EDG Mission Time

**Problem Statement**

The treatment of EDG mission time in MSPI is a significant contributor to overestimating the risk impact of EDG failures to run, and also provides excessive margin for failures to start and failures to load/run. A review of industry data indicate that ~75% of all plants will invoke the risk cap with 1 EDG failure to run, while it typically requires numerous failures to start or failures to load/run before challenging the Green/White Threshold. (COMMENT: Staff calculations of EDG Birnbaums (20074Q values) indicate that 32% of the plants will invoke the risk cap with 1 FTR>1H event (i.e., that event by itself results in >1.0E-6/rcry). Note that the table provided below appears to have only 2 plants of 18 that have a "Run" margin of zero, which indicates the risk cap will be invoked if that plant incurs a FTR>1H event.) 2 of 18 does not seem to jive with ~75%.) The impact is that an EDG Failure to Run is being counted over conservatively in MSPI while at the same time masking the significance of EDG Failures to Start and Load/Run. One major contributor to this is that MSPI uses the longest mission time that is considered in the PRA model, which is typically 24 hours. The PRA models, however, also consider the recovery of offsite power as a function of time since the start of the event. The net result is that the Birnbaum values used in MSPI are generally derived from a weighted average mission time, which is used in the model to quantify core damage frequency. This average mission time is typically around 6 to 8 hours. Use of the 24-hour mission time with these Birnbaum values therefore over estimates the impact of a failure to run by a factor of 3 to 4. (The table below shows the impact of mission time on failure margins for a typical plant.) The "Current Margin" is based on the assumption that there have been no failures and UAI is 0. As a result of the reduction in the mission time, the risk worth, of an EDG failure to run, decreases. Since the margin for failure to start and failure to load/run includes the negative contribution (since we are starting with 0 failures) from failure to run, and this negative value gets smaller, the result is less margin for failures to start and load/run.

| Plant | PRA Modeled Mission Time | Current Margin | | | Margin Using PRA Modeled Mission Time | | |
|---|---|---|---|---|---|---|---|
| | | Demand | Run | Load/Run | Demand | Run | Load/Run |
| PWR1 | 8 | 9 | 1 | 9 | 6 | 3 | 6 |
| PWR2 | 8 | 8 | 1 | 9 | 5 | 3 | 6 |
| PWR3 | 6 | 2 | 0 | 3 | 2 | 1 | 3 |
| PWR4 | 24 | 6 | 1 | 6 | 6 | 1 | 6 |
| PWR5 | 24 | 2 | 1 | 3 | 2 | 1 | 3 |
| PRW6 | 8 | 7 | 6 | 9 | 7 | 19 | 8 |
| PWR7 | 8 | 2 | 4 | 2 | 2 | 11 | 2 |
| PWR8 | 8 | 8 | 2 | 17 | 7 | 7 | 15 |
| PWR9 | 8 | 3 | 1 | 4 | 2 | 1 | 3 |
| PWR10 | 8 | 25 | 3 | 32 | 24 | 10 | 31 |
| PWR11 | 8 | 11 | 3 | 11 | 8 | 7 | 8 |
| PWR12 | 8 | 17 | 1 | 10 | 15 | 3 | 9 |
| BWR1 | 6 | 18 | 3 | 24 | 17 | 12 | 23 |
| BWR2 | 8.2 | 2 | 0 | 3 | 2 | 1 | 3 |
| BWR3 | 6 | 14 | 2 | 24 | 13 | 10 | 22 |
| BWR4 | 8 | 10 | 1 | 11 | 8 | 3 | 9 |
| BWR5 | 8 | 23 | 9 | 42 | 22 | 26 | 41 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| BWR6 | 8 | 9 | 8 | 12 | 9 | 25 | 11 |

**Proposed Resolution**

The mission time used for CDE input should be the longest mission time associated with the failure to run terms used to directly quantify the PRA model. Use of this mission time is justified as it is the bases for which the Birnbaum values used in MSPI and because it minimizes overestimating the importance of run time failures and underestimating the importance of start failures. However, for purposes of failure determination, a 24-hour mission time should be used. The use of 24-hours for failure determinations is justified to account for the potential need to run the EDG for longer duration loss of offsite power events, such as can be caused by severe weather.

**Discussion**

PRA studies estimate the loss of off-site power induced core damage frequency to involve the product of the LOSP initiating event frequency and the failure of the EDGs to successfully run the entire duration of the mission run (typically assumed to be 24 hours). However, the restoration of off site power prior to an EDG failure to run will avert core damage. Thus, the probability of core damage actually depends on the probability that off-site power is not recovered prior to the failure of the EDGs to run. The time interdependency between the decreasing probability that off-site power is not restored and the increasing probability of EDG failure to run should be accounted for in order to obtain an accurate estimate of the frequency associated with LOSP initiated core damage events. As a result, use of the maximum mission time (24-hours) for MSPI calculations can overestimate the risk significance of EDG run failures which can mask the risk impact from EDG start and load/run failures.

**Proposed Guidance Changes**

1. **Page F-41, Line 14, change:**

   $T_m$ is the mission time for the component based on plant specific PRA model assumptions. Where there is more than one mission time for different initiating events or sequences (e.g., turbine-driven AFW pump for loss of offsite power with recovery versus loss of feedwater), the longest mission time is to be used.

   **To**:

   $T_m$ is the mission time for the component based on plant specific PRA model assumptions. For EDGs, the mission time associated with the Failure To Run Basic event with the highest Birnbaum value is to be used. For all other equipment, where there is more than one mission time for different initiating events or sequences (e.g., turbine-driven AFW pump for loss of offsite power with recovery versus loss of feedwater), the longest mission time is to be used.

2. **Page F-25, Line 11, change:**
In general, a failure of a component for the MSPI is any circumstance when the component is not in a condition to meet the performance requirements defined by the PRA success criteria or mission time for the functions monitored under the MSPI. This is true whether the condition is revealed through a demand or discovered through other means.

**To:**

In general, a failure of a component for the MSPI is any circumstance when the component is not in a condition to meet the performance requirements defined by the PRA success criteria or mission time for the functions monitored under the MSPI. For EDGs, the mission time for failure determinations should be the maximum mission time considered in the PRA model (generally 24-hours), even if a shorter mission time is used for input into CDE. Note that a run failure that occurs beyond 24 hours is counted as a MSPI failure, as this failure could have occurred prior to 24 hours. In addition, such failures are included in the data used to generate the baseline failure rates.

3. **Page-2, Section G 1.4 Mission Time (Lines 8, 9), change:**
**This section documents the risk significant mission time, as defined in Section 2.3.6 of Appendix F, for each of the identified monitored functions identified for the system.**

**To:**

**This section documents the risk significant mission time, as defined in Section 2.3.6 of Appendix F, for each of the identified monitored functions identified for the system. The following specific information should be included to support of the EDG mission time:**

| |
|---|
| EDG Mission Time |
| Basic Event and Description (basis for Birnbaum) |
| Other Emergency Power Failure to Run Basic Events, Descriptions and Birnbaums (those not selected) |
| Method for reduced mission time (e.g., Convolution, Multiple Discrete LOOP Initiating Events, Other) |
| Loop Initiating Events, Description and Frequency |
| Basis for LOOP Frequency (Industry/NRC Reference) |
| Basis for LOOP Non-recovery Failure (Industry/NRC Reference) |
| Credit for Emergency Power Repair (Yes/No) |
| If repair credited, failure probability of repair and basis |

**Discussion**

The current treatment of equipment failures in MSPI can significantly overestimate the risk impact resulting from human errors, component trips, inadvertent actuations or unplanned unavailability that are introduced as part of ~~a~~ test or maintenance activity. These types of events should NOT be counted as failures as long as they are immediately revealed and promptly reported to the control room during the test or maintenance activity. "Immediately revealed and promptly reported" requires clear and unambiguous indication of the equipment failure and requires control room notification prior to the performance of corrective actions or the departure of lead test/maintenance personnel from the location of the test or maintenance activity. Local communication capability (e.g., locally located phone or radio communication) is expected. Notification should occur at the earliest point where it can be safely performed. Control Room annunciation without prompt verbal conformation is not sufficient. This applies to test/surveillance/maintenance activities that are performed while considering the MSPI train/segment to be available. Treatment of these types of events as failures overestimates the risk impact, as the equipment is never in an unknown failed condition, and would not have resulted in a failure during an actual demand. In all cases, however, unplanned unavailability should be counted from the time of the event until the equipment is returned to service. Test and maintenance errors that result in damage to the equipment are excluded from this special treatment. That is, they are counted as equipment failures. This exclusion avoids the potentially difficult process of demonstrating that the damage was unique to the testing or maintenance activity.

**Impact of Failures on MSPI**

The inclusion of a failure of a component in the index calculation is equivalent to a given amount of unavailability. The following illustrates the amount of unavailability that is accounted for through the assumption of a failure of a component as opposed the actual risk accrued by the event.

The approach taken here is to first develop a known case, as if perfect knowledge existed. This case will be used as a reflection of "truth" and the right answer to the question; *What is the probability that a system is unable to perform its function when called upon?* This known case will then be evaluated using the MSPI approach to illustrate which methods reproduce the correct result.

**Definition of Known Cases**

Two known cases will be developed for this illustration. Both cases will assume a one-year period of experience for simplicity. The known cases will consider an Emergency AC power system with two Emergency Diesel Generator (EDG) trains, A and B. Each EDG is run on a monthly basis for 4 hours. Thus in a year's time there are 24 total start demands and 96 hours of runtime. The mission time for each EDG is 24 hours. For simplicity, the two EDGs will be assumed to have equal risk importance.

With this information common to all three cases, the following specific "known" circumstances will be considered.

1. The EDG-A fails due to operator error during a test run, resulting in the EDG Failing to Start. The EDG is restored in 1 hour.
2. The EDG-A fails due to operator error during a test run in the month four hours into the test run, just prior to the end of the test (to make the math simpler). The EDG is restored in 1 hour.

## Comparison of Methods

The practice of Bayesian updating has been left out of the following illustration. In practice both of the approaches used here, the "correct answer" method and the MSPI method would be subject to Bayesian updating to get the final answer, but this complexity is not necessary to illustrate the difference between the methods.

Case 1

If the times of component unavailability are known, then the probability that a component will not perform its function when called upon can be determined from the times. This approach takes the view that the unavailable times are known and the random variable is the occurrence of a demand, which has an equal probability of occurrence throughout the year. In this case the EDG-A was unavailable for 1 hour out of 8760 hrs/year because it was not in a condition to respond to the start demand. Thus, the probability that the EDG-A was unable to respond as required is given by:

$$P_A = \frac{\text{Time EDG - A was Unavailable}}{\text{Total Time the Function was Requitred}} = \frac{1\,\text{Hour}}{8760\,\text{Hours}} = 0.00011$$

And the probability that EDG-B was unable to respond as required would be given by:

$$P_B = \frac{\text{Time EDG - B was Unavailable}}{\text{Total Time the Function was Requitred}} = \frac{0\,\text{Hours}}{12\,\text{Months}} = 0.0$$

The MSPI takes the view that the operating history of both components should be taken into account to determine the probability and then that probability should be applied to both components. Using this approach, the probability of an EDG failing to respond as required is given by:

$$P_{EDG} = \frac{\text{Time any EDG was Unavailable}}{\text{Total Time the Function was Required}} = \frac{1\,\text{Hour}}{2*8760\,\text{Hours}} = 0.000057$$

Note that the result above is the same as would result from averaging $P_A$ and $P_B$.

If human errors are treated as failures, the approach taken for MSPI is to use the failure and demand history to determine the probability of an EDG failing to respond as required. Following the approach of combining the failure and demand history from both EDGs, the probability is given by:

$$P_{EDG} = \frac{\text{Total number of failures}}{\text{Total number of start demands}} = \frac{1\,\text{Failure}}{24\,\text{Demands}} = 0.042$$

Thus it is seen that for human errors that result in demand related failures (including EDG Failure to Load/Run), the approach taken in the MSPI can result in significantly overestimating the impact of the failure. It is the same as assuming that the equipment was unavailable for the entire period since the last successful test, when, in fact, it is known that the equipment was available until the time of the induced failure.

Case 2

This case treats the condition where the human error results in failure to run. Following the same approach the "correct answer" for this case is determined in a similar manner, by the ratio of the time the EDG was unable to perform its function to the total time required. The time that the EDG was unable to perform its function, in this case, is the same as for failure to start (i.e., the repair time).

$$P_{EDG} = \frac{\text{Time any EDG was Unavailable}}{\text{Total Time the Function was Required}} = \frac{1\,\text{Hour}}{2 * 8760\,\text{Hours}} = 0.000057$$

In MSPI the failure probability is given by

$$P_{EDG} = \lambda * Tm = \frac{\text{total number of failures}}{\text{total number of run hours}} * Tm\,.$$

Where

$\lambda$ is the failure rate

And

*Tm* is the mission time of the component.

In this case the total run hours is given by (4 run hours per month)*(12 months)*(2 EDGs) = 96 hours.

$$P_{EDG} = \frac{1\,\text{failure}}{96\,\text{run hours}} * 24\,\text{hours} = 0.25$$

Again, the MSPI approach significantly overestimates the time the EDG was not able to perform its function.

Conclusion

The MSPI methodology of using reliability as a surrogate for estimating the unavailability of a component significantly overestimates the risk impact of a human induced failure.

**Examples**

1) During an EDG load surveillance, an engineer placed a meter on the incorrect location when monitoring voltage on an essential service water pump. This resulted in a trip of the pump. As the first action following the trip, the engineer reported the testing error trip to the control room. This does not count as a failure as the test that was being performed would not have been occurring during an actual demand.

2) A temporary test instrument used to monitor EDG voltage has an internal fault, resulting in a fuse ~~failure~~, which tripped the EDG. This would be considered an MSPI failure as part of the monitored component boundary (the fuse) was damaged unless failure of the fuse was alarmed in the control room per the existing guidance regarding alarmed control circuit failures.

**Proposed Guidance Changes**

Page F-26, "Treatment of Demand and Run Failures"
Add the following:

Human errors/component trips, inadvertent actuations or unplanned unavailability introduced as part of a test or maintenance activity are not indicative of the reliability of the equipment had the activity not been performed, and should NOT be counted as failures as long as they are immediately revealed and promptly reported to the control room.

This applies to human errors which result in tripping an MSPI component that:

1. occur while the MSPI train/segment is considered available;
2. do not result in actual equipment damage;
3. are immediately revealed through clear and unambiguous indication;
4. are promptly reported to the control room prior to the performance of corrective actions or the departure of lead test/maintenance personnel from the location of the test or maintenance activity, and;~~.~~
5. are clearly associated with a test or maintenance activity such that the failure sequence would not have occurred and can not occur if the test or maintenance activity was not being performed.

Unplanned unavailability should be counted from the time of the event until the equipment is returned to service.

Latent failures that are introduced as part of maintenance or test activity are considered failures, unless they are identified during the post maintenance test.

September 23, 2008
Rev 0

# Staff White Paper on Revising the MSPI Rounding Calculation

The staff proposes to revise the MSPI rounding calculation guidance to ensure that the full contributions of Unavailability Index (UAI) and Unreliability Index (URI) are considered. Present guidance has resulted in a reduction in this contribution due to this rounding process. To address this issue, the staff proposes the direct addition of the UAI and URI values, and proposes to display the result of this addition to three significant figures (truncating the remaining values).

The staff proposal does not increase the significant figures reported by the industry but recognizes that the MSPI is constructed of two key elements: UAI and URI. The value for each of these elements is the best estimate to two significant figures and is the calculated system performance. From the standpoint of the indicator, there is no uncertainty in the contribution of UAI or URI. They are exactly as stated.

Not withstanding the preciseness stated above, it is understood that there are many uncertainties in the calculation of the indices. However, the application of the NEI guidance, the PRA standard, industry best practices and staff and industry reviews are used to minimize this impact. The issue of this white paper is that once the UAI and URI values are determined, their precise addition should determine the indicator's value. The uncertainties that are present in the calculation of the Birnbaum values are independent of the precision expected when combining UAI and URI.

The staff understands that "rounding" is the process of reducing the number of significant digits in a number. The result of rounding is a "shorter number having fewer non-zero digits yet similar in magnitude. The result is less precise but easier to use [http://en.wikipedia.org/wiki/Rounding]. The case of combining UAI and URI precision is important. As the UAI and URI numbers are considered to be the exact numbers, their sum should be exact.

This proposal also recognizes that frequently, the contributions from UAI and URI have an order of a magnitude or greater difference and that applying the standard rounding process could and has resulted in the reduction in the calculated index or, in one case, the elimination of the UAI contribution. For example, the actual performance reported by one plant in the second quarter of 2007 had a URI contribution of 1.0E-6 and a UAI contribution of 1.4E-8. Both values are reported to two significant figures. Both values are valid indications of the system's performance. As the UAI is two orders of magnitude below the URI value, its contribution is eliminated due to the rounding process and the resulting value of 1.0E-6 is determined. In this case the valid contribution of UAI is ignored. There are also several examples associated with reported values of UAI and URI values being of the same order of magnitude. For example, URI = 7.8E-7 and UAI = 2.3E-7. The sum exceeds the 1E-6 green/white threshold but the calculated value using the current rounding guidance results in 1E-6. The precision of each of these contributors clearly indicates that the indicator is exceeded. Similar issues apply to the white/yellow threshold and the yellow/red threshold.
The staff is aware that the industry uses Consolidated Data Entry (CDE) to monitor margins and thresholds and may choose to modify these reports to reflect this change at some cost. However, the staff is suggesting that the option to use the 2-digit UAI and URI results submitted by INPO to the NRC and report the sum with 3 digits (as NRC currently does on its website) with no rounding would require no modification to CDE or to how the industry currently reports MSPI data.

Bases:

The MSPI calculation within the CDE software rounds the PI index values to two significant figures. This results in MSPI index values between >1.00E-6/per reactor critical year (rcry) and <1.05E-6/rcry being rounded down to 1.0E-6/rcry, which is evaluated as green rather than white. This rounding scheme was agreed to early in the MSPI development, based on the impression that MSPI results lying within the range >1.00E-6/rcry and <1.05E-6/rcry would be rare and the impact on the number of whites would be negligible. However, historical experience indicates that this is occurring more often, as indicated in Table 1. Historically, slightly more than one plant MSPI index every quarter (on average) lies within this range and is evaluated as green rather than white. Therefore, the expectation of this occurring rarely is not being met. The staff proposal to use three significant figures when adding UAI and URI rather than two would convert such events (as they occur in future quarters) back to white to eliminate this bias around the >1.00E-6/rcry threshold introduced by the two-significant-figure rounding guidance.

The MSPI results presented in the NRC public website show MSPI results to three significant figures. This leads to confusing results where, for example, the MSPI is 1.04E-6/rcry (Farley 2 RHR for 20082Q), which is shown as white in the plant detailed results figure (green/white/yellow/red bands). However, in the summary chart, the event is shown as green. The staff proposal would eliminate such inconsistencies in the website.

Other uses of a 1.0E-6 criterion within the MSPI, such as the elimination of valves and circuit breakers with Birnbaum importances <1.0E-6, are not required to use a two-significant figure rounding scheme.

Table 1. MSPI non-green occurrences (with and without rounding) by quarter and plant type.

| Quarter | Number of Non-Green Occurrences | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | EAC (MS06) | | HPI (MS07) | | HRS (MS08) | | RHR (MS09) | | CWS (MS10) | | Total | | Total |
| | BWRs | PWRs | BWRs | PWRs | BWRs | PWRs | BWRs | PWRs | BWRs | PWRs | BWRs | PWRs | All |
| 20062Q | 3 | 1 (2) | 0 | 1 | 0 | 2 | 0 | 0 | 0 | 2 (1) | 3 | 6 (8) | 9 (11) |
| 20063Q | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 2 | 5 | 7 |
| 20064Q | 2 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 2 | 7 | 9 |
| 20071Q | 4 | 4 (6) | 0 | 0 | 0 | 1 (2) | 0 | 0 (1) | 0 | 1 | 4 | 6 (10) | 10 (14) |
| 20072Q | 4 | 3 (1) | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 (1) | 5 | 6 (8) | 11 (13) |
| 20073Q | 4 | 0 | 1 | 0 | 0 | 1 (2) | 0 | 1 | 1 | 1 | 6 | 3 (4) | 9 (10) |
| 20074Q | 1 | 1 | 1 | 0 | 0 | 1 (2) | 0 | 1 | 0 | 1 | 2 | 4 (5) | 6 (7) |
| 20081Q | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 3 | 4 |
| 20082Q | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 (1) | 0 | 1 | 1 | 2 (3) | 3 (4) |
| Total | 20 | 17 (21) | 5 | 1 | 0 | 10 (13) | 0 | 4 (6) | 1 | 10 (12) | 26 | 42 (53) | 68 (79) |

Abbreviations - BWR (boiling water reactor), CWS (cooling water systems), EAC (emergency ac power system), HPI (high-pressure injection system), HRS (heat removal system), MS (mitigating system), PWR (pressurized water reactor), RHR (residual heat removal system)

Grey entries reduced because of rounding procedure. Entries in parentheses indicate numbers of non-green occurrences if rounding is not used.

# Staff White Paper on Counting MSPI Failures that Occur after Maintenance has been Completed but Prior to the Equipment Being Returned to an Operable Status

## Background:

It appears that current industry practice is to declare this equipment "available," upon completion of the maintenance work even if the post maintenance test has not yet been performed. It also appears that some licensees may decide to wait to perform the post maintenance test (PMT) on equipment after completion of the maintenance work for up to several days before the scheduled PMT is conducted. This practice is believed to vary widely as to the degree of operator awareness and the treatment of the equipment in the on-line maintenance risk assessment process, and is not limited to any particular type of component or system. It is also the staff's understanding that this practice has been in effect for a long time; perhaps back to the 1980s when on-line maintenance was beginning to gain prominence.

The concern is that the equipment is declared available after completion of the maintenance work, while remaining inoperable due to the delayed PMT. In this situation, the licensee stops accruing UA, either planned or unplanned. The licensee also does not count any demands or failures during this period of time. Yet, the equipment is apparently relied upon by control room operators to perform its intended function should an event occur with the same expectation as equipment that is in an operable state.

If the PMT fails its acceptance criteria, the industry practice is to go back and declare all the time from when it was declared available, as unavailability time, instead of recording a failure - if the failure was related to the maintenance performed. NEI 99-02, Appendix F, pages F25-26 states that failures resulting from the PMT do not count if the failure was related to the maintenance performed. Also, any demands prior to the successful completion of the PMT are not counted. It should be noted that NEI 99-02 Appendix F is silent on the situation where the equipment can be in an available status, but not operable. The staff believes that during the maintenance window and prior to the successful completion of the PMT, the equipment should be unavailable, or if declared available, any failures (and demands) should be counted in this indicator.

The staff has been informed that this practice is consistent with that used for the implementation of the Maintenance Rule. However, the staff's review of NUMARC 93-01, Rev2 (and Rev3), "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," found Section 9.4.5 which provides examples of events that are not considered maintenance preventable functional failures, and it includes the following statement: "If the failure that caused an MPFF recurs during post maintenance testing but before returning the SSCs to service, it could be indicative of unacceptable corrective actions but is not considered an additional MPFF." Note that two conditions are required to satisfy screening the failure: the failure recurs during post-maintenance testing and the failure occurs before returning the SSCs to service.

The term “before returning the SSCs to service” appears to be equivalent to “before making the SSCs available.” Therefore, this guidance appears to support the position that if equipment is declared available, any failure (and demands) should be counted.

The concerns with the industry approach can be summarized into four issues:

- Undercounting the impact of a failure
- Over confidence in equipment reliability
- Minimizing the available/not operable condition
- Unclear approach to on-line risk assessment

**Undercounting the Impact of a Failure**

As demonstrated in Industry’s white paper on the treatment of human errors, the impact of a failure on MSPI is larger than the associated unavailability impact. Declaring equipment available implies that it is ready for operation and this declaration potentially changes the mindset of operations with regards to the plant’s mitigation capability and allowed maintenance configurations. Therefore the impact of a failure on plant operations given the equipment is considered available is greater than that associated with an unavailable condition that occurs prior to the PMT.

**Over Confidence in Equipment Reliability**

Declaring equipment available prior to the PMT places the equipment in an unknown condition and potentially gives operators greater confidence in its functionality than warranted. Although the equipment maintenance has been completed, the equipment’s safety function has not been demonstrated. If the operators believe that the equipment is available, then their reliance on the equipment could potentially adversely affect their decision process (e.g., performing maintenance on other equipment that places the plant at greater risk then that if the equipment were considered unavailable). If the operators believe the equipment is not available, then coding the equipment as available appears to be inappropriate.

**Minimizing the Available/Not Operable Condition**

Due to the uncertainty of the Available/Not operable condition, it is in the best interest of public safety to minimize this condition. Accounting for this condition as unavailable time is consistent with the design of the technical specifications that limit the time equipment is not operable. Accounting for this condition within MSPI re-enforces the desire to minimize it duration.

**Unclear Approach to On-line Risk Assessment**

Additionally, it is unclear as to proper means to account for this available/not operable state when assessing and managing risk in support the Maintenance Rule A4 process. Licensees that recognize the equipment as being available in the risk assessment

process may underestimate the associated on-line risk. Licensees that do not recognize the equipment as being available appear to be in conflict with availability credit that is being taken in the MSPI program.

Recommendation:

NEI 99-02, Appendix F, pages 25-26 should be revised to require that failures that occur with the equipment in an available status but prior to the equipment being declared operable be counted toward this indicator, as well as any associated demands. If the equipment remains in an unavailable status, then the licensee need not count any subsequent demand or failure of a MSPI component if the failure was related to the maintenance performed, and planned or unplanned UA must be accrued.

# Staff White Paper on NEI 99-02 Guidance Changes for MSPI for Clarification of Planned UA Expectations

## Background:

The staff conducted a review of MSPI planned unavailability (UA) baselines and found that there are some plants that have made large UA changes or continuous frequent baseline changes. MSPI does not penalize a licensee unless their UA exceeds the baseline UA value. The downside of constant baseline changes is that a licensee may never see any UAI contribution if the delta between actual and baseline UA is very small (or zero), as would be the case for frequent baseline revisions. NEI 99-02, Revision 5 provides guidance that allows licensees to revise their planned UA baseline with no periodicity restriction when changes in maintenance program philosophy occur. However, this should not be interpreted to mean it is desirable to change baseline planned unavailability to accommodate emergent work or frequent periodic maintenance activities.

## Proposal:

To address the problem of having too frequent baseline revisions, the staff is proposing to clarify the definition of maintenance program philosophy and the addition of a requirement to ensure that changes in the UA baseline are consistent with the unavailability assumptions contained in the PRA.

### Maintenance Program Philosophy

Section F.1.2.1 of NEU-99-02 Rev 5 states that “Planned unavailable hours: These hours include time a train or segment is removed from service for a reason other than equipment failure or human error. Examples of activities included in planned unavailable hours are preventive maintenance, testing, equipment modification, or any other time equipment is electively removed from service to correct a degraded condition that had not resulted in loss of function.” Therefore, planned unavailability includes all unavailability not related to failures and, as defined, is beyond those activities associated with preventive maintenance and testing which could be considered the typical scope of a maintenance program.

Section F1.2.2 states that “The initial baseline planned unavailability is based on actual plant-specific values for the period 2002 through 2004. (Plant specific values of the most recent data are used so that the indicator accurately reflects deviation from expected planned maintenance. These values are expected to change if the plant maintenance philosophy is substantially changes with respect to on-line maintenance or preventive maintenance. In these cases, the planned unavailability baseline value should be adjusted to reflect the current maintenance practices, including low frequency maintenance evolutions.” The focus of changing the planned unavailability values is philosophy changes to the on-line maintenance or preventive maintenance program.

Section F1.2.2 also includes a discussion of significant maintenance events and states that “Some significant maintenance evolutions such as EDG overhauls, are performed at an interval greater than the three year monitoring period (5 or 10 year intervals). The baseline planned unavailability should be revised as necessary during the quarter prior to the planned maintenance evolution and then removed after twelve quarters.” This guidance recognizes that some program variations can occur and should result in revisions to the planned unavailability values.

As this UA baseline definition includes all non-failure activities, the concept of making changes to the UA baseline tied solely to the maintenance program philosophy appears to have created inconsistencies in the implementation of maintenance program philosophy changes. It is the staff’s expectation that the performance or condition of the SSCs is effectively controlled by preventive maintenance and testing programs (a maintenance rule expectation). These programs and condition monitoring activities should be periodically evaluated to ensure that the objective of preventing failures of SSCs through maintenance is appropriately balanced against the objective of minimizing unavailability of SSCs. Changes to the maintenance program philosophy refer to changes to the preventive maintenance and testing programs. Other additions of unplanned unavailability such as equipment modifications or responses to degraded conditions are not considered to be a change in maintenance program philosophy.

This is not to say that hours associated with equipment modification, or any other time equipment is electively removed from service (to correct a degraded condition that had not resulted in loss of function) are not allowed in the baseline. The initial baseline planned unavailability is based on actual plant-specific values for the period 2002 through 2004 likely includes these types of activities. However, it is expected that changes in these activities will reflect the appropriate balancing of preventing failures of SSCs against the objective of minimizing unavailability of SSCs and as such the unavailability should not be increasing with time unless a maintenance program philosophy change has been implemented.

**UA Baseline Changes Consistent with PRA**

The Birnbaum values used in the MSPI are derived from plant-specific PRAs and are dependent, in part, on the unavailability values assumed in the PRA. Therefore, it is staff’s expectation that the UA baseline is consistent with that used in the PRA and that changes to the UA baseline are tested to ensure they do not result in significant changes to the MSPI Birnbaum values (greater than 10%).

<u>Recommended Changes</u>

Change Section F1.2.2 (lines 35 to 41) from:

The initial baseline planned unavailability is based on actual plant-specific values for the period 2002 through 2004. (Plant specific values of the most recent data are used so

that the indicator accurately reflects deviation from expected planned maintenance. These values are expected to change if the plant maintenance philosophy is substantially changes with respect to on-line maintenance or preventive maintenance. In these cases, the planned unavailability baseline value should be adjusted to reflect the current maintenance practices, including low frequency maintenance evolutions.

To:

The initial baseline planned unavailability is based on actual plant-specific values for the period 2002 through 2004. (Plant specific values of the most recent data are used so that the indicator accurately reflects deviation from expected planned maintenance. These values are expected to change if the plant maintenance philosophy substantially changes with respect to on-line maintenance or preventive maintenance. In these cases, the planned unavailability baseline value should be adjusted to reflect the current maintenance practices, including low frequency maintenance evolutions." Prior to implementation of an adjusted planned unavailability baseline value, the impact of the adjusted values on all MSPI PRA inputs should be assessed. If the PRA inputs change by 10% or greater, they are expected to be updated with the implementation of the updated UA baseline value.

The following changes are considered a "change in plant maintenance philosophy:"

- A change in frequency or scope of a current preventative maintenance activity or surveillance test.
- The addition of a new preventative maintenance activity or surveillance test.
- The occurrence of a periodic maintenance activity at a higher or lower frequency during a three year data window (e.g., a maintenance overhaul that occurs once every 24 months will occur twice 2/3 of the time and once 1/3 of the time)
- Planned maintenance activities that occur on a frequency of greater than 3 years (e.g., 5 or 10 year overhauls).

The following changes are not considered a "change in plant maintenance philosophy:"

- The performance of maintenance in response to a degraded condition (even when it is taken out of service to address the degraded condition).
- Planned maintenance activity that exceeds its planned duration or is the result of emergent work.
- The performance of an on-line modification.

| Plant Code | Failure ID | Event Date | MSPI Failure Mode | MSPI Failure Mode Decoded | Suggested Failure Mode | Brief Description |
|---|---|---|---|---|---|---|
| 1 | 41279 | 02/22/2007 | MSPI-SD (Y) | FTS | NF | Test equipment improperly connected during test. |
| 1 | 33568 | 02/25/2004 | MSPI-S (Y) | FTS | NF | Output breaker would fail to open with an accident on the bus. |
| 2 | 32492 | 08/14/2004 | MSPI-SD (Y) | FTS | FTLR | Relay problems allowed output circuit breaker to close without validation that loads had been shed. |
| 3 | 28850 | 07/24/2003 | MSPI-SD (Y) | FTS | FTLR | After 1 to 3 minutes at load, KVAR and amps started varying widely. |
| 4 | 42700 | 08/29/2007 | MSPI-SD (N) | NF | FTR>1H | After 1 h of paralleling to grid. KVARs started swinging widely. Operator manually opened output breaker to prevent possible damage to generator. |
| 5 | 31651 | 11/05/2003 | MSPI-SD (Y) | FTS | FTLR | EDG tripped immediately upon parallel and locked out. |
| 6 | 40668 | 11/17/2006 | MSPI-L (Y) | FTLR | NF | Test leads used in slow start misconnected, causing fuse to open. Caused faulty indications in control room. |
| 6 | 40667 | 11/28/2006 | MSPI-L (Y) | FTLR | NF | Test leads used in slow start misconnected, causing fuse to open. Indications in control room immediately lost. |
| 7 | 37363 | 11/08/2005 | MSPI-S (N) | NF | FTR>1H | Output breaker opened unexpectly after 72 min. of operation. It reclosed 23 sec. later. |
| 7 | 38541 | 04/22/2006 | MSPI-L (Y) | FTLR | NF | Fuel injection pumps seized during post-maintenance testing. Errors during maintenance. |
| 7 | 43666 | 12/04/2007 | MSPI-S (N) | NF | FTS | EDG failed to start during slow test. Air line became disconnected. Other subtrain isolated to test. |
| 8 | 40617 | 11/01/2006 | MSPI-SD (Y) | FTS | FTLR | Output breaker would not close. |
| 9 | 37703 | 01/20/2006 | MSPI-R (Y) | FTR>1H | NF | Maintenance error caused failure during post-maintenance test. |
| 10 | 38267 | 03/25/2006 | MSPI-SD (Y) | FTS | FTR>1H | During 24-h load test, EDG failred to operate at power less than 0.87 as required. |
| 11 | 38264 | 11/23/2005 | MSPI-SD (Y) | FTS | NF | Alarm from overheated contactor for lube oil heater. Loss of function of contactor does not cause EDG failure. |
| 12 | 37635 | 01/10/2006 | MSPI-SD (N) | NF | FTS | Pusher on overspeed governor and trip mechanism had been painted, causing pusher failure. |
| 13 | 36707 | 06/14/2005 | MSPI-L (Y) | FTLR | NF | Breaker would not trip open. Would not prevent EDG from performing its intended function. Breaker would have closed and |
| 14 | 33590 | 08/06/2004 | MSPI-S (Y) | FTS | FTR>1H | Abnormal CO samples during run and speed increase during cooldown portion of load reject. Failure of blower caused aluminum to be distributed throughout engine. |
| 14 | 38187 | 04/04/2005 | MSPI-SD (Y) | FTS | NF | Loss of underfrequency trip functon of output breaker. This protection is needed only during testing (paralleled connecton to bus). |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | 43336 | 11/03/2007 | MSPI-SD (Y) | FTS | FTLR | EDG load breaker failed to close. |
| 16 | 31930 | 08/18/2004 | MSPI-S (N) | NF | FTS | EDG failed to obtain rated voltage (2200 rather than 4160 v). |
| 17 | 35974 | 06/10/2005 | MSPI-SD (Y) | FTS | FTLR | EDG breaker failed to close. |
| 18 | 34300 | 02/14/2005 | MSPI-L (N) | NF | FTLR | Output breaker failed to close. |
| 19 | 38529 | 10/03/2003 | MSPI-SD (Y) | FTS | NF | EDG failed to reach and maintain rated speed. Maintenance error caused failure during post-maintenance test. |
| 20 | 34443 | 04/02/2005 | MSPI-SD (Y) | FTS | NF | Component cooling water pump breaker failed to trip when required. |
| 21 | 39395 | 06/28/2006 | MSPI-R (Y) | FTR>1H | NF | Keep warm system is malfunctioning. |
| 21 | 41348 | 03/08/2007 | MSPI-R (N) | NF | FTR>1H | EDG fuel oil leak excessive and caused unplanned shutdown and inoperability. |
| 22 | 30321 | 10/26/2003 | MSPI-SD (N) | NF | FTLR | No output KW observed during SIAS pushbutton portion of test. Actual load lowered using alternate indications. |
| 23 | 37222 | 09/27/2005 | MSPI-R (N) | NF | FTR>1H | Water found in rocker arm lube oil reservoir after operability run. |
| 23 | 43444 | 10/20/2007 | MSPI-L (Y) | FTLR | NF | Problems during loading after a 1-wk maintenance outage. Post-maintenance test. |
| 24 | 33339 | 01/11/2005 | MSPI-L (Y) | FTLR | FTS | No control room indication of voltage or frequency after 15 - 25 sec. |
| 25 | 35322 | 02/29/2004 | MSPI-SD (Y) | FTS | NF | Coolant leak of 6 dpm discovered. |
| 25 | 37901 | 03/13/2006 | MSPI-S (Y) | FTS | FTLR | Governor need valve not optimally adjusted for actuator /oil temparature increase and resultant viscosity decrease. |
| 26 | 36777 | 10/17/2005 | MSPI-SD (Y) | FTS | FTR>1H | Approximately 5 h into run, 3/8" lube oil line broke. EDG immediately unloaded and shut down. |
| 27 | 35398 | 08/09/2005 | MSPI-S (Y) | FTS | FTLR | EDG output voltage reached >3740 VAC within 10 sec. but failed to properly maintain required steady state voltage output (4080 - 4300 VAC). |
| 27 | 38459 | 06/18/2006 | MSPI-S (N) | NF | FTS | EDG did not build up any generator output voltage/frequency during start attempt. |
| 28 | 31535 | 06/14/2004 | MSPI-SD (Y) | FTS | FTLR | EDG started but failed to maintain electrical output during load sequencing. |
| 28 | 33612 | 12/31/2004 | MSPI-SD (Y) | FTS | FTR>1H | During unplanned demand, EDG started and loaded. Prior to shutdown, jacked water gasket leak (>1.6 gph) developed. EDG cold not have supported the Key Safety Function. |
| 29 | 42677 | 08/30/2007 | MSPI-L (Y) | FTLR | NF | "EDG Running" alarmed numerous times in control room during test at full load. Engine running relay problem. |
| 29 | 37468 | 12/27/2005 | MSPI-R (N) | NF | FTR>1H | 10 gph leak of jacket coolant during EDG operation. |
| 30 | 41125 | 01/04/2007 | MSPI-SD (Y) | FTS | FTLR | Engine run for 30 min unloaded. When paralleling to bus, problems occurred. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 30 | 41104 | 02/23/2007 | MSPI-S (Y) | FTS | FTLR | EDG KW indication began cycling and increased in magnitude until test was terminated. |
| 30 | 41921 | 05/15/2007 | MSPI-S (N) | NF | FTLR | At 45 minutes into 1-h loaded run, power oscillations occurred (+/- 150 kW) about the 2600kW load setting. |
| 30 | 39955 | 10/25/2006 | MSPI-SD (Y) | FTS | FTLR | During monthly test, fuel oil leak was large enough that engine was shut down and declared inoperable. |
| 31 | 35313 | 04/11/2005 | MSPI-SD (N) | NF | FTR>1H | High crankcase pressure caused oil to spray from shaft seals. EDG unloaded and then shut down because of high pressure. |
| 32 | 38836 | 02/04/2004 | MSPI-SD (Y) | FTS | NF | Problem with manual start button. Would have started in an |
| 33 | 28439 | 08/31/2003 | MSPI-SD (N) | NF | FTS | Engine did not meet idle speed criteria. Later, engine did not even |
| 33 | 40516 | 08/12/2006 | MSPI-S (Y) | FTS | NF | MVAR became erratic while in droop mode. Automatic Voltage Regulator problem. |
| 34 | 42639 | 03/03/2007 | MSPI-S (Y) | FTS | NF | MVAR found to be erratic in droop mode. |
| 34 | 43577 | 12/22/2007 | MSPI-S (Y) | FTS | NF | EDG paralleled to grid for monthly test. Perturbation in MW meter noted in control room. Swing was within design capability of EDG. |
| 35 | 36931 | 12/07/2005 | MSPI-SD (Y) | FTS | FTLR | Voltage spiked to 5331 v and could not be controlled after startup. |
| 35 | 39441 | 08/31/2006 | MSPI-SD (Y) | FTS | FTLR | Failure occurred while performing operability test. |
| 36 | 34960 | 07/03/2005 | MSPI-SD (Y) | FTS | FTLR | Breaker trip logic not functional. Inability of blackout load sequencing logic to electrically trip breaker, preventing EDG from |
| 36 | 42648 | 08/24/2007 | MSPI-SD (Y) | FTS | NF | Fire OPS allowed damper to close, causing engine crankcase pressure switches to cause unit lockout. |
| 37 | 32070 | 09/01/2004 | MSPI-SD (N) | NF | FTS | EDG took 10.3 sec to start (but problems with fuel rack appeared to be severe enough to consider this a FTS). |
| 38 | 31008 | 04/11/2004 | MSPI-L (N) | NF | FTLR | Loads not sequenced onto bus. Sequencer did not receive a Diesel Generator Breaker Closure signal. |
| 39 | 35427 | 03/26/2005 | MSPI-S (Y) | FTS | FTLR | EDG breaker did not close. |
| 40 | 39920 | 10/27/2006 | MSPI-S (N) | NF | FTS | EDG failed to start within 10 sec (it took 30 sec). Caused by maintenance, but PMT bypassed and operability test performed. |
| 41 | 38636 | 05/23/2006 | MSPI-L (Y) | FTLR | NF | EDG ABT did not swap back over to its normal power supply after being transferred to its emergency power supply. |
| 42 | 34472 | 11/07/2004 | MSPI-SD (N) | NF | FTS | Moisture in starting air supply system prevented air start valve from opening within required start failure time out (3 sec). |
| 43 | 37161 | 12/11/2005 | MSPI-SD (Y) | FTS | FTLR | EDG synchronized to bus. Several load changes observed and EDG response was erratic. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 44 | 37169 | 11/29/2005 | MSPI-SD (Y) | FTS | FTLR | Tarp inadvertently covered flow path for cooling and combustion air to EDG. EDG would have started but likely would have overheated or stalled shortly thereafter. |
| 45 | 44636 | 02/12/2007 | MSPI-R (N) | NF | FTR>1H | Failure of fuel oil system (inadvertent closure of valve) caused trip of EDG during a surveillance run. |
| 46 | 35186 | 04/13/2005 | MSPI-SD (Y) | FTS | FTLR | Generator loaded and reached full load. 20 min. later output breaker tripped open. |
| 46 | 43525 | 12/20/2007 | MSPI-S (Y) | FTS | FTLR | Erratic output. |

Siren systems may be designed with equipment redundancy, multiple signals or feedback capability. It may be possible for sirens to be activated from multiple control stations or signals. If the use of redundant control stations or multiple signals is in approved procedures and is part of the actual system activation process then activation from either control station or any signal should be considered a success. A failure of both systems would only be considered one failure, whereas the success of either system would be considered a success. If the redundant control station is not normally attended, requires setup or initialization, it may not be considered as part of the regularly scheduled test. Specifically, if the station is only made ready for the purpose of siren tests it should not be considered as part of the regularly scheduled test.

In order to ensure test results indicate the actual as-found condition of the ANS, a licensee should avoid performing any maintenance or test of the ANS immediately prior to the conduct of the regularly scheduled ANS test. Although periodic scheduling conflicts may not always be unavoidable, scheduling preventative maintenance soon before a regularly scheduled ANS test should be avoided to the extent practical. Unplanned corrective maintenance needed to restore ANS operability, and the post-maintenance testing associated with that maintenance, prior to a regularly scheduled ANS test is acceptable.

If a siren is out of service for scheduled planned refurbishment or overhaul maintenance performed in accordance with an established program, or for scheduled equipment upgrades, the siren need not be counted as a siren test or a siren failure. However, sirens that are out of service due to unplanned corrective maintenance would continue to be counted as failures. Unplanned corrective maintenance is a measure of program reliability. The exclusion of a siren due to temporary unavailability during planned maintenance/upgrade activities is acceptable due to the level of control placed on scheduled maintenance/upgrade activities. It is not the intent to create a disincentive to performing maintenance/upgrades to ensure the ANS performs at its peak reliability.

**NRC Proposed Change to IE03 to clarify the 72-hour clock start time**

**Definition of Terms**

*Unplanned changes in reactor power* are changes in reactor power that are initiated less than 72 hours following the discovery of an off-normal condition (as further clarified below), and that result in, or require a change in power level of greater than 20% of full power to resolve. Unplanned changes in reactor power also include uncontrolled excursions of greater than 20% of full power that occur in response to changes in reactor or plant conditions and are not an expected part of a planned evolution or test.

**Clarifying Notes**

Starting at page 13, line 40, to page 14, line 9:

The 72 hour period between discovery of an off-normal condition and the corresponding change in power level is based on the typical time to assess the plant condition, and prepare, review, and approve the necessary work orders, procedures, and necessary safety reviews, to effect a repair. The key element to be used in determining whether a power change should be counted as part of this indicator is the 72-hour period and not the extent of the planning that is performed between the discovery of the condition and initiation of the power change. The 72-hour clock starts when a licensee recognizes the possible need for a downpower in a documented plan created to troubleshoot the problem.

In developing a plan to conduct a power reduction, additional contingency power reductions may be incorporated. These additional power reductions are not counted if they are implemented to address the initial condition.

Page 15, lines 17-22, will be moved to page 14, line 10 and modified as follows:

This indicator captures changes in reactor power that are initiated following the discovery of an off-normal condition. If a condition is identified that is slowly degrading and the licensee prepares documented plans to reduce power when the condition reaches a predefined limit, and 72 hours have elapsed since the condition was first identified, the power change does not count. If, however, the condition suddenly degrades beyond the predefined limits and requires rapid response, this situation would count.

Reference: FAQ 447