August 1, 1997 SECY-97-173

FOR: The Commissioners

FROM: L. Joseph Callan /s/
Executive Director for Operations

SUBJECT: POTENTIAL REVISION TO 10 CFR 50.65(a)(3) OF THE MAINTENANCE RULE TO REQUIRE LICENSEES TO PERFORM SAFETY ASSESSMENTS

PURPOSE:

To obtain Commission agreement with the staff's recommendation that the staff develop a proposed rulemaking to revise the maintenance rule to require that licensees assess the impact on safety when removing equipment from service for preventive maintenance.

SUMMARY:

The staff recommends that a revision to 10 CFR 50.65(a)(3) should be pursued to require licensees to assess the impact on safety when removing equipment from service for preventive maintenance. Three alternatives, including not changing the rule, would be considered as part of the regulatory analysis for proposed rulemaking. The final proposal for changing the maintenance rule would be based on the results of the analysis.

Contact:
Thomas A. Bergman, NRR
(301) 415-1021

The maintenance rule baseline inspections identified a substantial number of preventive maintenance plant configurations where safety assessments were not performed (including some that caused a significant increase in risk) and weaknesses in licensees' programs that also could result in failures to perform safety assessments prior to removing equipment from service for maintenance. In addition, the staff believes that industry would be supportive of this rule change because if licensees have (a)(3) safety assessment programs of sufficient quality, licensees may be able to use these programs to support other risk-informed initiatives, such as risk-informed allowed outage times in technical specifications. Contingent upon Commission agreement with the staff's recommendation, the staff can present the proposed rulemaking to the Commission for approval in about six months. This much time is necessary because of: (1) the limited availability of staff resources (the staff responsible for revising the rule also supports the baseline inspections and the Probabilistic Risk Assessment [PRA] Implementation Plan), and (2) the effort necessary to develop the proposed rulemaking, including regulatory and backfit analyses, and regulatory guidance for the proposed change.

BACKGROUND:

The maintenance rule, 10 CFR 50.65, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants," was issued on July 10, 1991, and became effective on July 10, 1996. The staff has periodically sent the Commission papers and provided briefings on the status of the maintenance rule, the last Commission paper being SECY 97-055, "Maintenance Rule Status, Results, and Lessons Learned," dated March 4, 1997. The staff briefed the Commission on the same subject on March 10, 1997. In response to the briefing, the Commission issued a staff requirements memorandum (SRM) on April 11, 1997, asking the staff to: (1) consider clarifying paragraph (a)(3) of the maintenance rule; (2) provide specific examples of weak programs or safety assessments found during baseline inspections and the staff's basis for its findings; (3) address how the staff would monitor the quality of the (a)(3) safety assessments and; (4) determine the efficacy of the rule in general. This Commission paper responds to the first two issues in that SRM, the other two issues are addressed in the recently issued SECY 97-172, "The Maintenance Rule: Monitoring the Quality of 10 CFR 50.65(a)(3) Safety Assessments and Methods for Monitoring its Efficacy," dated August 1, 1997.

DISCUSSION:

Paragraph (a)(3) of the maintenance rule currently states, in part, "In performing monitoring and preventative maintenance activities, an assessment of the total plant equipment that is out of service should be taken into account to determine the overall effect on performance of safety functions." The use of the word "should" means that licensees are not *required* to perform the safety assessments. The staff's expectation for the (a)(3) safety assessments is that the level of assessment be based on the safety significance of the equipment involved. Structures, systems, and components (SSCs) of high safety significance would involve more quantitative approaches, while SSCs of low safety significance (especially those not modeled in the PRA) could be assessed more qualitatively.

Importance of Configuration Control

The bases for granting the operating license for a nuclear power plant include analyses of the equipment and configuration of the plant to ensure that it conforms to regulatory requirements. Certain regulatory requirements are related to design configuration control. For example, the general design criteria (Appendix A to 10 CFR Part 50) require that consideration be given to ensuring that the design can withstand a single failure and to including adequate redundancy to allow for testing of individual systems. Once an operating license is granted, the technical specifications required by 10 CFR 50.36 contain a means of configuration control by requiring shutting the plant down in the event that certain equipment is individually or simultaneously out of service for more than a limited period of time. The regulations were not developed to address the current operating practice by many licensees, which is to conduct substantial amounts of maintenance while at power and with multiple components out of service. The result of this practice is that while the baseline risk (no equipment out of service) remains low, significant risk "spikes" can occur for brief periods during maintenance activities even though the licensee is in compliance with the regulations. Probabilistic risk assessments have shown that configuration control for accident prevention and mitigation equipment is very risk significant.

Original Intent of the Maintenance Rule

The statements of consideration for the maintenance rule indicate that the use of the word "should" in paragraph (a)(3) was intentional, although the basis for this decision is not explicit. The statements of consideration imply that the *expectation* was that a safety assessment would be performed in all cases. For example, the statements of consideration state that, "Assessing the cumulative impact of the out-of-service equipment on the performance of safety functions, as called for under paragraph (a)(3), is intended to ensure that the plant is not placed in risk-significant configurations."

The statements of consideration also indicate that the rigor of the assessments would vary. It notes that, "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 upon the circumstances involved. The assessments may range from simple deterministic judgments to the use of on-line living PRA." The Commission also expected that the sophistication of the assessments would change with time since the statements of consideration state that, "It is expected that, over time, assessments of this type will be refined based upon technological improvement and experience."

The staff continues to agree that the sophistication of the safety assessments should vary. For some SSCs of low safety significance, a qualitative assessment based on licensee knowledge may be sufficient to justify removing those SSCs from service. Additionally, other strategies may not need a specific safety assessment as described in paragraph (a)(3), for example, when a licensee only removes a single SSC from service at a time. This is because short term unavailability of many risk significant SSCs has already been determined to be acceptable as part of the licensing basis.

However, as the number and safety significance of SSCs out-of-service increases, the level of sophistication of the analysis should likewise increase as noted by the statements of consideration. Observations during inspections indicate that the simultaneous unavailability of

multiple SSCs is common. The conduct of maintenance while at power[1] has significantly increased since the maintenance rule was issued[2] partly due to the economic incentive to maximize unit availability and reliability. This further emphasizes the need for licensees to maintain substantial oversight of configuration control.

Use of Safety Assessment Program in Other Risk-Informed Initiatives

Some licensees have tried to use their paragraph (a)(3) safety assessment program as a basis for other initiatives, such as including risk-informed allowed outage times in technical specifications. Because this provision of the maintenance rule is not a requirement, the staff has not allowed this as a basis for these initiatives unless the licensees commit to perform the safety assessments as part of the other risk-informed initiative (e.g., in effect make paragraph (a)(3) safety assessments of the maintenance rule part of technical specifications). On the basis of a presentation by a Nuclear Energy Institute (NEI) manager during the 1997 Regulatory Information Conference, the staff believes that industry is supportive of revising paragraph (a)(3) to require the safety assessments because all licensees inspected to date are treating the (a)(3) safety assessment provision as a requirement. Additionally, if licensees have (a)(3) safety assessment programs of sufficient quality, licensees may be able to use these programs to support other risk-informed initiatives.

Staff Experience During Baseline Inspections

Staff experience during the maintenance rule baseline inspections has indicated that all licensees have developed programs to implement the safety assessment provision of paragraph (a)(3). The safety assessment portion of the inspections includes a review of the licensee's program for performing the assessments, plus a review of a *sample* of actual preventive maintenance configurations to determine if the licensee had performed an assessment of the configuration in accordance with the licensee's procedures.

Of the 21 baseline inspections for which inspection reports had been issued as of May 27, 1997, five sites had (a)(3) assessment programs in place where the staff found no weaknesses. At five other sites, the inspectors noted situations in which the licensee had failed to assess the impact on safety before entering one or more specific maintenance configurations. The other 11 sites had weaknesses in their (a)(3) safety assessment programs but no instances of failures to perform safety assessments were observed. A summary of the (a)(3) safety assessments results follows. See Attachment 1 for a discussion of the (a)(3) safety assessments results for each baseline inspection.

---

[1]The maintenance rule applies to all modes. The staff expects that the (a)(3) safety assessments be performed in all modes.

[2]For example, in a speech delivered during the Institute of Nuclear Power Operations (INPO) 1996 Chief Executive Officer (CEO) Conference, Alfred C. Tollison, Jr., Executive Vice President, INPO, stated that the median refueling outage duration dropped from about 78 days in 1990 to 52 days in 1995, due in part to more thoughtful online maintenance. The staff expects this trend to continue because of economic deregulation.

The five sites that had no noted weaknesses with their (a)(3) safety assessment programs tended to have some common features. The involvement of the PRA staff was evident (1) in all phases of maintenance planning and scheduling, and (2) in routine interactions with the operations staff. The programs also addressed emergent work, typically through models that can account for real-time changes in configuration, or through consultation between the operations, maintenance, and PRA staffs.

The five sites that failed to perform safety assessments (for the sample of preventive maintenance configurations reviewed) had programs for assessing safety; however, weaknesses in their programs or implementation contributed to the failure to perform safety assessments. At two sites it appears that the licensees simply did not perform the safety assessments in isolated cases; at one site the failure to perform the assessment resulted from emergent work occurring between the time the maintenance schedule was "frozen" and the planned maintenance outage began; at one site maintenance activities were added after the schedule was analyzed; and at one site some of the equipment that was out of service was not included in the licensee's "risk matrix"[3] and the impact of this equipment on safety was not considered even though, in combination with other out-of-service equipment, the risk was significantly higher than implied by the matrix. The causes of the failures to perform safety assessments included inadequate procedures, insufficient involvement by PRA staff, failure to follow procedures, and insufficient knowledge of the PRA insights by operators and scheduling staff.

Although the safety significance of the unassessed preventive maintenance configurations was not quantitatively determined during the inspection in all cases, it appears that some of the unassessed configurations resulted in the plant being in a state of substantially greater risk than was assumed. Further, the licensees' lack of awareness of the level of risk is of significant regulatory concern because the weaknesses in the licensees' programs or licensees' staff performance that led to the lack of awareness could allow preventive maintenance configurations of even greater risk to be entered without being adequately assessed. Given that the inspections review only a sample of the preventive maintenance configurations, the staff considers the number of missed assessments and their apparent risk significance to be a safety concern.

The other 11 sites had weaknesses in their (a)(3) safety assessment implementation that ranged from minor training weaknesses to poor procedures and methods that did not include all the SSCs of high safety significance in the risk matrix. Most of these licensees adequately addressed the impact of removing SSCs of high safety significance from service, but often did not have a clear method for assessing the removal from service of SSCs of low safety

[3]The risk matrix refers to one method of implementing this provision of the rule. Typically, the licensee lists equipment on the axes of the matrix and then notes which combinations are acceptable and sometimes adds a color coding to the combinations to indicate different levels of risk. This approach has limitations due to the amount of equipment that can be practically listed, and the inability to handle more than two out-of-service equipment per combination. However, when the limitations are addressed, this approach can result in an acceptable method.

significance[4] or for assessing combinations outside of the pre-analyzed matrix. Another common finding was procedural weaknesses for addressing emergent work. Although at these 11 sites the inspectors did not identify specific instances where safety assessments were not performed in the sample of preventive maintenance configurations reviewed, the weaknesses in these programs had the potential that an assessment may not have been performed.

In summary, the baseline inspection findings show that about 75% of the licensees inspected to date have had weaknesses in their methods for performing (a)(3) safety assessments (and one-third of these have had instances of not performing safety assessments). The staff believes that these findings do not meet the staff's or the Commission's current expectations regarding paragraph (a)(3).

Alternatives Considered

To address the staff's concerns related to implementation of paragraph (a)(3), the staff considered three alternatives.

Alternative 1: No Change to Paragraph (a)(3)

The first alternative considered was to not revise paragraph (a)(3). As noted in SECY 97-055, licensees have, for the most part, voluntarily complied with the safety assessment provision in paragraph (a)(3) because of the obvious connection between safety and out-of-service equipment. Given that all licensees inspected to date have voluntarily complied with the safety assessment provision in the rule, and some have indicated a willingness to improve their programs to address weaknesses during inspections, the existing rule language could be considered sufficient. Where inspections identify deficiencies in individual licensee's programs, the staff could continue to encourage those licensees to improve their performance.

The advantage to Alternative 1 is that no additional burden would be placed on licensees or on the staff that would occur with a rulemaking.

The disadvantages to Alternative 1 are that: (1) the staff cannot enforce this provision of the rule, (2) licensees cannot take credit for their safety assessment programs under other risk-informed initiatives (unless they make the safety assessments a requirement through the other initiative), and (3) because the safety assessments are not required, some licensees could view any efforts to encourage the safety assessments as a potential backfit.

[4]Even though the SSCs not on the matrix were of low safety significance, the unavailability of SSCs of low safety significance could, depending on other SSCs out of service, substantially increase risk.

Alternative 2: Change the Word "Should" to "Shall"

The second alternative considered was to revise (a)(3) to require that safety be assessed before equipment is removed from service for preventive maintenance. This alternative would consist of a simple change to paragraph (a)(3): replace the word "should" with "shall." The advantages to Alternative 2 are that: (1) if licensees fail to perform a safety assessment (as in the case of five of the 21 sites inspected), the staff could use enforcement to require corrective actions that ensure licensees perform the safety assessments in the future; (2) licensees would retain maximum flexibility to operate within configurations allowed by their current license as envisioned when the rule was originally issued; (3) there would be little or no burden on most licensees since the weaknesses that could lead to failures to perform safety assessments identified during the baseline inspections could be corrected relatively easily; and (4) where appropriate, it would allow licensees to take credit for their paragraph (a)(3) safety assessment program in other regulatory initiatives.

The disadvantages to Alternative 2 are that: (1) licensees are, in general, treating this provision as a requirement and thus the staff may be unnecessarily expending resources on a rule change, and (2) it would not address the weaknesses identified during the baseline inspections pertaining to the quality of licensees' methods for performing the safety assessments. Therefore, licensees could theoretically use methods that the staff considered technically inferior, would not necessarily optimize recovery from emergent work, and could perform maintenance in a configuration involving more risk than the staff would consider prudent; and still be in compliance with the rule as long as the licensee assessed safety before performing the preventive maintenance.

Alternative 3: Comprehensive Revision to Paragraph (a)(3)

As described previously, the statements of consideration for the maintenance rule note that the safety assessments would be refined based upon technological improvement and experience. Therefore, as the third alternative, the staff considered a comprehensive revision of the paragraph (a)(3) safety assessment provision to reflect current techniques. In order to remain performance based, the rule would not prescribe a specific approach. Rather, it would provide criteria that assessment methodologies would be required to meet, while continuing to give licensees the flexibility to develop specific approaches that best suit each licensee's needs. Also consistent with the definition of performance-based regulation, specific limits on the risk associated with maintenance activities could be established (e.g., limit total risk, incremental risk per maintenance outage, limit cumulative risk per time period).

The advantages to Alternative 3 are that: (1) it would require licensees to evaluate and control maintenance activities through technically sound methods, (2) would provide specific limits to the risk associated with preventive maintenance activities, and (3) would establish a foundation upon which other risk-informed regulation could build. Thus, Alternative 3 would address all of the weaknesses identified during the baseline inspections, and allow the use of the enforcement policy to require corrective actions on any of the weaknesses.

The disadvantages of Alternative 3 are: (1) such a rule would have a broad impact on other current and proposed rules (e.g., technical specifications and the proposed shutdown rule) and should thus be part of a separate rulemaking that would be used for risk-informed regulation in general; (2) since it would likely result in the use of probabilistic methods, it would impose a substantial burden on both licensees and the staff; (3) because of the greater burden on licensees it may be less likely to have industry support relative to Alternative 2; and (4) additional resources would be expended for rulemaking even though industry is, in general, treating this provision as a requirement.

Conclusions

On the basis of (1) the importance to safety of licensees' understanding risk associated with preventive maintenance configurations, (2) the increased performance of preventive maintenance while at power, (3) the licensees' proposed use of their (a)(3) safety assessment programs in other risk-informed initiatives, and (4) staff experience during the maintenance rule baseline inspections, the staff concludes that it should proceed with a proposed rulemaking to require safety assessments (i.e., Alternative 2 as a minimum). The staff would evaluate all three alternatives as part of the regulatory analysis. The final recommendation as to which alternative should be pursued would be based on the results of this regulatory analysis.

RESOURCES:

The staff expects that the proposed rulemaking, regulatory and backfit analyses, and associated guidance documents can be done with existing staff resources in six months.

COORDINATION:

The Office of the General Counsel has no legal objection to this paper. The Office of the Chief Financial Officer has no resource-related objection to this paper. The Office of the Chief Information Officer has reviewed this paper for information technology and information management implications and concurs.

RECOMMENDATION:

That the staff develop a rulemaking proposal on the basis of a regulatory and backfit analysis for the three alternatives presented above.

SCHEDULE:

Contingent upon Commission agreement with the staff's recommendation, the staff can perform the regulatory analysis, and if warranted, present the proposed rulemaking to the Commission for approval in about six months. This length of time is necessary because of (1) the limited availability of staff resources (the staff responsible for revising the rule also supports the baseline inspections and the PRA Implementation Plan) and (2) the effort necessary to develop the proposed rulemaking, if warranted, including regulatory and backfit analyses, and regulatory guidance for the proposed change.

L. Joseph Callan
Executive Director
for Operations

Attachment: Baseline Inspection Results for Maintenance Rule Safety Assessments

Baseline Inspection Results for Maintenance Rule Safety Assessments

In this attachment, the staff has summarized the paragraph (a)(3) safety assessments inspection findings for every maintenance rule baseline inspection for which an inspection report had been issued as of May 27, 1997.[1] This attachment is based solely on the information in the inspection reports. The reports are alphabetically by plant within three categories: programs with no noted weaknesses, programs with examples of failure to perform paragraph (a)(3) safety assessments (i.e., would have potentially been cited for violations had the recommended rule change been in place at the time of the inspection), and programs that had weaknesses. No inspection has identified a program that was unacceptable. The plants in each category follow:

Programs With No Noted Weaknesses

Plant	Inspection Complete	Report Date
Millstone 3	March 17, 1997	May 8, 1997
Nine Mile Point 1	October 11, 1996	January 15, 1997
Palisades	February 10, 1997	April 16, 1997
Seabrook	January 31, 1997	March 31, 1997
Waterford	January 31, 1997	March 21, 1997

Programs with Failures to Perform Paragraph (a)(3) Safety Assessments

Plant	Inspection Complete	Report Date
Cooper	August 16, 1996	October 7, 1996
D.C. Cook	September 13, 1997	November 14, 1997
Grand Gulf	March 3, 1997	April 8, 1997
Perry	November 8, 1996	January 29, 1997
Surry	January 17, 1997	February 20, 1997

Programs With Weaknesses

Plant	Inspection Complete	Report Date
Catawba	February 10, 1997	March 20, 1997
Davis-Besse	January 17, 1997	March 6, 1997
Hatch	October 21, 1996	November 22, 1996
Hope Creek	February 24, 1997	April 18, 1997
Indian Point 3	December 13, 1996	February 14, 1997
Palo Verde	July 19, 1996	August 21, 1996
Peach Bottom	August 9, 1996	October 7, 1996
Prairie Island	October 11, 1996	January 10, 1997
Sequoyah	December 6, 1996	January 2, 1997
St. Lucie	September 20, 1996	October 16, 1996
WNP-2	November 22, 1996	January 29, 1997

[1]The inspection reports are available from the public document rooms. In addition, the baseline inspection reports are available online for those with access to the NRC internal server at http://nrr10.nrc.gov/adt/drch/mrhome.htm. The (a)(3) safety assessment portions of the report may be viewed by following the M1.5 thread. This information collection is expected to be available on the public server soon through the "reactors" page (http://www.nrc.gov/reactors.html).

PROGRAMS WITH NO NOTED WEAKNESSES

MILLSTONE 3

- Used a 12-week rolling schedule. Schedule established predetermined system work windows. All recurring work activities including surveillances were analyzed using probabilistic safety insights and operating judgment to reduce risk peaks.

- The work scope was frozen three weeks before implementation. The probabilistic risk assessment (PRA) group and operations shift manager reviewed the schedule to ensure risk was minimized and verified compliance with technical specifications.

- Licensee used the equipment out-of-service (EOOS) program to assess risk of planned activities. The program conservatively assumed all work scheduled for a particular day was performed simultaneously, rather than in sequence, when determining plant risk.

- Licensee used the EOOS system for shutdown conditions. Licensed operators also assured adequate defense in depth before releasing any work activity.

- Procedure required that all changes to the work schedule after it is frozen, such as emergent work, require a PRA review or management approval or both before implementation.

NINE MILE POINT 1

- Used a 13-week rolling schedule based on work windows. The schedule was analyzed for risk to eliminate peaks during each week.

- Emergent work was evaluated for risk on a daily basis. The daily schedule identified initiating events of concern, and equipment and operator actions of increased importance on the basis of work scheduled for the day.

- Situation-specific PRAs can be requested, although this process was not formalized. The licensee initiated actions during the inspection to enhance the program in this area.

- The station shift supervisor was responsible for evaluating the impact of unplanned outages and determining the need to expedite the return of equipment to improve plant safety.

- The licensee appeared to have adequate controls in place for shutdown risk management.

PALISADES

- Used a 13-week rolling schedule. Maintenance and testing for each system were distributed through the schedule as opposed to the practice of removing major portions of an entire train from service simultaneously. System windows were developed for online and outage scheduling under specific plant conditions.

- The licensee had controls over emergent work, and was in the process of implementing the EOOS software. No instances were identified in which the licensee failed to analyze emergent work.

- The probabilistic safety analysis (PSA) engineer was routinely involved in the weekly outage schedule about one week in advance. The PSA engineer was not routinely involved in emergent work situations, but the licensee had developed adequate qualitative guidance for these situations.

- Maintenance scheduling staff and operators had an adequate level of knowledge of PSA and removing equipment from service for maintenance.

SEABROOK

- Used a 48-week rolling schedule based on system weeks and protected trains. The schedule was analyzed for risk to eliminate peaks during each week.

- The weekly work plan and analysis identified risk-significant or risk-related activities, start dates of work activities, and projected out-of-service times for each activity. Recommendations were made concerning which activities should not be done concurrently or that required close monitoring.

- The licensee did not clearly proceduralize treatment of emergent work under all conditions; however, the inspection team found no cases of a risk analysis being needed but not done.

- Shutdown risk management was well controlled and monitored.

- The PRA group was very active in the online maintenance program for planned and emergent work activities.

WATERFORD

- Used a 12 week rolling schedule, which was analyzed for risk. Work schedule was frozen 10 days preceding the week of work implementation.
- Licensee used the EOOS software for quantitative evaluations of risk impact when removing equipment from service for maintenance.
- Licensee had procedures for evaluating shutdown risk during maintenance outages.
- The EOOS monitor used color-coded risk levels. Higher risk configurations required senior management approval preceding entry.

PROGRAMS WITH FAILURES TO PERFORM PARAGRAPH (a)(3) SAFETY ASSESSMENTS

COOPER

- Used a risk matrix to determine acceptable combinations of equipment that would be simultaneously out of service. Color coding indicated how long the outage could last, and "red" combinations were prohibited.

- Procedure required reliability engineering to determine the risk associated with any combination of risk-significant equipment not addressed by the matrix before removing the equipment from service. Some operations personnel were unfamiliar with this requirement.

- Procedures did not address actions to be taken when an equipment failure occurred while in a risk-significant window.

- Procedures did not address assessing risk when removing structures, systems, and components (SSCs) of low risk significance from service for maintenance.

- Procedures did not clearly delineate responsibility to perform a risk assessment after the workweek schedule was frozen or when emergent work was identified.

- The inspectors identified 20 additional maintenance activities (including the removal of safety-related equipment from service) that were added to workweek schedules with no apparent risk assessment performed. None of the configurations appeared to be of high risk (a violation of 10 CFR Part 50, Appendix B, Criterion V, "Instructions, Procedures, and Drawings," was issued as a result).

- The licensee's reliability engineering group trended plant instantaneous and cumulative risk due to work activities to gain feedback on the risk assessment process and to improve risk management.

- The inspectors concluded that the licensee's safety assessment process had significant procedural and performance weaknesses.

D.C. COOK

- Used a risk matrix approach. One weakness was identified related to calculational methodology for determining acceptable risk of configurations. The approximations used by the licensee could have underestimated the risk of some configurations, leading to instantaneous CDF values greater than 10E-4/yr.

- Procedure for controlling scheduling of elective maintenance (applicable to Modes 1-3) was considered acceptable by the inspectors with one caveat. The procedure cautions that cross-train maintenance was not to be scheduled at power, and the risk matrix was predicated upon this assumption. Therefore, the case of simultaneous outage between train A and train B was not covered by the matrix.

- The licensee identified three instances of failure to follow its procedure for assessing risk before elective maintenance.

- Procedure for controlling maintenance during shutdown was considered acceptable.

GRAND GULF

- Used a 12-week rolling schedule, with the schedule frozen 2 weeks before implementation week.

- Used EOOS software to assess risk of maintenance activities.

- The EOOS tool was given to operators shortly preceding the inspection, but the team was unable to assess its effectiveness because operators had not had sufficient experience with EOOS. The inspectors noted that additional training appeared necessary.

- A heightened sensitivity to equipment of high safety significance had been established for the conduct of maintenance activities.

- In one instance, the licensee did not perform a risk assessment using the risk tool before removing an EDG from service for preventive maintenance.

- Operations personnel lacked sensitivity to assuring the tracking and evaluation of equipment unavailabilities and changing risk configurations (an inspection followup item (IFI) was associated with this finding).

PERRY

- Used a risk matrix approach. Depending on the risk category, different levels of supervision, evaluation, and/or compensatory actions were required.

- The risk matrix had a minimal number of pre-analyzed configurations and was considered to be a significant weakness.

- The licensee had a planned Division 1 outage that removed the residual heat removal (RHR) train A, low pressure core spray system (LPCS), emergency closed cooling (ECC) train A, emergency service water (ESW) train A, and the Division 1 emergency diesel generator (EDG) from service. The pre-analyzed core damage frequency (CDF) estimate of this configuration was 7.7E-5 per year. In addition, the control rod drive (CRD) pump train B and reactor core isolation cooling (RCIC) system were removed from service for emergent work. This new configuration, which was not analyzed, could have been of such higher risk that the licensee's procedures would have required compensatory actions (a 10 CFR Part 50, Appendix B, Criterion V violation was issued in this instance).

- The PRA engineer was involved in evaluating divisional outages one week preceding implementation. The PRA engineer was not consistently involved in emergent work situations or in attending scheduling meetings.

- Maintenance scheduling staff and operations personnel had generally weak knowledge of the PRA and the impact of balance of plant (BOP) on plant risk.

SURRY

- Used a risk matrix, color coded to indicate maintenance configuration durations and unacceptable configurations. The matrix was considered deficient because it covered only 12 of 44 SSCs of high safety significance and only two SSCs of low safety significance.

- Five occurrences of unanalyzed configurations were identified by the inspectors. All of the unanalyzed conditions occurred because the licensee did not take into account that, since April 1996 (inspection took place in January 1997), the licensee had operated Unit 1 with one pressurizer spray valve unavailable and one power-operated relief valve (PORV) blocked because of a continuous leak through the PORV. The other equipment simultaneously out of service with these valves (the other equipment had been analyzed, but not in conjunction with the two valves):

  - second pressurizer PORV, an emergency switchgear (ESG) room chiller, and one centrifugal charging pump
  - EDG (two separate occasions)
  - train B containment spray, train B recirculation spray, and number 3 EDG
  - both motor-driven auxiliary feedwater (AFW) pumps sequentially removed (one at a time)

- Schedulers and operators lacked a general understanding of the plant's PRA insights, nor were they aware that the matrix was very limited in terms of equipment combinations that were addressed.

- The procedure contained no guidance for assessing the risk for taking more than two SSCs out-of-service concurrently. There were no procedural restrictions on the number of SSCs of low safety significance that could be simultaneously removed from service. There was no guidance regarding the actions needed following an emergent equipment failure. In addition, there was no guidance regarding restoration priorities with proper consideration of risk significance.

- Licensee had an adequate process, with one exception, for addressing shutdown risk.

PROGRAMS WITH WEAKNESSES

CATAWBA

- Used a 12-week rolling schedule for planning surveillance and preventive maintenance.

- Used a risk matrix approach to assess single and double equipment outages. Matrix was used by planners to prevent planned concurrent outages that would place the plant in a high-risk situation. Operators used the matrix to assess impact of emergent work.

- The inspectors considered the risk matrix weak in terms of construction and use of PRA information. Qualitative assessments were solely relied upon for assessing combinations of equipment, no quantitative assessments were performed for any equipment combination on the matrix. Neither the matrix nor the procedures contained guidance for assessing combinations of three or more functions simultaneously out of service. Matrix used an heuristic approach to limit the number of low-safety-significant functions that could exist together, but had only evaluated them two at a time. No procedural restrictions were placed on the number of functions or SSCs that could be removed from service concurrently. No guidance was given for recovery from high-risk configurations (the order in which pieces of equipment should be returned to service).

- The licensee had evaluated out-of-service combinations during Unit 1 Cycle 9 and determined that no high-risk configurations had occurred.

DAVIS-BESSE

- Used a 12-week rolling schedule for planning surveillance and preventive maintenance.

- Used a risk matrix approach for assessing risk of out-of-service combinations of SSCs of high safety significance. High-risk combinations were indicated on the matrix. Work planners used the matrix to avoid planning high-risk concurrent outages. Operators performed final evaluation of planned outages against the matrix one week before implementation.

- For configurations not covered by the matrix, operators and planners used their experience and judgment to evaluate plant risk.

- Inspectors considered the matrix weak in terms of the effective use of individual plant examination (IPE) information. The matrix gave no explicit guidance for assessing risk for three or more concurrent equipment outages. There was no guidance for recovery from high risk configurations.

- Licensee procedures for shutdown conditions appeared to be the standard industry approach.

HATCH

- Used a risk matrix approach. The matrix contained various equipment maintenance configurations that had been quantitatively evaluated by the PRA organization and that addressed activities during power operations and forced outages. Used by work schedule dispatchers and operators to ensure that proposed scheduled maintenance had been previously analyzed and found acceptable from a risk perspective. Licensee staff were to contact the PRA group prior to entering configurations involving SSCs of high safety significance that were not specifically addressed by the matrix.

- Weaknesses identified by the inspectors in the matrix included the failure to consider in the matrix all SSCs of high safety significance, and the matrix did not explicitly address the additional risks that could be incurred when conducting maintenance associated with SSCs of low safety significance.

- Procedure contained limited weak guidance regarding actions to be taken following an emergent failure. An evaluation of the risk associated with the failure and the work in progress was not required. The procedure directed operators to restore equipment with the highest risk achievement worth (RAW) values first. However, the RAW values are based on a single function out of service and may not result in restoration priorities being properly established on the basis of the present configuration.

- The inspectors identified a strength in the risk assessment of plant configurations in terms of the extensive calculations that had been done to support the matrix approach. The team did not identify any periods of operation in a high-risk state or any deviations from procedural requirements.

- A separate shutdown safety assessment process was used for planned outages. The inspectors considered this a good approach.

HOPE CREEK

- Used multiple matrices that graphically represented 58 system or component outage combinations and their corresponding instantaneous risk. Matrices were developed for two and three system or component combinations.

- Risk matrix manual also listed other prohibited combinations and potential compensatory actions for higher risk combinations.

- Assumed a nominal equipment outage length of 72 hours. For systems in which this assumption exceeded 50 percent of the technical specification allowed outage time, additional review and approval was required.

- Weaknesses included failing to include all SSCs of high safety significance in the matrices, failing to consider SSCs of low safety significance, and treatment of surveillance testing.

- The PRA group gave safety assessment support for longer outages and emergent work, and support was available on request at other times. Operations and maintenance personnel were very familiar with the matrices, and the long-range planning was thorough and rigorous, thus compensating for some of the weaknesses.

- The licensee had a shutdown risk management process, and used the outage risk assessment and management program (ORAM) computer software. Mode 2 (startup) did not appear to be addressed (an IFI is associated with this finding).

INDIAN POINT 3

- Procedure specified that only one system of high safety significance may be out of service at a time. If this condition cannot be met and two or more components of high safety significance are also out of service, then the safety impact of the combination must be reviewed by the nuclear system analysis (NSA) group.

- The NSA group uses quantitative and qualitative methods to assess the acceptability of planned or emergent configurations. The licensee uses a 1E-6 core damage probability to evaluate the acceptability of planned or emergent work configurations.

- The team noted that emergent work was handled effectively, and work was frequently rescheduled to later weeks to avoid undesirable equipment outage combinations.

- The safety procedure did not explicitly address assessing the unavailability of SSCs of low safety significance; however, the impact of these unavailabilities was considered through operator knowledge and training of the workweek risk assessors.

- The licensee's process for managing risk during plant shutdowns included good guidance.

- Personnel were knowledgeable of work scheduling risk assessment requirements and the handling of emergent work.

PALO VERDE

- Used a risk matrix method (Modes 1-3). Both operators and work schedulers used this matrix when assessing impact on safety for removing combinations of equipment from service for maintenance. The combinations had been partially pre-analyzed using the PRA model. The matrix also identified configurations prohibited by technical specifications.

- The inspectors found that the method used to determine the cumulative impact of multiple equipment outages lacked an analytical basis, and would not in all cases yield a conservative estimate of the risk of the configuration (the licensee agreed to review this approach).

- The guidance for assessing configurations not specifically addressed by the matrix was weak (the licensee agreed to review this approach).

- The licensee had a separate process for handling Modes 4-6 that conformed to industry guidance on shutdown management.

- Before performing online maintenance, plant conditions were analyzed and operational logs were reviewed to ensure that opposite train equipment is not degraded.

PEACH BOTTOM

- Process for assessing and limiting the impact of equipment removed from service included the following: procedural restrictions, which prohibit the concurrent removal of specific systems from service on the basis of their contribution to the CDF; technical specification limitations; consultation with the PSA group as-needed; multi-disciplinary schedule reviews; and operating experience. The inspectors concluded that this approach had the potential for a system to be removed from service without a proper plant safety assessment since the procedure for performing the assessments did not include all maintenance rule SSCs, and outage planning and licensed operators may not identify the need for a PSA review because they may be unfamiliar with the specific systems covered by the rule.

PRAIRIE ISLAND

- Used EOOS software. A weakness was noted because users of the EOOS software were not aware of some of the limitations of this approach. However, the inspectors found no configurations that were entered where these limitations would have been significant.

- The licensee implemented a separate program for controlling shutdown risk. The inspectors found the approach acceptable.

- The inspectors observed a PRA group at a plan of the day meeting and noted their active involvement.

SEQUOYAH

- Used a 12-week rolling schedule for planning surveillance and preventive maintenance.

- Used a risk matrix approach for evaluating plant risk from single and double equipment outages. The work planners used the risk matrix to prevent planned concurrent equipment outages that would place the plant in a high-risk situation. Operators used the risk matrix for emergent work. For combinations of equipment outages not addressed by the matrix, operators used experience and judgment to evaluate plant risk.

- The inspectors noted several weaknesses with the risk matrix, including the following: not all SSCs of high safety significance were covered by the matrix; no guidance was given for assessing risk when three or more pieces of equipment were concurrently out of service; there was no distinction in actions for low versus medium risk situations; and there was no guidance for recovery from high-risk configurations (the order in which pieces of equipment should be returned to service). The licensee issued a revised matrix during the inspection to address most of these concerns.

- The standard industry approach was used for managing shutdown risk.

ST. LUCIE

- Used a risk matrix approach with pre-analyzed configurations for Modes 1-3. The risk matrix was deficient because it did not include all of the SSCs of high safety significance identified in the licensee's maintenance program. The matrix also did not explicitly address additional risk that could be incurred when conducting maintenance associated with SSCs of low safety significance that are removed from service. In addition, different licensee organizations had different interpretations of what constituted "maintenance." The licensee agreed that enhancements were warranted to its risk matrix in these areas.

- A separate shutdown safety assessment process was used for Modes 5 and 6. The failure to consider Mode 4 was a weakness (the licensee agreed to address Mode 4).

- The operations and planning staffs were directed by guidance to contact the PSA group when configurations not specifically addressed by the matrix or emergent maintenance occurred that exceeded the scope of pre-analyzed configurations.

- Used a 12-week rolling schedule. PSA evaluations on the frozen work schedule were provided for changes to the work schedule if high-risk configurations were encountered.

- Risk assessment process was controlled through a procedure. The procedure required a PSA to evaluate impact on safety preceding voluntary entry into technical specifications for corrective maintenance. Procedure also contained list of SSCs of high safety significance to alert operators and planners to the safety impact of performing work on these systems.

- The team identified weaknesses with the procedure, including the following: the procedure did not include all SSCs of high safety significance; there was no guidance regarding the necessity of performing a risk assessment after the workweek schedule was frozen or when emergent work was identified; and there was no guidance for assessing the impact on safety when SSCs of low safety significance were removed from service.