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 promptly (i.e., within 15 minutes) revealed during the test or maintenance activity. 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.

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

λ 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. 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 either annunciated in the control room or immediately 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 identified, and;
4. Would not have resulted in a failure during an actual demand.

Treatment of these types of events as failures overestimates the risk impact, as the equipment is never actually failed, 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.

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

BACKGROUND

Based on recent FAQs at Duane Arnold (FAQ 436) and Perry (FAQs 439 and 440), it is apparent that the guidance on NEI 99-02, Rev 5, page 10, lines 11-14, and page 11, lines 4 and 5 requires clarification. In his decision on the Duane Arnold FAQ Appeal, Fred Brown wrote:

> For purposes of the discussion to communicate this decision, I understand why this FAQ was not resolved before getting to me. I don't think that you can have a conclusion that is fully consistent with all the guidance and answers to earlier FAQs. I also do not think that this issue represented a performance issue at Duane Arnold. My decision impacts the broad wording used in answering previous FAQs, and staff and NEI should consider ways to clarify the existing guidance and FAQs so that licensees have clearer guidance in the future.

In addition, a survey including a summary of the Perry scrams was sent to the BWRs, approximately 50% responded to the survey, none of the respondents would have considered the Perry scrams to be an Unplanned Scram in accordance with NEI 99-02.

NEI 99-02, Rev 5, page 10, lines 11-14, defines an unplanned scram as:

> Unplanned scram means that the scram was not an intentional part of an evolution or test as directed by a normal operating or test procedure. This includes scrams that occurred during the execution of procedures or evolutions in which there was a high chance of a scram occurring but the scram was neither planned nor intended.

NEI 99-02, Rev 5, page 11, lines 4 and 5 provide the following as an example of scrams that are not included in the PI:

> Scrams that are planned to occur as part of a test (e.g. a reactor protection system actuation test), or scrams that are part of a normal planned operation or evolution.

The industry believes the above guidance to be consistent with the following guidance in SECY 99-07A:

Deleted: is interpreting

Deleted:

> The objective of the Initiating Events Cornerstone is to limit the frequency of those events that upset plant stability and challenge critical safety functions. Such an event can lead to either an automatic scram when a plant parameter exceeds a setpoint or a manual scram when directed by an abnormal procedure or an emergency operating procedure.

In other words, industry believes that the intent of the words in NEI 99-02 and the words in SECY 99-07A are consistent and they define unplanned scrams, for the purpose of the PI, as those scrams that are automatic, or are directed by an abnormal procedure or emergency operating procedure, or are initiated immediately upon discovery of an off-normal plant parameter. Planned scrams include those that are part of planned operation or evolution

Deleted: are properly interpreted as meaning that

Deleted: re

The following evidence is offered in support of the industry position:

- A review of historical FAQs
- A review of the INPO LER database for 1996-1998

Deleted: <#>A comparison of the LERs reported in CDE for 1996 – 1998 and the INPO LER database¶

REVIEW OF HISTORICAL FAQS

FAQ 5 The principle espoused in FAQ 5 is that scrams that are conducted in accordance with the normal plant shutdown procedure do not count, while scrams conducted outside of the normal plant shutdown procedure do count. Industry agrees with this principle and the proposed guidance change supports it.

FAQ 159 The principle re-iterated in FAQ 159 is that scrams that are conducted in accordance with the normal plant shutdown procedure do not count. Industry agrees with this principle and the proposed guidance change supports it.

FAQ 255 FAQ 255 is an Appendix D FAQ, but the principle is that a controlled shutdown does not count, but if immediate actions are taken to scram the plant in response to emergent conditions, it does count. Industry agrees with this principle and the proposed guidance change supports it.

FAQ 275 In FAQ 275, operators took an immediate action to scram the plant based on their belief that an automatic scram was imminent. Industry agrees that this type of scram counts and the proposed guidance change supports it.

FAQ 296 N/A – question deals with an unplanned power change in addition to the scram

FAQ 354 The principle espoused in FAQ 354 is that there is no external or environmental exception for a scram. The proposed guidance change does not impact this principle.

FAQ 382 N/A – question deals with a subcritical scram

FAQ 402 N/A – question deals with a shutdown from low power (6%)

REVIEW OF THE INPO LER DATABASE FOR 1996-1998

A search of the INPO LER database was conducted. The search was limited to the years 1996 – 1998. LERs with the keywords scram, trip, and shutdown in the title were identified. The hits were reviewed using the scram definition provided above and 206 scrams were found, or an average of 2 per site. Albeit the time period is slightly different, this is consistent with SECY 99-07, page H-6, which states that "the data in the draft AEOD study on initiating events (INEEL/EXT-98-00401, April 1998) indicates that the average number of scrams is 2.1/reactor year."

CONCLUSION

In the case of Duane Arnold and Perry, the plants' normal shutdown operating procedures were used and the evolution was planned. In addition, the scrams were NOT automatic, directed by an abnormal procedure or emergency operating procedure, or initiated immediately upon discovery of an off-normal plant parameter.

The area of disagreement seems to lie in the phrase "the normal sequence of a planned shutdown" found on NEI 99-02, Rev 5, page 11, line 10. Industry believes these words to be consistent with NEI 99-02, Rev 5, page 11, lines 4 and 5, as part of a planned shutdown or evolution. The NRC has recently interpreted these words to imply specific power levels and plant configurations that are not described anywhere in NEI 99-02, SECY 99-07, SECY 99-07A, or SECY 00-49. Therefore, in order to clarify the guidance and remain consistent with the intent of NEI 99-02 and SECY 99-07 and 99-07A, the following guidance change is proposed.

RECOMMENDED NEI 99-02 GUIDANCE CHANGES

Page 11, line 10

10 Scrams that ~~occur as part of the normal sequence of~~ are initiated in accordance with normal operating procedures (i.e., not an abnormal procedure or emergency operating procedure) to complete a planned shutdown and ….

Deleted: to the industry interpretation, according to this interpretation,

Deleted: that would count under the industry interpretation

Deleted: ¶
¶
¶
¶
COMPARISON OF LERS REPORTED IN CDE AND THE LER DATABASE¶
¶
Some plants entered data into CDE beginning in 1996 and 1997. Scrams reported as Unplanned Scram in IE-1 in 1996, 1997 and 1998 were reviewed against the INPO LER database using the above industry definitioninterpretation of what would constitute an unplanned scram. There was a 100% correlation.¶

Formatted: Font: Bold, Underline

Deleted: interprets

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. 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)

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.

Deleted: ¶
¶
¶

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.

Table 2

Component	Component boundary
Diesel Generators	The diesel generator boundary includes the generator body, generator actuator, lubrication system (local), fuel system (local), cooling components (local), startup air system receiver, exhaust and combustion air system, dedicated diesel battery (which is not part of the normal DC distribution system), individual diesel generator control system, cooling water isolation valves, circuit breaker for supply to safeguard buses and their associated control circuit (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]).
Motor-Driven Pumps	The pump boundary includes the pump body, motor/actuator, lubrication system, cooling components of the pump seals, the voltage supply breaker, and its associated control circuit (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]).
Turbine-Driven Pumps	The turbine-driven pump boundary includes the pump body, turbine/actuator, lubrication system (including pump), extractions, turbo-pump seal, cooling components, and associated control system (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]) including the control valve.
Motor-Operated Valves	The valve boundary inc1udes the valve body, motor/actuator, the voltage supply breaker (both motive and control power) and its associated control circuit (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]).
Solenoid Operated Valves	The valve boundary includes the valve body, the operator, the supply breaker (both power and control) or fuse and its associated control circuit (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]).
Hydraulic Operated Valves	The valve boundary includes the valve body, the hydraulic operator, associated local hydraulic system, associated solenoid operated valves, the power supply breaker or fuse for the solenoid valve, and its associated control circuit (relay contacts for normally auto actuated components, control board switches for normally operator actuated components[1]).

[1]If the control circuit for any normally auto actuated component includes the control board switch and a failure of the control board switch prevents auto actuation of the component, it is considered to be a failure of the control circuit within the component boundary.