NUCLEAR ENERGY INSTITUTE

Anthony R. Pietrangelo
DIRECTOR, LICENSING
NUCLEAR GENERATION DIVISION

November 8, 1999

Mr. Bruce A. Boger
Director
Division of Inspection Program Management
Office of Nuclear Regulatory Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555-0001

SUBJECT: Final Draft Revisions to NUMARC 93-01, *Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,* to Address Final Rulemaking to 10 CFR 50.65

Dear Mr. Boger:

Enclosed for NRC's review and endorsement is a modified final draft of revisions to NUMARC 93-01, reflecting additional changes from the version forwarded to you on October 8. These revisions were developed to serve as implementation guidance for the plant configuration assessment provision of the maintenance rule as published in the *Federal Register* on July 19, 1999.

The enclosure has been revised following additional meetings with the NRC staff and the Advisory Committee on Reactor Safeguards. NRC staff has stated that no major issues remain with regard to NRC endorsement of the guidance. We therefore request NRC endorsement of the guidance, following a public comment period, through issuance of NRC regulatory guidance.

If you or your staff have any questions, please contact me at (202) 739-8081 or Biff Bradley at (202) 739-8083.

Sincerely,

Anthony R. Pietrangelo

99-197

REB/ARP/ngs
Enclosure

YG01

c: Mr. Theodore R. Quay, NRC/NRR
Mr. Richard P. Correia, NRC/NRR

1776 I STREET, NW SUITE 400 WASHINGTON, DC 20006-3708 PHONE 202.739.8000 FAX 202.785.4019

11.0 ASSESSMENT OF RISK RESULTING FROM PERFORMANCE OF MAINTENANCE ACTIVITIES

11.1 Reference

10 CFR 50.65(a)(4)

Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.

11.2 Background

Maintenance activities must be performed to provide the level of plant equipment reliability necessary for safety, and should be carefully managed to achieve a balance between the benefits and potential impacts on safety, reliability and availability.

The benefits of well managed maintenance conducted during power operations include increased system and unit availability, reduction of equipment and system deficiencies that could impact operations, more focused attention during periods when fewer activities are competing for specialized resources, and reduction of work scope during outages. In addition, many maintenance activities may be performed during power operation with a smaller net risk impact than during outage conditions, particularly for systems whose performance is most important during shutdown, or for which greater functional redundancy is available during power operations.

11.3 Guidance

This section provides guidance for the development of an approach to assess and manage the risk impact expected to result from performance of maintenance activities. Assessing the risk means using a risk-informed process to evaluate the overall contribution to risk of the planned maintenance activities. Managing the risk means providing plant personnel with proper awareness of the risk, and taking actions as appropriate to control the risk.

The assessment is required for maintenance activities performed during power operations or during shutdown. Performance of maintenance during power operations should be planned and scheduled to properly control out-of-service time of systems or equipment. Planning and scheduling of maintenance activities during

shutdown should consider their impact on performance of key shutdown safety functions.

11.3.1 Assessment Process, Control, and Responsibilities

The process for conducting the assessment and using the result of the assessment in plant decisionmaking should be proceduralized. The procedures should denote responsibilities for conduct and use of the assessment, and should specify the plant functional organizations and personnel involved, including, as appropriate, operations, engineering, and risk assessment (PSA) personnel. The procedures should denote responsibilities and process for conducting the assessment for cases when the plant configuration is not covered by the normal assessment tool.

11.3.2 General Guidance for the Assessment - Power Operations and Shutdown

1. Power Operating conditions are defined as plant modes other than hot shutdown, cold shutdown, refueling, or defueled. Section 11.3.3 describes the scope of SSCs subject to the assessment during power operations. Section 11.3.5 describes the scope of SSCs subject to the assessment during shutdown.

2. The assessment method may use quantitative approaches, qualitative approaches, or blended methods. In general, the assessment should consider:

   - Technical specifications requirements
   - The degree of redundancy available for performance of the safety function(s) served by the out-of-service SSC
   - The duration of the out-of-service condition
   - The likelihood of an initiating event or accident that would require the performance of the affected safety function.
   - The likelihood that the maintenance activity will significantly increase the frequency of a risk-significant initiating event (e.g., by an order of magnitude or more).
   - Component and system dependencies that are affected.
   - Significant performance issues for the in-service redundant SSCs

3. The assessment may also consider the following factors, if desired:

- the risk impact of performing the maintenance during shutdown with respect to performing the maintenance at power.

- the impact of transition risk if the maintenance activity would require a shutdown that would otherwise not be necessary

4. The assessments may be predetermined or performed on an as-needed basis.

5. The degree of depth and rigor used in assessing and managing risk should be commensurate with the complexity of the planned configuration.

6. The assessment may take into account whether the out-of-service SSCs could be promptly restored to service if the need arose due to emergent conditions. This would apply to surveillance testing, or to the situation where the maintenance activity has been planned in such a manner to allow for prompt restoration. In these cases, the assessment may consider the time necessary for restoration of the SSC's function, with respect to the time at which performance of the function would be needed.

7. Emergent conditions may result in the need for action prior to conduct of the assessment, or could change the conditions of a previously performed assessment. Examples include plant configuration or mode changes, additional SSCs out of service due to failures, or significant changes in external conditions (weather, offsite power availability). The following guidance applies to this situation:

   - The safety assessment should be performed (or re-evaluated) to address the changed plant conditions on a reasonable schedule commensurate with the safety significance of the condition. Based on the results of the assessment, ongoing or planned maintenance activities may need to be suspended or rescheduled, and SSCs may need to be returned to service.

   - Performance (or re-evaluation) of the assessment should not interfere with, or delay, the operator and/or maintenance crew from taking timely actions to restore the equipment to service or take compensatory actions.

   - If the plant configuration is restored prior to conducting or re-evaluating the assessment, the assessment need not be conducted, or re-evaluated if already performed.

11.3.3 Scope of Assessment for Power Operating Conditions

10 CFR 50.65(a)(4) states "The scope of the Systems, Structures and Components (SSCs) to be addressed by the assessment may be limited to those SSCs that a risk-informed evaluation process has shown to be significant to public health and safety".

Thus, the scope of SSCs subject to the (a)(4) assessment provision may not include all SSCs that meet sections (b)(1) and (b)(2) maintenance rule scoping criteria.

The probabilistic safety assessment (PSA) provides an appropriate mechanism to define the assessment scope, as the PSA scope is developed with consideration of dependencies and support systems, and, through definition of top events, cutsets, and recovery actions, includes those SSCs that could, in combination with other SSCs, result in significant risk impacts. Thus, the (a)(4) assessment scope may be limited to the following scope of SSCs:

1. Those SSCs included in the scope of the plant's level one, internal events PSA, and;

2. SSCs in addition to the above that have been determined to be high safety significant (risk significant) through the process described in Section 9.3 of this document.

   The PSA used to define the (a)(4) assessment scope should have the following characteristics:

   - The PSA should reflect the as-built plant, and the plant operating practices.

   - The PSA 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. The licensee should evaluate whether these dependencies are adequately modeled in the PSA. PSA peer review information may be used to facilitate this evaluation. 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 (a)(4) assessment scope.

   - A PSA is typically modeled at the component level, whereas the concern of the (a)(4) assessments is the safety function of a system that the component supports. Thus the phrase "SSCs modeled in the PSA" should be interpreted as identifying the systems, trains, and segments of systems included in the high level logic structure of the PSA model, rather than the individual components. Appendix E provides information on PSA attributes, and further detail on methods to evaluate the PSA with regard to its use in defining the (a)(4) scope.

- SSCs within the plant PSA scope may be evaluated and determined to have low safety significance regardless of plant configuration. These SSCs need not be included in the scope of the (a)(4) assessments. The expert panel may be used to facilitate these determinations.

- If the plant PSA includes level two considerations (containment performance, release frequency), the scope of the (a)(4) assessment may optionally include the scope of the level two PSA. Otherwise, inclusion within the assessment scope of SSCs important to containment performance may be covered by inclusion of high safety significant SSCs as discussed in item 2 above. Section 9.3.1 of this document discusses the importance of containment performance as a consideration in identifying risk significant (high safety significant) SSCs.

11.3.4 Assessment Methods for Power Operating Conditions

Removal from service of a single structure, system (when not composed of redundant trains) or component, is adequately covered by existing Technical Specifications requirements, including the treatment of dependent components. Thus, the assessment for removal from service of a single SSC for the planned amount of time (e.g., the Technical Specifications allowed out-of-service time, or a commensurate time considering unavailability performance criteria for a non-Technical Specification high safety significant SSC), may be limited to the consideration of unusual external conditions that are present or imminent (e.g., severe weather, offsite power instability).

Simultaneous removal from service of multiple SSCs requires that an assessment be performed using quantitative, qualitative, or blended (quantitative and qualitative) methods. Sections 11.3.4.1 and 11.3.4.2 provide guidance regarding quantitative and qualitative considerations, respectively.

11.3.4.1 Quantitative Considerations

1. The assessment process may be performed by a tool or method that considers quantitative insights from the PSA. This can take the form of using the PSA model, or using a safety monitor, matrix, or pre-analyzed list derived from the PSA insights. In order to properly support the conduct of the assessment, the PSA must have certain attributes, and it must reasonably reflect the plant configuration. Appendix E provides information on PSA attributes. Section 11.3.7.2 provides guidance on various approaches for using the output of a quantitative assessment to manage risk.

2. If the PSA is modeled at a level that does not directly reflect the SSC to be removed from service (e.g., the RPS system, diesel generator, etc. have each been modeled as a "single component" in the PSA), the assessment should include

consideration of the impact of the out of service SSC on the safety function of the modeled component. SSCs are considered to support the safety function if the SSC is significant to the success path for function of the train or system (e.g., primary pump, or valve in primary flowpath). However, if the SSC removed from service does not contribute significantly to the train or system safety function (e.g., indicator light, alarm, drain valve), the SSC would not be considered to support the safety function.

11.3.4.2 Qualitative Considerations

1. The assessment may be performed by a qualitative approach, by addressing the impact of the maintenance activity upon key safety functions, as follows:

   - Identify key safety functions affected by the SSC planned for removal from service.

   - Consider the degree to which removing the SSC from service will impact the key safety functions.

   - Consider degree of redundancy, duration of out-of-service condition, and appropriate compensatory measures, contingencies, or protective actions that could be taken if appropriate for the activity under consideration.

2. For power operation, key plant safety functions are those that ensure the integrity of the reactor coolant pressure boundary, ensure the capability to shut down and maintain the reactor in a safe shutdown condition, and ensure the capability to prevent or mitigate the consequences of accidents that could result in potentially significant offsite exposures.

   Examples of these power operation key safety functions are:

   - Containment Integrity (Containment Isolation, Containment Pressure and Temperature Control);

   - Reactivity Control;

   - Reactor Coolant Heat Removal; and

   - Reactor Coolant Inventory Control.

3. The key safety functions are achieved by using systems or combinations of systems. The configuration assessment should consider whether the maintenance activity would:

- Have a significant impact on the performance of a key safety function, considering the remaining degree of redundancy for trains or systems supporting the key safety function, and considering the likelihood of an initiating event

- Involve a significant potential to cause a scram or safety system actuation

- Result in significant complications to recovery efforts.

4. The assessment should consider plant systems supporting the affected key safety functions, and trains supporting these plant systems.

5. Qualitative considerations may also be necessary to address external events, and SSCs not in the scope of the level one, internal events PSA (e.g., included in the assessment scope because of expert panel considerations).

6. The assessment may need to include consideration of actions which could affect the ability of the containment to perform its function as a fission product barrier. With regard to containment performance, the assessment should consider:

   - Whether new containment bypass conditions are created, or the probability of containment bypass conditions is increased;

   - Whether new containment penetration failures that can lead to loss of containment isolation are created; and.

   - If maintenance is performed on SSCs of the containment heat removal system (or SSCs upon which this function is dependent), whether redundant containment heat removal trains should be available.

7. External event considerations involve the potential impacts of weather or other external conditions relative to the proposed maintenance evolution. For the purposes of the assessment, weather, external flooding, and other external impacts need to be considered if such conditions are imminent or have a high probability of occurring during the planned out-of-service duration. An example where these considerations are appropriate would be the long-term removal of exterior doors, hazard barriers, or floor plugs.

8. Internal flooding considerations (from internal or external sources) should be addressed if pertinent. The assessment should consider the potential for maintenance activities to cause internal flood hazards, and, for maintenance activities to expose SSCs to flood hazards in a manner that degrades their capability to perform key safety functions.

11.3.5 Scope of Assessment for Shutdown Conditions

The scope of the Systems, Structures and Components (SSCs) to be addressed by the assessment for shutdown conditions are those SSCs necessary to support the following sh*utdown key safety functions* (from Section 4 of NUMARC 91-06):

- Decay heat removal capability
- Inventory Control
- Power Availability
- Reactivity control
- Containment (primary/secondary)

The shutdown key safety functions are achieved by using systems or combinations of systems. The shutdown assessment need not be performed for SSCs whose functionality is not necessary during shutdown modes, unless these SSCs are considered for establishment of backup success paths or compensatory measures

11.3.6 Assessment Methods for Shutdown Conditions

NUMARC 91-06, Guidelines for Industry Actions to Assess Shutdown Management, Section 4.0, provides a complete discussion of shutdown safety considerations with respect to maintaining key shutdown safety functions, and should be considered in developing an assessment process that meets the requirements of 10 CFR 50.65(a)(4).

Performance of the safety assessment for shutdown conditions generally involves a qualitative assessment with regard to key safety functions, and follows the same general process described in Section 11.3.4.2 above. (Those plants that have performed shutdown PSAs can use these PSAs as an input to their shutdown assessment methods.) However, some considerations from those associated with the at-power assessment. These include:

1. The shutdown assessment is typically focused on SSCs "available to perform a function" versus SSCs "out of service" in the case of power operations. Due to decreased equipment redundancies during outage conditions, the outage planning and control process may involve consideration of contingencies and backup methods to achieve the key safety functions, as well as on measures that can reduce both the likelihood and consequences of adverse events.

2. Assessments for shutdown maintenance activities need to take into account plant conditions and multiple SSCs out-of-service that impact the shutdown key safety

functions. The shutdown assessment is a component of an effective outage planning and control process.

3. Maintenance activities that do not necessarily remove the SSC from service may still impact plant configuration and impact key safety functions. Examples could include:

    - A valve manipulation that involves the potential for a single failure to create a draindown path affecting the inventory control key safety function

    - A switchyard circuit breaker operation that involves the potential for a single failure to affect availability of AC power.

Because of the special considerations of shutdown assessments, additional guidance is provided below with respect to each key safety function:

11.3.6.1 Decay Heat Removal Capability

Assessments for maintenance activities affecting the DHR system should consider that other systems and components can be used to remove decay heat depending on a variety of factors, including the plant configuration, availability of other key safety systems and components, and the ability of operators to diagnose and respond properly to an event. For example, assessment of maintenance activities that impact the decay heat removal key safety function should consider:

- initial magnitude of decay heat

- time to boiling

- time to core uncovery

- time to containment closure (PWR)

- initial RCS water inventory condition (e.g., filled, reduced, mid-loop, refueling canal filled, reactor cavity flooded, etc.)

- RCS configurations (e.g., open/closed, nozzle dams installed or loop isolation valves closed, steam generator manways on/off, vent paths available, temporary covers or thimble tube plugs installed, main steam line plugs installed, etc.)

- natural circulation capability with heat transfer to steam generator shell side (PWR)

If the fuel is offloaded to the spent fuel pool during the refueling outage, the decay heat removal function is shifted from the RCS to the spent fuel pool. Assessments for maintenance activities should reflect appropriate planning and contingencies to address loss of SFP cooling.

11.3.6.2 Inventory Control

Assessments for maintenance activities should address the potential for creating inventory loss flowpaths. For example,

- For BWRs, maintenance activities associated with the main steam lines (e.g., safety/relief valve removal, automatic depressurization system testing, main steam isolation valve maintenance, etc.) can create a drain down path for the reactor cavity and fuel pool. This potential is significantly mitigated through the use of main steam plugs.

- For BWRs, there are potential inventory loss paths through the DHR system to the suppression pool when DHR is aligned for shutdown cooling.

- For PWRs, assessments for maintenance activities during reduced inventory operations are especially important. Reduced inventory operation occurs when the water level in the reactor vessel is lower than 3 feet below the reactor vessel flange

- A special case of reduced inventory operation for PWRs is mid-loop operation, which occurs when the RCS water level is below the top of the hot legs at their junction with the reactor vessel. Similar conditions can exist when the reactor vessel is isolated from steam generators by closed loop isolation valves or nozzle dams with the reactor vessel head installed or prior to filling the reactor cavity. Upon loss of DHR under these conditions, coolant boiling and core uncovery can occur if decay heat removal is not restored or provided by some alternate means. In addition, during mid-loop operation, DHR can be lost by poor RCS level control or by an increase in DHR flow (either of which can ingest air into the DHR pump).

11.3.6.3 Power Availability

Assessments should consider the impact of maintenance activities on availability of electrical power. Electrical power is required during shutdown conditions to maintain cooling to the reactor core and spent fuel pool, to transfer decay heat to the heat sink, to achieve containment closure when needed, and to support other important functions.

- Assessments for maintenance activities involving AC power sources and distribution systems should address providing defense in depth that is

commensurate with the plant operating mode or configuration.

- Assessments for maintenance activities involving the switchyard and transformer yard should consider the impact on offsite power availability.

- AC and DC instrumentation and control power is required to support systems that provide key safety functions during shutdown. As such, maintenance activities affecting power sources, inverters, or distribution systems should consider their functionality as an important element in providing appropriate defense in depth.

11.3.6.4 Reactivity Control

The main aspect of this key safety function involves maintaining adequate shutdown margin in the RCS and the spent fuel pool. For PWRs, maintenance activities involving addition of water to the RCS or the refueling water storage tank have the potential to result in boron dilution. During periods of cold weather, RCS temperatures can also decrease below the minimum value assumed in the shutdown margin calculation.

11.3.6.5 Containment - Primary (PWR)/Secondary(BWR)

Maintenance activities involving the need for open containment should include evaluation of the capability to achieve containment closure in sufficient time to mitigate potential fission product release. This time is dependent on a number of factors, including the decay heat level and the amount of RCS inventory available.

For BWRs, technical specifications may require secondary containment to be closed under certain conditions, such as during fuel handling and operations with a potential to drain the vessel.

In addition to the guidance in NUMARC 91-06, for plants which obtain license amendments to utilize shutdown safety administrative controls in lieu of Technical Specification requirements on primary or secondary containment operability and ventilation system operability during fuel handling or core alterations, the following guidelines should be included in the assessment of systems removed from service:

- During fuel handling/core alterations, ventilation system and radiation monitor availability (as defined in NUMARC 91-06) should be assessed, with respect to filtration and monitoring of releases from the fuel. Following shutdown, radioactivity in the RCS decays fairly rapidly. The basis of the Technical Specification operability amendment is the reduction in doses due to such decay. The goal of maintaining ventilation system and radiation monitor availability is to reduce doses even further below that provided by the natural decay, and to avoid unmonitored releases.

- A single normal or contingency method to promptly close primary or secondary containment penetrations should be developed. Such prompt methods need not completely block the penetration or be capable of resisting pressure. The purpose is to enable ventilation systems to draw the release from a postulated fuel handling accident in the proper direction such that it can be treated and monitored.

11.3.7 Managing Risk

The assessment provides insights regarding the risk-significance of maintenance activities. The process for managing risk involves using the result of the assessment in plant decisionmaking to control the overall risk impact. This is accomplished through careful planning, scheduling, coordinating, monitoring, and adjusting of maintenance activities.

The objective of risk management is to control the temporary and cumulative risk increases from maintenance activities such that the plant's average baseline risk is maintained within a minimal range. This is accomplished by using the result of the (a)(4) assessment to plan and schedule maintenance such 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. These thresholds may be set on the basis of qualitative considerations (example – remaining mitigation capability), quantitative considerations (example – temporary increase in core damage frequency), or blended approaches using both qualitative and quantitative insights

Management of risk involves consideration of temporary risk increases, as well as cumulative risk impacts. Cumulative risk impacts are controlled to a degree through maintenance rule requirements to establish and meet SSC performance criteria. These requirements include consideration of the risk significance of SSCs in establishing performance goals. Plants that routinely perform on-line maintenance on multiple SSCs should consider additional measures to address cumulative risk, and the cumulative risk impacts should be reflected in the baseline PSA. The permanent change guidelines discussed in NRC Regulatory Guide 1.174 should be used to address the thresholds of cumulative risk impacts.

The PSA provides valuable insights for risk management, because it realistically assesses the relationship of events and systems. Risk management can be effectively accomplished by making use of qualitative insights from the PSA, rather than sole reliance on quantitative information. Removing equipment from service may alter the significance of various risk contributors from those of the baseline PSA. Specific configurations can result in increased importance of certain initiating events, or of systems or equipment used for mitigation of accidents. Evaluation of a specific configuration can identify "low order" cutsets or sequences, which are accident

sequences that could result from a small number of failures. These considerations are important to risk management.

The most fundamental risk management action is planning and sequencing of the maintenance activities taking into account the insights provided by the assessment. In conjunction with scheduling the sequence of activities, additional risk management actions may be undertaken that have the effect of reducing the temporary risk increase as determined by the assessment. Since many of the risk management actions address non-quantifiable factors, it is not expected that the risk reduction achieved by their use would necessarily be quantified. The assessment provides the basis for consideration of their use. The following sections discuss the establishment of thresholds for the use of risk management actions.

11.3.7.1 Establishing action thresholds based on qualitative considerations

The risk management action thresholds may be established qualitatively by considering the performance of key safety functions, or the remaining mitigation capability, given the out-of-service SSCs. Qualitative methods to establish risk management actions would generally be necessary to address SSCs not modeled in the PSA, and assessments for shutdown conditions. However, the use of qualitative methods is not limited to these applications, and is an acceptable approach for establishing risk management actions for (a)(4) assessments in general. This approach typically involves consideration of the following factors from the assessment:

- Duration of out-of-service condition, with longer duration resulting in increased exposure time to initiating events
- The type and frequency of initiating events that are mitigated by the out-of-service SSC, considering the sequences for which the SSC would normally serve a safety function
- The impact, if significant, of the maintenance activity on the initiating event frequencies
- The number of remaining success paths (redundant systems, trains, operator actions, recovery actions) available to mitigate the initiating events
- The likelihood of proper function of the remaining success paths

The above factors can be used as the basis for establishment of a matrix or list of configurations and attendant risk management actions.

11.3.7.2 Establishing action thresholds based on quantitative considerations

The thresholds for risk management actions may be established quantitatively by considering the magnitude of increase of the core damage frequency (and/or large early release frequency) for the maintenance configuration. This is defined as the incremental CDF, or incremental LERF.

The incremental CDF is the difference in the "configuration-specific" CDF and the baseline (or the zero maintenance) CDF. The configuration-specific CDF is the annualized risk rate with the unavailabilities of the out-of-service SSCs set to one. The configuration-specific CDF may also consider the zero maintenance model (e.g., the unavailability of the out-of-service SSC(s) is set to one, and the maintenance unavailability of the remaining SSCs is set to zero). This more closely reflects the actual configuration of the plant during the maintenance activity.

Plants should consider factors of duration in setting the risk management thresholds. This may be either the duration of a particular out-of-service condition, or a specific defined work interval (e.g. shift, week, etc). The product of the incremental CDF (or LERF) and duration is expressed as a probability (e.g., incremental core damage probability – ICDP, incremental large early release probability – ILERP).

The EPRI PSA Applications Guide (EPRI TR-105396), section 4.2.3, includes guidance for evaluation of temporary risk increases through consideration of the configuration-specific CDF, as well as the ICDP and ILERP. When combined with the other elements of the maintenance rule, and other quantitative or qualitative measures as necessary to control cumulative risk increases, this guidance provides one acceptable alternative for (a)(4) implementation. The guidance is as follows:

1. The configuration-specific CDF should be considered in evaluating the risk impact of the planned maintenance configuration. Maintenance configurations with a configuration-specific CDF in excess of 10^{-3}/year should be carefully considered before voluntarily entering such conditions. If such conditions are entered, it should be for very short periods of time and only with a clear detailed understanding of which events cause the risk level.

2. ICDP and ILERP, for a specific planned configuration, may be considered as follows with respect to establishing risk management actions:

ICDP		ILERP
> 10^{-5}	- configuration should not normally be entered voluntarily	> 10^{-6}
10^{-6} - 10^{-5}	- assess non quantifiable factors - establish risk management actions	10^{-7} - 10^{-6}
< 10^{-6}	- normal work controls	< 10^{-7}

Another acceptable approach would be to construct a similar table using ICDF and ILERF, expressed as either an absolute quantity or as a relative increase from the plant's baseline CDF and LERF.

Due to differences in plant type and design, there is acknowledged variability in baseline core damage frequency and large early release frequency. Further, there is variability in containment performance that may impact the relationship between baseline core damage frequency and baseline large early release frequency for a given plant or class of plants. Therefore, determination of the appropriate method or combination of methods as discussed above, and the corresponding quantitative risk management action thresholds, are plant-unique activities.

11.3.7.3 Risk Management Actions

Determination of the appropriate actions to control risk for a maintenance activity is specific to the particular activity, its impact on risk, and the practical means available to control the risk. Actions, similar to the examples shown below, may be used singularly or in combinations. Other actions may be taken that are not listed in the examples.

Normal work controls would be employed for configurations having nominal risk significance. This means that the normal plant work control processes are followed for the maintenance activity, and that no additional actions to address risk management actions are necessary.

Risk management actions should be considered for configurations that result in a minimal increase from the plant's baseline risk. As discussed previously, the benefits of these actions are generally not quantifiable. These actions are aimed at providing increased risk awareness of appropriate plant personnel, providing more rigorous planning and control of the activity, and taking measures to control the duration of the increased risk, and the magnitude of the increased risk. Examples of risk management actions are as follows:

Actions to provide increased risk awareness and control:

- Discuss planned maintenance activity with operating shift and obtain operator awareness and approval of planned evolution.
- Conduct pre-job briefing of maintenance personnel, emphasizing risk aspects of planned maintenance evolution.
- Request the system engineer to be present for the maintenance activity, or for applicable portions of the activity.
- Obtain plant management approval of the proposed activity.

Actions to reduce duration of maintenance activity:

- Pre-stage parts and materials.
- Walk-down tagout and maintenance activity prior to conducting maintenance.
- Conduct training on mockups to familiarize maintenance personnel with the activity.
- Perform maintenance around the clock.
- Establish contingency plan to restore out-of-service equipment rapidly if needed.

Actions to minimize magnitude of risk increase:

- Minimize other work in areas that could affect initiators [e.g., RPS equipment areas, switchyard, D/G rooms, switchgear rooms] to decrease the frequency of initiating events that are mitigated by the safety function served by the out-of-service SSC
- Minimize other work in areas that could affect other redundant systems [e.g., HPCI/RCIC rooms, auxiliary feedwater pump rooms], such that there is enhanced likelihood of the availability of the safety functions at issue served by the SSCs in those areas.
- Establish alternate success paths for performance of the safety function of the out-of-service SSC (note: equipment used to establish these alternate success paths need not necessarily be within the overall scope of the maintenance rule).
- Establish other compensatory measures

A final action threshold should be established such that risk significant configurations are not normally entered voluntarily.

11.3.8 Documentation

The following are guidelines for documentation of the safety assessment:

1. The purpose of this section of the maintenance rule is to assess impacts on plant risk or key safety functions due to maintenance activities. This purpose should be effected through establishment of plant procedures that address process, responsibilities, and decision approach. It may also be appropriate to include a reference to the appropriate procedures that govern planning and scheduling of maintenance or outage activities. The process itself should be documented.

2. The normal work control process suffices as a record that the assessment was performed. It is not necessary to document the basis of each assessment for removal of equipment from service as long as the process is followed. For evaluation of removal from service of multiple SSCs using a predetermined approach (such as a safety monitor, list, or matrix), no further documentation is necessary unless additional special considerations (such as compensatory measures, or consideration of issues beyond the scope of the assessment tool) are involved.

APPENDIX B

Definitions

Current definition of **Unavailability**:

The numerical complement of availability. An SSC that cannot perform its intend function. An SSC that is required to be available for automatic operation must be available and respond without human action.

Proposed definition of **Unavailability**

Unavailability is defined as follows:

$$\frac{\text{planned unavailable hours + unplanned unavailable hours}}{\text{required operational hours}}$$

Unavailability is considered in two cases:

1) Maintenance activities

   Equipment out of service (e.g. tagged out) for corrective or preventive maintenance is considered unavailable. Support system unavailability may be counted against either the support system, or the front line systems served by the support system. The treatment of support system unavailability for the maintenance rule should be consistent with its treatment in the plant PSA. Performance criteria should be established consistent with whichever treatment is chosen.

2) Surveillance testing

   SSCs out of service for surveillance testing are considered unavailable, unless the test configuration is automatically overridden by a valid starting signal, or the function can be restored either by an operator in the control room or by a dedicated operator stationed locally for that purpose. Restoration actions must be contained in a written procedure, must be uncomplicated (generally, a single action), and must not require diagnosis or repair. Credit for a dedicated local operator can be taken only if (s)he is positioned at the proper location throughout the duration of the test for the purpose of restoration of the train should a valid demand occur. The intent of this paragraph is to allow licensees to take credit for restoration actions that are virtually certain to be successful (i.e., probability nearly equal to 1) during accident conditions.

APPENDIX E

PSA attributes:

The PSA used for the (a)(4) assessment is important for two aspects:

1. Determination of scope of SSCs to which the assessment applies

2. Evaluation of risk impact of the maintenance configuration (or as the basis for the risk monitor, matrix, or other tool), if the assessment is performed quantitatively.

The PSA model should include the following characteristics, or, if not, its limitations for use in supporting the assessment should be compensated for by additional qualitative evaluation. The EPRI PSA Applications Guide (EPRI TR-105396) discusses considerations regarding PSA attributes, maintenance, and use in decisionmaking. This guidance should be considered in determining the degree of confidence that can be placed in the use of the PSA for the assessment, and whether additional qualitative considerations should be brought to bear:

1. The PSA should address internal initiating events.

2. The PSA should provide level one insights (contribution to core damage frequency).

3. The PSA is not required to be expanded to quantitatively address containment performance (level 2), external events, or conditions other than power operation. Use of such an expanded PSA is an option.

4. The PSA should be reviewed periodically and updated as necessary to provide reasonable representation of the current plant design.

5. The PSA should include consideration of support systems and dependencies for SSCs that impact plant risk. NEI document 99-XX, "Industry PSA Peer Review Process," includes additional information for evaluation of the correct treatment of these attributes in a PSA.