Enclosure 6
Dec. 2008 FAQ Log
Meeting Summary of the 12/10/08 Reactor Oversight Process Working Group Public Meeting
Dated December 30, 2008

TempNo.	PI	Topic	Status	Plant/ Co.
85.0	MSPI	MSPI Risk Cap	10/22 Introduced, Discussed and Tentatively approved	Salem
85.1	MSPI	Mission Time	10/22 Introduced, Discussed and Tentatively approved	Generic
85.3	MSPI	Human Error	10/22 Introduced, Discussed and Tentatively approved	Generic
86.0	MSPI	Operator Recovery Actions	12/10 Introduced and Discussed	Kewaunee

FAQ 85.0

Plant:	Salem Generating Station Unit 1
Date of Event:	3Q07 and 1Q08
Submittal Date:	October 13, 2008
Licensee Contact:	Brian Thomas Tel/email: 856-339-2022/brian.thomas@pseg.com
NRC Contact:	Dan Schroeder Tel/email: 856-935-5151/ DLS@NRC.gov

Performance Indicator: MS – Mitigating System Performance Index

Site-Specific FAQ (Appendix D)? No

FAQ requested to become effective when approved.

Question Section

NEI 99-02 Guidance needing interpretation (include page and line citation):

NEI 99-02 Rev. 5, Appendix F, Section F.3, "Establishing Statistical Significance", page F-43 Lines 19 through 21:

"This limit on the maximum value of the most significant failure in a system is only applied if the MSPI value calculated without the application of the limit is less than 1.0E-05. This calculation will be performed by CDE software; no additional input values are required."

Event or circumstances requiring guidance interpretation:

During NRC inspection activities at Salem Unit 1, the NRC questioned why Salem Unit 1 had applied the risk limit (risk cap) during the third quarter 2007 and first quarter 2008 performance indicator submittals for the EAC MSPI indicator. Based upon review of the data in the INPO CDE database, the non-risk cap MSPI value for both of these quarters was 1.0E-05. However, the INPO CDE database applied the risk cap and calculated the indicator as Green with a risk cap. Based on the current written guidance in NEI 99-02 Section F.3, the risk cap would only be applied when the non-risk cap MSPI value is less than 1.0E-05. Currently the formula in the INPO CDE database applies the risk cap when the non-risk cap MSPI value is less than or equal to 1.0E-05. It appears that the guidance contained in NEI 99-02 Section F.3 is in error and was intended to reflect the formula that currently resides in the INPO CDE database. As stated in Line 21 of NEI 99-02, the application of the risk cap is determined by the CDE database, not by the Utility, upon entry of any availability and reliability data.

NUREG 1816, 'Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for the Pilot Plants," Section D.3.3 states that, "the proposed frontstop only applies to the GREEN/WHITE threshold. If the calculated risk, without the frontstop adjustment, exceeds the WHITE/YELLOW threshold of $1x10^{-5}$, the adjustment is not applied. This approach maintains the basic criterion of the WHITE/YELLOW threshold." Since the WHITE/YELLOW threshold is greater than 1.0E-05, it was intended as stated in NUREG-1816 to apply the risk cap (frontstop) if the non-risk cap MSPI value is less than or equal to 1.0E-05.

If licensee and NRC resident/region do not agree on the facts and circumstances explain:

The NRC Senior Resident has reviewed the contents of the FAQ and agrees with the contents of this FAQ.

Potentially relevant existing FAQ numbers:

The response to FAQ 356 states:

> CDE has been demonstrated to accurately collect the ROP data and generate the associated quarterly NRC data files and change files.

Response Section

Proposed Resolution of FAQ:

Revise Section F.3 lines 19 through 21 to be consistent with the INPO CDE risk cap determination and the value for exceeding the White MSPI threshold (less than or equal to 1.0E-05).

If appropriate, provide proposed rewording of guidance for inclusion in next revision.

"This limit on the maximum value of the most significant failure in a system is only applied if the MSPI value calculated without the application of the limit is less than or equal to 1.0E-05.
This calculation will be performed by CDE software; no additional input values are required."

FAQ 85.1

Plant: Generic
Date of Event: NA
Submittal Date: October 17, 2008
Licensee Contact: Roy Linthicum
NRC Contact: Nathan Sanfilippo

Performance Indicator: MSPI

Site-Specific FAQ (Appendix D)? No

FAQ requested to become effective 1st Quarter 2009 (provided basis document is updated and input into CDE by end of 1st quarter)

Question Section

Appendix F Page F-41 Line 14
Appendix F Page F-25 Line 11

Background

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 a significan number 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.

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.

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.

If licensee and NRC resident/region do not agree on the facts and circumstances, explain
The licensee and the NRC agree on this change

Potentially relevant existing FAQ numbers
None

Response Section
If appropriate, provide proposed rewording of guidance for inclusion in next revision.

Page F-41, Line 14, change:

> *Tm* 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:**
>
> *Tm* 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.

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 after the EDG is started is still counted as a MSPI failure. This accounts for the time during which the EDG was in an unknown condition when it would have been unable to run for a full 24 hours In addition, such failures are included in the data used to generate the baseline failure rates.

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 if a value less than 24 hours is used:

- EDG Mission Time with highest Birnbaum
- Basic Event and Description (basis for Birnbaum)
- Other Emergency Power Failure to Run Basic Events, Descriptions, mission time and Birnbaums (those not selected)
- Method for reduced mission time (e.g., Convolution, Multiple Discrete LOOP Initiating Events, Other)
- Loss of Offsite Power (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

FAQ 85.3

Plant: Generic
Date of Event: NA
Submittal Date: October 17, 2008
Licensee Contact: Roy Linthicum
NRC Contact: Nathan Sanfilippo

Performance Indicator: MSPI

Site-Specific FAQ (Appendix D)? No

FAQ requested to become effective 1st Quarter 2009

Question Section

Appendix F Page F-26

Background

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 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:

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

FAQ 85.3

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 PA and PB.

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.

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

- 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.
- A temporary test instrument used to monitor EDG voltage has an internal fault, resulting in a fuse, 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.

If licensee and NRC resident/region do not agree on the facts and circumstances, explain

The licensee and the NRC agree on this change

Potentially relevant existing FAQ numbers

None

Response Section

If appropriate, provide proposed rewording of guidance for inclusion in next revision.

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 without delay prior to the performance of corrective actions, and;
5. Are clearly associated with a test or maintenance activity such that the failure sequence would not have occurred and cannot 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 (failures that existed prior to the maintenance) that are discovered as part of maintenance or test activity are considered failures.

FAQ 86.0

Plant: Kewaunee Power Station, Dominion Energy Kewaunee
Date of Event: July 2, 2008 and other various dates
Submittal Date: _____
Licensee Contact: Paul Miller Tel/email: 920-388-8350 / paul.c.miller@dom.com
NRC Contact: Steve Burton Tel/email: 920-388-3156 / sxb3@nrc.gov

Performance Indicator: Mitigating System Performance Index

Site-Specific FAQ (Appendix D)? **No**

FAQ requested to become effective **when approved**

Question Section

NEI 99-02 Guidance needing interpretation:
NEI 99-02, Rev. 5, page F-6, lines 31-40 and page F-7, lines 1-21 states:

31 Credit for Operator Recovery Actions to Restore the Monitored Functions
32
33 1. *During testing or operational alignment*:
34
35 Unavailability of a monitored function during testing or operational alignment need not be
36 included if the test or operational alignment configuration is automatically overridden by a
37 valid starting signal, or the function can be promptly restored either by an operator in the
38 control room or by a designated operator[11] stationed locally for that purpose. Restoration
39 actions must be contained in a written procedure[12], must be uncomplicated (*a single action or*
40 *a few simple actions*), must be capable of being restored in time to satisfy PRA success

[11] Operator in this circumstance refers to any plant personnel qualified and designated to perform the restoration function.
[12] Including restoration steps in an approved test procedure.

1 criteria and must not require diagnosis or repair. Credit for a designated local operator can be
2 taken only if (s)he is positioned at the proper location throughout the duration of the test or
3 operational alignment for the purpose of restoration of the train should a valid demand occur.

4 The intent of this paragraph is to allow licensees to take credit for restoration actions that are
5 virtually certain to be successful (i.e., probability nearly equal to 1) during accident
6 conditions.
7
8 The individual performing the restoration function can be the person conducting the test or
9 operational alignment and must be in communication with the control room. Credit can also
10 be taken for an operator in the main control room provided (s)he is in close proximity to
11 restore the equipment when needed. Normal staffing for the test or operational alignment may
12 satisfy the requirement for a dedicated operator, depending on work assignments. In all cases,
13 the staffing must be considered in advance and an operator identified to perform the
14 restoration actions independent of other control room actions that may be required.
15
16 Under stressful, chaotic conditions, otherwise simple multiple actions may not be
17 accomplished with the virtual certainty called for by the guidance (e.g., lifting test leads and
18 landing wires; or clearing tags). In addition, some manual operations of systems designed to
19 operate automatically, such as manually controlling HPCI turbine to establish and control
20 injection flow, are not virtually certain to be successful. These situations should be resolved
21 on a case-by-case basis through the FAQ process.

Event or circumstances requiring guidance interpretation:

A procedure is used to periodically drain water from between two normally closed containment isolation valves and the containment sump. The containment isolation valves provide a suction path to the Residual Heat Removal Pumps (RHR) from the containment sump. The isolation valve closest to the sump is opened and then a drain valve between the two containment isolation valves is opened to perform the draining. Two dedicated operators are used during this procedure. One is stationed in the control room, dedicated to closing the containment isolation valve if notified by the control room operator that a safety injection has occurred. The other operator is stationed in the field at the drain valve and will close it upon being notified by the control room operator that a safety injection has occurred. Restoration actions are contained in a written procedure, are uncomplicated (*a single action for each operator*), are capable of being restored in time to satisfy PRA success criteria and do not require diagnosis or repair. The operator in the control room performing the procedure (not one of the two dedicated operators) is responsible for identifying the condition and notifying the two dedicated operators to perform their dedicated functions.

The operator stationed in the field to close the drain valve is the operator dedicated to restoring the MSPI monitored function. The MSPI monitored function for RHR includes the flow path from

the containment sump to the RHR pumps that is normally isolated and only used post-LOCA to cool and recirculate water from the containment sump following depletion of RWST inventory, to provide decay heat removal. The containment isolation valves are motor operated and do not have automatic open or close features. The containment isolation valve closest to the RHR pump suction remains closed during performance of the procedure. The dedicated operator used to close the inboard containment isolation valve is in place to restore the containment isolation function. Containment isolation is not a monitored function for MSPI. Therefore, only one dedicated operator is used to restore the MSPI monitored function.

The restoration actions taken by the station for this procedure fulfill the dedicated operator qualifying conditions:

- Are contained in a written procedure
- Are uncomplicated (*a single action or a few simple actions*),
- Are capable of restoring the system in time to satisfy PRA success criteria
- Actions for restoration do not require diagnosis or repair
- Operators are positioned at the proper location throughout the duration of the test
- Operators are in communication with the control room
- Operators are in close proximity to restore the equipment when needed
- Staffing is considered in advance
- Operators are identified to perform the restoration actions independent of other control room actions

The licensee credits operato r recovery actions and unavailability of the RHR system is not counted for MSPI during this procedure.

If licensee and NRC resident/region do not agree on the facts and circumstances explain:

The NRC contends that NEI 99-02 only discusses the use of a dedicated operator in a singular manner (NEI 99-02, page F-6, lines 37-38, "the function can be promptly restored either by an operator in the control room or by a designated operator stationed locally for that purpose."). The procedure in question uses two dedicated operators and an operator in the control room as described above. The operator in the control room performing the evolution is procedurally instructed to notify the two dedicated operators to perform their dedicated functions if conditions warrant. Therefore, the NRC believes that unavailability should be counted for the stated condition.

Potentially relevant existing FAQ numbers

N/A

Response Section

Unavailability need not be counted during the described evolution since all the criteria are met for a dedicated operator in accordance with NEI 99-02, Rev. 5, page F-6, lines 31-40 and page F-7, lines 1-21. The MSPI function in question is for RHR, which NEI 99-02 defines as:

> The function monitored for the PWR residual heat removal (RHR) system is the long term decay heat removal function to mitigate those transients that cannot rely on the steam generators alone for decay heat removal. These typically include the low-pressure injection function and the recirculation mode used to cool and recirculate water from the containment sump following depletion of RWST

inventory to provide decay heat removal. The pumps, heat exchangers, and associated piping and valves for those functions are included in the scope of the RHR system.

For the event in question, one dedicated operator is used to restore the MSPI monitored function. The operator stationed in the field to close the drain valve is the operator dedicated to restoring the MSPI monitored function. If the drain valve is open when placing containment sump recirculation into service, the potential exists to affect the RHR monitored MSPI function.

The operator located in the control room that is responsible for closing the containment inboard isolation valve is supporting restoration of the containment isolation function, which is not an MSPI monitored function. With the inboard containment isolation valve open, it is in the proper position for performing the MSPI monitored function. Therefore, repositioning is not required to restore the MSPI monitored function.
Unavailability need not be counted in the scenar io provided. The NEI 99-02 requirements for a dedicated operator ar e met.

Proposed Resolution of FAQ

The purpose of the guidance for dedicated operator in NEI 99-02 is to allow licensees to take credit for restoration actions that are virtually certain to be successful during accident conditions. Initially this scenario was described as using multiple dedicated operators during the event to be responsible for restoring the MSPI monitored function. It has been clarified that only one dedicated operator is used to retore the MSPI monitored function and one is used to restore a non-monitored function. The issue of using more than one dedicated should still be clarified in NEI 99-02, even if it does not apply in this event. Using more than one operator fulfills the intent and safety function of the process. Licensees should not be required to incur unavailability for using multiple dedicated operators for actions that are virtually certain to be successful.

If appropriate, proposed rewording of guidance for inclusion in next revision.

In NEI 99-02, pages F-6 and F-7, section F.1.2.1.1, under Credit for Operator Recovery Actions to Restore the Monitored Functions, replace the term "operator" with the term "operator(s)" when referring to designated operator and dedicated operator.

As an alternative, in the same section, "or" could be changed to "and/or." As example, page F-6, lines 37-38, "...the function can be promptly restored either by an operator in the control room **and/or** by a designated operator stationed locally for that purpose."