are limited and to take additional actions beyond routine work controls to address situations where the temporary risk increase is above a certain threshold.

Section 11.3.7.2 of NUMARC 93-01 provides the quantitative thresholds for planned maintenance configurations that require risk management actions to be established. The action thresholds are based on the consideration of incremental core damage probability (ICDP) and incremental large early release probability (ILERP), or configuration-specific CDF value, due to the temporary risk increase of a planned maintenance configuration. If a plant configuration exceeds the quantitative risk thresholds and the maintenance activity needs to be conducted, then the licensee should implement the following risk management actions:

- actions to provide increased risk awareness and control,
- actions to minimize duration of maintenance activity,
- actions to minimize magnitude of risk increase.

The implementation of these practices is a prudent approach to ensure that the risk of maintenance activities involving risk-significant configurations is effectively managed. The SRA/risk analyst should verify that these practices are employed in the licensee's process for risk management.

The Probabilistic Safety Assessment Branch (SPSB) and the Quality Assurance, Vendor Inspection, Maintenance, and Allegations Branch (IQMB) of the Office of Nuclear Reactor Regulation (NRR) are available to assist with specific questions that may arise during the execution of this procedure.

Specific Guidance

Not all inspection requirements listed in Section 2 of this IP have to be performed during the inspection. Depending on the findings from the execution of Inspection Procedure (IP) 71111.13, NRC management may decide to perform a broad-scope programmatic inspection of the adequacy of the licensee's implementation of Maintenance Rule (a)(4) requirements or a more focused inspection of selected aspects of the licensee's configuration risk assessment and risk management program. The inspection resources and inspection scope would be established to support the NRC management determination.

03.01 Scope of SSCs for (a)(4) Assessments

From a sample of 10 to 12 SSCs, including high safety-significant SSCs (e.g., balance-of-plant SSCs) that are not explicitly modeled in the licensee's PSA and SSCs which have been removed from the (a)(4) list of SSCs modeled in the PSA as a result of expert panel decisions, review the licensee's bases for excluding these SSCs

from the scope of SSCs subject to (a)(4) assessments. Evaluate the licensee's bases for excluding SSCs from the scope for (a)(4) assessments on the basis of probabilistic and deterministic considerations.

a. Probabilistic Considerations

1. Would the excluded SSC, singularly or in combination with other SSCs, have a significant impact on the likelihood of a risk-significant initiating event (e.g., by an order of magnitude or more) if the SSC was out of service?

2. Does the excluded SSC have no inter-system dependencies with the support systems modeled in the PSA? (The licensee should provide the plant systems dependency matrix for review.)

3. Did the licensee adequately assess the safety significance of SSCs outside the scope of its PSA? (See Appendix A.)

4. Is the level of detail of the PSA adequate to support the SSC scoping determinations? (See Appendix A.)

5. Does the quality of the PSA support the SSC scoping determinations?

   a. Is the SSC correctly modeled in the PSA?

   b. Are the assumptions used in the PSA regarding the SSC valid?

   c. Does the licensee's PSA quality process appear adequate, using internal and/or industry peer reviews or other appropriate processes?

6. Are the licensee's PSA truncation limits low enough to support the SSC scoping determination? (See Appendix A.)

b. Deterministic Considerations

1. Does the excluded SSC have significant operator actions needed to safely operate the facility or to mitigate an event?

2. Does the excluded SSC have multiple applications in the plant and is it susceptible to generic or common-mode failures that could affect redundant trains or multiple plant systems?

3. Does the excluded SSC account for the SSC's functions in maintaining containment integrity and/or containment isolation?

4. Does the excluded SSC account for the SSC's safety functions during low power operation, shutdown, refueling, and transitional modes of operation?

5. Does the excluded SSC account for the SSC's safety functions during external events such as fires, earthquakes and high winds?

6. Has the SSC been improperly excluded due to in-service redundant systems that perform the same safety function and therefore masked the significance of the SSC?

If the SRA/risk analyst identifies problems regarding the scope of the licensee's SSCs subject to (a)(4) assessments, then the

SRA/risk analyst should expand the sample size to include another 10 SSCs to better assess the extent of the problems. If the SRA/risk analyst did not identify any problems and if time permits, the SRA/risk analyst should also consider expanding the size of the inspection sample to include another 10 SSCs.

If the SRA/risk analyst identified problems with the scope of the licensee's SSCs subject to (a)(4) assessments, then the SRA/risk analyst shall assess the licensee's process(es) for making these determinations. Evaluate the licensee's scoping process on the basis of the adequacy of the procedural controls and expert panel decision making.

a. Procedural Controls

    1. Was the level of guidance in Maintenance Rule procedures adequate?

    2. Did the licensee follow the requirements of their Maintenance Rule procedures?

b. Performance of the Maintenance Rule Expert Panel (See Appendix B)

    1. Were the Maintenance Rule expert panel's composition, its responsibilities, and its methods adequately defined?

    2. Did the panel use clear criteria in determining the scope of SSCs subject to (a)(4) assessments?

    3. Did the panel have adequate guidance to address the technical or analytical limitations of the plant-specific PSA?

    4. Did the panel objectively consider deterministic and PSA information?

    5. Did the panel incorporate lessons learned from its activities or the experiences of implementing line organizations?

    6. Were Maintenance Rule expert panel activities, including dissenting views, documented so that the bases for important decisions and SSC scope are recorded?

If the SRA/risk analyst did not identify any problems (or inspection findings) with the scope of the licensee's SSCs for (a)(4) assessments, then the SRA/risk analyst can conclude that, based on the inspection sample, the licensee has adequately established the scope of SSCs required for the 10 CFR 50.65 (a)(4) assessment. If the SRA/risk analyst identified problems with the scope of the licensee's SSCs for (a)(4) assessments, then the SRA/risk analyst needs to do the following:

a. Determine if the problems are the result of programmatic weaknesses or failure to properly implement the program (i.e., failure to follow Maintenance Rule procedures).

b. Assess the safety impact of the problems qualitatively, if necessary.

c. Determine if the problems represented potential violations. See Enforcement Manual for the most recent guidance.

03.02 Configuration Risk Assessments

Review the licensee's safety assessments of configurations during selected maintenance periods. The selected periods of high

maintenance activities during power operation should be periods when trains of components were removed from service or when components from different trains are out of service simultaneously for surveillance or maintenance. In the case of shutdown conditions, the selected time periods should be periods of reduced reactor coolant system inventory, reduced shutdown cooling availability, reduced electric power availability, or reduced containment integrity. Verify the licensee's safety assessments encompassed all the SSCs that have significant impact on public health and safety, and determine if the licensee adequately evaluated the risks resulting from the surveillance or maintenance activities.

In evaluating the licensee's prior maintenance activities, the SRA/risk analyst should consider the following risk factors:

a. The likelihood that a given maintenance activity will significantly increase the frequency of a risk-significant initiating event (e.g., by an order of magnitude or more).

b. The probability that the activity will affect the ability to mitigate the initiating event.

c. The probability that the activity will affect the ability to use the containment as a measure of defense in depth.

Additionally, the SRA/risk analyst's assessments should consider the following factors:

a. Were multiple trains affected by the maintenance activity?

b. What assurances were made to prevent the concurrent unavailability of important combinations of equipment necessary for accident mitigation?

c. What methods were employed to determine the duration of the maintenance and what was the projected duration?

In the event that the licensee chooses to use an approach such as a matrix of predefined allowable configurations, the SRA/risk analyst should determine the following:

a. What is the analytical basis for the allowed configurations? (i.e., is the matrix based on quantitative or qualitative considerations?)

b. What provisions exist for accommodating possible configurations which are not encompassed by the matrix? The licensee should have a well-documented process which specifies the procedures to be used in assessing the acceptability of such a configuration. Additionally, licensee procedures should provide guidance for rapid restoration of equipment to service if the plant configuration is found to be either unacceptable or which cannot be adequately assessed.

In the event that the licensee chooses to quantify the proposed maintenance configurations using a "risk monitor" or an equivalent configuration risk profile methodology, if applicable, the SRA/risk analyst should determine the following:

a. The underlying analysis should be sound with respect to the technical attributes of the "risk monitor" model related to scope, level of detail, and quality. (See Appendix A.)

b. Did the "risk monitor" model accurately reflect the actual maintenance configuration?

c. Did the licensee validate the adequacy of the "risk monitor" model compared to the PSA?

In reviewing the adequacy of the licensee's risk assessment tools, the SRA/risk analyst should verify the following:

a. Were external events (e.g., fire, flood, or seismic event) considered in the risk assessment tool?

b. Were external conditions (e.g., inclement weather, electrical grid stability) considered in the risk assessment tool?

If these items were not considered in the licensee's risk assessment tool, the SRA/risk analyst should request for additional information to review the licensee's bases for not considering these aspects in the assessment tool.

In the event that the licensee has elected to assess risk by the development of risk profile windows (i.e., assessed configurations in a rolling maintenance schedule), the SRA/risk analyst should determine if the licensee has appropriately utilized PSA insights in developing these windows. If problems are encountered while assessing the licensee's risk profile windows for evaluating risk due to maintenance, then the SRA/risk analyst should contact a Headquarters PSA specialist for assistance to determine whether a more detailed risk profile could be performed.

If the SRA/risk analyst did not identify any significant problems with (or any inspection findings on) the licensee's process for assessment of plant configuration risk resulting from maintenance activities, then the SRA/risk analyst can conclude that, based on the inspection sample, the licensee does not have problems associated with the assessment of risk due to maintenance activities. If the SRA/risk analyst identified problems with the licensee's process for assessment of plant configuration risk, then the SRA/risk analyst needs to do the following:

a. Determine if the problems are the result of programmatic weaknesses or failure to properly implement the program (i.e., failure to follow procedures).

b. The SRA/risk analyst should also assess the effect of the weakness on plant safety.

c. Determine if the problems represented potential violations. See Enforcement Manual for the most recent guidance.

03.03 Risk management

On the basis of the licensee's safety assessments of selected maintenance configurations, determine if the licensee adequately implemented the appropriate risk management actions for each of the assessed plant maintenance configurations. The following categories of risk management actions should have been considered by the licensee in the development of the procedures for risk management of assessed plant configurations.

a. Risk awareness and control

1. Was the planned maintenance activity discussed with the operating shift? Were the operators aware of the maintenance activity and did they approve the planned evolution?

2. Was a prejob briefing of the planned maintenance evolution conducted for the maintenance personnel?

3. Was approval by plant management obtained before entering the configuration?

b. Reducing duration of maintenance activity

1. Did the licensee prestage parts and materials for the maintenance activity?

2. Did the licensee conduct a walkdown of the tagouts and maintenance activity prior to conducting maintenance?

3. Did the licensee conduct training on mockups to familiarize maintenance personnel with the activity?

4. Did the maintenance personnel perform maintenance around the clock?

5. Did the licensee establish contingency plans to restore out-of-service equipment rapidly if needed?

c. Minimizing magnitude of risk increases

1. Did the licensee minimize other work in areas (e.g., on reactor protection system equipment areas, switchyard, diesel generator rooms, electrical switchgear rooms) that could increase the frequency of initiating events that are mitigated by the safety function served by the out-of-service SSCs?

2. Did the licensee minimize other work that could affect redundant SSCs (e.g., reactor core isolation cooling/high pressure coolant injection system rooms, auxiliary feedwater pump rooms) so the safety functions provided by the SSCs would more likely be available?

3. Did the licensee establish alternate success paths for the performance of the safety function of the out-of-service SSCs?

4. Did the licensee establish other compensatory measures?

If the SRA/risk analyst identified problems with the licensee's process for risk management of plant configurations, then the SRA/risk analyst shall assess the licensee's process(es) for managing risk of maintenance activities.

a. Determine if the licensee has procedural requirements for risk management actions for maintenance activities involving plant maintenance configurations with risk increases exceeding the action thresholds.

b. Determine if the guidance for risk management actions is adequate and is being implemented.

If the SRA/risk analyst did not identify any significant problems with(or inspection findings on) the licensee's management of plant configuration risk resulting from maintenance activities, then the SRA/risk analyst can conclude that, based on the inspection sample, the licensee does not have problems with managing the risk of maintenance activities. If the SRA/risk analyst identified problems with the licensee's management of plant configuration risk, then the SRA/risk analyst needs to do the following:

a. Determine if the problems are the result of programmatic weaknesses or failure to properly implement the program (i.e., failure to follow procedures).

b. The SRA/risk analyst should also assess the effect on plant safety resulting from this weakness.

c. Determine if the problems represented potential violations. See Enforcement Manual for the most recent guidance.

## 62709-04 RESOURCE ESTIMATE

The resources required to complete this procedure will vary greatly depending upon the nature of specific issues. Generally a Regional SRA or Headquarters Risk Analyst would be expected to need about 60 hours resources to perform this procedure.

## 62709-05 REFERENCES

U.S. Code of Federal Regulations, 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants"

NUMARC 93-01, Section 11, "Assessment of Risk Resulting from Performance of Maintenance Activities"

Inspection Procedure 71111-13, "Maintenance Risk Assessment and Emergent Work Control"

END

Appendices

A. Considerations in Reviewing PSA Attributes

B. Qualitative Judgment for Scoping Determination

APPENDIX A

CONSIDERATIONS IN REVIEWING PSA ATTRIBUTES

1. Scope of Analysis. Where quantitative results are used, the underlying analysis should be reviewed to understand if the PSA is of sufficient scope to incorporate all of the necessary SSCs. For example, a typical Level 1 PSA would not include SSCs related solely to containment integrity. Thus, reliance on such an analysis would overlook the important SSCs related to containment performance. Similarly, systems related to spent fuel pool cooling and radioactive waste disposal are not typically addressed in such an analysis. Some important plant systems may only be applicable to shutdown configurations and therefore would not be addressed by the Level 1 PSAs. (Level 1 PSAs are developed for the plant conditions at full power operation.) Additionally, some important SSCs needed to cope with external initiating events (such as fire, flood, and seismic events) or external conditions (such as inclement weather and electrical grid instability) are also not addressed in the Level 1 PSA. The scope of the PSA model used in quantitative analyses should be examined to determine the extent to which the baseline plant configuration has been modeled. The scope of the Maintenance Rule extends to a variety of SSCs which are not commonly modeled in traditional PSA studies. The methods by which the licensee incorporates known limitations of the scope of the analysis should be evaluated to ensure that important SSCs are not excluded from the (a)(4) assessments. Where it has been shown that the PSA model is not of sufficient scope to incorporate all of the relevant SSCs for the (a)(4) assessment process, the licensee should demonstrate that a qualitative decision-making process has addressed the deficiencies.

2. Level of Detail. The licensee's PSA model must be of sufficient detail to support decisions regarding SSC scope determinations. Ideally, the PSA model should visibly and accurately treat dependencies and interfaces among the plant safety functions, system responses, and operator actions needed for accident mitigation. For (a)(4) assessments, the PSA model should include both front-line/support system dependencies and support system/support system dependencies to the extent that these inter-system dependencies would have a significant effect on the key plant safety functions. Typically, the licensee’s PSA documentation would provide dependency matrices which show the systematic evaluation of inter-system dependencies. If the modeling of inter-system dependencies is determined to be inadequate, the licensee should either revise the PSA to address the inter-system dependencies or add the SSCs to the scope of (a)(4) assessments. The modeling of SSCs with respect to component boundaries can be an important factor in determining the level of detail in the PSA model. One important issue is whether electrical power breakers are included within the component boundaries for individual pieces of equipment. Similarly, certain auxiliary equipment (cooling fans, lube oil pumps, etc.) is often subsumed within the component boundary of larger components. Many complex systems are commonly modeled as super components or "black boxes" in PSA studies (e.g., diesel generators, certain relay/logic switching circuits, turbine trip systems). Since the concern of (a)(4) assessments is the safety function of a system

that the component supports, the phrase "SSCs modeled in the PSA" should be interpreted as identifying the systems, trains, and portions of systems that mitigate accident conditions. If the licensee's implementation of the Maintenance Rule (a)(4) requirements does not address the limitations of the PSA model associated with the determination of the scope of SSCs, inappropriate decisions may result. The modeling of support system dependencies should be evaluated to determine its adequacy to support the types of decisions which are being made. In those areas where the level of detail in support system modeling may not be sufficient, the licensee's qualitative decision-making process should address the deficiencies.

3. Quality of Analysis. The overall quality of the PSA must be sufficient if it is to be used to support quantitative and/or qualitative decisions of safety significance. In this context, quality refers to various attributes of the data, assumptions, and methodology which have been used, as well as consistency of the results. Additionally, the PSA should have been subjected to some type of formal review process. Ideally, the review process should include both internal and external peer reviews. Also, a comparison of other studies based on similar plant designs could provide important insights. Any significant deviations between the comparison study and the licensee's PSA should be fully understood.

With respect to the reliability and unavailability data used in the PSA analyses, the data should reflect plant-specific information to the maximum extent practicable. This data should be subjected to periodic reviews by the licensee and updated on a periodic and as-needed basis. The data should be of sufficient fidelity to provide meaningful results, i.e., the data should be derived from valid operational and test results. The empirical bases for the licensee's reliability and availability estimates should be evaluated to determine if the supporting information reflects actual observed operational experience, i.e., for a sample of 20 SSCs, compare the assumed estimates with actual plant records to determine whether the assumptions are consistent with actual observations. It is not expected that actual statistical estimations of SSC reliability are to be performed; rather, actual observed failure rates and unavailability hours should be compared with those assumed in the PSA.

Reliability data should also be consistent with industry operating experience, i.e., the basis for an SSC reliability estimate should include considerations of unique operational problems with a particular SSC in other similar facilities that would be applicable to the licensee’s facility. Licensee event reports (LERs), accident sequence precursor (ASP) reports, vendor information bulletins, and other information should provide insights for developing a more realistic best estimate of SSC reliability.

The basic assumptions used in the PSA can influence the decision-making process. Overly conservative assumptions could elevate the importance of certain SSCs and mask the true importance of others. For example, a given success criterion which specifies that two out of three pumps be available when in fact only one pump is required would represent an unnecessary conservatism. This could cause PSA importance measures associated with the pumps to be artificially higher, and possibly mask the importance of other components. Similarly, erroneous assumptions regarding

the reliability or maintenance unavailability of SSCs could also skew the results. For example, concurrent outages of equipment could cause changes in the relative importance of individual SSCs. Therefore, the impact of these systemic effects on the relative risk ranking of SSCs must be carefully evaluated, if the licensee has chosen to exclude low safety-significant SSCs from the scope of (a)(4) assessments. The licensee should evaluate these effects on the risk ranking methodology to support the bases for excluding any particular low safety-significant SSC from the (a)(4) assessment scope.

4. Uncertainty. As with any PSA calculation, the numerical results of the (a)(4) safety assessments are subject to uncertainty. The concern in every case is whether the uncertainties alter the decision being made. In general, the types of uncertainty that impact PSA results are parameter uncertainty, model uncertainty, and completeness uncertainty. Although most PSA computer codes have the capability to calculate the uncertainty distribution due to propagation of uncertainties in individual parameters through the PSA model, a formal uncertainty analysis may not be necessary if the state-of-knowledge correlation is shown to be unimportant. This involves a demonstration that most of the contributing scenarios (cutsets or accident sequences) do not involve multiple events that rely on the same parameter for their quantification. Furthermore, the acceptable risk management action thresholds are set at sufficiently low values that the need for an uncertainty analysis of the risk estimates for a maintenance configuration may not be necessary. With regard to PSA model uncertainty and completeness, sensitivity studies may be performed to evaluate the impact of uncertainties in specific assumptions on the predicted PSA numerical results. The licensee could use the sensitivity study results or qualitative arguments to show that the PSA results are insensitive to uncertainties, and therefore, that the numerical values of point estimates can be used as reasonable risk metrics for practical purposes.

5. Truncation. In quantifying the PSA model, truncation limits are imposed to manage the size and number of cutsets and sequences. Depending on the risk model and quantification tool, the truncation cutoff values will vary. The truncation limit should be low enough that there is convergence toward a stable result. To ensure that determinations of the scope of SSCs for (a)(4) assessments are not affected by truncated events and sequences, the total number of post-truncation cutsets and the core damage frequency (CDF) value should not be impacted by the selected cutoff values. Ideally, sensitivity studies could be performed to show that conclusions on the SSC scope would not be affected when higher truncation limits (1E-8 to 1E-9) were used. If a PSA model has a modularized logic structure (i.e., module of basic events structured as a supercomponent), the extent of modularization must be evaluated to determine the reasonableness of a selected truncation limit.

With the fast-calculating algorithms in current PSA software and current computers, cutoffs at 1E-11 are quite easily achieved. Ideally, a full requantification of the PSA is desirable to ensure that all low likelihood events associated with highly reliable SSCs are included in the final scope of SSCs for (a)(4) assessments. In certain plant configurations, these low likelihood events may become important contributors to the plant risk profile.

The truncation limit imposed by the licensee on the PSA results should be evaluated. When cutoffs higher than 1E-9 are used, results should be carefully reviewed. If the PSA model is modularized, a truncation limit of 1E-9 might actually be closer to a 1E-11 limit once the PSA logic structure is demodularized. If a presolved cutset model is used, the licensee should demonstrate that enough cutsets have been retained to ensure that a few dominant sequences cannot hide the contribution of other potentially important sequences. Therefore, the selected truncation value should be verified to ensure a very high percentage (e.g., 98 percent) of total risk is covered.

END

# APPENDIX B

## QUALITATIVE JUDGMENT FOR SCOPING DETERMINATION

PSA insights should be used to complement traditional engineering considerations. The licensee should consider quantitative and qualitative PSA results in conjunction with traditional engineering evaluations and operating experience to make an integrated assessment of the safety significance of the SSCs when determining the scope of SSCs for (a)(4) assessments. NUMARC 93-01 provides general guidance on how to determine the scope of SSCs for (a)(4) assessments. SSCs determined by quantitative PSA results to be low safety-significant can be excluded from the scope of (a)(4) assessments using qualitative judgment. The Maintenance Rule expert panel may be used to facilitate these determinations. The Maintenance Rule expert panel decision-making process should provide consistent decision outputs on the SSC scope. For example, the panel's decisions should be similar even when the panel is comprised of different individuals. The licensee should be able to provide documentation supporting the rationale behind the decision-making on the SSC scope for review.

END