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 years 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 know 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 mont)*(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 triped 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 promptly (i.e., within 15 minutes) revealed during the activity.

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, and;
3. are promply identified.

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.