'3 1

DRAFT

NUMARC 87-00

GUIDELINES AND TECHNICAL BASIS FOR NUMARC INITIATIVES

REVISION 1

AUGUST 28, 1989

APPENDIX D

EDG RELIABILITY PROGRAM

DRAFT

56pp

DRAFT

INTRODUCTION

This appendix provides guidance on actions that may be implemented as appropriate to ensure that (1) Emergency Diesel Generator (EDG) performance is maintained at acceptable levels (i.e. allowed target reliability per Section 3.2.4) and that (2) nuclear unit EDGs whose performance deviates significantly from acceptable levels are subject to additional efforts to restore performance. Suggested guidance on important elements for EDG reliability, recommended action levels and remedial efforts for EDG performance that deviates significantly from acceptable levels are provided. The action levels and remedial efforts are based on statistical analysis and programmatic experience and constitute a graded response to declining EDG reliability.

This appendix consists of three sections. Section D.1 provides definitions of key terms related to the EDG Reliability Program. Section D.2 provides guidance on methods to monitor the overall effectiveness of the nuclear unit EDG reliability efforts and describes actions that should be taken to improve performance. Section D.3 describes the critical review elements that are the core of the EDG Reliability Program. These elements are derived from current and recommended industry practices that have proven effective in enhancing EDG reliability.

All utilities are required to have a reliability program to ensure that the EDGs credited in each facility's station blackout coping assessment are maintained at acceptable levels throughout the remaining plant life. The guidance in this document provides an acceptable EDG reliability program. The definitions, concepts, and methodologies presented in this appendix are consistent with the Institute of Nuclear Power Operations (INPO) Plant Performance Indicator Program (PPIP) methodology.

Utilities are encouraged to review their existing efforts on EDG reliability against the guidance in this Appendix and consider changes to their reliability efforts that may be necessary to improve reliability. The EDG reliability program does not have to be a unique single function effort. In most facilities the EDG reliability elements set forth in this Appendix are currently being performed by various organizational units. This Appendix imposes no additional requirement to realign responsibility for the various elements of EDG reliability.

Certain facilities have EDGs of a specific manufacturer that have already been the subject of EDG reliability efforts assessed by the NRC. To the extent that any EDG reliability elements in this Appendix are currently addressed by reliability efforts previously assessed by the NRC, these efforts are deemed to satisfy the corresponding EDG reliability efforts contained in this Appendix.

DRAFT

D.1 DEFINITIONS

DRAFT

NUMBER OF START DEMANDS

All valid and inadvertent start demands, including all start-only demands and all start demands that are followed by load-run demands, whether by automatic or manual initiation. A start-only demand is a demand in which the emergency generator is started, but no attempt is made to load the generator. See "Exceptions" below.

NUMBER OF START FAILURES

All valid start failures. Any failure within the emergency generator system that prevents the generator from achieving specified frequency (or speed) and voltage is classified as a valid start failure. (For the monthly surveillance test, the generator can be brought to rated speed and voltage in a time that is recommended by the manufacturer to minimize stress and wear. Similarly, if the generator fails to reach rated speed and voltage in the precise time required by technical specifications, the start attempt is not considered a failure if the test demonstrated that the generator would start in an emergency.) See "Exceptions" below. Any condition identified in the course of maintenance inspections (with the emergency generator in the standby mode) that would have resulted in a start failure if a demand had occurred should be counted as a valid start demand and failure.

NUMBER OF LOAD-RUN DEMANDS

All valid load-run demands. To be valid, the load-run attempt must follow a successful start and meet one of the following criteria: (See "Exceptions" below.)

- a load-run of any duration that results from a real (e.g., not a test) automatic or manual signal
- a load-run test to satisfy the plant's load and duration test specifications
- other operations (e.g., special tests) in which the emergency generator is planned to run for at least one hour with at least 50 percent of design load

NUMBER OF LOAD-RUN FAILURES

All valid load-run failures. A load-run failure should be counted when the emergency generator starts but does not pick up load and run successfully. Any failure during a valid load-run demand should be counted. See "Exceptions" below. (For monthly surveillance tests, the generator can be loaded at a rate that is recommended by the manufacturer to minimize stress and wear.

DRAFT

Similarly, if the generator fails to load in the precise time required by technical specifications, the load-run attempt is not considered a failure if the test demonstrated that the generator would load and run in an emergency.) Any condition identified in the course of maintenance inspections (with the emergency generator in the standby mode) that would have resulted in a load-run failure if a demand had occurred should be counted as a valid load-run demand and failure.

EXCEPTIONS

Unsuccessful attempts to start or load-run should not be counted as valid demands or failures when they can be definitely attributed to any of the following:

- spurious operation of a trip that would be bypassed in the emergency operation mode (e.g., high cooling water temperature trip)
- malfunction of equipment that is not required to operate during the emergency operating mode (e.g., synchronizing circuitry)
- intentional termination of the test because of alarmed or observed abnormal conditions (e.g., small water or oil leaks) that would not have ultimately resulted in significant emergency generator damage or failure
- component malfunctions or operating errors that did not prevent the emergency generator from being restarted and brought to load within a few minutes (i.e., without corrective maintenance or significant problem diagnosis)

Each emergency generator failure that results in the generator being declared inoperable should be counted as one demand and one failure. Exploratory tests during corrective maintenance and the successful test that is run following repair to verify operability (prior to declaring operability) should not be counted as demands or failures.

UNIT EDG RELIABILITY: The average reliability of all EDGs being combined at an individual nuclear unit.

EXCEEDENCE TRIGGER VALUE: The value (based on number of failures during a comparative number of demands) at which additional actions to review the effectiveness of EDG reliability efforts are initiated.

CORRECTIVE MAINTENANCE: Maintenance performed to correct a component or subcomponent which is determined to be incapable of performing its function.

PREVENTATIVE MAINTENANCE: Maintenance performed with the expectation of preventing a component or subcomponent from failing to perform its function.

DRAFT

D.2 PROCEDURE FOR MONITORING EFFECTIVENESS OF EDG RELIABILITY ELEMENTS

This procedure provides methodology to monitor, maintain, and improve unit EDG reliability. The procedure utilizes samples of EDG test and operating data and compares this data with predetermined values to determine a proper course of action to support EDG reliability goals. It should be noted that a reliability value derived from a sample is only an approximate indication of an EDG's true underlying reliability. This is because the reliability from samples will vary from the underlying reliability because of statistical variations based upon the sample sizes. Therefore, this procedure employs reliability indicators which are calculated from the number of EDG failures experienced in a sample of test data. The method of calculating these reliability indicators is given in Section D.2.2.

The data sample sizes used to determine EDG reliability for purposes of establishing a target reliability in Section 3.2.4 and the data sample sizes used in this Appendix are somewhat different due to the different end uses. The data sample sizes used to determine the selected EDG target reliability were chosen to represent the underlying value of EDG reliability for purposes of station blackout risk assessment without penalizing plants because of relatively recent or relatively old failures. Three sample sizes are chosen with three separate acceptance criteria. The data sample sizes used in this Appendix are based on establishing action levels for increased EDG reliability efforts over and above those normally performed. In establishing these sample sizes, care must be taken to ensure that unnecessary actions are not taken based solely on the uncertainty of the data sample size. This consideration must be balanced with the need to provide assurance that the underlying unit EDG reliability supports the selected reliability goals. These considerations are addressed by selecting appropriate data sample sizes, corresponding trigger levels, and subsequent actions.

The procedure in this Section consists of five parts:

(1) maintaining data on EDG successes and failures

(2) evaluating the unit EDG reliability indicators for the last 50 and last 100 demands as well as EDG performance over the last 20 demands via the prescribed methodology

(3) relating the calculated EDG reliability indicators to trigger values established for the selected target reliability

(4) taking remedial actions for individual failures and for exceedence of one or more trigger values

(5) reporting all EDG failures.

The sample size and action levels are based on the assumption that the minimum surveillance testing interval for each EDG is once per month. Details of each step are presented in the sections that follow.

The procedure incorporates a graded approach for responding to indications of significantly decreasing reliability. Industry data indicate that existing activities to maintain EDG reliability at each unit are ensuring reliability levels at or above the selected target levels. Statistically based trigger values are used to signal the need for increased attention and remedial actions. These triggers are designed to assure that a re-examination of the effectiveness of critical elements is performed when needed. At the same time the triggers guard against the need for remedial actions that are artifacts, because of statistical variations, of a small sample size. The reporting requirements provide the documentation that the process activities are in place and effective.

D.2.1 Maintenance of EDG Reliability Data

All utilities should maintain records on EDG demands, successes, and failures. Each success or failure should be classified using the INPO Plant Performance Indicator Program (PPIP) methodology where applied to EDGs to establish valid demands, successful starts and successful load-runs. Information concerning demands, successes and failures should be maintained in such a manner that they can be made available for review at a later time. The rules governing the INPO methodology are similar to the intent of NSAC 108, The Reliability of Emergency Diesel Generators at U.S. Nuclear Power Plants [Wyckoff].

D.2.2 Determining Reliability Indicators

The determination of underlying EDG reliability from a sample contains inherent statistical uncertainty. The only straightforward indication of EDG reliability performance is based on the demand and failure data from actual EDG demands, both planned and unplanned. However, the nature of this EDG reliability data is such that a balance must be struck between the use of old, potentially unrepresentative data and the use of small data samples comprised of more recent representative data that is inherently uncertain. The method used to determine the reliability indicators in this section is by no means the only method for selecting appropriate data sample sizes, corresponding trigger levels, and actions. Other statistically valid techniques such as weighted averages and Bayes theorem may be equally appropriate to determine a reliability indicator. If such alternate reliability indicators are used, an appropriate set of corresponding actions should be used that are consistent with the set of actions contained in Sections D.2.4 and D.2.5.

In this Appendix, the reliability indicators are established through:

(1) the use of appropriate sample sizes based on statistical analyses of actual EDG data,

(2) the combination of unit EDG experience to obtain adequate sample size while ensuring representative data, and

(3) the comparison of the failure experience to reliability trigger values which have been developed specifically to acknowledge the variability inherent in the data.

Investigation of industry EDG failure experience has indicated that the evaluation of EDG reliability based solely on small data samples (i.e. < 20 demands) contains too great an uncertainty to allow the determination of an appropriate course of action. However, recent data (i.e. 3 failures in the last 20 demands) can serve as an EDG performance indicator that should be evaluated to provide early indication of potential problems. Additionally, sample sizes of greater than 100 demands could contain data which is more than four years old and unrepresentative of the current condition of the EDG.

For these reasons, the EDG performance and reliability indicators in this program are based on the failure experience in the most recent 20, 50 and 100 demands. The use of these sample sizes allows the development of a graded approach to potential reliability degradations as described in Section D.2.4.

The calculation of the overall EDG reliability of a nuclear unit is comprised of two components: (1) the start reliability and (2) the load-run reliability. Since not all EDG demands include both start and load-run demands, data on these two reliability components must be gathered and evaluated individually and then combined. An equal number of start demands and load-run demands may not occur in the same time interval.

D.2.2.1 Determining Unit EDG Performance Indicator for Last 20 Demands

Determining the unit EDG performance indicator for the past 20 demands is accomplished by summing the number of failures observed in the past 20 start demands and the number of failures observed in the last 20 load-run demands for all of the EDGs serving as standby power supplies to that unit.

D.2.2.2 Determining Unit EDG Reliability Indicator for Last 50 Demands

Determining the unit EDG reliability indicator for the past 50 demands is accomplished by summing the number of failures observed in the past 50 start demands and the number of failures observed in the last 50 load-run demands for all of the EDGs serving as standby power supplies to that unit. It is important to note that the last 50 start demands for the unit may not correspond in calendar time to the last 50 load-run demands for the unit since not all starts result in load-runs. Since load-run demands are typically less frequent than start demands, a time limit of four years is suggested on the load-run data.

D.2.2.3 Determining Unit EDG Reliability Indicator for Last 100 Demands

Determining the unit EDG reliability indicator in the past 100 demands is accomplished by summing the number of failures observed in the last 100 start demands and the number of failures observed in the last 100 load-run demands for all of the EDGs serving as standby power supplies to that unit. Since load-run demands are typically less frequent than start demands, a time limit of four years is placed on the load-run data.

Example: Determining the plant unit EDG reliability indicator for the last 50 demands

A site has one nuclear unit which has two EDGs (EDG-1 and EDG-2). The last 50 demands consisted of 30 start demands on EDG-1, 20 start demands on EDG-2, 20 load-run demands on EDG-1, and 30 load-run demands on EDG-2.

EDG-1 has experienced two starting related failures in the last 30 EDG-1 start demands and EDG-2 has experienced no starting related failures in the last 20 start demands. Thus, the unit has experienced two starting failures in the last 50 start demands.

EDG-1 has experienced one load-run failure in the last 20 load-run demands, and EDG-2 has experienced one load-run failure in the last 30 load-run demands. Thus, the unit has experienced two load-run failures in the last 50 load-run demands.

Reliability Indicator - The total number of nuclear unit EDG failures experienced in the last 50 demands is four (two start failures for the unit plus two load-run failures for the unit). Therefore the reliability indicator is four out of 50.

D.2.2.4 Special Conditions

The evaluation of a nuclear unit's EDG reliability indicator should take into account the demand and failure experience of all EDGs which provide standby power for the the unit. For units with fully shared EDGs between nuclear units (for example, four EDGs serving two units), the units should perform the same evaluation based on all the EDGs. For units with some dedicated and some shared EDGs, the failure experience of the EDG serving the specific unit are to be included.

Example: For a two unit plant with one EDG dedicated to the first unit, one EDG dedicated to the second unit and a third EDG shared between units, the EDG reliability indicator for the first unit should consider only the failure experience of its dedicated diesel and the shared diesel. Likewise, the EDG reliability indicator for the second unit should consider the failure experience of its dedicated EDG and the shared EDG. The shared EDG is applied to both units.

Some units have EDGs of different designs which serve the function of providing standby power supplies. EDGs that have different designs, operating procedures and maintenance procedures, may be evaluated separately if desired. In this case a unit would have more than one set of reliability indicator evaluations to perform and to compare to program triggers.

Example: A two nuclear unit site has five EDGs. Three are of the same manufacturer and design. Two of these three serve the emergency busses of one of the nuclear units and the third serves as a swing between nuclear units. The remaining two EDGs are of a different manufacturer and design than that of the first three. These remaining two serve the emergency buses of the second nuclear unit. Since each of these EDGs have the capability to provide for safe shutdown, they are roughly equivalent from a station blackout risk perspective. However, under this program, one 20, 50 and 100 demand reliability indicator is to be calculated using the combined experience of three EDGs of the same type and a second 20, 50 and 100 demand reliability indicator is to be calculated using the combined experience of the other two EDGs. The results of these separate evaluations are to be compared to appropriate reliability triggers as described in Section D.2.3. If either of the EDG reliability evaluations result in an exceedence of the triggers, then the corresponding nuclear unit is required to perform the actions called for in Section D.2.4.

Table D.2-1 provides methods that can be used for combining unit EDG experience for different EDG configurations.

Table D.2-1

METHODS FOR COMBINING UNIT EDG EXPERIENCE

EDG Configuration	Method for Combining
2,3,4 EDGs dedicated to a unit	Use combined failures of all EDGs
2,3,4 EDGs shared between units	Use combined failures of all EDGs for all units
1 dedicated EDG at each unit and 1 shared between units	Each unit uses the combined failures of its dedicated EDG and the shared EDG
2 dedicated EDGs at each unit and 1 shared between units	Each unit uses the combined failures of its dedicated EDGs and the shared EDG
2 dedicated EDGs and 1 or diverse EDGs within the same unit	Use the combined failures of similar EDGs and separately consider the failures of different EDGs

DRAFT

D.2.3 Comparison of Calculated Unit EDG Reliability Indicators to Trigger Values for Selected Target Reliability

D.2.3.1 Establishment of Exceedence Triggers

Failure rate triggers are used to indicate when EDGs do not meet the selected reliability targets. The exceedence triggers are used with, and matched to, the graded response approach for assuring an acceptable EDG reliability. In using a sample of past demands to gain perspective on the true underlying EDG reliability, a number of unique statistical factors must be addressed. The probability of experiencing a given number of failures in 50 samples of 50 demands is much greater than experiencing the same number of failures in one independent sample of 50 demands. The development of the trigger values as indicators of underlying EDG reliability must reflect this phenomenon.

A second factor that must be dealt with is the effect of normal statistical variations in concert with the inherent small sample sizes that are used. It is not appropriate to view one sample whose reliability indication is moderately out of range as a conclusive indicator of unacceptable underlying reliability. This is because a range of normal statistical variations always exists.

A third factor is that acceptable underlying reliabilities fall within a very small range (95 to 100%). Small normal statistical variations can incorrectly indicate that even a reliable EDG is outside this small range. Thus the trigger values must encompass the effects of statistical variations. In totality, these interweaving statistical factors cannot be accounted for using straight analytical methods. However, this behavior can be simulated accurately using computer based statistical methods that are based on Monte Carlo techniques. Using these techniques, sliding sample reliability can be determined for the range of probable underlying reliabilities. The probabilities of both false indications of unacceptable reliability and true indications can be determined and their relative values balanced. These are the techniques that have been used to select the exceedence trigger values in Table D.2-2.

D.2.3.2 Use of the Exceedence Trigger Values

This sub-section provides the method for selecting the proper trigger values for the selected reliability target values. Table D.2-2 provides the trigger value for 20, 50 and 100 demands based on the selected EDG target reliability. The selected EDG target reliability is the allowed underlying EDG target reliability used in Table 3.8 page 3-19. Table D.2-2 provides the exceedence trigger value for selected EDG target reliabilities of 0.95 and 0.975.

DRAFT

DRAFT

Table D.2-2

EXCEEDENCE TRIGGER VALUES

Selected Reliability Target	Failures In 20 Demands	Failures In 50 Demands	Failures In 100 Demands
0.95	3	5	8
0.975	3	4	5

The target reliability is the value selected in Section 3.2.4 in the coping assessment. This value represents the underlying unit EDG reliability value for purposes of establishing a coping duration for a station blackout. The exceedence trigger values for failures in 20 demands, failures in 50 demands and failures in 100 demands represent the values at which additional actions as set forth in this Appendix should be taken to evaluate the effectiveness of the EDG reliability efforts.

Periodic testing typically will be conducted at one month intervals for each EDG. Real demands may also occur between testing intervals. After each failure of an EDG, and prior to the next scheduled periodic test, the number of unit EDG failures in the last 20, 50 and 100 demands should be compared to the exceedence trigger values for the selected target reliability.

D.2.3.3 Successful Test/Demand

If the most recent test is successful, then no additional actions are required unless already in a past exceedence category (see Section D.2.4.4). Existing EDG reliability efforts should be continued.

D.2.3.4 Unsuccessful Test/Demand - No Trigger Values Exceeded

If the most recent test results in a failure and the failures in the last 20 demands, the failures in the last 50 demands, and the failures in the last 100 demands are less than the trigger values in Table D.2-2 for the selected reliability target, then the actions set forth in Section D.2.4.1, Actions for Plants That Do Not Exceed Either Trigger, should be followed.

<u>Example</u>: A unit has a selected EDG reliability target of 0.95. From Table D.2-2, the trigger values are three for failures in 20 demands, five for failures in 50 demands and eight for failures in 100 demands. The most recent failure was the second failure established as applicable to the failure in 20 demands test, the third failure established as applicable to the failure in 50 demands test and the sixth failure established as applicable to the

DRAFT

failure in 100 demands test. The two failures are less than the three failure trigger value for the failures in 20 demands, the three failures are less than the five failure trigger value for the failures in 50 demands and the six failures are less than the eight failure trigger for the failures in 100 demands. Hence. none of the trigger values were equaled or exceeded. The actions set forth in section D.2.4.1, Actions for Plants That Do Not Exceed Either Trigger, should be followed.

D.2.3.5 Unsuccessful Test/Demand - One Trigger Value Exceeded

If the most recent test resulted in a failure and either:

(1) the failures in 20 demands are equal to or greater than the trigger value for the selected reliability target in Table D.2-2,

<u>OR</u>

(2) the failures in 50 demands are equal to or greater than the trigger value for the selected reliability target in Table D.2-2,

<u>OR</u>

(3) the failures in 100 demands are equal to or greater than the trigger value for the selected reliability target in Table D.2-2,

then the actions set forth in Section D.2.4.2, Actions For Plants Exceeding A Single Trigger, should be followed.

<u>Example</u>: A unit has a selected EDG reliability target of 0.95. From Table D.2-2, the trigger values are three for failures in 20 demands, five for failures in 50 demands and eight for failures in 100 demands. The most recent failure was the third failure established as applicable for the failures in 20 demands test, the fourth failure established as applicable for the failures in 50 demands test, and the sixth failure established as applicable for the failures in 100 demands test. The three failures equals or exceeds the three failure trigger value for the failures in 20 demands, the four failures are less than the five failure trigger value for the failures in 50 demands, and the six failures are less than the eight failure trigger value for the failures in 100 demands. Hence, one trigger value was equaled or exceeded. The actions set forth in section D.2.4.2, Actions for Plants Exceeding a Single Trigger, should be followed.

DRAFT

D.2.3.6 Unsuccessful Test/Demand - 50 and 100 Demand Trigger Values Exceeded

If the most recent test resulted in a failure and:

(1) the failures in 50 demands are equal to or greater than the trigger value for the selected reliability target in Table D.2-2,

AND

(2) the failures in 100 demands is equal to or greater than the trigger value for the selected reliability target in Table D.2-2,

then the actions set forth in Section D.2.4.3, Actions For Plants That Exceed the 50 and 100 Demand Triggers, should be followed.

Example: A unit has a selected EDG reliability target of 0.975. From Table D.2-2, the trigger values are four for failures in 50 demands and five for failures in 100 demands. The most recent failure was the fourth failure established as applicable to the failure in 50 demands test and the fifth failure established as applicable to the failure in 100 demands test. The four failures equals or exceeds the four failure trigger value for the failures in 50 demands and the fifth failure equals or exceeds the five failure trigger for the failures in 100 demands. Hence, both trigger values were equaled or exceeded. The actions set forth in section D.2.4.3, Actions for Plants That Exceed the 50 and 100 Demand Triggers, should be followed.

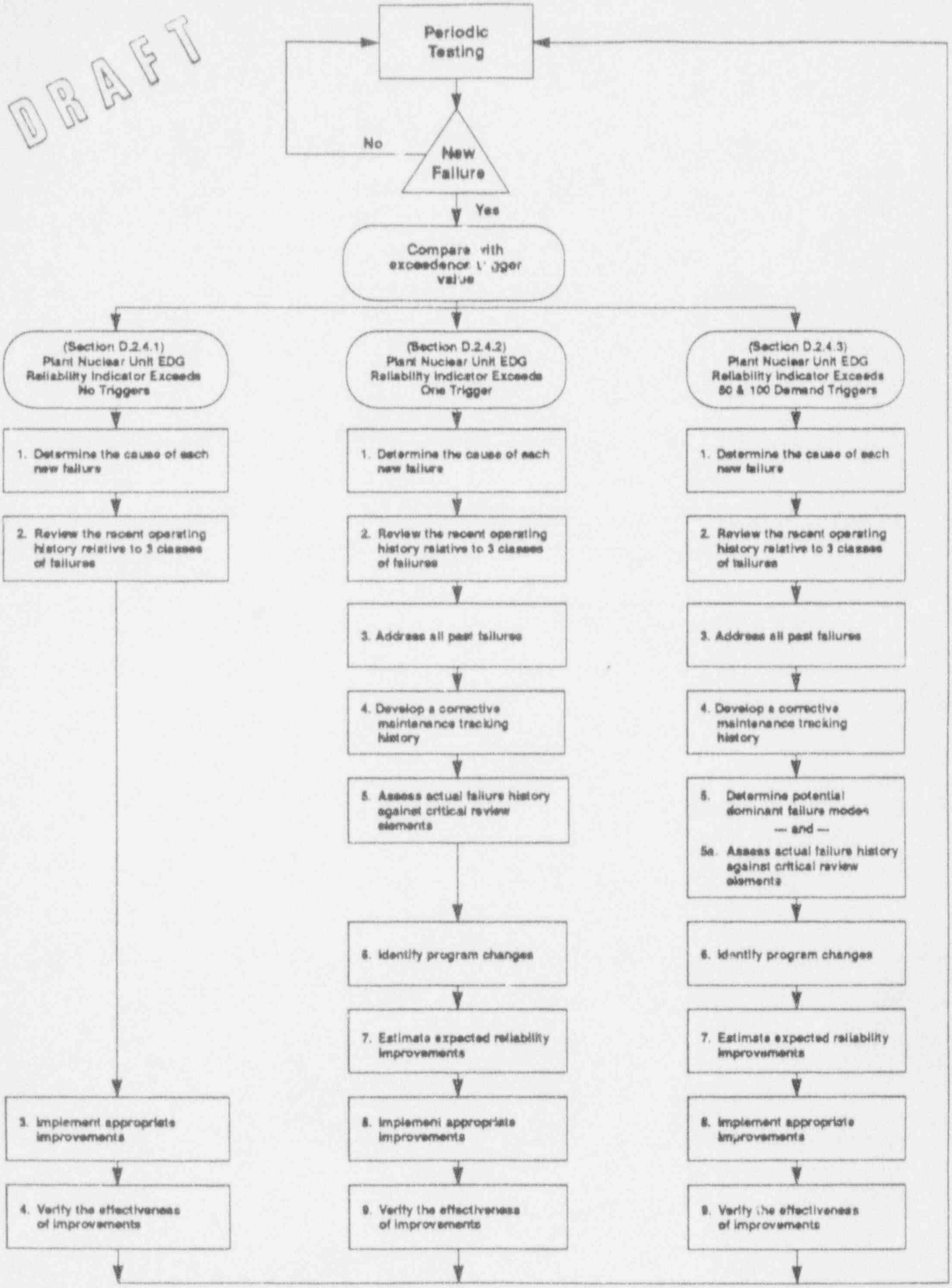
D.2.4 Actions for Individual Failures and for Exceedence of One or More Trigger Values

This section provides the response action guidelines to one or more EDG failures or the exceedence of one or more trigger values. Figure D.2-1 illustrates the actions to be taken. The left-most flow path represents actions to be taken when there is an EDG failure but when no trigger values are exceeded. These actions are detailed in Section D.2.4.1. The center flow path represents the actions to be taken when the trigger value for either 20, 50 or 100 demands is exceeded. These actions are detailed in Section D.2.4.2. The right flow path represents the actions to be taken when the trigger values for both the 50 and 100 demands have been exceeded. These actions are detailed in Section D.2.4.3.

Section D.2.4.4 provides details on the duration of actions arising from exceeding one or more of the trigger values.

DRAFT

FIGURE D.2-1


Periodic Testing
New Failure
No
Yes
Compare with exceedence trigger value
(Section D.2.4.1) Plant Nuclear Unit EDG Reliability Indicator Exceeds No Triggers
(Section D.2.4.2) Plant Nuclear Unit EDG Reliability Indicator Exceeds One Trigger
(Section D.2.4.3) Plant Nuclear Unit EDG Reliability Indicator Exceeds 50 & 100 Demand Triggers
1. Determine the cause of each new failure
2. Review the recent operating history relative to 3 classes of failures
3. Implement appropriate improvements
4. Verify the effectiveness of improvements
1. Determine the cause of each new failure
2. Review the recent operating history relative to 3 classes of failures
3. Address all past failures
4. Develop a corrective maintenance tracking history
5. Assess actual failure history against critical review elements
6. Identify program changes
7. Estimate expected reliability improvements
8. Implement appropriate improvements
9. Verify the effectiveness of improvements
1. Determine the cause of each new failure
2. Review the recent operating history relative to 3 classes of failures
3. Address all past failures
4. Develop a corrective maintenance tracking history
5. Determine potential dominant failure modes
— and —
5a. Assess actual failure history against critical review elements
6. Identify program changes
7. Estimate expected reliability improvements
8. Implement appropriate improvements
9. Verify the effectiveness of improvements

DRAFT

D.2.4.1 Actions for Plants That Do Not Exceed Either Trigger Value

For plants whose observed number of failures in the past 20, 50 and the past 100 demands are less than the respective trigger values for the selected reliability target, but who have experienced an unsuccessful start or load-run, the following reliability actions should be performed:

(1) determine the cause of each new failure

(2) review the recent operating history relative to 3 classes of failures

(3) implement appropriate improvements

(4) verify the effectiveness of the improvements

It should be noted that the reliability actions described herein following an EDG failure do not preclude any immediate actions to fulfill regulatory requirements. Testing and response to failures (corrective actions) should be consistent with plant Technical Specifications.

The normal plant practices and procedures to accomplish the noted reliability actions do not need to be modified specifically for the EDGs. The results of these actions should be incorporated into appropriate corrective actions. Details of these reliability actions are provided below.

(1) Determine the Cause of Each New Failure

The cause of each new failure should be determined. A root cause analysis capability is generally agreed to be an effective part of the failure analysis process. A root cause analysis of any EDG failure should include:

a. the cause of failures be investigated in sufficient detail with appropriate cause codes for tracking Corrective Maintenance (CM),

b. the cause of all functional failures be determined to the highest level at which they can be addressed by an applicable and effective maintenance task, testing task, procedure change, operations change, or design modification.

Section D.2.5 provides additional guidance on root cause analysis.

If a detailed root cause analysis is not appropriate, the analysis would be done to the depth required to make such a determination of the cause of each failure. The threshold for performing/not performing detailed root cause analysis is a function of the failure being examined.

DRAFT

(2) Review the Recent Operating History Relative to 3 Classes of Failures

The utility should review the recent operating history to determine if any indications exist that suggest the presence of one of 3 classes of failures.

a. Failures with common cause potential (e.g., with the potential to cause failure of more than one diesel at a time).

b. Failures with a recurring root cause within a short interval.

c. Failures with severe (or potentially severe) consequences (e.g., substantial equipment damage and long repair times).

In carrying out the above review, plant personnel would pay special attention to closely spaced failures. These could be an indication of degradation or, if on different EDGs, of a common cause. If a root cause analysis had been performed for each previous failure, then reviewing those analyses should accomplish this action.

(3) Implement Appropriate Improvements

Improvements should be implemented in those areas indicated by the root cause analyses of the EDG failures. The improvements should be prioritized and scheduled based on the significance of their contribution to preventing a recurring failure. Timely and proper implementation of improvements will reduce the likelihood of future failures and help to prevent exceedence of reliability trigger values.

(4) Verify the Effectiveness of the Improvements

Measures should be taken to ensure that any changes that are implemented result in improvements to unit EDG reliability. Consideration should be given to special testing or an enhanced monitoring capability during normal surveillances that is focused on the area where the change was implemented. Additionally, other test data should be carefully reviewed following the implementation of a change to ensure that no undesired effects resulted from the change.

D.2.4.2 Actions for Plants Exceeding a Single Trigger

Nuclear units that exceed the last 20 demand failure trigger or the last 50 demand failure trigger or the last 100 demand failure trigger should take actions that are in addition to the current routine EDG reliability efforts for plants with new failures but no trigger value exceedences. The additional actions would focus on identifying and correcting the cause of the decrease in reliability based on the actual EDG failures that had occurred at the nuclear unit. The actions should be:

(1) determine the cause of each new failure

(2) review the recent operating history relative to 3 classes of failures

(3) address all past failures

(4) develop a corrective maintenance tracking history

(5) assess actual failure history against critical review elements

(6) identify program changes

(7) estimate expected reliability improvements

(8) implement appropriate improvements

(9) verify the effectiveness of the improvements

A detailed description of these actions is provided below.

(1) Determine Cause of Each New Failure

This action is to determine the cause of new failures as provided in Section D.2.4.1.

(2) Review the Recent Operating History Relative to 3 Classes of Failures

This action is to review the recent operating history relative to 3 classes of failures as provided in Section D.2.4.1

(3) Address All Past Failures

The review of observed EDG failures for all EDGs included in the trigger value calculation should be undertaken to identify specific improvements (e.g., in EDG testing, maintenance, operational practices, design changes, etc.) that would restore an EDG's reliability to an acceptable level. The scope of the investigation would encompass all applicable observed EDG failures. This investigation would strive to understand the failure modes and the underlying reasons for the failures. For this review all failure modes actually experienced are considered to be dominant modes. With this information it would be possible to specify actions that could be taken to preclude or minimize the recurrence of many of the observed failures. The product of this task action would be a list of potential applicable and effective changes that could be implemented. At this point, the list should not be constrained by practical considerations, such as cost, but rather should be a composite list of improvements.

DRAFT

4. Corrective Maintenance Tracking History

Nuclear units that have exceeded one trigger should implement an EDG Corrective Maintenance (CM) history and ongoing CM tracking. The history should review previous CM activities to the extent appropriate based on the nature of the failures. This history would provide cognizant plant personnel with additional information that would be useful in identifiying precursors to further reliability degradation. As part of this history, where available data permits, each CM related to an EDG system component failure would be evaluated and categorized in four improtant areas: severity of failure, functions affected, EDG subsystem involved and failure cause classification. The severity of each CM would be calssified in accordance with the IEEE Std 500 Reliability Data severity levels: catastrophic, incipient and degraded. A sample format for tracking EDG CMs is provided in Figure D.2-2.

Figure D.2-2

Corrective Maintenance Tracking History

CM # (1)	Component Involved (2)	Subsystem (3)	Catastrophic/ Incipient/ Degradent (4)	Function(s) Affected (5)	Description Of Failure (6)	Corrective Action(s) Taken (7)

Heading Definitions

1. **CM #** — A unique identifier for the work request or work authorization which was initiated in response to the failure.
2. **Component Involved** — The unique equipment piece number(s) for the component(s) involved in the failure.
3. **Subsystem** — The EDG subsystem affected by this failiure (i.e. fuel, starting air, engine, generator, cooling exhaust, lubrication or I & C)
4. **Catastrophic/Incipient/Degraded** — Classification of the failure according to the IEEE-500 severity index.
5. **Function(s) Affected** — identification of the function(s) of the EDG impacted by the failure (i.e. starting, loading, continued operations, shutdown, etc.)
7. **Corrective Action(s) Taken** — A brief description of action taken in response to failure (i.e. repair, replacement, redesign, etc.)

The Corrective Maintenance history and ongoing tracking should take care to distinguish between corrective maintenance actions and other actions that may use the normal plant work order system commonly used for corrective maintenance. The ongoing CM tracking should continue until the EDGs are no longer considered to be in an exceedence category as per Section D.2.5. After implementing the CM tracking program, plant personnel would have available regular summaries of the CM data to assist in monitoring and evaluating EDG performance.

DRAFT

DRAFT

5. Assess Failure History Against Critical Review Elements

Once the specific failures have been reviewed and potential program imporvements have been identified, an evaluation should be performed to determine if there are programmatic deficiencies. The evaluation should determine whether the observed reliability problems are being caused by deficiencies in any of six critical review element (CRE) areas. Each of the observed failures would be assessed by answering a few key questions aimed at identifying potential problems within the scope of each critical review element. If each observed failure had a rigorous root cause analysis performed, it may only be necessary to review each of these root cause analyses. Tables 1 through 6 provide questions that would satisfy the review for each of the six critical review elements. All questions for observed failures are applicable (the potential dominant failures are discussed in Section D.2.4.3). A discussion of each of the six critical review elements is provided in Section D.3.

To facilitate the review of the CREs, a matrix would be developed to correlate each failure to the CRE identified. A sample matrix is provided in Figure D.2-3.

Figure D.2-3

Identification of Implicated Critical Review Elements (1)

Failure/Failure Mode	Implicated Critical/Review Elements (2)					
	Surveillance Needs	Performance Monitoring	Maintenance Program	Failure/ Root Cause	Problem Close-out	Data Systems

1. For each failure or failure mode, any Critical Review Element implicated in response to the questions will be marked with an "x". Critical Review Elements implicated in more than one failure or failure mode will be evaluated on a programmatic basis.

2. Critical Review Elements consistent with NUREG/CR-5078.

DRAFT

DRAFT

Table 1

ASSESSSMENT OF EDG SURVEILLANCE NEEDS

For Observed Failures and Potential Dominant Failures

(1) Does the failure relate to equipment previously excluded from consideration as part of the EDG system ?
(2) Could the failure be prevented by a change in the content of surveillance practices (i.e., how the surveillances are conducted) ?
(3) Could the failure be prevented by a change in scheduling of surveillance practices (i.e., in the timing of surveillances) ?
(4) If the failure is one which proceeds from a degraded to a failed state, could it be identified by a surveillance before the failure occurs ?
(5) If the failure is related to aging, could surveillance detect the aged condition ?
(6) If the failure has common cause failure potential, could the common cause potential be identified through surveillance ?
(7) Does the severity of this failure warrant a change in surveillance practices ?
(8) Would the presence of a surveillance plan preclude this failure ?

For Observed Failures Only

(9) Should the existing surveillance program have identified this failure before it caused EDG failure ?

If the answer to any of these questions is yes, then mark the "Surveillance Needs" box for this failure.

Table 2

ASSESSMENT OF EDG PERFORMANCE MONITORING

For Observed Failures and Potential Dominant Failures

(1) Are there parameters (physical or statistical) that could be monitored which could preclude this failure ?
(2) Could the existence of alert levels or corrective action levels preclude this failure ?
(3) If existing alert levels or corrective action levels did not preclude this failure, should these levels be changed ?
(4) If the montoring procedures were improved, would the failure be precluded ?
(5) Is the monitoring frequency inadequate to detect this failure ?
(6) Could surveillance practices be changed to improve monitoring for this failure ?

DRAFT

(Table 2 continued)

For Observed Failures Only

(7) Is there a monitoring task in place which should have detected this failure before it caused EDG failure ?
(8) Should existing alert levels or corrective action levels have precluded this failure ?

If the answer to any of these questions is yes, then mark the "Performance Monitoring" box for this failure.

Table 3

ASSESSMENT OF EDG MAINTENANCE PROGRAM

For Observed Failures and Potential Dominant Failures

(1) If maintenance response to this failure is not based on the severity of the failure, then should it be ?
(2) If maintenance response to this failure is not based on expected repair time, then should it be ?
(3) Could preventive maintenance preclude this failure ?

For Observed Failures Only

(4) If maintenance actions contributed to this failure, could the actions have been identified in advance such as to preclude this failure ?
(5) If the maintenance organization was not involved in the failure and root cause analysis of this failure, should it have been ?
(6) Did spare parts play a role in this failure ?

If the answer to any of these questions is yes, then mark the " Maintenance Program" box for this failure.

Table 4

ASSESSMENT OF FAILURE ANALYSIS & ROOT CAUSE INVESTIGATIONS

For Observed Failures and Potential Dominant Failures

(1) Is the necessary information not routinely gathered to adequately assess the root cause of this failure ?

For Observed Failures Only

(2) Would an improved failure analysis and root cause investigation have precluded this failure ?

If the answer to any of these questions is yes, then mark the "Failure/Root Cause" box for this failure.

Table 5

ASSESSMENT OF EDG PROBLEM CLOSEOUT

For Observed Failures Only

(1) Did inadequate problem close-out through not implementing a previous corrective action contribute to this failure ?
(2) Could improved problem close-out procedures have precluded this failure?
(3) Would improved close-out criteria have precluded this failure ?
(4) Would special monitoring to enhance problem close-out have precluded this failure?

If the answer to any of these questions is yes, then mark the "Problem Close-out" box for this failure.

Table 6

ASSESSMENT OF EDG DATA SYSTEMS

For Observed Failures and Potential Dominant Failures

(1) Would an improved data system serve to preclude this failure ?

For Observed Failures Only

(2) Did an inadequate data system cause this failure (i.e., due to inaccessibility of either plant or generic data ?
(3) Would improved accessibility and retrievability of failure cause and root cause data have prevented this failure ?

If the answer to any of these questions is yes, then mark the "Data System" box for this failure.

Upon completion of the matrix, those CREs which were identified by two or more of the failures should be selected for further evaluation. This evaluation could lead to the need for additional, broader changes to the reliability program. For each CRE which is identified for further evaluation, a disposition should be developed to describe why actions were (or were not) taken to improve the reliability program in that area.

(6) Identify Program Changes

Through the study of actual present and past failures and the examination of the critical review elements in light of these failures, a comprehensive list of potential improvements would be available. This list would be evaluated by a plant team composed of knowledgeable personnel from engineering,

DRAFT

DRAFT

operations and maintenance. Their mission would be to select those improvements which would most effectively address the observed failures. To facilitate this process, the complete list of potential improvements would be prioritized on the basis of their expected effectiveness in improving EDG reliability for the observed failures. Cost, operational impact and other practical considerations should be factors in this prioritization. The product of this review would be a shorter list of improvements that would be implemented.

7. Estimate Expected Reliability Improvement

The reliability improvement estimate is based on the information available at the time combined with good engineering judgment. It is recognized that a reasonable period will be necessary to implement improvements. It is also recognized that conditions affecting EDG reliability have uncertainty, therefore the estimate must not be used to predict reliability. Once specific actions have been identified, the estimated reliability improvement of the EDGs should be assessed. This evaluation would focus on the numbers of previous failures which the improvement program would have eliminated (had it been previously implemented). If this evaluation indicated that the actions being taken would have precluded enough failures to avoid the original exceedence, no additional actions would be required. If insufficient past failures have been addressed by the actions (to have avoided target exceedence), additional actions could be proposed or a more detailed alternate EDG reliability improvement estimate could be made. This alternate determination would take into account the probability that each improvement would eliminate specific failures that had reduced EDG reliability below target values.

Methods for Estimating Expected Reliability

The purpose of this section is to describe an acceptable method for quantitatively extrapolating the effectiveness of EDG reliability program changes in reducing system unreliability (due to the elimination or a reduction in the frequency of specific failure modes). This quantification is influenced by several factors.

a. the number and frequency of failures which can be effectively addressed by changes in operating, maintenance or testing practices or by a design change;

b. the number and frequency of failures which can not be effectively addressed by changes in operating, maintenance or testing practices or by a design change; and

c. the impact of reliability program changes on the frequency of failures.

DRAFT

The methods described in this section are based on reliability centered maintenance (RCM) principles. However, a RCM program does not have to be in place for the expected reliability to be estimated. Two possible methods are presented (1) a method based solely on observed failures and implemented changes to the maintenance program, and (2) a method based on a full RCM program. These two methods differ only in the calculational technique and scope of failures considered. A description of the methods follows:

Step 1: Failure Impact Assessment
For each failure, assess the impact of improvements in the EDG reliability program on the identified failure mode. Changes in the EDG reliability program can influence failure modes by decreasing their frequency of occurrence or eliminating the failure mode altogether.

An example of decreasing the frequency of failure would be to increase the procedural emphasis placed on restoring the equipment configuration at the end of a CM or PM task. This change could result in a lower frequency of human error of leaving systems in non-standard configurations. The impact on frequency would be assessed by evaluating the expected impact of the changes.

An example of a change that would eliminate a failure mode would be a procedure change to avoid an activity that is known to cause a failure.

For each of the failure modes a confidence factor, Ri, can then be determined from Table D.2-3 by estimating the confidence in the change influencing the failure mode.

Table D.2-3

INDIVIDUAL CONFIDENCE FACTOR FOR FAILURE MODES

Confidence In Influencing Failure Mode	Impact of Change on Reliability (Ri)
No Confidence	0
Low	0.25
Moderate	0.50
High	0.90

For failures for which no impact is expected from reliability program changes, a value of 0 is used for Ri. For failures for which a direct impact with little or no potential for the failure mode to recur, a value of 0.90 is used.

Step 2: Estimate Expected Reliability

Two possible calculational methods have been developed for the estimation of expected reliability. One is based on observed failures in the EDG system. The second method would be used in conjunction with an RCM evaluation. A brief description of each of these methods follows:

Observed Failure Method
This method calculates expected reliability using the individual confidence factors for each of the observed failure modes. The general form of the equation is as follows:

INSERT EQUATION

where RE is the expected reliability, D is the number of demands in the sample evaluated, N is the total number of failures observed, and Ri is the individual confidence in managing the failure.

For example, assume that during the last 100 demands that were put on the EDGs at a unit five failures were observed. The five failures were dispositioned as follows:

Failure	Disposition	Ri
1	Not addressed by reliability program changes	0
2	Minor procedural modification, moderate confidence in eliminating	0.50
3	New maintenance procedure, low confidence in any impact	0.25
4	New PM testing, high confidence in improvement	0.90
5	Not addressed by reliability program changes	0

For this case, the equation becomes:

$$RE = 1 - \left(\frac{1}{100}\right) [(1-0) + (1-.50) + (1-.25) + (1-.90) + 1-0)]$$

$$= 1 - (.01)(3.35)$$

$$= 1 - .0335$$

$$= 0.9665$$

For a plant with a target reliability of 0.95, that expected reliability would be acceptable. For a plant with a target reliability of 0.975, that expected reliability would be unacceptable and further enhancements in the reliability program would be necessary.

RCM-Based Method

The alternate method of calculating expected reliability utilizes the output of an RCM program. As part of the RCM evaluation, dominant failure modes are obtained, and weighted by their expected frequency of occurrence. It is possible to calculate the expected reliability much in the same manner as the observed failure method. The form of the equation is as follows:

$$R_E = 1 - \sum_{i=1}^{N} F_i (1 - R_i)$$

where N is the number of dominant failure modes, Fi is the expected frequency of occurrence of the ith mode before RCM program implementation and Ri is the individual confidence factor from Table D.2-3.

(8) Implement Appropriate Improvements

This action is similar to that provided in Section D.2.4.1, except that the scope of improvements to consider is much larger and may include programmatic changes as a result of the evaluation against the critical review elements performed per action (5). The changes should be prioritized based on their contribution to overall unit EDG reliability in conjunction with the estimates calculated in action (7) above. Timely and proper implementation of changes that improve reliability will reduce the likelihood of subsequent failures and exceedence of another trigger value.

(9) Verification of Effectiveness of Improvements

A description of this action is provided in Section D.2.4.1.

D.2.4.3 Action for Plants That Exceed the 50 and 100 Demand Triggers

Nuclear units whose EDGs exceed both the 50 demand and the 100 demand failure triggers would take additional actions beyond those required of plants exceeding a single trigger value. The same basic actions as for nuclear units with a new failure with no trigger value exceedence and for nuclear units exceeding single trigger value should be performed. However, the scope of failures to be evaluated would be increased beyond those that actually had occurred by also including potential dominant failure modes. The actions should be:

(1) determine the cause of each new failure

(2) review the recent operating history relative to 3 classes of failures

(3) address all past failures

(4) develop a corrective maintenance tracking history

(5A) assess actual failure history and identify and assess potential dominant failure modes against critical review elements

(6) identify program changes

(7) estimate expected reliability improvements

(8) implement appropriate improvements

(9) verify the effectiveness of the improvements

All the actions noted above would apply to both actual observed failures and potential dominant failures. Action (5) is expanded to include assessment of the potential dominant failure modes against the critical review elements. A more detailed description of this action is provided below.

(5A) Assess Actual Failure History and Identify and Assess Potential Dominant Failure Modes Against Critical Review Elements

In addition to the evaluation of actual observed failures in Section D.2.4.2 a systematic identification of potential dominant failure modes would be carried out to ensure completeness.

Potential dominant failure modes are defined to be those which can fail an important EDG function and which :

a. are expected to occur frequently, or,

b. are unlikely but can have such significant consequences that they should be prevented from occurring even once.

Such a determination involves engineering judgement. Such judgements are routinely made in reliability analyses.

The following guidance is provided to assist utility engineers in the identification of potential dominant failure modes. This is to assure that the analysis is adequate but not unnecessarily detailed. Potential dominant failure modes are those that are relatively likely to occur and result in an actual failure of the machine to fulfill a clearly stated intended function. Thus, those failures which would not preclude adequate performance can be omitted and are not considered potential dominant failure modes. Similarly, those failures that on the basis of their low likelihood would not contribute to unreliability are not potential dominant failure modes and may be omitted from consideration. This requires judgement from the utility reliability analysts. Involvement from original equipment manufacturers of EDGs can be of great use in making these types of judgements. Guidance to assist utility reliability analysts in making these judgements could include a threshold which is well below the expected reliability. For example, a threshold of 10 E-4 per demand would screen out those that contribute less than 1% of the failures of a 0.99 reliable diesel. All failure modes which actually occurred at the plant are potential dominant failure modes. A comprehensive evaluation of the potential dominant failure modes should include an assessment of the likelihood and consequence to determine overall importance. This can be done in a number of ways:

a. A failure modes and effects analysis (FMEA) in conjunction with a logic tree analysis.

b. A detailed fault tree or GO analysis.

c. Other systematic methodologies such as expert review sessions.

Key inputs to these analyses would include EDG related plant maintenance histories, test data, LERs, NPRDS data for similar EDGs, and other industry data on failure modes and frequencies. The product of these analyses in conjunction with the evaluation of actual failures would be a list of the EDG dominant failure modes.

Normally, many of the potential dominant failure modes already are addressed through existing plant programs or can be addressed through minor changes to existing programs. For those failure modes which are not addressed, a decision must be made whether to implement maintenance program changes, modify the design to preclude the failure, or accept the failure because no cost-effective change can be identified.

After the dominant failure modes and potential improvements are identified, the critical review elements would be assessed in terms of these failure modes to see if any programmatic weaknesses exist. The questions in Tables 1 thru 6 would be directed at both observed failures and potential failure modes, where applicable. The matrix used for documenting the results of this evaluation would be the same as for single exceedences as shown in Figure D.2-2, except that both potential dominant failure modes and observed failure modes are addressed.

When the complete list of potential improvements is identified from the dominant failure mode analysis and critical review element assessment, the list would be evaluated. The assistance of original equipment manufacturers of EDGs can be of great usefulness in this process. Those changes that would be most effective in ensuring EDG reliability should be prioritized. Following the selection of the improvements to be implemented, an estimate of expected reliability improvement could be made. The method would be similar to that described for single exceedences. The objective would be to identify and implement improvements that address actual failures, to give promise that a target exceedence would not recur. In the event this estimate of reliability does not demonstrate a value above the target reliability, a quantitative evaluation could be made that is based on both observed and potential failure modes. This would indicate projected failure mode frequencies after the modifications are in place.

D.2.4.3.1 Previously Used Methods to Address Potential EDG Failures

Several techniques exist to perform systematic assessment of potential dominant failure modes. The technique used should be consistent with the problem being analyzed. Three techniques are discussed. These techniques include failure modes and effect analysis (FMEA), Demming methods, and Kepner-Tregoe. These techniques, if correctly implemented, are acceptable for addressing potential EDG failures. Other acceptable techniques exist, but these three are discussed here because they have been successfully used at operating utilities.

1. Failure Modes and Effects Analysis (FMEA)

Commonly used in reliability and safety analysis, the FMEA identifies failure modes for components of concern and traces their effects on other components, subsystems and systems. Emphasis is placed on identifying the problems that result from hardware failure.

Several steps are useful in preparing an FMEA. The systems to be analyzed should have its mission and operation defined with all interfaces clearly identified. Failure categories and environmental conditions are specified. The extent to which each of these steps proceeds is a function of available data and goal of the analysis. While it may be possible to breakdown the system to subcomponents, this level of breakdown may not be meaningful if no data is available for subcomponents.

At one operating plant the FMEA analysis was combined with actual operating experience to obtain the list of potential EDG failure modes. An example of this combined list based on FMEA and operating experience is shown in Table D.2-4. This represents only one such effort and may not be applicable to other plants or EDGs made by other manufacturers.

DRAFT

Table D.2-4

INTEGRATED LIST OF CRITICAL COMPONENTS
BASED ON FMEA AND EDG OPERATIONS DATA

1. Field flashing circuit
2. Generator excitation circuit
3. Voltage regulator (auto/manual)
4. Diesel generator "Start/Run" control circuit
5. Circuit breaker 152-108 closing coil
6. Generator lockout relay (186-1D1, 186-1D2)
7. Generator stator winding
8. Service water/jacket water heat exchanger
9. Service water motor-operated valve
10. Main lube oil pump strainer
11. Lube oil scavenging pump strainer
12. Air compressor unloader
13. Jacket water thermostatic control valve
14. Engine main bearings
15. Camshaft/timing gear
16. Generator bearing/coupling
17. Generator slip-rings and brushes
18. Crankshaft-to-piston connecting rod
19. Lube oil scavenging pump
20. Main lube oil pump
21. Engine jacket water pump
22. Crankshaft
23. Fuel oil day tank outlet valve
24. Lube oil cooler
25. Turbocharger aftercooler
26. Engine crankcase pressure instrument
27. Expansion tank
28. Annunciator
29. Engine speed control switch
30. Fuel oil transfer pump breaker
31. Voltage regulator selector switch

2. Quality Improvement Programs (Demming Methods)

Demming or other quality improvement programs contain methods to determine the dominant causes of failures. Three important portions of the quality improvement programs that are useful are potential dominant cause analysis, countermeasures and control charts. The analysis consists of constructing "fishbone" diagrams which start from the identified problem EDG failures and develop all possible causes. Countermeasures are developed for each cause and ranked for effectiveness. Control charts are used to measure the effectiveness of any actions taken. Demming methods are commonly used in a variety of industries and have been used successfully in the nuclear industry.

DRAFT

3. Kepner Tregoe Techniques

Kepner Tregoe is a structured decision analysis technique which consists of problem analysis, decision analysis, potential problem analysis, and direction and control.

Problem analysis defines the standard of performance, stating the problem as a deviation from the expected standard of performance by providing the what, when, where and extent of what the problem is and what the problem is not, and defining the actual deduced or most likely cause of the deviation.

Decision analysis consists of establishing objectives in terms of musts and wants, generating alternative solutions, comparing the alternative solutions against the objectives, and examining the best alternative for adverse consequences.

Potential problem analysis identifies potential deviations from the standard, and establishes the probability of occurrence, seriousness, and invisibility for each potential deviation.

Direction and control measures progress and determines action levels for actual and potential problems.

Kepner Tregoe techniques have been in use for over twenty years. Several utilities have used these techniques for both EDG and other equipment failures.

D.2.4.4 Post Exceedence Actions

Nuclear units which exceed one or more failure trigger values would continue to monitor the actual performance versus the trigger values. The plant would not revert to a no exceedence status until an exceedence no longer exists in the applicable number of demands, or two years from the last failure while in an exceedence, whichever occurs first. However, before a plant could revert to a no exceedence status, all planned improvement actions must be completed within the two year period.

Should a plant continue in an exceedence because of new failures, these failures would have to be evaluated against the improvement actions previously identified for implementation. The purpose of this evaluation would be to assess whether the failure should have been addressed by the identified improvements and if any of the conclusions of the previous evaluations should be modified based on the occurrence of the new failures.

For nuclear units which have exceeded both the 50 and 100 demand failure trigger values, it may be necessary to demonstrate that EDG performance has been restored to an acceptable level. Following corrective actions to address the failure that resulted in an exceedence of these trigger values, the data for each EDG included in the unit reliability calculation should be evaluated over the last 20 demands. If none of the EDGs included in the unit reliability calculation experienced 3 or more failures in the last 20 demands, then demonstration of acceptable EDG performance is not required. If any single EDG included in the unit reliability calculation experienced 3 or more failures in the last 20 demands, the following demonstration of acceptable EDG performance is required. For the EDG identified, the next five demands should be closely monitored. If no failures occur in these five demands, then demonstration of acceptable EDG performance is complete. If an additional failure does occur, then that EDG must undergo seven consecutive failure-free start and load-run tests (at a frequency no less than 24 hours and no more than seven days between each demand).

This process of evaluating recent demands and taking appropriate action on the individual EDG experiencing recurring failures is a key element in providing reasonable assurance that EDG performance is restored to an acceptable level.

D.2.5 Reporting Requirements

All plants when reporting all EDG failures in accordance with the provisions of 10CFR50.72, 10CFR50.73, 10CFR21, plant Technical Specifications, or other NRC reporting regulations should provide the following information:

(1) A description of the failure cause identified.

(2) The results of the important failures review.

(3) The nuclear unit EDG failure performance as compared to the appropriate 20 demand, 50 demand and 100 demand failure triggers.

For plants exceeding one or multiple triggers the following information should be retained by the licensee:

(1) A description of EDG reliability program improvements in response to trigger exceedence.

(2) The results of the critical review element assessment.

(3) The schedule for implementing improvements.

(4) An estimate of the effectiveness of actions being taken in terms of the numbers and types of failures addressed (or the results of an alternate reliability evaluation).

(5) Other corrective action taken in response to an EDG failure.

D.3 CURRENT AND RECOMMENDED INDUSTRY PRACTICES ON EDG RELIABILITY

A survey of current utility practices revealed that many important elements of EDG reliability are being conducted by utilities. In order to assist utilities in reviewing their current practice the results of this survey along with information obtained from published reports are synthesized in this section. This section should be considered a sourcebook for information on EDG reliability. To present this information, the section has been structured to follow six critical review elements of EDG reliability. These elements are:

(1) Surveillance Needs

(2) Performance Monitoring

(3) Maintenance Program

(4) Failure Analysis and Root Cause Investigation

(5) EDG Problem Closeout

(6) EDG Reliability Data Systems

D.3.1 Surveillance Needs

One of the basic building blocks of the EDG reliability program is the surveillance testing. EDG surveillance testing is performed at least once a month or more frequently consistent with existing plant-specific technical specifications requirements. The data obtained from this testing is used to determine EDG reliability and to spot potential problems.

An EDG surveillance program should consider the following factors:

(1) The effect that EDG support/auxiliary systems have on overall EDG reliability
(2) failures caused by surveillances
(3) Frequency and nature of surveillance testing affects reliability and unavailability
(4) The types of failures that can be detected by a surveillance program
(5) Detection of failures by parameter monitoring versus testing
(6) If testing to detect failures, the ability of the test to simulate actual operating conditions.

Manufacturer's information as well as industry experience play an important role in identifying the surveillance needs. Such information should be reviewed and dispositioned relative to its applicability to each EDG.

D.3.1.1 Reliability of Subcomponents and Support Systems

The first consideration should be to ensure that the surveillance efforts cover appropriate EDG subcomponents and auxiliaries as well as portions of systems which support the EDG. In many instances the portion of the support systems used by the EDG can be more important to EDG reliability than to the support system reliability. It should be noted that these support systems are vendor and plant specific. A list of typical EDG support systems is provided below:

Speed Control

Environmental Control

Start Control

Starting Air

Instrument Air

Service Water Engine Cooling

DC Power Source

Lube-oil System

Fuel-oil System

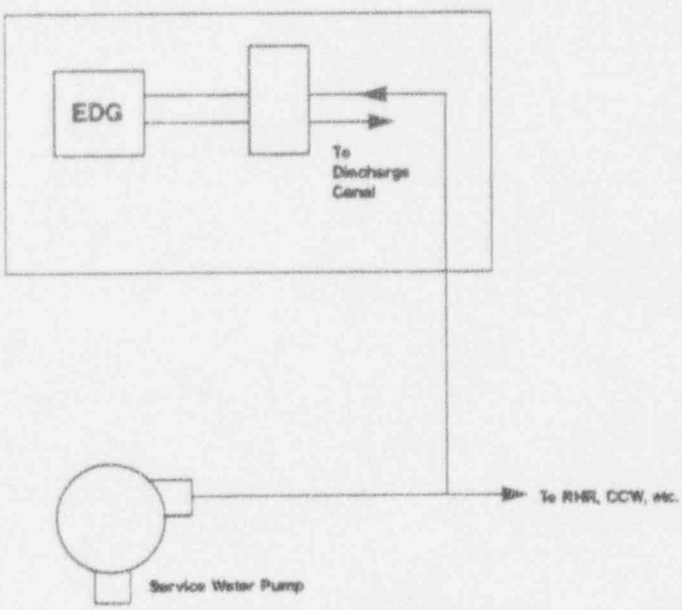
Engine combustion air supply/exhaust

Generator electro-mechanical including voltage regulator

Electrical and I & C (including field flash)

Example: The service water system provides a medium for the transfer of heat to the ultimate heat sink for a variety of plant systems. The EDG is only one of many systems for which service water may be required and is not a particularly large load. It is not necessary to consider the entire service water system as part of EDG reliability surveillance efforts. However, consideration should be given to the service water system components that are specifically used to ensure proper operation of the EDG. This is illustrated in Figure D.3-1 where the components within the dotted lines are designated as part of the EDG reliability surveillance efforts.

Figure D.3-1



Including portions of supporting systems into the EDG reliability efforts does not in itself make these portions of the EDG systems. However acknowledgement of this interdependency highlights that surveillance needs in these portions may be greater from an EDG reliability basis than from the basic supporting system requirements.

In factoring portions of EDG support systems into the EDG reliability surveillance efforts, it is desirable but not necessary to include EDG support system surveillance requirements in the EDG surveillance procedures. In particular, those support systems parameters that are critical to proper EDG operation should be monitored during the EDG surveillance testing.

D.3.1.2 Failures Caused By Surveillances

The main thrust of the failure review is to monitor the failures, observe anomolies discovered during surveillances, and, in doing so, potentially eliminate the cause of repeated failures. One source of failures is the surveillance procedure itself. Due to recommendations from various organizations, such as vendors, surveillance procedures are constantly being modified. While these changes may reduce potential problems in one area, they may also cause increased problems in other areas. These problems may not become apparent until the actual surveillance test is performed a number of times. Therefore, failures observed during the performance of a surveillance test should trigger a review of the surveillance procedure in order to determine if that particular failure can be eliminated.

<u>Example</u>: A particular vendor recommends operating the EDG at low rpms before loading in order to pre-warm and pre-lube the EDG during the monthly surveillance testing. However, after several months of testing, it is noticed that the cylinder temperatures are abnormally high during this pre-warming period. Further investigation finds that operating the diesel at low rpms fouls the injectors, causing the higher cylinder temperatures. The surveillance procedure is then changed to run at higher rpms during the pre-warming period which eliminates the potential for injector fouling.

Because of occurrences like this, each failure experienced during a surveillance test should be reviewed to determine the underlying or root cause. Besides taking actions to eliminate the cause of the failure, it should be determined if the surveillance procedures should be reviewed.

The following is a useful checklist for determining the necessity of reviewing surveillance procedures:

1. Does the failure relate to equipment previously excluded from consideration as part of the EDG reliability efforts?
2. Could the failure be prevented by a change in surveillance practices (i.e. scheduling or content)?
3. If the failure is one which proceeds from a degraded state to a failed state, could it be identified by a surveillance before the failure occurs?

4. If the failure has common cause failure potential, could the common cause potential be identified through surveillance?
5. Does the severity of this failure warrant a change in surveillance practices?
6. If the failure is related to aging, could surveillance have detected the aged condition?
7. Was the failure caused by inappropriate changes to procedures since the last surveillance?

D.3.1.3 Frequency and Scope of Surveillance Testing

The frequency of surveillance testing is based on recommendations from vendors, regulatory guides, industry good practice documents, judgement gained through experiences, and other factors. In addition to these, a utility should incorporate the experience gained through past history from their own EDGs as well as from those plants possessing similar EDGs. It should be noted that the testing frequency determined based on the above criteria could be the basis for establishing the Technical Specification requirements. The theoretical framework for establishing a testing frequency recognizes the impact of reduced availability and increasing failures with shortened testing frequencies. Typically there exists a desirable optimum range of values for test intervals.

In general, surveillances can be conducted on a shift, daily, weekly, monthly, quarterly, yearly or refueling outage basis. Typically surveillances for EDGs are performed on a daily, weekly, monthly, 6-month, and refueling outage basis.

Surveillance includes not only the overall EDG run/fail to run surveillances but also those of subcomponents and support systems. Certain important parameters are observed as part of the surveillance test in order to ascertain the overall status of machine.

Tables D.3-1, D.3-2 and D.3-3 provide typical examples of types and frequencies of periodic surveillances for EDGs in both standby and operating conditions. It should be noted that some of the parameters listed in these tables are not applicable to all EDGs. Vendor recommendations and industry experience should be integrated, as appropriate, into plant-specific surveillance requirements. When performing these surveillances it is important to capture the actual values of the parameters. This type of data is extremely useful in the subsequent determination of root causes of failures and for performance monitoring.

For these surveillances, the purpose of data collection and the meaning of the data collected should be clearly understood by the plant personnel involved.

Table D.3-1

SHIFT/DAILY/WEEKLY STANDBY EDG SURVEILLANCE

<u>Lube Oil System</u>
Lube Oil inlet temperature
Lube Oil outlet temperature
Lube Oil sump level

Lube Oil strainer/
filter differential pressure
Visual inspection for leaks

<u>Fuel Oil System</u>
Day tank level
Storage tank level
Bleed fuel oil filters
Visual inspection for leaks

<u>Jacket Water System</u>
Jacket water inlet temperature
Jacket water outlet temperature
Expansion tank level
Visual inspection

<u>Starting Air Systems</u>
Air receiver pressure
Blowdown air receiver
Compressor oil level
Compressor water traps

<u>Governor System</u>
Governor oil level
Verify load limit settings
Governor setting in Auto/Manual

<u>Diesel/Generator</u>
Oil level of pedestal bearing
Turbo oil level
Intercooler leak inspection
Turbocharger tube oil level
Drain moisture from exhaust
silencers
Verify alarms clear
Diesel starting selector
switches in remote
DG breaker remote local select
switch in remote
Verify auto-manual regulators
set in normal range
Check water and fuel hoses
Check starter motors
Check exhaust system

<u>Electrical</u>*
Auto/manual switch in Auto
Appropriate breakers racked in
Power to breaker is verified
Aligned to correct power source
Fault indicator

* Weekly surveillances

Table D.3-2

MONTHLY DYNAMIC EDG SURVEILLANCE

Diesel/Generator
Visually inspect fuel system for leaks
Visually inspect for exhaust leaks
Drain water from crankcase vent piping
Verify generator synchronization
Engine coolant level
Manifold pressure
Cranckcase pressure
Air inlet temperature
Turbo temperature
Intercooler outlet temperature
Ventilation fan operability
Cylinder exhaust temperatures
Cooling water supply temperature
Stator temperature
Gen frequency
Gen voltage
Gen Amps
Gen KW

Jacket Water System
Inspect for leaks
Check water treatment
HX outlet temperature
Engine outlet temperature
System pressure
Turbo outlet temperature

Governor System
Inspect linkage for loose parts
Verify all control settings
Check governor actuator oil level
Check automatic shutdown
Filter DP
Inspect for leaks
Day tank level
Storage tank level
Verify transfer pump operability
Fuel oil pressure (inlet/outlet)

Lube Oil System
Check lube oil for dilution
Lube oil chemical analysis
Inspect for leaks
LO filter DP
LO pressure
LO level
Turbo LO pressure
LO inlet temperature
LO outlet temperature

In addition to the above surveillances there are other less frequent inspections that may be considered. Examples of these include the following:

Table D.3-3

LESS FREQUENT EDG SURVEILLANCES

Periodic Surveillance:

Lubricating oil Chemical Analysis	Once every quarter
Fuel Oil Chemical Analysis	Once every quarter

Non-Periodic Surveillances:

Chemical analysis of new fuel oil	Upon delivery and prior to use
Chemical analysis of new lubricating Oil	Upon delivery and prior to use

DRAFT

D.3.2 Performance Monitoring

Performance monitoring is usually applied to equipment that is run on a continual or a near continual basis. The purpose is to monitor certain parameters on an ongoing basis in order to obtain information about the state of physical conditions that may potentially impact the operability of the particular piece of equipment, and which could be used for trending purposes. These trends may often signal a degradation in a particular condition. Evaluation of these conditions may enable a utility to predict the onset of failure and allow corrective actions to be taken before failure occurs.

Equipment that is normally in a standby condition, such as an EDG, can only be monitored on a limited basis. Monitoring of critical operational parameters is usually performed during monthly operational testing. This testing is also performed for a limited time which restricts the amount of data that can be collected. However, some benefit should be realized by recording critical operational parameters and comparing the results to that of previous testing.

In order for this monitoring to be effective, it should be applied to conditions that possess the following four traits:

1. The characteristic/parameter should be a measurable condition that is known to be related to an important failure mode.

2. The characteristic/parameter should be able to be measured conveniently and practically without incurring an inappropriately large EDG outage time.

3. The characteristic/parameter should be monitored in a manner such that it produces an accurate reading with a minimum number of false indications.

4. Parameters recorded are measured under the same conditions to the extent possible (i.e. load).

The actual values of the conditions should be recorded rather than simply verifying that they are within a specific range. A comparison between the values obtained from successive tests should be made in order to ascertain the possibility of a degrading condition.

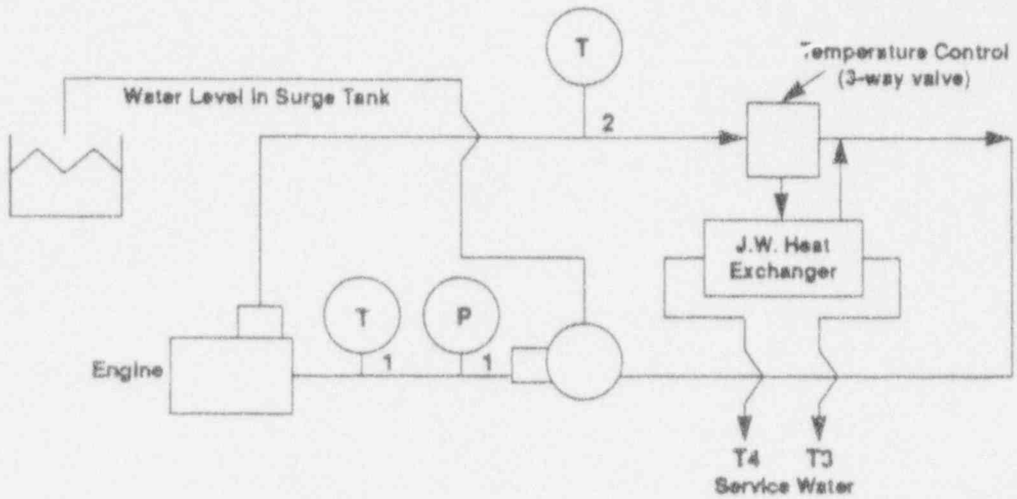
<u>Example</u>: Cooling Water
Intercoolers, heat exchangers, and other engine components are subject to build up of deposits and rust over a period of time. These deposits are usually reduced by various water chemistry practices such as the addition of corrosion inhibitors. However, the inhibitors used to control these buildups degrade over time causing excessive buildup and higher than desirable operating temperatures. Therefore, in addition to monitoring water chemistry, heat exchanger inlet and outlet temperatures should be recorded and compared to previous recordings. Either short term increases or long term general rise may be indicative of fouling.

DRAFT

Figure D.3-2 presents a typical diagram of a jacket water cooling system. Below this diagram are a set of curves depicting jacket water temperature over multiple surveillance tests.

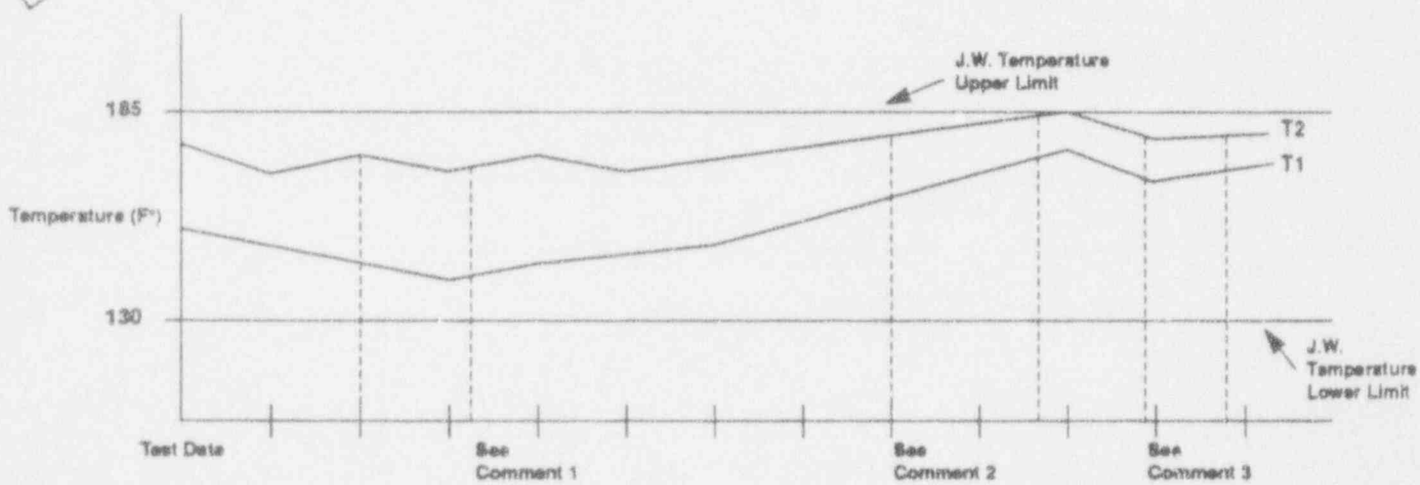
Figure D.3-2

Typical Jacket Water System



DRAFT

Trend Plotting – J.W. Temperature to Engine (T1) From Engine (T2)



In comment period 1 the relatively high delta T across the engine could be attributable to air in the system, combustion gas to jacket water leak, or a restriction in the jacket water system. In comment period 2 where the delta T appears normal but the trend is increasing temperatures, the upward trend might be attributable to heat exchanger fouling, a faulty three way temperature valve, service water system restricted, or service water inlet temperature is too high. Comment period 3 represents normal operating conditions.

In each of these cases, if observed trends are examined and their cause(s) sought, in many instances failures can be eliminated by taking appropriate actions.

Example: Lubricating Oil
Information gained by the monitoring of lubricating oil temperature during operation can be used to predict a variety of potential problems. Excessive temperatures can be caused by the deterioration of the lubricating oil medium, potential inefficiencies of the lubricating oil cooler, and dilution of the lubricating oil due to water or fuel oil. Ferritic and spectral analysis is relatively inexpensive and readily available. Monthly/Quarterly analysis of lubrication oil could be used as a forerunner to potential failures.

Example: Fuel Oil System
Physical separation, thickening and chemical changes can result from storage of distillate fuel oil. In addition, the accumulation of water and microbiological growth can form during long periods of storage. These factors can lead to fuel filter clogging as well as deterioration of fuel system components. Increasing differential pressure across the fuel oil filter can signal such conditions. Monitoring of fuel oil filter differential pressure can potentially avoid significant damage to the fuel system.

Dynamic, vibratory, and thermal stresses induce normal wear on an EDG from testing and valid demand loading. Degradation to engine parts from these stresses generally occur over time and in many instances may be detected before catastrophic failure occurs.

The symptoms of these stresses can appear in a variety of ways. For example, frictional wear to piston rings may result from loss of vacuum or excessive crankcase pressure. Inefficient fuel injectors caused by nozzle wear can be detected through high abnormal exhaust temperatures. In addition, degraded EDG operation can result from an inefficient electrical generator. These and many other conditions can be detected through monitoring of various parameters during operation. Parameters to be monitored are generally suggested by the manufacturer in the form of specific operating limits for temperature and pressure. By trending these parameters and correlating sudden changes with past operating experience and failure history, the approach of failures can be predicted and actions can be taken prior to the failure to correct the underlying cause.

A representative list of these example parameters is provided in Table D.3-4. Not all are applicable to all EDG manufacturers. However, consideration should be given as to the applicability of each parameter to each specific EDG.

Table D.3-4

EDG PERFORMANCE MONITORING PARAMETERS

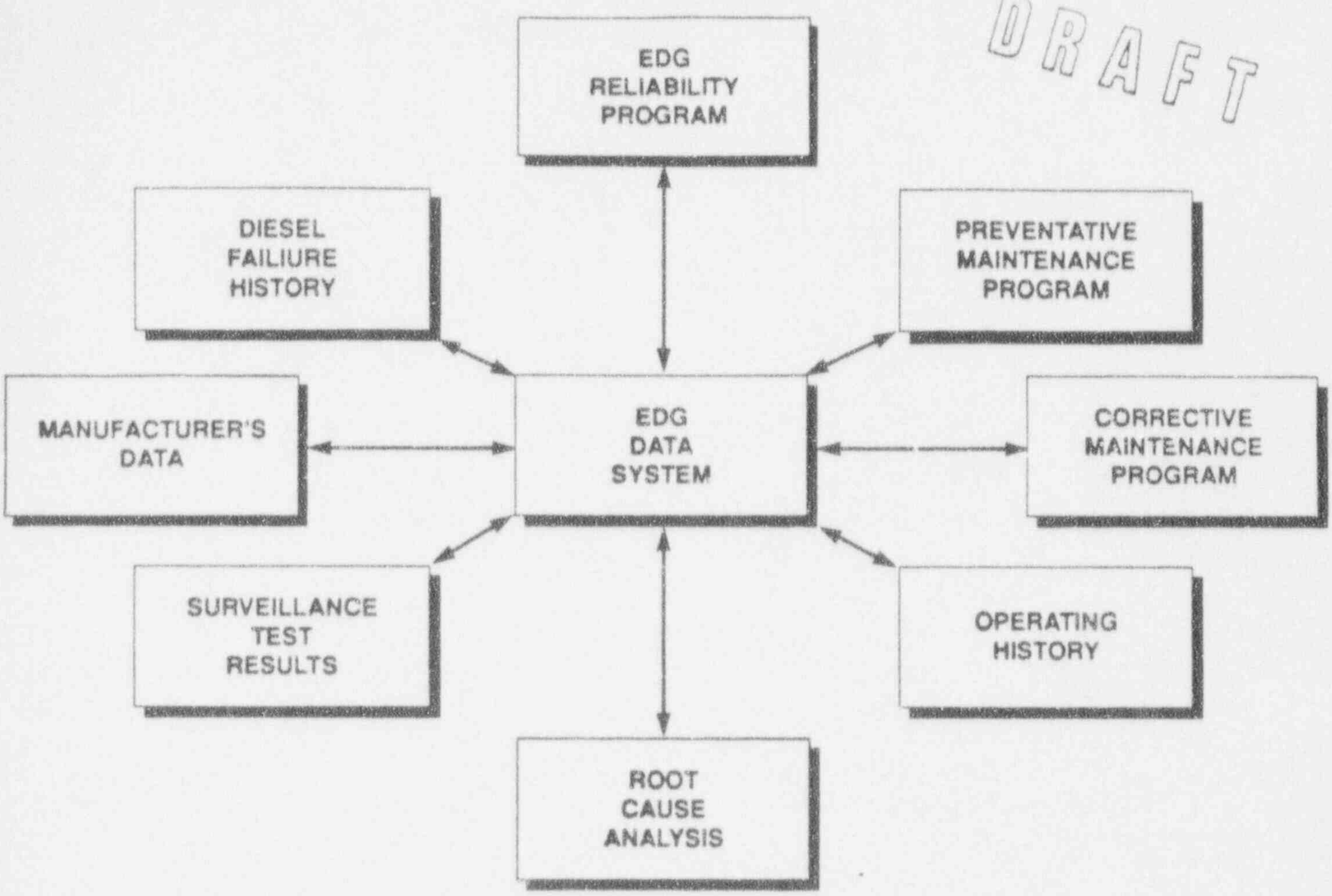
DIESEL	
	Cylinder exhaust temperatures
	Crankcase vacuum
	Jacket water inlet temperature
	Jacket water outlet temperature
	Lube oil inlet temperature
	Lube oil outlet temperature
	Lube oil pressure
	Fuel oil inlet pressure
	Fuel oil outlet pressure
	Air inlet temperature
	Turbocharger operating temperature
GENERATOR	
	Frequency
	Voltage
	Amps
	Kilowatts
	Temperature

D.3.3 Data Systems

D.3.3.1 Data Input

Current utility practices in surveillance, maintenance, and other areas capture considerable data that can be used to assure that EDG reliability targets are met. Areas that could capture data on EDGs are illustrated in Figure D.3-3. This data should be located in a retrievable manner such that an exchange of reliability information may occur between the various plant activities and programs where data pertaining to EDG reliability is captured.

FIGURE D.3-3



A systematic method of capturing data and retrieving data is effective in having data important to EDG reliability available to appropriate plant personnel. The data system need not be a special purpose system dedicated to EDG reliability and need not be centrally located. The system should, however, capture the important features of data available and be readily retrievable.

D.3.3.2 Data Capture

The types of data that should be considered in the formation of a data system include but are not limited to the following:

1. Surveillance Test Results
2. EDG Failure History
3. Root Cause Analysis
4. Manufacturer's Data
5. Input from Preventative Maintenance Program
6. Input from Corrective Maintenance Program
7. Industry Operating Experience

Each of these elements is discussed in greater detail in the following sections.

DRAFT

D.3.3.2.1 Surveillance Test Results

Surveillance test results include both physical and statistical parameter information. It is important to capture the values of operating parameters (e.g., exhaust temperatures), general observations (e.g. leaking oil near EDG), and retain failed or replaced parts for further examination (e.g., retain plugged oil filter for spectral analysis at a later time). Statistical parameters may include failures, successes, and number of demands.

D.3.3.2.2 EDG Failure History

Each observed failure of an EDG should be captured in the data system. The information listed below is representative of information that should be captured when a failure has occurred.

Originator -- the person discovering the failure

Department / Organization -- the plant department or organization of the originator

Unique Identifier -- a unique identifier that will allow tracking of the document used to identify the failure (work order number, LER, etc.)

Component -- the name and description of the component that failed

Location -- the location of the failed component

Subsystem -- the subsystem that the failed component belonged to

Date -- the date the failure occurred

Time -- the time the failure occurred

Failure Severity -- catastrophic, degraded, etc.

Repair Date -- date of repair completion

Repair Time -- time of repair completion

Failure Description -- a detailed description of the failure

Detailed cause of failure -- detailed description of the cause of the failure

Corrective Action -- detailed description of the actions taken to correct the failure including maintenance actions, changes to procedures, technical specifications, etc.

Method of detection -- description of the approaches used for failure detection

Root cause of failure -- description of the root cause

DRAFT

Contributing causes of failure -- description of causes contributing to failures

D.3.3.2.3 Root Cause Analysis

Information from the EDG root cause analyses should be captured and maintained to ensure that the root causes are identified accurately and to ensure that problems are not recurring .

D.3.3.2.4 Manufacturer's Data

Diesel generator manufacturers and owners groups may be a valuable source of information for obtaining additional data on specific diesel performance and operating histories.

D.3.3.2.5 Input fron Preventative and Corrective Maintenence Programs

A history of preventative maintenance should be captured by the EDG data system. The information to be recorded should include but not be limited to the following:

Originator - the name of the person responsible for performing the maintenance

Date -- the date the maintenance was performed

Maintenance Activity -- detailed description of the maintenance activity

Findings -- description of any abnormalities found during the performance of maintenance such as clogged filters, parts out of specification, etc.

Followup Actions -- description of any required actions such as the performance of a root cause analysis

D.3.3.2.6 Industry Operating Experience

Information on operating experience at facilities is available through a variety of sources. Below is a list of frequently used sources of industry information which include EDGs which captures EDG operating experiences:

INPO SOERs, OERs, and O&MRs
NPRDS Program
NRC LERs, Information Notices, Bulletins, and Generic Letters
Manufacturer's Information Letters

Current utility practices capture data from the above sources as part of ongoing vendor data review, INPO, or other similar programs.

D.3.3.3 Data Storage and Retrievability

An effective data system not only captures the data but also stores it in a retrievable manner. The information does not have to be in a centralized file but should be in a location(s) readily accessible to those using the information. It is important that appropriate personnel are knowledgeable about the location of the data and can, with normal efforts, retrieve the data for further study and analysis.

For example, proper coding of data in the existing computerized document retention system with easy terminal access can be an effective method for data storage and retrieval. Equally acceptable is the clear identification of storage locations of each type of data. Surveillance records could be stored in the maintenance area in clearly marked files. Preventative maintenance data could be stored in an area where the overall plant preventative maintenance program is conducted.

Data storage and retrieval should be consistent with the frequency of use of the data.

D.3.4 Maintenance Program

An important contributor to EDG reliability is the manner in which both preventative and corrective maintenance are performed. Generally speaking, an EDG maintenance program should include the following basic principals. Typically these are found in most overall plant maintenance programs.

1. Maintenance actions should be prioritized based on such factors as repair time, severity, likelihood of reoccurrence, etc.

2. The reliability characteristics of the EDG subsystems and components should be considered when planning EDG preventative maintenance

3. Maintenance programs should interface with the overall EDG reliability program.

The maintenance program has both a preventative and a corrective element. While the preventative program should be tailored to each specific EDG type, the following are typical examples of preventative maintenance activities conducted during a refueling outage.

Engine Lube-oil System
- clean and inspect lube-oil strainer
- replace lube oil filters
- replace turbocharger filter element
- inspect lube oil cooler

Engine Cooling System
- inspect cooling water pump
- drain and replace coolant
- inspect expansion tank

Fuel-oil System
- replace fuel oil filters
- clean and inspect fuel oil strainers
- Test fuel condition

Starting Air System
- clean and inspect air strainer
- replace compressor oil
- inspect compressor drive belts

Engine Maintenance
- replace inlet air filter oil
- inspect and clean inlet air filter
- inspect air box drains
- inspect air box cooling system
- check cylinder head to piston clearances
- inspect cylinder liners
- inspect rod bearings
- inspect main bearings
- inspect piston rings

D.3.5 Failure Analysis and Root Cause Investigation

While most utilities perform a root cause analysis, either formally or informally, there does not appear to be a uniform industry definition of what a root cause analysis is. In general there is agreement that a root cause analysis is an investigation as to the underlying cause of a particular problem or failure. However, there is some disagreement as to the depth of the analysis that is required to identify the underlying cause. Industry efforts are being initiated to develop guidance in this area. Until such industry guidance is generally available, the following guidance may be useful to utilities.

Before defining a "root cause" there must be a standard definition of the term failure. For the purpose of discussion, the definition of a failure is:

> "The loss of ability of the component to perform its intended function."

Furthermore, a component is considered to have failed if it is operating outside of its given Technical Specification range of operation.

DRAFT

Considering the above definition of failure a root cause can now be defined as:

> "The most basic, fundamental cause(s), which if corrected, will prevent recurrence of an event or condition."

When performing a root cause analysis the method of categorizing failures can be important to the effectiveness of the effort. In general there are two categories of failures: one due to human performance and the second is due to equipment failures. Table D.3-5 provides a list of factors causing human performance failures. Table D.3-6 includes a similar list of factors for equipment performance.

Table D.3-5

EVENT CAUSAL FACTORS FOR HUMAN PERFORMANCE PROBLEMS

Verbal communication
Written communication
Interface design or equipment condition
Environmental conditions
Work schedule
Work practice
Work organization/planning
Supervisory method
Training/Qualification method
Training/Qualification content
Change in management
Resource management
Managerial method

Table D.3-6

EVENT CAUSAL FACTORS FOR EQUIPMENT PERFORMANCE PROBLEMS

Plant/system design and analysis
Equipment manufacture and installation
Maintenance/testing
External
Plant/system operation

Effective root cause analysis programs are anticipatory instead of reactive in nature and improve plant availability by preventing repetitive or similar equipment and human performance problems through the identification of specific cause(s) of failures. In general the need for performing a root cause analysis is determined subsequent to the identification of a problem. Problems are normally identified because of an undesirable event, data trend, and/or management request There are a number of key elements in performing a root cause analysis. These elements are described below.

1. Identification of failure

The previous paragraphs described different categories of failures that may lead into performance of a root cause analysis. The vast majority of these events are caused by equipment malfunctions or human errors. In addition other factors including data trend or management request may initiate a root cause analysis.

2. Data collection

It is important to initiate data collection as soon as a problem is identified. This action includes photographing the area, reviewing plant documents (i.e. vendor manuals, drawings, procedures, LERs, etc.), and other information available in the industry.

3. Data Review

The primary objective of this task is to determine the significance of events and determine if additional information is required.

4. Event Evaluation

There are a number of techniques available and used routinely in different industries to evaluate events, determine root cause, and identify possible solutions to prevent recurrence. The following is a list of five methods utilized for evaluation of different type of failures described in previous sections. There are advantages and disadvantages associated with each method depending on the type of failure and other factors including availability of resources, expertise, etc.

a. Cause and effect task analysis method where a block diagram is used to identify questions to ask based on available information. This method is good for evaluating equipment failures.

b. Fault Tree Analysis used for solving programmatic problems but may fail to identify specific causes.

c. Change and situation analysis method used for single situations and focuses on elements that have changed, contributing to the cause. This method is helpful in evaluating equipment failures.

d. Barrier analysis is a systematic process that can be used when the failure seems to be pragmatic such as procedural and administrative problems.

e. Human performance evaluation utilizes the human performance evaluation system and analysis of the decision process.

5. Root Cause Determination

Once the event analysis is completed the root cause may be determined. The depth of this analysis should be commensurate with the event significance and/or complexity. The techniques described in the previous section can be used to further evaluate the actual cause.

DRAFT

6. Validation of Root Cause
In order to validate the root cause the following three criteria should be met.

a. The problem would not have occurred had the root cause(s) not been present;

b. The problem will not recur due to the same causal factor(s) if root causes are corrected or eliminated; and

c. Correction or elimination of the root cause(s) will prevent occurrence of similar conditions that could occur due to the same causal factor(s).

7. Identify and Implement Corrective Actions
Subsequent to the root cause identification, appropriate corrective actions should be taken to prevent the failure from recurrence.

8. Effectiveness Review
Ensure the effectiveness of the analysis by tracking the root cause(s) through the use of a data base.

9. External Notification
Consideration should be given to the sharing of the root cause information with other utilities.

10. Investigation Reports
The root cause investigation should be presented in a report to management with sufficient detail to allow an understanding of the event.

The above discussion on the elements of root cause analysis presents a brief description of one approach that may be considered. There are other industry efforts that are currently under development and that provide more detailed information on this subject. The following section focuses on the root cause problem close out process.

D.3.6 Problem Closeout

Attention should be given to the procedures and controls used to ensure the resolution or "closeout" of a particular problem. The closeout of a failure or problem that is detected during maintenance or surveillance should be closed out by means of a formal procedure. Such a formal plant-specific procedure may offer a means to prevent a recurrence of the particular failure or problem.

Most plants have a formal program for those problems covered by that portion of the QA program designed to meet criterion XV and XVI of Appendix B to 10CFR50. These programs require development of Non Conformance Reports (NCR) which contain a formalized tracking of the resolution to the particular deficiency. These NCRs, however, may not always include management oversight

DRAFT

or non QA related items. Therefore, the following sections provide guidance for developing a system for assuring adequate management attention and controls for problem closeout.

Criteria for Closeout

The criteria for the closeout of a particular failure or problem should be based on the performance of root cause analysis that will prevent the recurrence of the problem. It should identify if a root cause analysis was performed or the reason for not performing such analysis as appropriate.

Closeout Review

For problems or failures requiring the issuance of an NCR, a formal review of the closeout should be performed. This review should include a justification of the procedures and actions taken to closeout the problem.

Closeout Monitoring

A means of tracking the progress and resolution of the problem should be available. The originator of the corrective action should have a means of verifying the resolution of the problem.

Data System Interface

The EDG data system should contain sufficient information to track the progress and resolution of all problems and to verify the closeout of such problems.

8-21-89

BACKFIT ANALYSIS*

GSI B-56, "DIESEL GENERATOR RELIABILITY"

Background:

Generic Safety Issue (GSI) B-56, "Diesel Generator Reliability" is an adjunct safety issue related to the station blackout rule (10 CFR Part 50, Section 50.63). Regulatory Guide (RG) 1.155, "Station Blackout" (which provides guidance for compliance with the rule) also identifies the need for ensuring reliable operation of onsite emergency ac power sources by means of a reliability program designed to maintain and monitor the reliability level of each power source over time for assurance that selected reliability levels (i.e. => .95) are being achieved. RG 1.155 also provides general guidance regarding reliability program activities (or elements).

The resolution of GSI B-56 will be accomplished through the issuance of Regulatory Guide 1.9, Revision 3, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Plants". RG 1.9, Rev. 3 integrates into a singular regulatory guide pertinent guidance previously addressed in RGs 1.108 and 1.9, Rev. 2, and Generic Letter 84-15. This guide has been revised in response to comments received and discussions with NUMARC's B-56 working group.

RG 1.9, Rev. 3 better defines testing requirements, eliminates cold fast starts and minimizes accelerated testing, incorporates proven industry EDG surveillance and maintenance practices and also utilizes definitions from INPO's U.S. Plant Performance Indicator Program (PPIP) to enhance reporting consistency.

RG 1.9, Rev. 3 identifies the principal elements of an EDG reliability program that provides guidance with respect to surveillance and performance monitoring, maintenance, failure analysis, monitoring of unit reliability levels and associated actions, and thereby extends the brief guidance provided in RG 1.155. NUMARC has revised NUMARC-8700,"Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors", Appendix D (which deals with EDG reliability program guidelines) to provide guidance similar or identical to the reliability section of RG 1.9, Rev. 3, but in more detail.

Therefore the resolution of GSI B-56 will not introduce any regulatory requirements beyond those currently required for compliance with the station blackout rule.

The regulatory analysis for USI A-44 is reported in NUREG-1109, June 1988. The staff finds the regulatory analysis developed for

* This backfit analysis will be published in the FRN to be issued for RG 1.9, Rev. 3.

8-21-89

BACKFIT ANALYSIS*

GSI B-56, "DIESEL GENERATOR RELIABILITY"

Background:

Generic Safety Issue (GSI) B-56, "Diesel Generator Reliability" is an adjunct safety issue related to the station blackout rule (10 CFR Part 50, Section 50.63). Regulatory Guide (RG) 1.155, "Station Blackout" (which provides guidance for compliance with the rule) also identifies the need for ensuring reliable operation of onsite emergency ac power sources by means of a reliability program designed to maintain and monitor the reliability level of each power source over time for assurance that selected reliability levels (i.e. => .95) are being achieved. RG 1.155 also provides general guidance regarding reliability program activities (or elements).

The resolution of GSI B-56 will be accomplished through the issuance of Regulatory Guide 1.9, Revision 3, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Plants". RG 1.9, Rev. 3 integrates into a singular regulatory guide pertinent guidance previously addressed in RGs 1.108 and 1.9, Rev. 2, and Generic Letter 84-15. This guide has been revised in response to comments received and discussions with NUMARC's B-56 working group.

RG 1.9, Rev. 3 better defines testing requirements, eliminates cold fast starts and minimizes accelerated testing, incorporates proven industry EDG surveillance and maintenance practices and also utilizes definitions from INPO's U.S. Plant Performance Indicator Program (PPIP) to enhance reporting consistency.

RG 1.9, Rev. 3 identifies the principal elements of an EDG reliability program that provides guidance with respect to surveillance and performance monitoring, maintenance, failure analysis, monitoring of unit reliability levels and associated actions, and thereby extends the brief guidance provided in RG 1.155. NUMARC has revised NUMARC-8700,"Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors", Appendix D (which deals with EDG reliability program guidelines) to provide guidance similar or identical to the reliability section of RG 1.9, Rev. 3, but in more detail.

Therefore the resolution of GSI B-56 will not introduce any regulatory requirements beyond those currently required for compliance with the station blackout rule.

The regulatory analysis for USI A-44 is reported in NUREG-1109, June 1988. The staff finds the regulatory analysis developed for

* This backfit analysis will be published in the FRN to be issued for RG 1.9, Rev. 3.

USI A-44 also applicable to the resolution of GSI B-56 and therefore a new regulatory analysis will not be developed for GSI B-56.

The information which follows is provided in answer to specific requirements of paragraph (c) of 10 CFR 50.109.

(1) Statement of specific objectives that the proposed backfit is to achieve.

(a) The primary objective of the B-56 resolution is to provide guidance for an EDG reliability program which is needed to achieve and maintain EDG reliability levels selected for compliance with 10 CFR 50.63.

(b) Incorporate guidance into a singular regulatory guide that has been addressed through two regulatory guides and a generic letter.

(2) General description of activity that would be required by the license or applicant in order to complete the backfit.

Although RG 1.9, Rev. 3 defines an EDG reliability program, the guidelines provided are similar to currently employed practices and major changes are not expected. Licensees currently have plant specific EDG maintenance and operational surveillance programs which have resulted in industry-wide EDG averaged reliabilities on the order of 98%. The resolution of B-56 provides guidelines for monitoring EDG performance and taking corrective actions if a deteriorating situation comes into existence.

Furthermore, the resolution of B-56 is consistent with NUMARC's expanded guidelines and INPO monitoring methods.

(3) Potential change in the risk to the public from accidental offsite release of radioactive material.

The risk estimates provided in NUREG-1109 are applicable. In the absence of an adequate EDG reliability program, assurance would be lacking that proper levels of EDG reliability were being maintained to minimize station blackout.

(4) Potential impact of radiological exposure of facility employees.

No radiological exposure is projected.

The implementation of an EDG reliability program is not expected to require personnel to be exposed to radiological effects.

(5) Installation and continuing costs associated with the backfit, the cost of facility downtime or the cost of construction delay.

No facility downtime or construction delays are envisioned due to the resolution of B-56. The continuing costs associated with maintaining a diesel reliability program should be small since most operating plants currently have some form of an EDG reliability and maintenance program. Cost estimates for improving EDG reliability were estimated at $150,000 to $400,000 per reactor as part of the USI A-44 regulatory analysis (NUREG-1109).

(6) The potential safety impact of changes in plant or operational complexity including the relationship to proposed and existing regulatory requirements.

None

(7) The estimated resource burden on the NRC associated with the proposed backfit and the availability of such resources.

The principal cost to the NRC would be associated with reviewing EDG reliability programs at the respective plants sites via the Temporary Instructions. It is estimated that such efforts would not exceed 0.5 per-months per site. At an estimated $12,000 per staff month and 50 sites, the total cost would be $300,000.

NUMARC's B-56 working group has developed guidelines for EDG reliability programs (NUMARC-8700, Appendix D) which will enhance conformity of reviews, which should minimize NRC review costs.

(8) The potential impact of differences in facility type, design or age on the relevance and practicality of the proposed backfit.

Minimal

(9) Whether the proposed backfit is interim or final and, if interim, the justification for imposing the proposed backfit on an interim basis.

The proposed action is final.

8-16-89
[7590-01]

DRAFT FEDERAL REGISTER NOTICE
(Ref. Resolution GSI B-56)

NUCLEAR REGULATORY COMMISSION
Regulatory Guide; Issuance, Availability

The Nuclear Regulatory Commission has issued a revision to a guide in its Regulatory Guide Series. This series has been developed to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the staff in its review of applications for permits and licenses.

Regulatory Guide 1.9, Revision 3, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants," integrates into a single regulatory guide pertinent guidance previously addressed in Regulatory Guide 1.108, "Periodic Testing of Diesel Generator Units used as Onsite Electric Power Systems at Nuclear Power Plants," Regulatory Guide 1.9, Revision 2, and Generic letter 84-15. Guidance provided in RG 1.9, Rev. 3 supersedes RG 1.108, and RG 1.108 is hereby withdrawn.

In addition, regulatory position 6 of RG 1.9, Rev. 3 provides guidance acceptable to the NRC staff for emergency diesel generator reliability programs designed to meet the requirements of 10 CFR 50.63, "Station Blackout," and thereby represents the resolution of Generic Safety Issue B-56, "Diesel Generator Reliability."

Comments and suggestions in connection with (1) items for inclusion in guides currently being developed or (2) improvements in all published guides are encouraged at any time. Written comments may be submitted to the Regulatory Publications Branch, Division of Freedom of Information and Publications Services, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Regulatory guides are available for inspection at the Commission's Public Document Room, 2120 L. Street NW., Washington, DC. Copies of issued guides may be purchased from the Government Printing Office at the current GPO price. Information on current GPO prices may be obtained by contacting the Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082, Washington, DC 20013-7082, telephone (202) 275-2060 or (202)275-2171. Issued guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161.

(5 U.S.C. 552(a))

Dated at __________ this _____ day of _________ 1989.
For the Nuclear Regulatory Commission

____
Eric S. Beckjord, Director
Office of Nuclear Regulatory Research