Use of Performance-Monitoring to Improve Reliability of Emergency Diesel Generators

by

Jeffrey D. Dulik

B.S., Mechanical Engineering
Massachusetts Institute of Technology, 1996

Submitted to the Department of Nuclear Engineering
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Nuclear Engineering

at the

Massachusetts Institute of Technology

February 1998

Signature of Author .....
Nuclear Engineering Department
December 15, 1997

Certified by .....
Michael W. Golay
Professor of Nuclear Engineering
Thesis Supervisor

Certified by .....
Neil E. Todreas
KEPCO Professor of Nuclear Engineering
and Professor of Mechanical Engineering
Thesis Reader

Accepted by .....
Lawrence Lidsky
Chairman, Department Committee on Graduate Students

Use of Performance-Monitoring to Improve Reliability of Emergency Diesel Generators

by

Jeffrey D. Dulik

Submitted to the Nuclear Engineering Department
on December 15, 1997, in partial fulfillment of the
requirements for the degree of
Master of Science

Abstract

Emergency diesel generators are one of the most important contributors to the core damage failure rate of nuclear power plants. Current required testing and maintenance procedures are excessively strict and expensive without any real justification. Probabilistic risk assessment is used to propose a monitoring system and Technical Specification changes to reduce EDG unavailability without jeopardizing safety, and to ease the excessive deterministic requirements.

The EDG fault tree is analyzed to identify the critical failure modes of the EDG, the failure of service water pumps, the failure of EDG building ventilation dampers, and the failure of the EDG "supercomponent," which includes the fuel oil, lubricating oil, cooling water, and starting air systems.

We use data from the nuclear industry and the U.S. Navy to identify the most significant EDG supercomponent failure modes, including system fluid leakages, instrumentation & controls failures, electrical power output failures, and the fuel system governors.

The monitoring system proposed includes instrumentation for twenty-one of the 121 basic events in the fault tree, for a total of 94.9% of EDG failure contributions. The failure modes identified with industry data are monitored, as are diesel engine mechanical failures currently assessed with teardown inspections. With a 50% reduction in these twenty-one basic event failure rates, the EDG system failure rate is reduced by 41.6%, from 0.097 per year to 0.059 per year.

With this reduced failure rate, we propose to extend the EDG surveillance interval from one month to twelve months, to lengthen the running tests from one hour to twenty-four hours, and to eliminate the tear-down inspections conducted during refueling outages.

To fully assess the benefits of these proposed changes, the monitoring system should be installed on an EDG on a trial basis. The work reported here demonstrates the feasible gains which can be realized, and proposes a method for evaluating the efficacy of the system as realized through experimentation.

Thesis Supervisor: Michael W. Golay
Title: Professor of Nuclear Engineering

Acknowledgements

I would like to thank the Institute for Nuclear Power Operations, for their generous support through the National Academy for Nuclear Training fellowship. This research was funded by the Idaho National Engineering and Environmental Laboratory through the project on Integrated Models, Data Bases, and Practices Needed for Performance-Based Safety Regulation.

I am grateful to Professor Michael Golay for his support, assistance, advice and patience with this project and my graduate education. I would also like to thank Professor Neil Todreas for his help and support in both this project and my graduate studies.

I'd like to thank my colleagues, Shantel Utton and Sarah Abdelkader, for all the help and support I've gotten from them throughout the course of this research project. I also wish them all the best as they complete their research.

I am also grateful to Changwoo Kang and Jong Beom Lee for all their help and valuable discussions on monitoring systems, and to Feng Li, for his assistance with the NPRDS database.

I would like to thank the personnel of Northeast Utilities Services Company, particularly Sunil Weerakoddy, Rick Labrecque, and Brian Shanahan at Millstone 3, and Stephen Stadnick at Millstone 2. Their experiences and insights were invaluable in understanding the functioning of the emergency diesel generators, as well as for crash courses in probabilistic risk assessment. The amount of support and assistance offered has not gone unnoticed.

This research also would not have been complete without the assistance and input from Gary Grant, of the Idaho National Engineering and Environmental Laboratory. His help with finding the answers I was looking for was invaluable, as was the study produced by him and his colleagues at INEEL.

Contents

List of Figures

List of Tables

List of Acronyms

ALWR	Advanced Light Water Reactor
BNL	Brookhaven National Laboratory
BWR	Boiling Water Reactor
CCF	Common-Cause Failure
CDA	Containment Depressurization Accident
CDF	Core Damage Failure
DG	Draft Guide
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EPRI	Electric Power Research Institute
ESF	Engineered Safety Feature
FSAR	Final Safety Analysis Report
ICAS	Integrated Condition Assessment System
IEEE	Institute of Electrical and Electronics Engineers
INEL	Idaho National Engineering Laboratory
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
MCS	Minimal Cutsets
MOOS	Maintenance Out Of Service
MP-3	Millstone 3 Nuclear Power Plant
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
NUSCO	Northeast Utilities Services Company
PBR	Performance-Based Safety Regulation
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RAT	Reserve Auxiliary Transformer
RG	Regulatory Guide
SBO	Station Blackout
SIS	Safety Injection Signal
SR	Surveillance Requirement

STS	Standard Technical Specifications
SwRI	Southwest Research Institute
TMI-2	Three Mile Island Unit 2
UAT	Unit Auxiliary Transformer

Chapter 1

Introduction

1.1 General

In 1975, *The Reactor Safety Study* [1] was issued by the Nuclear Regulatory Commission (NRC), the civilian nuclear power regulatory agency in the United States. The study, also known as WASH 1400 or the Rasmussen Report, used a method of assessing risk known today as Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA). WASH 1400 was the result of a study initiated in 1972 by Dr. James Schlesinger, the chairman of the predecessor of the NRC, the Atomic Energy Commission, to respond to the concerns of the U.S. Congress Joint Committee on Atomic Energy regarding the dangers that commercial nuclear power plants posed to the general public.

PRA differed from deterministic or prescriptive risk assessment, which had been used previously, both in the method of application and in how conservative the results were. Deterministic methods focus on designing plants to contain a worst possible accident sequence; these are extremely conservative. PRA considers which accidents occur most frequently and what the probability is of a certain outcome, such as a loss of coolant accident (LOCA) and the possible release of radiation; PRA gives much more realistic risk assessments, subject to the accuracy of the failure model used and the probabilities assigned to certain events.

Since the WASH 1400 report, all reactors in the U.S. have been required to submit

an Individual Plant Examination (IPE); one approach taken by some plants was the creation of a PSA to help reduce risk by determining where weaknesses lie. By focusing on these weaknesses, safety levels can be improved most effectively and most economically, instead of indiscriminately.

Using a PRA, one system of a nuclear power plant which figures prominently in many possible risk scenarios is the Emergency Diesel Generator (EDG), which supplies the power to safety-critical components, such as cooling pumps, in the event of a loss of offsite power (LOOP). If the power supplied to a reactor fails due to equipment failures or external conditions such as inclement weather, the EDGs are required to supply electrical power needed to safely shut down the reactor.

The focus of the work reported here is the improvement of the reliability and availability of the EDGs by using performance monitoring. The PRA method has been used here to identify a component which contributes a great deal of risk of failure to the reactor, such that money spent on safety improvements can have the most effect. By focusing on risk-critical components and their failure modes, resources can be used most effectively.

We anticipate that by using performance monitoring, several benefits can be realized. First, by tracking certain critical engine operating parameters, equipment failures can be predicted before components break and render the diesel inoperable. This kind of preventive maintenance allows repairs to be scheduled for times when the reactor is down for other maintenance, and helps to prevent further damage. For example, the failure of a lubricating oil pump could reduce the flow of oil to the power cylinders, causing scoring of the cylinder liners. Such propagating failures can cause more major repairs, or can cause flaws which aren't detected and thus are not repaired, further weakening the EDG and the plant as a whole. Second, the use of monitors can more effectively guarantee the performance of the EDG, by examining potential failure modes which aren't immediately obvious from simply running the engine. Third, monitoring can help operators to assess engine conditions which currently are assessed only by tearing an engine apart in order to verify internal conditions, leading them effectively to rebuild it. These inspections are expensive and

intrusive, often causing more damage than they detect. These inspections also leave the EDG unavailable to the plant, requiring that the reactor not be operating at power while the EDGs are being serviced [2].

In the face of deregulation of the electrical power industry, nuclear power plants must be made more competitive if they are to survive. They must eliminate tasks which do not contribute to safety so that available resources are not wasted, but rather are focused upon important safety-related matters. This generally means reducing operating and maintenance costs, while increasing revenues. Since reducing safety levels to save money is certainly not an option, there are two ways to improve the competitiveness of nuclear power plants: reduce the outage time of nuclear plants (and thus increase revenues), and reduce the unnecessary maintenance costs where possible. Monitoring can help by improving safety levels and saving money, which can also be used to further enhance safety levels in the plant.

1.2 Summary

The work reported here has been conducted as a part of the project on Integrated Models, Data Bases, and Practices Needed for Performance-Based Safety Regulation, funded by the Idaho National Engineering Laboratory (INEL). This project was created to demonstrate the benefits of using Performance-Based Safety Regulation (PBR) and to illustrate how to implement it in a beneficial, feasible manner.

With the industrial collaborator for this project, the Northeast Utilities Services Company (NUSCO), the EDGs at the Millstone 3 (MP-3) nuclear power plant were chosen as the focus of this research. The EDGs are a large contributor to the plant's total core damage failure (CDF) probability, making them a primary target for safety improvement. They also require frequent and intensive testing and mandated maintenance while no real need for these requirements was ever established. The high maintenance costs, combined with their large CDF contributions, suggest that improving the EDGs would provide significant economic and safety benefits.

The goal of the work reported here is to provide a framework for implementing such

a performance-based system, and for evaluating the benefits and risks associated with it. Failure data are analyzed and recommendations for an EDG monitoring system are made, but no actual EDG has been modified as recommended. This project provides the framework for such an implementation and an estimate of the gains to be recognized by moving from prescriptive to performance-based regulation.

This report first offers background on Probabilistic Risk Assessment and on the role and elements of the emergency diesel generator and its associated support systems.

Failure data are presented in order to determine the most significant failure modes. These data are culled from the PRA for MP-3 [3], from Licensee Event Reports (LERs) [4] [5], from the Nuclear Plant Reliability Data System (NPRDS) [6], from U.S. Navy EDG failure data [7], and from observations made at MP-3 [8].

The utilities are required to file Licensee Event Reports with the NRC whenever some part of the plant fails to operate as required. This is different from the data in the NPRDS database, which are maintained by voluntary cooperation of the utilities, for the use of other members of the Institute of Nuclear Power Operations (INPO), which maintains NPRDS. These data are more general, and include any problems discovered in the plant that may not have affected plant operations, and thus, were not Licensee Events.

Current monitoring and surveillance practices are discussed. The testing procedures currently used are also reviewed.

Based upon the failure modes identified, monitoring systems are proposed to help reduce the failure rate of the EDG system. The effects of these improvements upon the EDG failure rate, and thus upon the failure rate of the whole plant, are estimated. The possible risk increase due to the new monitoring system is also discussed.

The real effects of reduced failure rates are recognized at the operational level in changes to the way in which the diesels are tested and maintained. Recommendations for changes to the testing frequency, the test duration, and how tests are conducted are also made.

1.3 Previous Work

A great deal of research has been conducted in the areas of PRA/PSA, PBR, and EDG reliability, beginning with WASH 1400 [1]. WASH 1400 established the use of PRA in the nuclear industry, with the review board finding the methodology used to be sound. However, it was highly criticized for its understatement of the uncertainties of the method. In 1990, NUREG-1150, *Severe Accident Risks: Assessment for Five U.S. Nuclear Power Plants* [9], was issued to update the risk assessments of WASH 1400 and to correct its lack of uncertainty estimates. Together, these documents provide sound justification for the use of PRA.

WASH 1400 was only one of a series of reports which made an estimation of the failure rate of EDGs, among other components. Other NRC documents which include assessments of the EDG failure rate include NUREG/CR-2989, *Reliability of Emergency AC Power Power Systems at Nuclear Power Plants* [10], NUREG/CR-4347, *Emergency Diesel Generator Operating Experience: 1981-1983* [11], and NUREG/CR-4550, *Analysis of Core Damage Failure from Internal Events* [12]. The first two reports focused entirely on EDG systems in the period from 1976 to 1983, and the latter regarded the analysis of core damage frequencies in general, including the effects of the EDGs.

More recently, in the same vein, Electric Power Research Institute (EPRI) documents on the new Advanced Light Water Reactors (ALWRs) [13] also provide estimates of failure rates for many systems on power plants, including the EDGs. These rates include the ability to recover a failed EDG, while some of the previous sources only offer failures to start or run an EDG.

Concerns over the safety and reliability of the EDGs prompted several NRC responses with new Regulatory Guides and new procedures for the plants, making recommendations for older plants, and updating the licensing bases for the newer plants. Regulatory Guide 1.108, *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants* [14], was issued in 1977 to more clearly establish a periodic testing method for EDGs. This new test procedure

differed from the previous requirements primarily in determining the required frequency of tests. The previous licensing basis held that unless there were four or more failures of the EDG in the last twenty-five valid tests, EDGs would only be tested monthly. Per RG 1.108, the EDG test frequency was based upon the last 100 valid tests; two or more failed tests could increase the required test frequency to biweekly, weekly, or even every three days for four or more failures. RG 1.108 also established a firm basis for determining which attempted EDG starts were in fact valid tests of the system. RG 1.108 offers recommendations only, as plants licensed prior to 1977 are bound only by their individual technical specifications.

NRC concerns over the contribution of loss of offsite power to the core-damage failure rate of the reactor prompted the Station Blackout (SBO) Rule in 1980 [15] [16], supported by Regulatory Guide 1.155 [17]. SBO set specific EDG reliability goals for each plant, based on the weather conditions and electrical connections at each site. In some cases, plants added additional EDGs in order to satisfy SBO requirements.

Continuing the issue of Station Blackout, the NRC issued Generic Letter 84-15 [18] in 1984. In an effort to improve EDG reliability, the NRC authorized two major changes to the licensing basis, a reduction in the frequency of fast EDG starts, and the use of pre-lubrication of EDGs. Fast starts, typically bringing a cold EDG to full power in ten seconds, were reduced from once per month to once every six months. EDG operators were also encouraged to follow diesel manufacturers' recommendations to pre-lubricate the EDGs for all tests in order to reduce unnecessary wear, and thus, to improve EDG reliability.

More recent NRC guidance has addressed the testing methods for EDGs, particularly Regulatory Guide 1.9, *Selection, Design, Qualification, and Testing of Emergency Diesel Generator Units Used as Class 1E Onsite Electric Power Systems at Nuclear Power Plants* [19]. RG 1.9 compliments RG 1.108 by including recommendations for pre-operative tests and the reporting of EDG performance. RG 1.9 is based on the Institute of Electrical and Electronics Engineers (IEEE) Standard 387 [20].

In continuing efforts to establish the reliability of EDGs, reports have been published from the Idaho National Engineering Laboratory, through EPRI from the

Southwest Research Institute (SwRI), and from Brookhaven National Laboratory (BNL). In 1988, the SwRI report *Surveillance, Monitoring, and Diagnostic Techniques to Improve Diesel Generator Reliability* [4] was published to recommend new surveillance and diagnostic techniques for application in nuclear power plants. Where applicable, this report recommends changes in design, surveillance, and maintenance, and recommends monitoring techniques in order to help indicate failures of the remaining modes. A cost proposal for the design, development, and implementation of a monitoring system is also included.

In 1994, the BNL report *Emergency Diesel Generator: Maintenance and Failure Unavailability, and Their Risk Impacts*, NUREG/CR-5994, [21] was published. This report assessed the unavailability of the EDGs due to testing, preventive and corrective maintenance, and actual failures. It also makes the connection between additional maintenance time or reduced failures and the core damage frequency for the plant.

In 1996, the INEL report *Emergency Diesel Generator Power System Reliability 1987-1993* [5] was released. The INEL report evaluated actual reliability of the EDGs using performance data, and made comparisons to RG 1.108, SBO, and other reliability targets. Additionally, conclusions regarding the effects of excessive out of service time due to maintenance and testing were drawn, with differences noted between periods with the reactor at power and with the reactor in a shut down mode. The failure rate of the EDG was also found to vary with increasing run time. Grant et al. chose to define the failure rate of the EDG as a function of run time; they discuss the effect of a time-dependent failure rate on the effectiveness of short diesel run tests.

Similar work to that proposed here has been underway in the U.S. Navy for improving the reliability of EDGs on nuclear-powered vessels [7]. The Navy has begun using a new condition-based maintenance system, known as ICAS, the Integrated Condition Assessment System. It is their new monitoring and trending system. In addition to tracking performance, it provides alarm warnings when performance becomes unfavorable, and recommends corrective or diagnostic measures. Reports on the reliability of Naval EDGs are included in these studies.

Recognizing the importance of using PRA to improve plant reliability, the NRC has issued the draft form of a Regulatory Guide, DG-1065, *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications* [22]. Though still in draft form, this Guide is used here to evaluate safety concerns caused by changes to current operating practices proposed here.

It is the goal of the work reported here to propose monitoring similar to that in the SwRI report, but with the intent of improving EDG reliability most substantially with a relatively selective set of monitors; this improved reliability is then used to extend the surveillance test interval and make EDG tests as effective as possible. Cursory economic assessments of these changes are also made. The reliability problems illustrated in the INEL report, the EPRI report, and in the U.S. Navy reports are used as the roadmap for improvements needing to be made. Throughout our study, the generic data presented in NUREGs 4550, 2989, 4347, and 1150 are used with the PRA of Millstone 3. Finally, using DG-1065, these proposed changes are evaluated for safety risks, as the NRC would require of any utility proposing these changes.

1.4 Ongoing Research

Additional research performed within this project has concerned different areas of PBR for EDGs. One effort is conducted as is this study, from the perspective of the licensee, or the company operating the power plant [2]. A separate effort is working from the perspective of the regulator, the NRC [23].

Utton's work has been conducted on the need for and effects of the intensive teardown inspections of the EDGs during reactor refueling outages, currently every eighteen months. By comparing the requirements and operating basis of nuclear power plant EDGs to those used by the U.S. Navy and in various civilian applications, she shows that the current maintenance procedures are not only unnecessary but even counter-productive, causing damage and new failures at great expense. Her work also shows the effect of changes to the technical specifications regarding EDGs on plant-wide core-damage failure and other reactor failure events.

Abdelkader is conducting research to develop a scheme for the review of proposed changes to the deterministic regulations. Prospective changes proposed by the "licensee" are reviewed by the "regulator" for approval. She is developing a standard for changes to requirements and for the burden of proof placed upon licensees proposing changes. Her research also includes the propagation of uncertainties in basic event probabilities through fault trees describing the EDG and the plant as a whole.

Chapter 2

Probabilistic Risk Assessment

2.1 Introduction

This chapter briefly introduces Probabilistic Risk Assessment as it has been used in the work reported here. First, PRA is distinguished from prescriptive risk assessment. Then, the applications of probabilities, fault trees, and minimal cutsets are presented. Finally, the effects of surveillance and testing are discussed.

2.2 Prescriptive vs. Probabilistic

PRA differs significantly from prescriptive or deterministic safety assessment, the methods used prior to the development of PRA and the WASH 1400 report. A deterministic risk assessment defines the physical conditions that the worst possible accident would cause (a design basis accident), and requires engineering designs to fully compensate for such an accident. A PRA considers what events, or combinations of events, have the highest probability of occurring, and what the effects are of these occurrences.

As an example, consider the Three Mile Island Unit 2 (TMI-2) accident of 1979. A small loss of coolant accident (LOCA) occurred, and the emergency core cooling system (ECCS) failed to operate as required [24]. The reactor at TMI-2 had been designed deterministically under the worst-case scenario large LOCA. However, WASH

1400 [1] shows that the combined failure of the ECCS and a small LOCA has the highest probability of damaging the core. Both a large LOCA and a small LOCA with an ECCS failure have the same net effects, yet the most likely way that the core can melt is the focus of only PRA, not of a prescriptive risk assessment.

2.3 PRA Basics

A PRA is comprised of three levels in moving from the basic initiating events to the effects of radiation release outside of the reactor containment [1]. Basic events are small component failures, external conditions, and improper human actions which can cause system failures.

In a Level 1 PRA, a Plant Model is created, whereby the basic events are linked to cause plant damage states, situations in which some safety-critical systems are damaged or inoperable. The analysis in the work reported here is restricted to the Level 1 PRA, considering the basic events which can damage the EDG or leave it inoperable.

In a Level 2 PRA, a Containment Model is created, which shows, based upon the plant damage states, what the release states would be, or how much radiation would be released from the containment.

The final step is a Level 3 PRA, a Site Model. The site model takes the release states and generates final damage states in the surrounding area. These final states include the radiation exposure of the air, land, and water surrounding the site, and the health impacts on the nearby population.

The accuracy of the PRA is subject to two kinds of uncertainty: aleatory and epistemic [25]. Aleatory (depending on chance, luck, or contingency) uncertainty is simply the statement that while one expects a certain system to have a certain number of failures over a certain period of time, one can't predict exactly when or how such a failure will occur. Epistemic (having to do with knowledge) uncertainty is the possible error in the models used in each level of the PRA, or in the values of basic event frequencies. These uncertainties limit the accuracy of the PRA.

Each basic event, such as the failure of a valve or switch to close, or the failure of a pump to operate, has a failure rate or a frequency assigned to it. For example, if a pump is expected to fail to operate once in every 10000 hours of operation, it has a failure rate or frequency of 0.0001 per hour. If this pump is expected to run continuously (i.e. 8760 hours per year) then the probability of the pump failing during the year can be found with Equation 2.1.

$$P_f = 1 - e^{-\lambda t} \tag{2.1}$$

For the failure rate, λ, equal to 0.0001 per hour, and the time t equal to 8760 hours, the failure rate, P_f is 0.584. For short periods of time, the failure rate is approximately equal to λ times t. (All probabilities must lie between 0 and 1, with 0 corresponding to an impossibility, and 1 corresponding to a certainty.)

For use in PRAs, tables of empirically-derived failure rates are available for many components and actions for nuclear power plants. NUREG/CR-2989 [10] and NUREG/CR-4347 [11] provide calculations of these failure rates for EDGs, while WASH 1400 [1], NUREG/CR-4550 [12], and EPRI ALWR reports [13] provide larger sets of failure rates for many different components.

For the PRA of Millstone 3, the EDG basic events are listed with their probabilities in Appendix A, Table A.1.

2.4 Fault Trees

A fault tree is the collection of basic events, logical operators, and top events which describe how a system can fail [26]. Logical operators in fault trees include **and** and **or**. An **and** operator is used when two or more events must all occur for the operator to be true. An **or** operator is used when only one event has to occur for the operator to be true. An **and** operator and an **or** operator are shown in Figure 2-1.

Also shown in Figure 2-1 are the symbols for basic events, top events, and intermediate events. Top and intermediate events both use the same symbolic notation. As was previously discussed, basic events are the failures of simpler components, such

as pumps, valves, and switches. Top events are the reason for using a PRA; the top event is the actual system failure which depends on the behavior of many basic events. Intermediate events can also be defined to make the PRA more easily understood; intermediate events are quite similar to top events, except that many intermediate events can be compiled to make a top event.

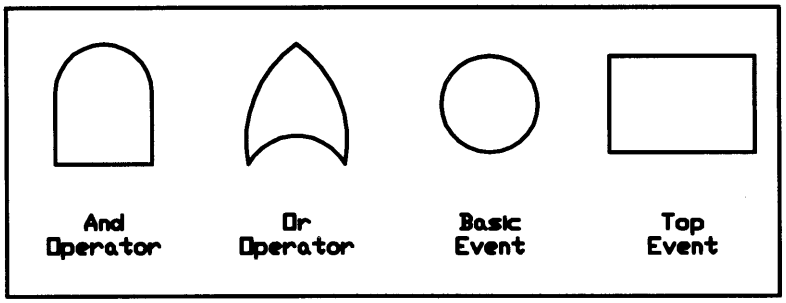


Figure 2-1: Fault Tree Operators and Symbols

Figure 2-2 is a simple fault tree for being able to see while driving a car at night. The three basic events are labeled L, for "Left headlight goes out due to lamp failure," R, for "Right headlight goes out due to lamp failure," and A, for "Alternator fails." The top event is C, for "Illumination fails." An intermediate event is also included, B, for "Both headlights are out." The fault tree could be drawn without the use of B, but its presence makes the logic of the tree easier to understand.

This model of the system assumes that one can drive with one headlight out, and that the alternator (ignoring the battery) is used to power the headlights. If both headlights burn out, the driver can't see, or, even if both lights are perfect, one cannot see without electrical power from the alternator.

Starting from the bottom of the tree, the left and right headlights are joined under an **and** gate. This means that for B (Both headlights out) to be true, both L (Left headlight out) and R (Right headlight out) must be true. In the terminology of probability, using Boolean operators, this can be written as $B = L \cap R$.

The events B (Both lights out) and A (Alternator fails) are joined under an **or** gate, meaning that if either A or B is true, C will be true. (This includes the

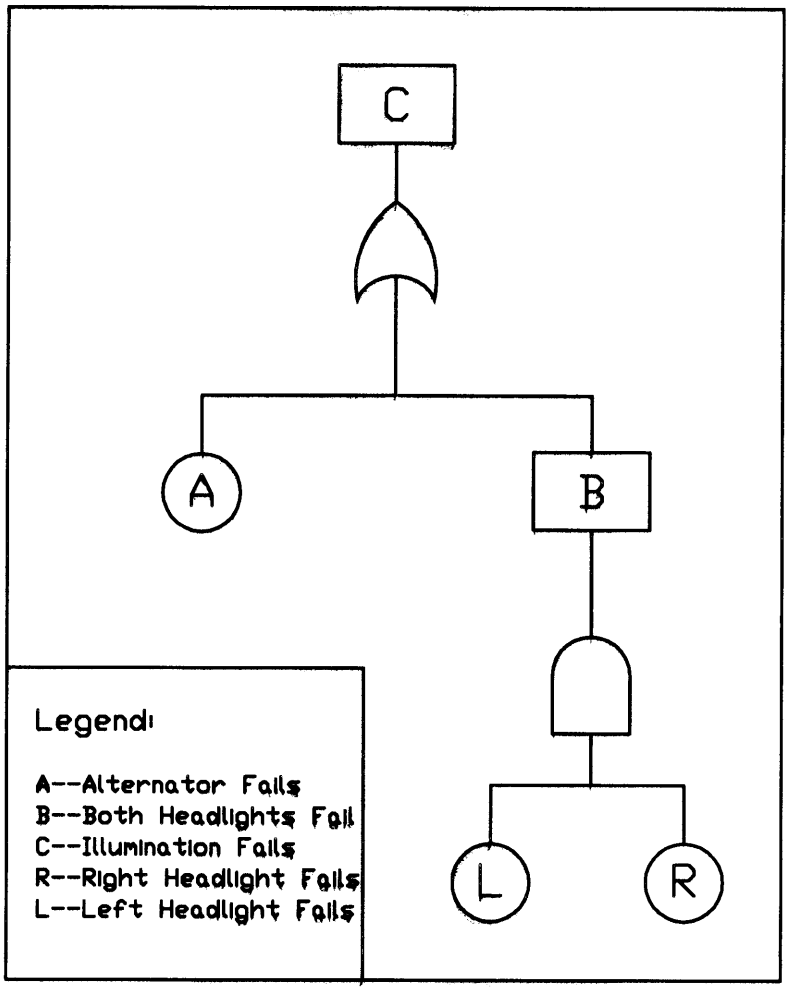


Figure 2-2: A Sample Fault Tree

possibility that *both* are true.) This can be written as $C = A \cup B$. Knowing $B = L \cap R$, we can write C in terms of only the basic events, as $C = A \cup (L \cap R)$.

To predict the failure rate for the driver's ability to see, failure rates for the basic events L, R, and A are needed. Assume that on a given night of driving, the probability of event L is $P_L = \frac{1}{100} = 0.01$. For two identical headlights, the probability of R is $P_R = P_L = \frac{1}{100} = 0.01$ (for independent failures). Assume that the probability of A is $P_A = \frac{1}{500} = 0.002$. One can observe that a single headlight is five times more likely to fail than the alternator.

For an **and** gate, the probability of event B is $P_B = P(L \cap R) = P_L \cdot P_R$. With the values assumed, $P_B = \frac{1}{10000} = 0.0001$. For an **or** gate, the probability of top event C

is given in Equation 2.4.

$$\begin{aligned} P_C &= P(A \cup B) && (2.2)\\ &= 1 - (1 - P_A) \cdot (1 - P_B) && (2.3)\\ &= 1 - (1 - P_A) \cdot (1 - P_L \cdot P_R) && (2.4) \end{aligned}$$

With the values assumed above, $P_C = 0.0021$. In other words, there is a 0.21% chance that a driver won't be able to see on a given night, or it is expected that a driver will be unable to see once in every $\frac{1}{0.0021} = 476$ nights.

While a headlight is five times more likely to fail than the alternator, the alternator contributes much more to the top event probability; this is because there are two headlights, which are referred to as a redundant system. Only one headlight is really needed, but having a second greatly reduces the failure probability of the whole system. There is only one alternator, so if it fails, the whole system fails as well.

The fault tree for one EDG train of Millstone 3 is included in Appendix A, Section A.2. There are two redundant EDG trains, and most of the support systems (such as the EDG's "alternator," the control power supply system) are redundant as well.

2.5 Minimal Cutsets

A minimal cutset (MCS) is the smallest set of basic events which causes the top event to occur. In the simple headlight example, there are two minimal cutsets: one (MCS_1) is the failure of the alternator (event A), and the other (MCS_2) is the failure of both headlights (event B, or events L and R). In an MCS, every member of the set must fail in order to cause system failure.

In a more complex fault tree, such as that of the MP-3 EDGs, the contribution of each basic event to the total failure probability is not so obvious, and thus minimal cutsets are useful tools. The MCS for the MP-3 EDG are shown in Appendix A, Table A.2. In order to evaluate the contribution of each basic event to the top event probability, the Fussell-Vesely value, a tool for comparing different basic events, can

be calculated. The Fussell-Vesely value for a component is simply the sum of the probabilities of all the minimal cutsets which include that component, normalized by the total probability. For a component i which participates in m minimal cutsets (MCS_{i_1}, MCS_{i_2}, ... , MCS_{i_m}) in a system with a total of n minimal cutsets (MCS_1, MCS_2, ... , MCS_n), the Fussell-Vesely value for component i, FV_i is defined in Equation 2.5. The denominator of the equation, the sum of all minimal cutsets, is the total failure risk of the whole system.

$$FV_i = \frac{P_{MCS_{i_1}} + P_{MCS_{i_2}} + \cdots + P_{MCS_{i_m}}}{P_{MCS_1} + P_{MCS_2} + \cdots + P_{MCS_n}} \tag{2.5}$$

For the headlight example, the probability of MCS_1 (P_{MCS_1}) is P_A, or 0.002. The probability of MCS_2 (P_{MCS_2}) is $P_A \cdot P_B = 0.0001$, since both L and R must occur in this cutset. The Fussell-Vesely values of the alternator, the right headlight, and the left headlight, FV_A, FV_R, and FV_L, respectively, are found with Equation 2.5, as shown in Equations 2.6, 2.7, and 2.8.

$$FV_A = \frac{P_{MCS_1}}{P_C} = \frac{0.002}{0.0021} = 0.9524 \tag{2.6}$$

$$FV_R = \frac{P_{MCS_2}}{P_C} = \frac{0.0001}{0.0021} = 0.048 \tag{2.7}$$

$$FV_L = \frac{P_{MCS_2}}{P_C} = \frac{0.0001}{0.0021} = 0.048 \tag{2.8}$$

The higher the Fussell-Vesely value, the more important that component is to the reliability of the system.

By ranking the Fussell-Vesely values, the components which most influence the top event probability are identified. For the top event being a core damage event in a nuclear reactor, the EDGs have the highest Fussell-Vesely values, and thus are the target of improved reliability studies. Ranking components by Fussell- Vesely values for contribution to CDF, the EDG is found to contribute 33% of the CDF. Ranking events instead of components places loss of offsite power (LOOP) at the top of the list, contributing over 68% of the CDF; large LOCA, the deterministic design basis accident, only contributes 4% to the CDF [27]. In focusing on EDG failures, the

supply of cooling water to the EDG is, in turn, the most important contributor to EDG failures, according to its Fussell-Vesely values.

2.6 Effects of Surveillance

Surveillance and testing are used to reduce the probability of failure in standby systems, such as the EDGs. Typically, a single EDG train has a failure rate of just under 10% per year, or $\lambda = 0.1$ failures per year [3]. This failure rate is not an absolute quantity, as is discussed in the definitions of PRA. This failure rate is a calculated value based upon the assumptions of the PRA fault tree, and the failure rates for the 121 basic events included in the fault tree. Changes to these failure rates or the logic of the fault tree can change this top event probability.

The probability that the EDG will fail to function (the unreliability of the EDG) at a time t is given in Equation 2.5, and is repeated in Equation 2.9 with the short-time approximation.

$$Q(t) = 1 - e^{-\lambda t} \approx \lambda t \tag{2.9}$$

This assumes a given constant failure rate λ [25]. Typically, Q refers to the *unavailability* of the EDG. In the case where repair is not considered, the unreliability and the unavailability are the same. By saying that repair is not considered does *not* mean that the diesels are never fixed. It simply means that, if there is a demand for the diesel, and the diesel fails to perform, we are not interested in how long it takes to fix the EDG, only that it failed to work when needed.

This failure probability is a function of time, which gets larger as time passes. The Station Blackout Rule established a target EDG reliability of 0.975, or a maximum unreliability of 0.025 [17]. Using this value in Equation 2.1, it is found that within 0.25 years, or three months, the reliability is no longer acceptable.

However, by testing the EDG, it is verified that all systems tested function properly, and the probability of failure is reset nearly to zero. Not all possible failure modes can be tested, so the probability of failure immediately after a test is not necessarily equal to zero. Figure 2-3 (not drawn to scale) shows both the unavailability

of the EDG without testing, as well as the effects of periodic testing.

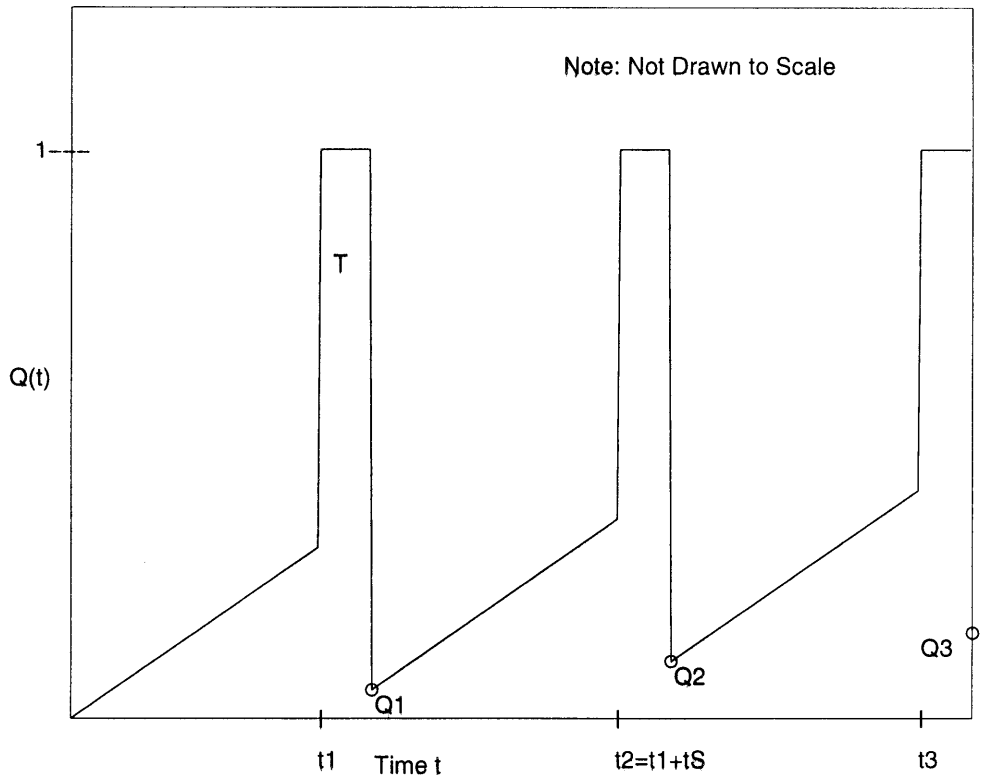


Figure 2-3: Effects of Testing on the Unavailability of a Standby System

In Figure 2-3, the effects of testing a standby system are demonstrated. At times t_1, t_2, and t_3, tests are conducted of the standby system. Each test lasts a period of time τ. The interval between tests $t_S = t_3 - t_2 = t_2 - t_1$ is chosen to minimize the average unavailability of the system. During testing, the unavailability of the system is set to 1, meaning that the system can not be used while tested. It is this restriction which prevents excessively frequent tests. The time for testing also includes any repairs suggested through the test procedure.

After each test, the unavailability of the system nearly returns to 0. Three small offsets, Q_1 and Q_2, and Q_3 are present in the figure because not all failure modes are examined on every surveillance. These offsets increase with time, but more slowly than $Q(t)$ would without any testing. Thus, $Q_3 \geq Q_2 \geq Q_1$. These offsets can only be reset to zero by actual successful demands of the standby system, or by more realistic tests conducted less frequently.

Unavailability due to repair work is not explicitly shown in Figure 2-3, but it can be considered part of the testing period. With more explicit notation, the effects of repair work can be separated from the testing procedure; not all tests require repair work, but all tests should be of equal length. Using τ as the test length and t_S as the testing interval, an average unavailability can be found; the average unavailability for a cycle is a quantity which can readily be used to compare many different testing cycles. To model the repair process, f_R is defined as the fraction of tests which are followed by repair work, and t_R is the average time per repair. The length of the entire testing cycle, operation, testing, and repairs, is represented by t_C. The cycle length is

$$t_C = t_S + \tau + f_R \cdot t_R \tag{2.10}$$

where $f_R \cdot t_R$ represents the average amount of time spent in repairs per cycle. Using this definition of t_C, the average unavailability can be defined as

$$\langle Q \rangle = \frac{1}{t_C} \int_0^{t_C} Q(t) dt \tag{2.11}$$

or

$$\langle Q \rangle = \frac{(\frac{\lambda t_S^2}{2} + \tau + f_R \cdot t_R)}{t_C} \tag{2.12}$$

for later use.

In cases where testing does not fully test all possible failure modes, the offset values, (Q_1, Q_2, and Q_3 from Figure 2-3) have a negative effect on the average uncertainty. These will grow as $Q_1 = \lambda_C \cdot t_1$, $Q_2 = \lambda_C \cdot t_2$, etc., where λ_C is defined in

Equation 2.14. The term λ_C represents the failure contributions which are not reset to zero by a one-hour monthly test. These failures can be treated as a system failure rate which is only reset by a more thorough test, conducted far less frequently. In these cases, average uncertainty should be evaluated for several testing cycles until the unavailability is completely reset to zero by a more thorough test.

In a general case, where there is an initial offset value Q_0, the average unavailability over n cycles becomes

$$\langle Q \rangle = \frac{1}{t_C} \cdot (\frac{\lambda t_S^2}{2} + \tau + f_R t_R + Q_0 t_S) + \frac{t_S}{n t_C} \cdot \sum_{i=1}^{n-1} (n-i)(Q_i - Q_{i-1}) \quad (2.13)$$

$$\langle Q \rangle = \frac{1}{t_C} \cdot (\frac{\lambda t_S^2}{2} + \tau + f_R t_R + Q_0 t_S) + \lambda_C \cdot (n-1) \cdot \frac{t_S^2}{2 \cdot t_C} \quad (2.14)$$

but for the sample unavailability in Figure 2-3, $Q_0 = 0$ [28]. The failure rate λ_C is used to describe the accumulation of unavailability due to imperfect tests; it is defined more explicitly in Chapter 4. This form of the average unavailability is the most useful for real systems which cannot test all possible failure modes.

2.7 Summary

In the assessment of the EDG system, the work reported here uses several principles of PRA, particularly fault trees and minimal cutsets. Any changes proposed in the work reported here are evaluated by first updating the failure rates for the basic events, then using the fault tree to evaluate the impact these changes have on EDG reliability and availability. Changes to the failure rate logically suggest changes to the surveillance test frequency, and the change in average unavailability or average unreliability is evaluated. In order that the proposed changes are as effective as possible, the minimal cutsets for the EDG fault tree are used, and those components with the highest Fussell-Vesely, or risk contribution, values are the focus of attention.

Chapter 3

EDGs and the Electrical System

3.1 Introduction

The EDGs have been established as a highly critical system for the safe operation of the nuclear power plant. In order to better understand the role of the EDG and its associated subsystems, this chapter introduces the electrical power system and the function of the EDG. The failure data which are presented include failures of the support systems, so the boundaries of the EDG are presented to show how each support system failure affects the EDG, and how these failures are reported.

The details presented regarding the diesel engine and the support systems are only for familiarity with the components which are discussed with failure data, and for a better understanding of how each component can render the EDG inoperable.

In the next chapter, current monitoring and surveillance of the EDGs are presented.

The actual configuration of the EDGs and support systems can vary from plant to plant, but is fairly universal. Definite similarities exist between plants from the same reactor manufacturer of approximately the same age. For the purposes of the work reported here, two NUSCO plants, Millstone 3 and Seabrook, are described. Both are relatively new Pressurized Water Reactors (PWRs) of Westinghouse design.

The information describing these plants is taken from three sources: the Seabrook Probabilistic Safety Assessment (PSA) [29], the Millstone 3 Final Safety Analysis

Report (FSAR) [30], and the Standard Technical Specifications (STS) for plants of Westinghouse design [31]. The PSA, as discussed earlier, is a plant-specific assessment of Seabrook using the methods of PRA. A Final Safety Analysis Report is the result of all deliberations on the construction and licensing of a plant. The Standard Technical Specifications are the generic form of the NRC operating requirements applied to all plants. Included with the FSAR as the licensing basis for the plant, small differences can exist between the Technical Specifications of two plants, but these discrepancies are very small for similar plant designs.

3.2 Electrical System

The Standard Technical Specifications [31] and the Final Safety Analysis Report [30] define requirements for the electrical power systems at a nuclear power plant. Typically, two or more connections to the local power grid are available for delivering offsite power to the reactor. This electrical power is used for all equipment loads, both safety-related (termed Class 1E) and non-safety-related (termed non Class 1E).

The power is delivered to electrical distribution networks called buses, which in turn deliver power to all plant equipment loads. In event of a loss of offsite power, non-safety-related loads are shed from the supply buses as necessary. The function of the EDG is to supply power for the safety-critical loads which remain, such as reactor cooling systems and control rod power.

Figure 3-1 is a block diagram of the Class 1E Electric Power System, taken from the Seabrook PSA [29]. Safety- related loads are carried by two redundant DC power buses (DC11A and DC11B) and two redundant 4.6kV AC power buses (BE5 or BE6). These buses are closely related by the battery system and its AC-powered chargers. AC buses E5 and E6 power the battery chargers, and the batteries (BA and BB) power buses 11A and 11B. The DC buses provide control power to the EDGs and other safety- critical systems, while the actual operating power is taken from the AC buses.

Buses E5 and E6 are normally powered with offsite power (OP), through a step-

up transformer (GT), unit auxiliary transformers (UATs, labeled UA and UB), and normal supply breakers (NBE5 and NBE6).

Each of these offsite power supplies to the emergency buses are backed up by reserve auxiliary transformers (RATs, labeled RA and RB). In the event of low voltage on the supply through a UAT, an RAT is connected by opening a reserve supply breaker (RBE5 or RBE6).

If this switch to reserves is unsuccessful, or if it fails to alleviate the low voltage signal, an emergency diesel generator (DGA or DGB) is automatically started. Each diesel generator is supported by independent support systems (DGAS and DGBS), and is connected to buses E5 or E6 through diesel generator supply breakers (DBE5 and DBE6).

In the event of an emergency including a loss of offsite power, the AC buses each carry loads associated with redundant sets of emergency shutdown equipment such as the centrifugal charging pumps, safety injection pumps, residual heat removal pumps, primary component cooling water pumps, service water pumps, cooling tower pumps and fans, containment spray pumps, and emergency feedwater pumps. The DC buses also similarly carry loads for redundant trains comprised of controls for all essential AC buses, reactor trip breakers, diesel generators, and emergency power sequencers.

In the case of our industrial collaborator, the MP-3 plant is served by two redundant diesel generator trains, similarly to the Seabrook system described above. These emergency diesel generators are described in the next section.

Additionally, a third diesel generator is supplied to satisfy the Station Blackout (SBO) Rule, Regulatory Guide 1.155 [17].

The two battery systems which back up the DC power source are charged using AC power. Each system is comprised of two batteries. With AC charging power available, each battery system can carry all safety-related control loads for up to twenty-four hours. Without AC power available, both batteries can run all necessary safety shutdown control functions for six hours, or one battery can run for two hours.

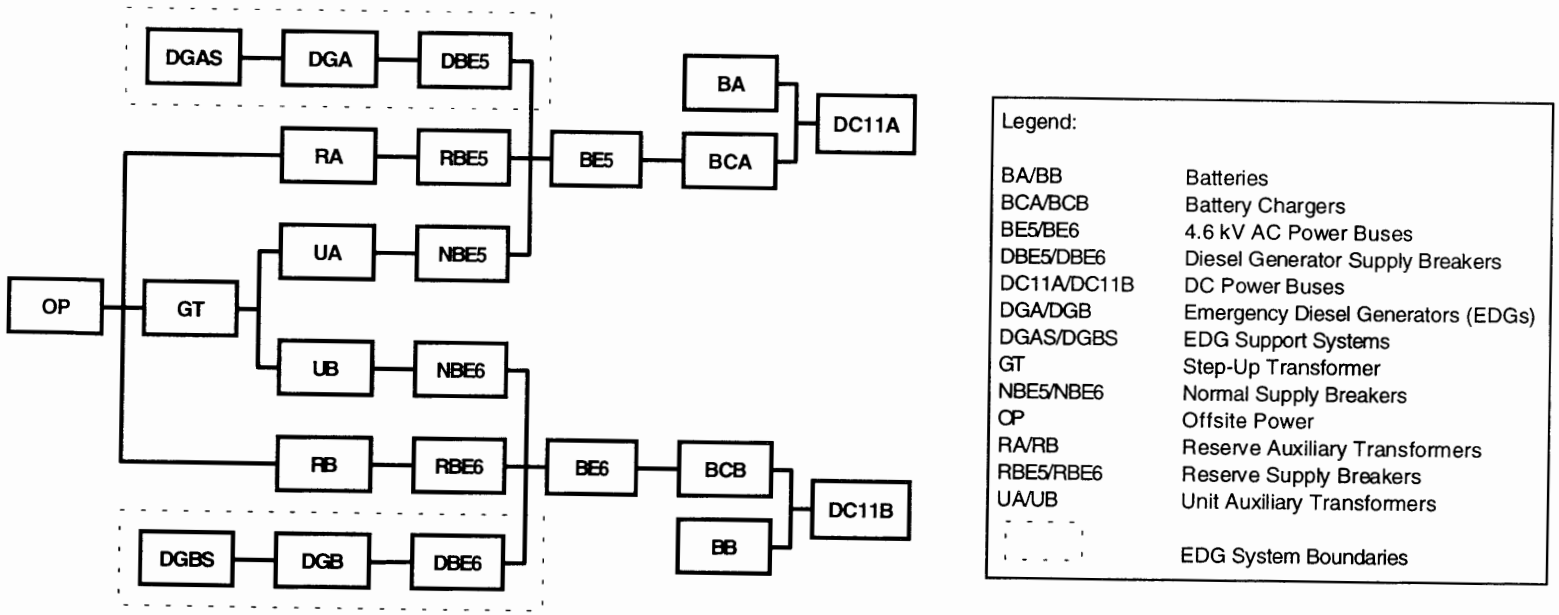


Figure 3-1: Class 1E Emergency Power System [29]

3.3 Emergency Diesel Generators

In the example of MP-3, the emergency diesel generators used are 4.16kV, 3 phase, 60 Hertz diesel-engine driven synchronous generators, made by Colt- Pielstick, model PC2V. They are rated at 4,986kW (6,685 HP) continuous power, and 5,335kW (7150 HP) for 2,000 hours [30]. These diesels can be operated for up to 24 hours unloaded or loaded less than 20% of the rated load without suffering any buildup of combustion or lubrication products in the exhaust system. They each are supplied by a 32,760 gallon (124 kL) fuel system. These supplies are sufficient for a six-day diesel run [30].

Each EDG can be started four ways: by a Loss of Offsite Power (LOOP), by a Safety Injection Signal (SIS)/Engineered Safety Feature (ESF), by a Containment Depressurization Accident (CDA), or manually. Loading is handled by a dedicated load sequencer, but in tests, loading is often carried out manually.

The emergency diesel generators can be operated in four modes: standby (default), testing, SIS/"hot standby", and operation. The EDGs are almost always in standby, available to start on demand. Each month, approximately one hour is spent in testing mode. In the event of an SIS signal, a diesel is automatically started, but no loads are applied; it is run in a hot standby mode, already started and running at speed in the event of a LOOP. Finally, in the event of an emergency demand, the diesel can be operated at load, supplying necessary power to the emergency systems necessary to safely shut down the reactor.

The third diesel generator on site is a 2,600kW (3485 HP), 3 phase, 0.8 power factor, 60 Hertz, 4.16kVAC diesel generator. It is capable of powering the safety buses through either diesel train in the event of a station blackout (SBO). The SBO diesel is a stand-alone system with an independent fuel supply, sufficient for running at rated load for up to sixteen hours.

Each emergency diesel generator system is comprised of several support systems, including cooling, air systems, fuel and lubricating oil, instrumentation and controls, and turbochargers or superchargers. Figure 3-2 shows the support systems of the EDG, as well as the external systems which influence EDG operation. Two sys-

tem boundaries are shown in Figure 3-2. All of the systems enclosed by the larger boundary, labeled "EDG System," are analyzed in the work reported here. Within the "EDG System" boundary is a "PRA Diesel" boundary. For the MP-3 PRA, some support systems, such as lubricating oil, exhaust, EDG cooling water, the turbocharger, parts of the fuel oil, and starting air systems, are lumped in with the mechanical diesel engine (the PRA diesel is called a "supercomponent," because it has only one failure rate for many components). The work reported here separates these internalized support systems for more complete and accurate analysis.

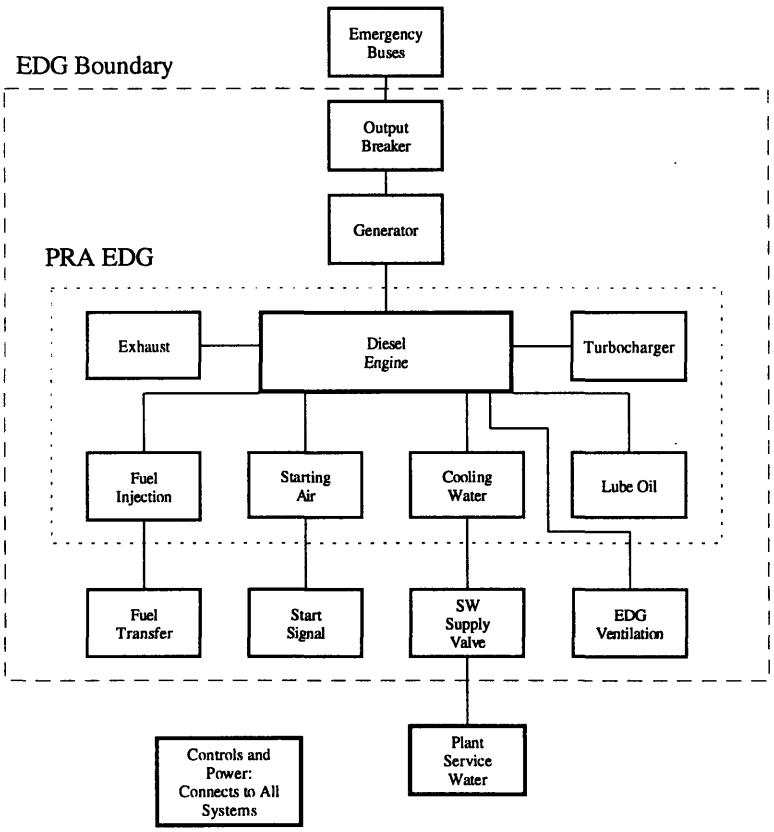


Figure 3-2: EDG System Boundaries

Each of these subsystems is described in further detail after the next section on diesel engines themselves (the mechanical functioning and different types). With noted exceptions, these subsystems are located physically within the EDG rooms,

and are subject to the same protection from external failure agents as the EDGs themselves.

3.4 Diesel Engines

There are two main types of diesel engines, valved engines, such as the PC2V used at MP-3, and opposed piston engines. The basic setup of a valved engine is very similar to the familiar fuel-injected automobile engine, shown below in Figure 3.4. In contrast is the opposed piston engine, a schematic of which is pictured below in Figure 3.4. Most newer engines are valved, though opposed piston engines offer some space-saving advantages.

There are few practical operating differences between these two types of diesel engines, but one physical difference between them has shown to be important. A failure mode unique to the opposed piston engine has been identified in the course of the work reported here, and is discussed in greater detail with the other recommendations.

The valved engine has one piston per cylinder, and engine intake and exhaust pass through valves located above the piston. The crankcase, and thus most of the lubricating oil, is kept at the piston and below. The piston compresses the fuel and air above it on the upward stroke; the mixture combusts by heat of compression only. Here the valved diesel differs from the gasoline engine, which uses a timed spark (from a spark plug) to detonate the combustible mixture. The cylinders may be lined up in a row, or may be canted to the left or right in a "V"-arrangement at an angle anywhere from 40 to 75 degrees. One arrangement has one set of cylinders to the left, and one to the right, where the angle between them is 180 degrees. This is known as an opposed-cylinder engine, different from an opposed-piston engine described below. Opposed-cylinder has one piston per lateral cylinder, but opposed-piston has two pistons per upright cylinder [32].

The opposed piston engine has an upper piston and a lower piston in each cylinder. Both pistons move together, simultaneously compressing the combustible gases, which combust from the heat of compression (see Figure 3.4), then separating together,

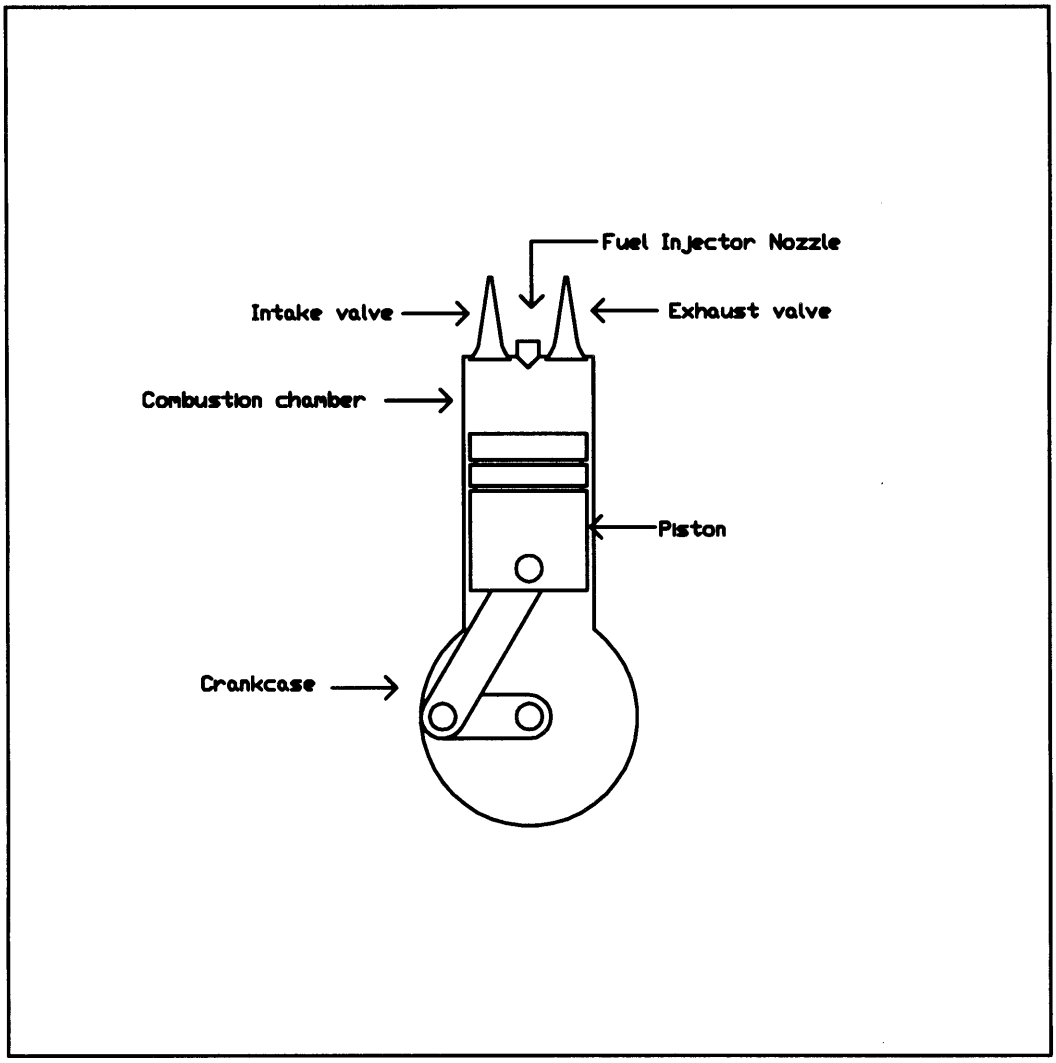


Figure 3-3: Valved Diesel Engine Cylinder

expanding the compression chamber volume, turning the crankshaft, allowing exhaust gases to be forced out of the chamber and fresh air to be drawn in (see Figure 3.4). As these figures show, there is both an upper and a lower crankcase, and thus half of the lubricating oil is used above the combustion chamber, and half below.

Since the opposed piston engine uses about half of its lubricating oil above the combustion chamber, a new failure mode is introduced by prelubrication. When prelubrication is used, gravity can draw upper crankcase oil past weak seals, allowing it to drip into the combustion chambers and cause complete EDG failures. The above description of the valved diesel engine, with all crankcase oil *below* the seals, should

demonstrate that only the opposed piston engine is subject to such concerns.

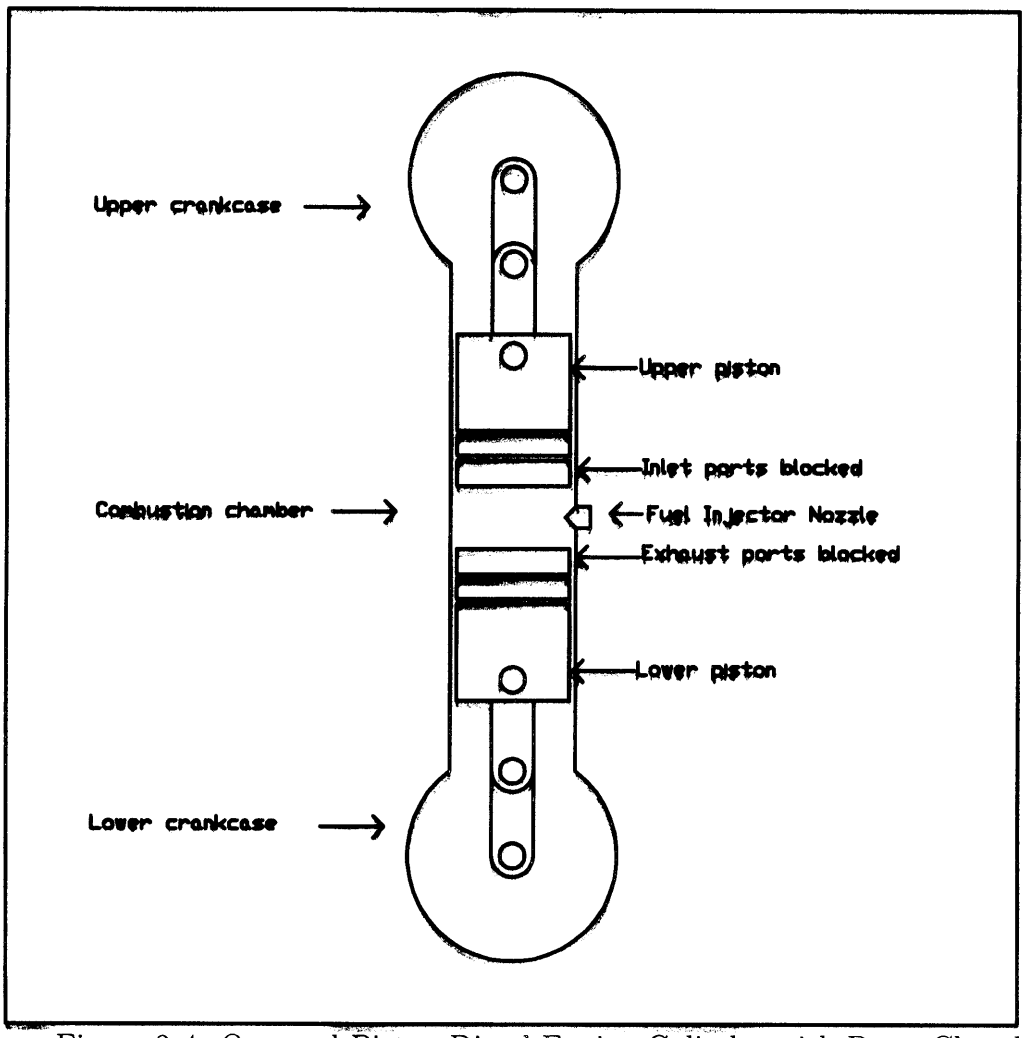


Figure 3-4: Opposed-Piston Diesel Engine Cylinder with Ports Closed

One main difference between a diesel engine and a fuel-injected gasoline engine was already mentioned: the method of ignition. The diesel uses only heat of compression, not an externally introduced spark. This saves the diesel from common component failure modes typical to the gasoline engine, such as batteries, ignition, electrical distributors, and spark plugs. The disadvantage is that diesel engines can be harder to start at cold temperatures; to resolve this problem, many diesel engines use "glow plugs," which assist in increasing the combustion chamber temperature during cold starts. However, the EDGs in nuclear service do not usually use glow plugs, as the

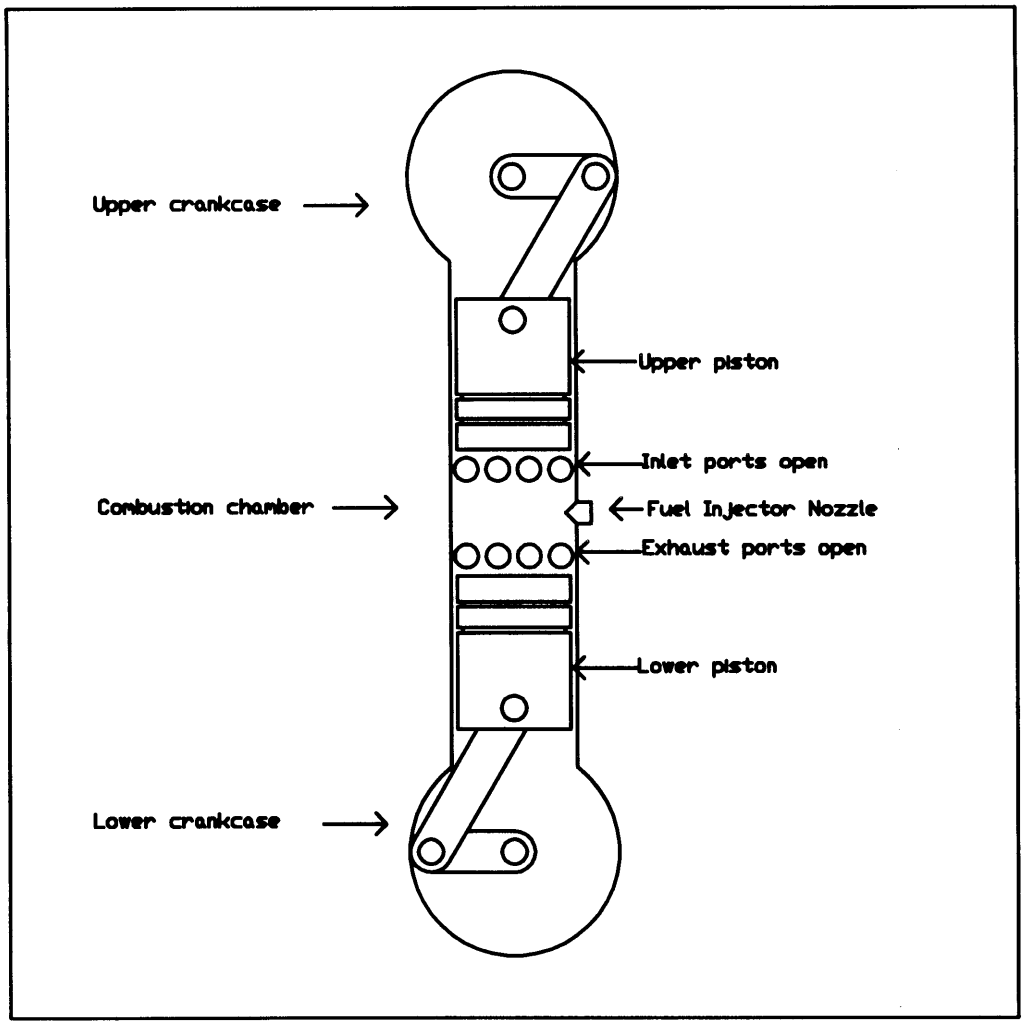


Figure 3-5: Opposed-Piston Diesel Engine Cylinder with Ports Open

building, the coolant, and the lubricating oil are kept at elevated temperatures to ease starting.

The other major difference between diesel engines and gasoline engines is the amount of fresh air needed to support combustion. Diesels require significantly more air, so turbochargers or superchargers are routinely used to increase the pressure of fresh air delivery, and thus the mass delivered to the fixed volume. These chargers are discussed further in the next section.

3.5 Diesel Subsystems

3.5.1 Cooling Systems

There are two separate types of cooling systems provided for the EDG: Generator Building Ventilation and EDG Cooling Water.

The generator building is cooled by a forced-air ventilation system specific to the EDG. The EDG ventilation system for MP-3 is described in Section 9.4.10 of the FSAR [30]. The system is designed to keep the ambient temperature of the diesel room below 120 degrees Fahrenheit. Ventilation inlet and outlet dampers are motor-operated, but are designed to fault to the open position in the event of a failure, to better assure proper ventilation. In addition to cooling, the ventilation system includes electrical space heaters (actuated by local thermostats) for cold-weather operation.

The ventilation system is tested with each EDG test run, as operating conditions would necessitate air cooling. A diagram of the ventilation system taken from MP-3 FSAR Figure 9.4.10-1 [30] is provided in Figure 3-6.

The EDG cooling water is a closed coolant system for each EDG, used only for the diesel and its associated subsystems. The EDG cooling water system is described in Section 9.5.5 of the FSAR [30]. The EDG service water is cooled by the plant-wide service water system by means of a shell (EDG water) and tube (raw service water) type heat exchanger. The MP-3 EDG cooling water system is shown below in Figure 3-7, taken from Figure 9.5.5-1 of the FSAR [30]. Hot water is pumped out of the diesel and is checked for having an excessive temperature, then is split between a water expansion tank (capacity of 5% of total cooling water system) and the shell and tube heat exchanger. This exchanger can be bypassed in order to heat the engine to operating temperatures quickly.

Three water feeds are taken from the expansion tank, and one feed is taken from the heat exchanger. One expansion tank feed is driven by a recirculating pump and mixed with the heat exchanger feed to cool the EDG lubricating oil. This output is mixed with the other two expansion tank feeds, then pump-driven back to the diesel

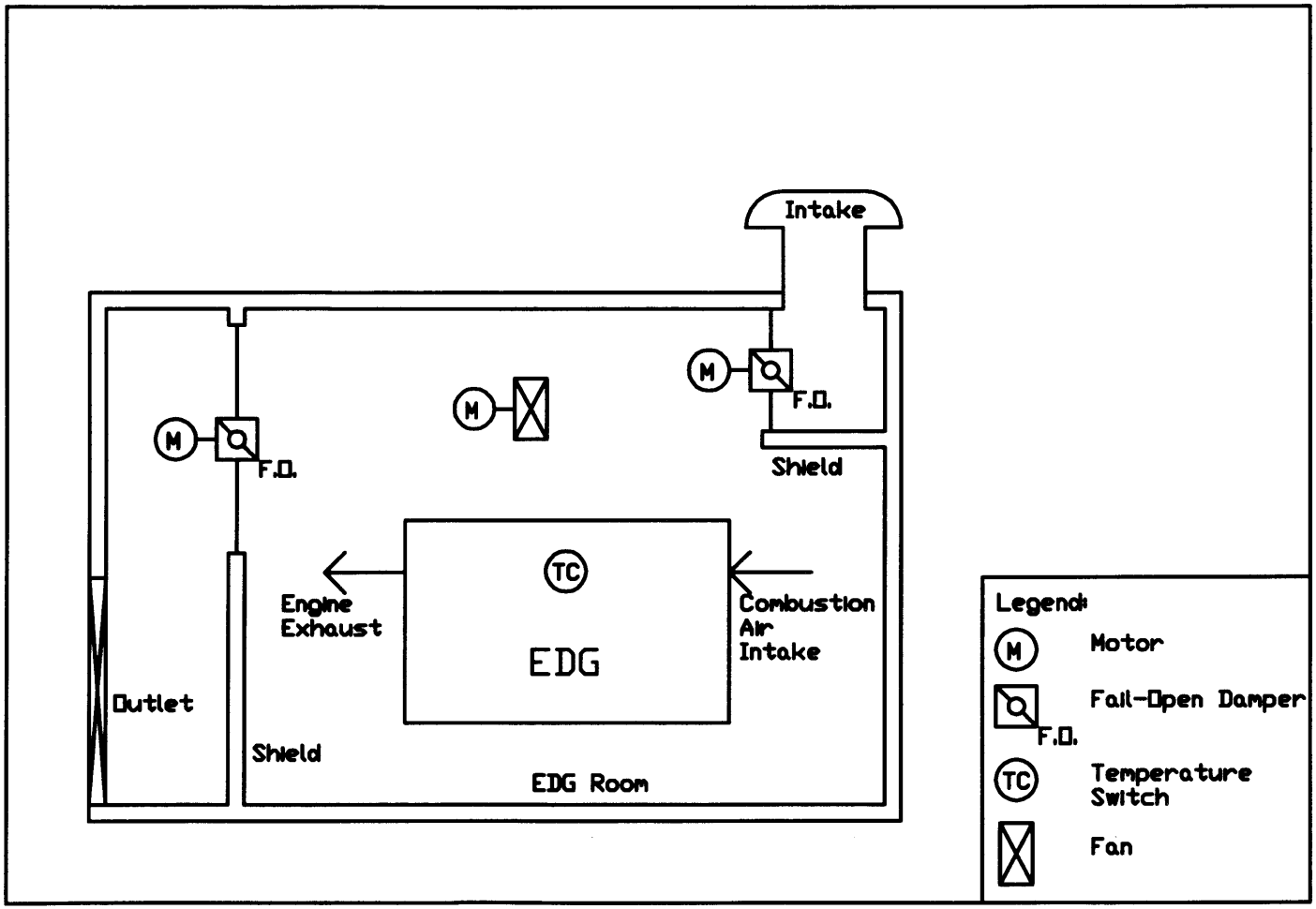


Figure 3-6: EDG Ventilation System

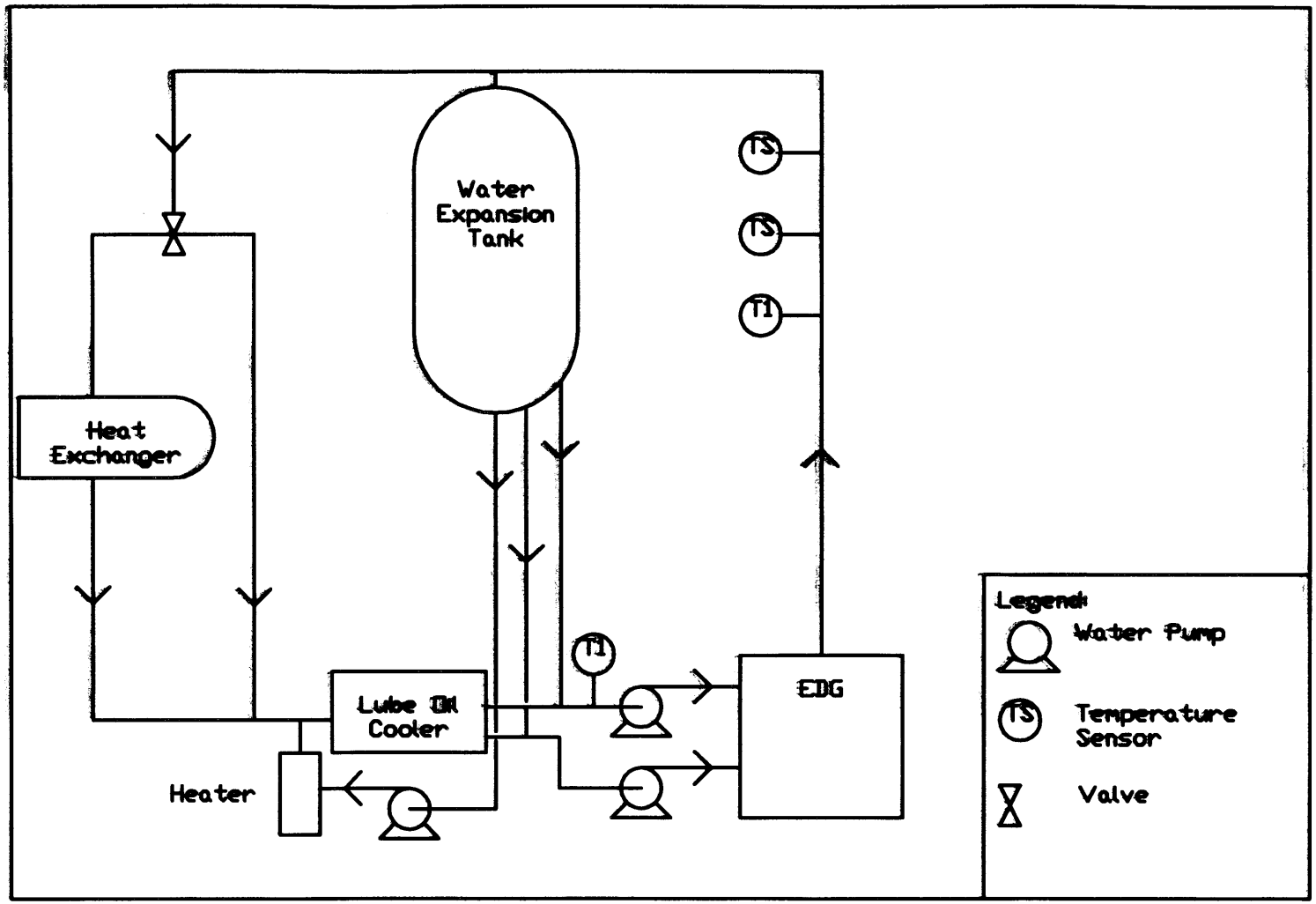


Figure 3-7: EDG Cooling Water System

engine. By this routing method, the lubricating oil can be kept at a lower temperature than the engine jacket, where the cooling water flows.

An electrical heater is also provided to keep the engine warm, as a part of the hot, pre-lubricated starts allowed in Generic Letter 84-15 [18]. The heater in the cooling system is tasked to maintain constant water temperature of 125 degrees Fahrenheit in an ambient environment of 50 degrees Fahrenheit.

3.5.2 Air Systems

There are four air systems that support the EDGs: air start, engine intake, engine exhaust, and crankcase ventilation.

Each EDG has two independent air start systems, described in FSAR Section 9.5.6 [30]. Each system is capable of starting an EDG five times (three times automatically, and twice more manually) before outside power is required at the air compressors to recharge the group of air tanks. Alternately, each system can crank the diesel generator for sixty seconds without recharging. A diagram of the air starting system is shown in Figure 3-8, taken from Figure 9.5.6-1 of the FSAR.

Each independent starting system is comprised of one AC motor-driven air compressor, three air storage tanks, an air-start motor, and valves. The two independent systems are linked by cross-tie, allowing either air compressor to charge both batteries of air start tanks. Each compressor can charge one battery of tanks from minimum starting pressure to maximum starting pressure in thirty minutes.

The remaining air systems are described in Appendix D of the Seabrook PSA [29]. Both engine intake and exhaust pass through the turbocharger (if one is used), or only intake air passes through a supercharger. The intake air is drawn in from the atmosphere, dried and filtered, then passed to the turbocharger or supercharger. The function of these components is discussed below. Engine exhaust is routed through the turbocharger, if present, then through a muffler and into the atmosphere, via weather and projectile-protected dampers, as is building ventilation.

Crankcase ventilation is provided for in the Seabrook PSA by means of crankcase exhaust fans. Crankcase exhaust is utilized for a process known as scavenging,

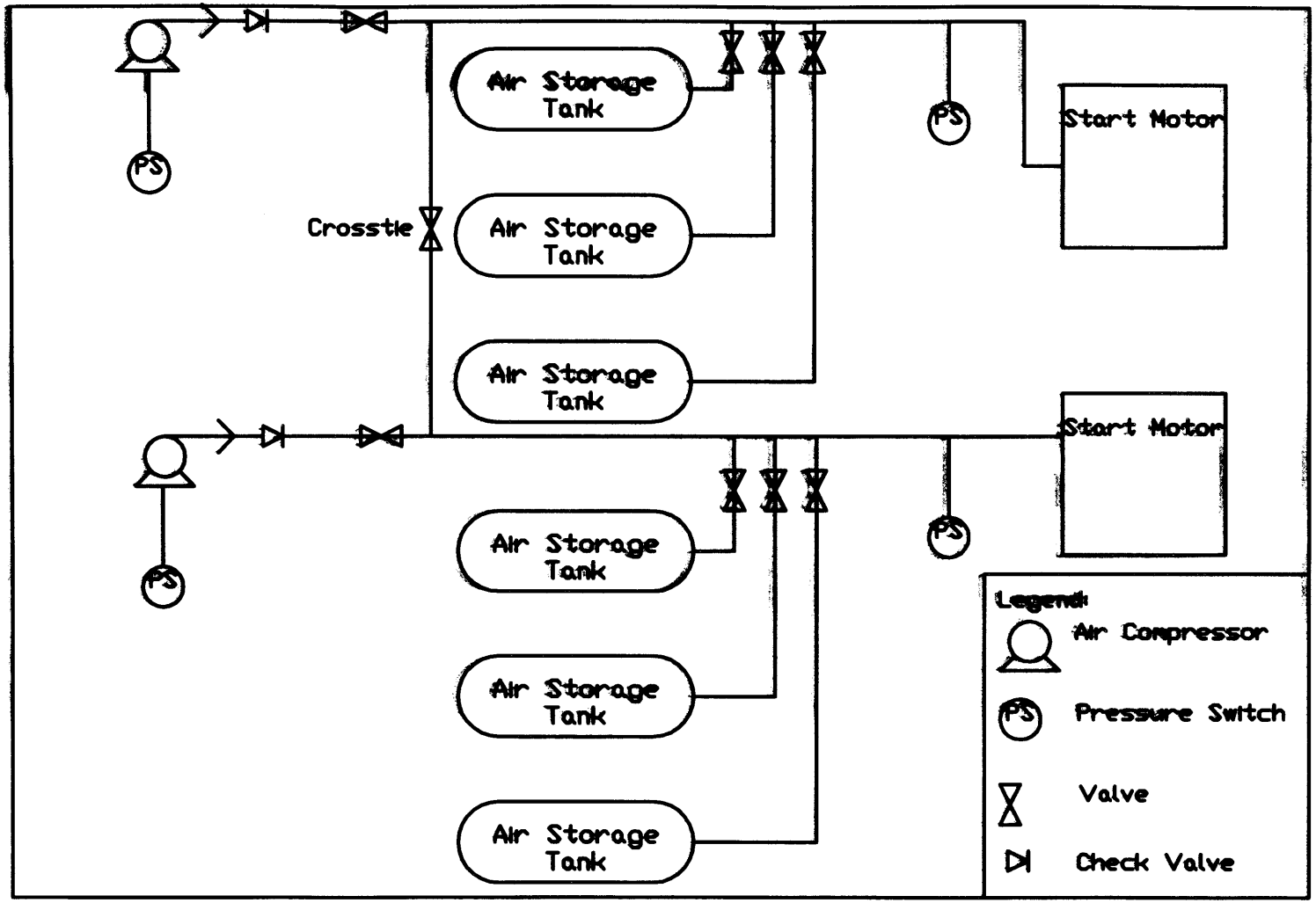


Figure 3-8: EDG Air Start System

whereby the overpressure created beneath the piston by the downward stroke is used to force fresh air into the underpressured combustion chamber to better remove exhaust gases [32]. This also removes any combustible gases from the crankcase which may have slipped past the rings. A failure known as a crankcase detonation can occur in the absence of proper ventilation.

3.5.3 Fuel Oil System

The fuel oil system is describe in FSAR Section 9.5.4 [30]. No. 2 diesel fuel oil is supplied to each EDG by two independent motor-driven fuel pumps, drawing from the dedicated day tank. Each day tank, in turn, is supplied by two independent electric motor-driven fuel transfer pumps from its corresponding storage tank. Each storage tank contains 32,760 gallons (124 kL) of fuel oil, and each day tank contains 550 gallons (2,080 l). The fuel supply in the storage tanks is sufficient for three-and-a-half days of continuous, rated-load operation of both EDGs.

Each day tank contains enough fuel for a one-and-a-half hour run before low level switches activate the fuel transfer pumps. Figure 3-9 shows the fuel flow diagram, taken from Figure 9.5.4-1 of the FSAR.

3.5.4 Lubricating Oil System

Each EDG has its own independent lubricating oil system, described in FSAR Section 9.5.7 [30]. The lubricating oil system is pictured in Figure 3-10, taken from Figure 9.5.7-1 of the FSAR. The lubricating oil is pumped by both engine-driven pumps and by AC motor-driven pumps. Cooling of the oil is discussed under cooling water, above. Filters and strainers are also used to ensure oil quality. Instrumentation is included to monitor engine oil pressures. Low lubricating oil pressure tends to indicate a leak, which would result in a trip of the diesel. Current surveillance practices use lubricating oil as an indicator of the health of the entire engine, by sampling the oil for chemical analysis as any wear, combustion, or contamination products would be present here.

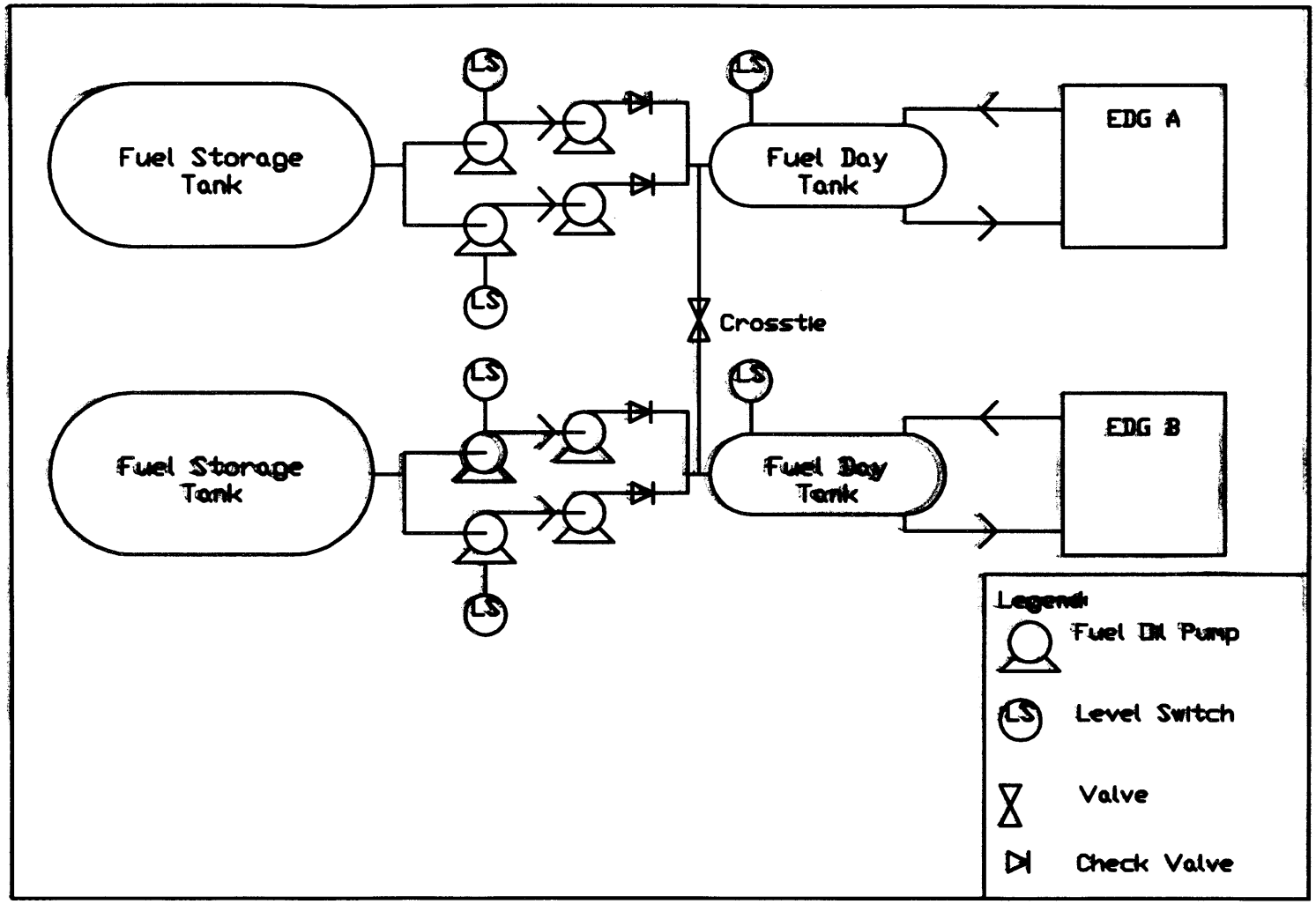


Figure 3-9: EDG Fuel Oil System

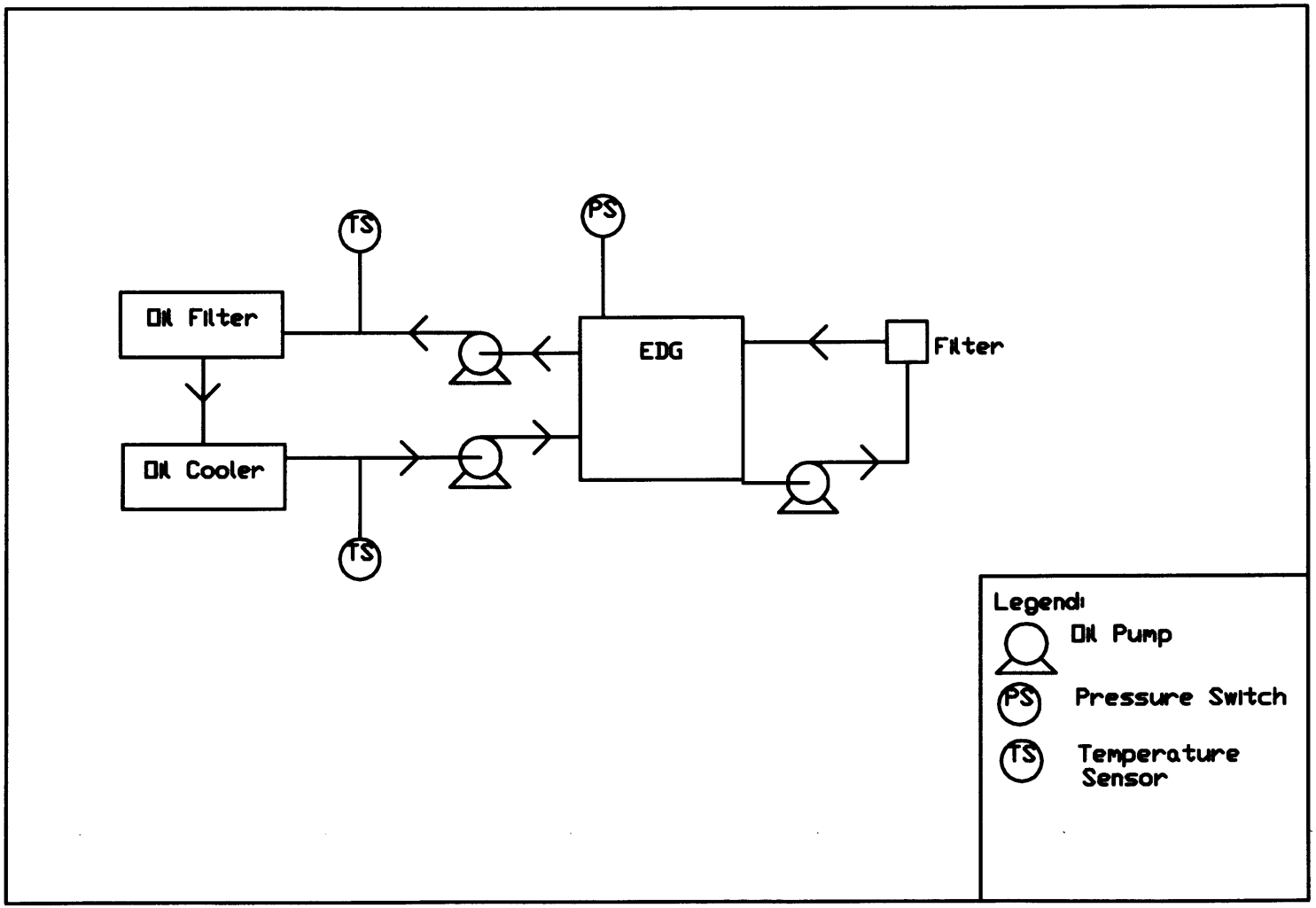


Figure 3-10: EDG Lubricating Oil System

3.5.5 Instrumentation and Control Systems

The instrumentation and control (I&C) systems are described more fully in the next section, on current monitoring systems in place. This report proposes to increase the amount of instrumentation in use of the EDGs. The current I&C are a source of failures for the EDGs, consisting primarily of false trips of the diesels during testing, where sensors falsely report a negative condition which protectively shuts down the diesels. As is discussed below, many of these trips are bypassed in actual emergency situations.

3.5.6 Turbochargers and Superchargers

Each EDG in use at MP-3 has a turbocharger dedicated to it. The turbocharger takes high pressure engine exhaust air, and, as a turbine, extracts mechanical energy from the flow. This energy is used to turn an air pump, which compresses engine intake air drawn from the atmosphere and forces it into the combustion chambers. This use of high-pressure air increases the mass of oxygen delivered to each cylinder, which increases the amount of power which can be generated.

A turbocharger is a specialized form of a supercharger. In general, a supercharger uses some outside energy source, such as an electrical motor or the engine crankshaft to power an air pump, which increases the intake air delivery pressure. A turbocharger is a more efficient type of supercharger, utilizing an otherwise lost power source and gaining extra output from a waste product.

The process of crankcase scavenging also adds a small amount of supercharge to the diesel, by increasing the pressure of air delivery and flushing out burned exhaust gases for replacement with fresh air [32].

3.6 Summary

The EDG is tasked in the electrical power system to provide enough electricity to run all safety-related loads in the event of a loss of offsite power. Other than the diesel

engine itself, included in the scope of the work reported here are the cooling, lubricating, fuel, air, instrumentation & controls, and turbocharger systems associated with the EDG.

Failure data collected from the industry are separated to describe these basic support systems and the components within them.

Chapter 4

Current Monitoring, Maintenance, and Surveillance

4.1 Introduction

The Final Safety Analysis Report [30] and the Probabilistic Safety Assessment [29] describe the current monitoring practices and methods used for EDGs. The monitoring currently in place does not provide the opportunity to trend performance or to carry out preventive maintenance. Generally, the function of the monitoring system is to prevent EDG operation in conditions which could cause severe damage to the EDG train, and to notify plant operators of the status of the generator system.

Maintenance and surveillance are discussed primarily in the STS, and are specific to the manufacturer of the EDG. The maintenance recommendations from the EDG vendors are the same as those for diesels used in marine service and as full-time power-producing units. While EDGs are used in standby service, typically operating about twenty hours per year, the requirements they are held to apply more to engines which run in excess of 8000 hours per year. With no prior experience in standby service, EDG vendors recommended the only procedures they were familiar with and could be sure of. The result is an overly critical inspection procedure which typically finds no wearout of parts and tends to cause more problems than it resolves [5] [8] [33] [34]. The nuclear application also differs from marine applications in the number

of engine starts, and the speed with which the engines are started. Marine diesels are started very infrequently, and rarely in as little as ten seconds, as is required for nuclear plant EDGs.

These and other weaknesses of the current surveillance system are examined in this section as well.

4.2 Monitoring

Monitoring systems currently in place for the EDGs fall into two categories: fault protective devices and annunciated alarms. Fault protective devices are intended to prevent operation of the diesels in a manner which could ultimately do damage to the EDGs. Fault protective devices cause the diesel generator or some associated subsystem to "trip," or to turn themselves off.

An annunciated alarm indicates some element of the status of the diesel generator and its ability to respond to a demand for power. These alarms and devices are identified in the Final Safety Analysis Report and/or the Probabilistic Safety Assessment. The following groups of alarms and devices are found both in Chapter 8.3 of the MP-3 FSAR [30] and in Appendix D of the Seabrook PSA [29].

4.2.1 Annunciated Alarms

There are thirteen alarm functions which are annunciated in the control room for the diesel generators. A lesser subset of these is reported locally, and a different subset is reported to computer controllers in the case of Seabrook. These thirteen annunciated alarms are listed in Table 4.1. Of the thirteen alarms, only one (day tank level low) regards the diesel engine itself, and the other twelve focus on the electrical power production and distribution.

1.	Emergency Generator not Ready for Auto Start
2.	Emergency Generator Auto Start
3.	Emergency Generator Differential Relay
4.	Emergency Generator Emergency Shutdown
5.	Emergency Generator Overvoltage
6.	Emergency Generator Underfrequency
7.	Day Tank Fuel Oil Level Low
8.	Emergency Generator Breaker Auto Close Blocked
9.	Emergency Generator Control - Local
10.	Emergency Generator Local Panel - Trouble
11.	Emergency Generator Overload
12.	Emergency Generator Supply Auto Trip
13.	Emergency Generator Neutral Auto Trip

Table 4.1: EDG Alarms Annunciated in MP-3 Control Room

4.2.2 Fault Protective Devices

There are fourteen conditions under which a trip of the diesel generator or its output breaker results, while the diesel is in "Test" mode. In Table 4.2, any one of the fourteen conditions will trip the air circuit breaker open while testing. Only the first ten conditions will trip the diesel itself while testing.

In the case of low lubricating oil pressure, a two-out-of-three voting system is used to reduce unnecessary diesel engine trips. This means that three oil pressure sensors are installed, and that low pressure must be detected on two of the three before a warning signal is sent.

In the event of a safety injection signal, a containment depressurization actuation, or in the event of a loss of power, only the first three conditions, generator differential, low lubricating oil pressure, and engine overspeed, will automatically trip the diesel generator. In such an emergency demand scenario, the need is to provide power to the emergency shutdown systems. As warning alarms warrant, the operator may choose to shut down the questionable EDG, once another power source has been secured. During an actual demand, any of the eleven bypassed trips will trigger an annunciated alarm in the control room, but will not automatically trip the diesel.

1.	Generator Differential
2.	Lube Oil Pressure Low
3.	Engine Overspeed
4.	Jacket Coolant Pressure Low
5.	Jacket Coolant Temperature High
6.	Lube Oil Temperature High
7.	Ground Overcurrent
8.	Loss of Field
9.	Reverse Power
10.	Voltage Restrained Time Overcurrent
11.	Bus Differential
12.	Load Center Phase Overcurrent
13.	Generator Underfrequency
14.	Generator Overvoltage

Table 4.2: EDG Trip Conditions for MP-3

4.3 Surveillance, Testing, and Maintenance

The testing and surveillance of the EDG systems are established in two places: the technical specifications and the vendor recommendations. The technical specifications are the legal requirements for surveillance which are applied in virtually the same form for every plant in the country. Vendor recommendations are applied more specifically on a plant-by-plant basis, according to the manufacturer of the diesel equipment. The basis for following additional procedures is established in the Standard Technical Specifications [31] in Surveillance Requirement (SR) 4.8.1.1.2.g.1.

Beyond these requirements, additional maintenance and inspection procedures are performed on a plant-by-plant basis. For vendor recommendations and plant-specific maintenance, those of the MP-3 plant are used. MP-3 utilizes two Colt-Pielstick PC2V valved diesel generators, plus one auxiliary Station Blackout generator to satisfy Regulatory Guide 1.155 [17].

Test Number	Tests	Frequency
SR 3.8.1.1	Verify breaker alignment	Weekly
SR 3.8.1.2 SR 3.8.1.3	Start and load DG, Run DG 60 minutes	See Table 4.4
SR 3.8.1.4 SR 3.8.1.5	Verify day tank fuel level and remove water	Monthly
SR 3.8.1.6	Verify fuel transfer system	Quarterly
SR 3.8.1.7	Start, load DG in 10 seconds, Run 60 minutes (satisfies 3.8.1.2)	Bi-annually
SR 3.8.1.8 to SR 3.8.1.13	Verify power transfer, load rejection, high-power trips, LOOP and ESF start	Refuel outage (currently every 18 months)
SR 3.8.1.14	24 hour DG run	Refuel outage
SR 3.8.1.15 to SR 3.8.1.19	Verify restart, recovery, sequencing, and ESF with LOOP	Refuel outage
SR 3.8.1.20	Verify independence	Decennially

Table 4.3: Surveillance Requirements for MP-3 EDGs

Number of failures in last 25 tests	Test Period
≤ 3	31 days
≥ 4	7 days

Table 4.4: EDG Test Schedule According to Technical Specifications

4.3.1 Standard Technical Specifications

The surveillance and testing requirements are found in the Standard Technical Specifications, specifically SR 3.8.1.1 through 3.8.1.20. A summary of these requirements is presented in Table 4.3.

The STS also include surveillance requirement bases to further detail these tests. Breaker alignment is checked to verify that offsite electrical power is available to the onsite distribution network. Start and run tests are conducted to verify the availability and performance of the EDGs. The sixty minute run time is said to stabilize engine

Number of failures in last 100 tests	Test Period
≤ 1	31 days
2	14 days
3	7 days
≥ 4	3 days

Table 4.5: MP-3 EDG Test Schedule, Recommended by RG 1.108

temperatures, while minimizing run time. The frequency of diesel generator run tests is determined by the number of failures to start which have occurred in the last 25 valid tests. The frequencies are given in Table 4.4.

It is proposed in Regulatory Guide 1.108 [14] to modify these frequencies and the interval over which they are determined. Table 4.5 shows RG 1.108 recommendations for testing frequency based on the number of failures in the last 100 valid tests. RG 1.108 also establishes the current basis for distinguishing a valid test from an invalid test. These criteria are discussed further under the section on operating experiences.

Fuel tank tests establish that sufficient fuel is available to allow a one-hour, full-power run of each EDG in the event of a fuel-transfer failure. Water is removed from the tanks in order to reduce the risk of microbiological fouling and water entrainment into the fuel oil system. A separate test insures performance of the fuel-transfer system.

During refueling outage, several tests are conducted to verify the status of the emergency power system, including automatic and manual transfer of offsite power from the usual circuit to the reserve circuit, rejection of large loads, operation of the EDG at high loads, including load rejection, LOOP load shedding and automatic starting, Engineered Safety Feature (ESF) starting and sequencing, return of EDG to ready-to-load operation under ESF, and operation under combined LOOP and ESF conditions.

One group of refuel outage tests focus on the diesel engine itself, including a twenty-four hour run, a hot restart of the diesel within ten seconds, bypass of non-critical DG trips under combined LOOP and ESF, and recovery of loads to offsite

power.

4.3.2 Vendor Recommendations

The vendor recommendations discussed below are those as applied to the EDGs in use at the MP-3 plant, supplied by Colt-Pielstick.

The supplemental maintenance instructions include daily, weekly/biweekly, quarterly, refuel, and two-to-three-year instructions. The refuel outage instructions are of particular interest, and are listed below in Table 4.6. The remainder of the instructions are as follows.

On a daily basis, oil levels in the turbochargers, sumps, outboard bearings, governor, and air systems are checked; temperatures of lubricating oil and water are compared to a defined minimum; jacket water surge level is verified; and the control panel is verified to show no annunciated alarms.

On a weekly/biweekly basis, rocker pre-lubrication pumps are operated, fuel racks are exercised, control power is verified, fuel tanks and the engine systems are inspected for leakage, and generator brushes are checked for arcing.

Quarterly, auxiliary systems are to be serviced, jacket water and lubricating oil are sampled, seals are checked for leaks, and rockers are randomly selected for examination.

During refuel outage, the steps listed in Table 4.6 are carried out, which make up an intrusive teardown inspection. These are the steps which can largely be replaced with increased monitoring and engine analysis. In the section on proposed monitoring, relevant monitoring to eliminate each problematic step of this process are identified.

During alternating refueling outages, it is recommended to check backlash of the gear train, to test fuel control leakage pins for tightness, and to remove and repair one pair of exhaust valve cage assemblies.

4.3.3 Plant Inspection and Maintenance

In addition to the requirements listed above, there are additional Maintenance Procedures carried out by MP-3 personnel. These are taken from maintenance forms specific to MP-3, but with content typical of other EDGs from various manufacturers [8].

On a weekly basis, each engine is wiped down and inspected for leaks. The control panel is cleaned, and all combustibles are removed from the diesel room.

Each month, all sacrificial zinc anodes in water jackets and intercoolers are replaced, checks are made for marine fouling and chafing, and fuel racks and controls are lubricated.

Annually, outlet piping and the exhaust system are checked for corrosion, and the pre-lubrication oil pump strainer is cleaned.

During each refuel outage, lube oil analysis is reviewed for significant variance, and all Colt Service Information Letters are reviewed. These letters are additional recommendations based on experiences or concerns which have arisen after the general recommendations were issued. Crankcase covers, oil connections, balance weights, thrust clearance, oil separators, and O-rings are checked. Turbocharger discharge bolts and pipe connections are checked for tightness. The heat exchangers are checked for corrosion, and fuel injection pump hold down bolts are tested. Lubricating oil, fuel oil, and air filters are checked for cleanliness, and oil strainers are cleaned.

As data to be presented show, these support systems are highly critical for diesel reliability, and these additional procedures should be retained, as they are not overly intrusive while providing necessary testing.

4.4 Review of Surveillance Effectiveness

The surveillance of the EDGs is described in Section 4.3.1. The basic surveillance procedures for the EDGs are a one-hour run once per month (more frequently for previous failures) and a twenty-four-hour run during each refueling outage, currently every eighteen months.

1.	Perform all weekly, monthly, and annual procedures.
2.	Remove and check injection nozzles for operation and opening pressure.
3.	Remove, disassemble, clean, and repair all air start valves and air start distributors. Clean/replace air start distributor filter.
4.	Drain and refill governor and turbochargers with approved oil.
5.	Drain, flush, and refill outboard bearing with approved oil.
6.	Check tightness on all foundation, block to base, and oil and water line bolts.
7.	Check sample of rocker lube oil for condition and contaminants.
8.	Check turbocharger inlet casing and turbo casing water passages for scale. The inside surface of these casings is the best indication for adequacy of water treatment.
9.	Check for tightness of exhaust manifold flange bolts to cylinder head (165-195 foot-pounds).
10.	Check all safety and shutdown controls for appropriate pressures and temperatures.
11.	Borescope all cylinder liners.
12.	Inspect the crankcase end of all cylinder liners.
13.	Check main bearing cap tightness (9950-11000 psi hydraulic) and side bolts (hammer tight). Alternately confirm cap tightness to frame and saddle to 0.0015 in. feeler gauge.
14.	Visually examine gear train and drives, cam shafts and bearings, push rods and rocker arms.
15.	Check crankshaft alignment and bearing clearances.
16.	Check connecting rod bearing clearances with feeler gauge.
17.	Inspect all ledges and corners in crankcase for debris which could indicate other mechanical problems. Confirm all cotters, safety wire, and lock tabs are in place and tight.
18.	Water test engine and inspect for internal and external leaks. Isolate jacket water surge tank and test entire systems at 40 psi. After engine is restored to operation and has reached normal operating temperature, remove each rocker cover and inspect for water leaks at top area of cylinder head.
19.	Check alternator coils and poles for indication of movement (visual).
20.	Drain and refill alternator bearing lube sump. If oil has contaminants, pull bearing cap and inspect journal.
21.	Inspect and clean (if required) overspeed trip mechanism. Check operation according to overspeed trip test instructions.

Table 4.6: Vendor Recommendations for Refuel Outage Inspections [2]

In the INEL report [5], Regulatory Guide 1.108 [14] positions on the effectiveness of these surveillances are discussed. The function of the tests conducted during refueling outages, referred to as "cyclic" tests, are listed in Table 4.7. The cyclic tests very closely simulate actual demands of the EDG, including the method of starting the diesel, the duration of the diesel run, the loading of the generator, and the functioning of the sequencer circuits. As a result of the thoroughness of the cyclic test, the EDG train unavailability can effectively be set back to zero (no remaining offsets) after a cyclic test.

The major objection to the current cyclic test is that it is conducted after the lengthy and intrusive inspection described in Table 4.6. As such, it does not provide much information about the condition of the diesel over the previous eighteen months. However, it effectively verifies the reliability of the EDG train for the next cycle, and it tests the diesel through the "infant mortality" period (when failures may be more frequent) following the rebuild, when the EDG is most likely to fail due to maintenance or restoration errors.

1.	To start the EDG by the safety features actuation system (SFAS) signal and verify the start circuits.
2.	To test the EDG sequencing circuits for loss of offsite power and SFAS loading schemes and time intervals and loading of actual loads to the maximum extent possible without damaging plant systems.
3.	To demonstrate the EDG operates for 24 hours, during which the first 2 hours the diesel generator is loaded to the maximum rated load, and the following 22 hours is loaded to the rated load.
4.	To demonstrate the EDG can reject the largest load without tripping.
5.	To satisfy other technical specifications testing requirements.
6.	To verify the EDG will start from an auto-start signal within 5 minutes of its shutdown following the 24-hour run while simulating a loss of offsite power in conjunction with a SFAS signal.

Table 4.7: Functions of the Cyclic (18-month) Test

In contrast to the cyclic tests are the monthly surveillance tests. The functions of the monthly test are listed in the first column of Table 4.8. The monthly tests are basically useful for verifying the availability of support systems, such as control power, fuel delivery, and EDG building ventilation. They do not simulate realistic starting, loading, or running practices. The EDG does not have to exceed 50% of its rated load to pass the surveillance test. As such, the monthly tests are not effective for completely restoring the unavailability of the EDG train to zero. The second column of Table 4.8 lists the basic failure events from the fault tree which are completely reset, and the third column lists the basic events which are only partially reset. These events are listed in Table A.1 in Appendix A. Events listed in pairs, such as "19/20," represent cases where two independent systems, such as fuel transfer pumps, are used, but only one is used in a given test. This suggests that only one of these failure rates is reset to zero in testing.

Some failure events are defined for twenty-four-hour run times, so they can not be completely assessed with a one-hour test. There is also the special case of initiating events. Initiating events (events 1-12 on the basic event list in Appendix A) are events external to the EDG train, but which have the ability to disable the EDG. Primarily, these are failures of the service water supply system and the control power system, shown outside the EDG boundary in Figure 3-2. These are not standby systems, but systems which operate on a full-time (8760 hours per year) basis. The surveillance verifies that these failures have not occurred, so their contribution to EDG failure rates can be set to zero immediately following an EDG test.

To assess the effectiveness of surveillance tests which leave offsets in the unavailability after testing, the failure rate λ can be redefined as the sum, or superposition, of two smaller failure rates. The failures which are reset by monthly surveillance tests can be represented by the failure rate λ_M. The failures which are not reset by monthly surveillance tests, but by cyclic tests, can be represented by λ_C. With the superposition definition, while the monthly and cyclic failures are independent, the

Function	Events Fully Tested by Monthly Tests	Events Partially Tested by Monthly Tests
To verify that the EDG starts slow from a manual signal and accelerates to rated or idle speed and attains generator voltage and frequency (engine prelubrication is permitted)	38, 69	
To verify operability of at least one of many diesel fuel oil transfer pumps	19/20, 53/54, 56/58, 70, 71	55/57
To verify quantities in the diesel fuel oil day tank and storage tank		64, 65
To verify after the EDG is synchronized that it loads to rated power and operates with this load for a period of at least 60 minutes		39
To verify that all interlocks of the service cooling water or radiators cooling system will start automatically if it is not already running when the EDG starts	89-92, 101, 102	
To verify the normal "standby status" lineup of the EDG and its supporting auxiliary systems upon completion of this surveillance test		
Ventilation:	22, 23, 36, 37, 40-43, 46, 47, 49, 50, 67	45, 48
Service Water:	81, 81, 83, 84, 97-100, 103, 105, 106, 108	82, 104, 107
Control Power:	79	14-16, 18, 26-29, 66, 72-78
Initiating Events:	1-4, 6-12	

Table 4.8: Functions of and Basic Events Interrogated by the Monthly Test

total failure rate λ is represented in Equation 4.1.

$$\lambda = \lambda_M + \lambda_C. \tag{4.1}$$

At the end of a monthly surveillance, the failures which have been reset (λ_M) do not contribute to the overall unavailability. So, the unavailability at the end of each monthly test (the offset values) is defined by λ_C. This λ_C is the same as the λ_C introduced in Equation 2.14.

To evaluate the values for these failure rates, consider the fault tree and the failure events for the period of time immediately after the surveillance test has ended. At that exact moment, any event which has been reset to zero by the test can be considered to have a failure rate of zero. For example, the EDG building ventilation fans were just running, so there is almost no chance of them failing to run if they were demanded again. It is only as time passes without testing that the unavailability grows.

One complication to this method is that some failure modes are only partially reset, those listed in the third column of Table 4.8. These events are evaluated in the PRA for twenty-four operation. The fact that the train ran successfully for one hour reduces the failure rate, but not completely. The INEL report includes a method for determining when failures occur.

The INEL report includes the definition of a time-dependent failure rate for the EDG trains. The proposed values for the per hour failure rate of the train to run are $\lambda_{0-0.5hours} = 2.5E-02$, $\lambda_{0.5-14hours} = 1.8E-03$, and $\lambda_{14-24hours} = 2.5E-04$. This result is shown in Figure 4-1, where the failures observed in the LER data are normalized by the total number of failures observed within twenty-four hours. The plotted line represents the cumulative fraction of failures expected at each point in time, for one day. As the mission is defined in the PRA is a twenty-four hour run, failures which occur after twenty-four hours are rare, but not of interest within the analysis.

From Figure 4-1, it can be observed that after one hour, only 34.5% of failures have occurred. This is useful in assessing the effectiveness of the monthly surveillance.

For the events listed in the third column of Table 4.8, only 34.5% of failures which are anticipated in twenty-four hours would be observed within one hour. So, while the failure rates of these events can't be reset to zero at the end of the hour-long run, they can be reduced by 34.5%.

To evaluate the new failure rates, λ_C and λ_M, the basic events affected by monthly testing (Table 4.8) are re-evaluated. The top event failure rate for the EDG fault tree is recalculated with "end of test" values for the events in Table 4.8. At the end of a monthly test, the failure rates of all the basic events listed in the middle column of Table 4.8 are reset to zero (as they have just been demonstrated to be operating correctly). The failure rates of the basic events listed in the third column of Table 4.8 are not reset to zero, but are reduced by 34.5%, as the one-hour test could not fully verify their operability. These new values are used in place of the values in Table A.1, and the logic of the fault tree is used to calculate a new top event probability.

The new top event failure rate found is 0.033. This failure rate is λ_C, as it represents the part of the failure rate *not* reset by a monthly test; only a cyclic, twenty-four-hour test can reset the failure rate to zero. From the fault tree in Appendix A, the top event probability, λ, is calculated to be 0.097 per year. λ_M can be calculated as 0.064 per year from Equation 4.1. This suggests that 66% of failures (and 66% of the failure rate) are reset by monthly tests. Using these values, the unavailability of the EDG system can be accurately assessed with the equations already defined.

Figure 4-2 shows the same concepts as the sample figure, Figure 2-3, but uses the actual values of the failure parameters. The testing periods are not shown in Figure 4-2, because, with unavailability values of unity, they are significantly off the scale of the figure.

From Figure 4-2, the average unavailability can be evaluated with Equation 2.14, repeated in Equation 4.2.

$$\langle Q \rangle = \frac{1}{t_C} \cdot \left(\frac{\lambda t_S^2}{2} + \tau + f_R t_R + Q_0 t_S\right) + \lambda_C \cdot (n-1) \cdot \frac{t_S^2}{2 \cdot t_C}. \tag{4.2}$$

To evaluate $\langle Q \rangle$, the values $t_S = 730hrs$, $\tau = 1hr$, $f_R = 0.26$ [21], $t_R = 23.3hrs$ [21],

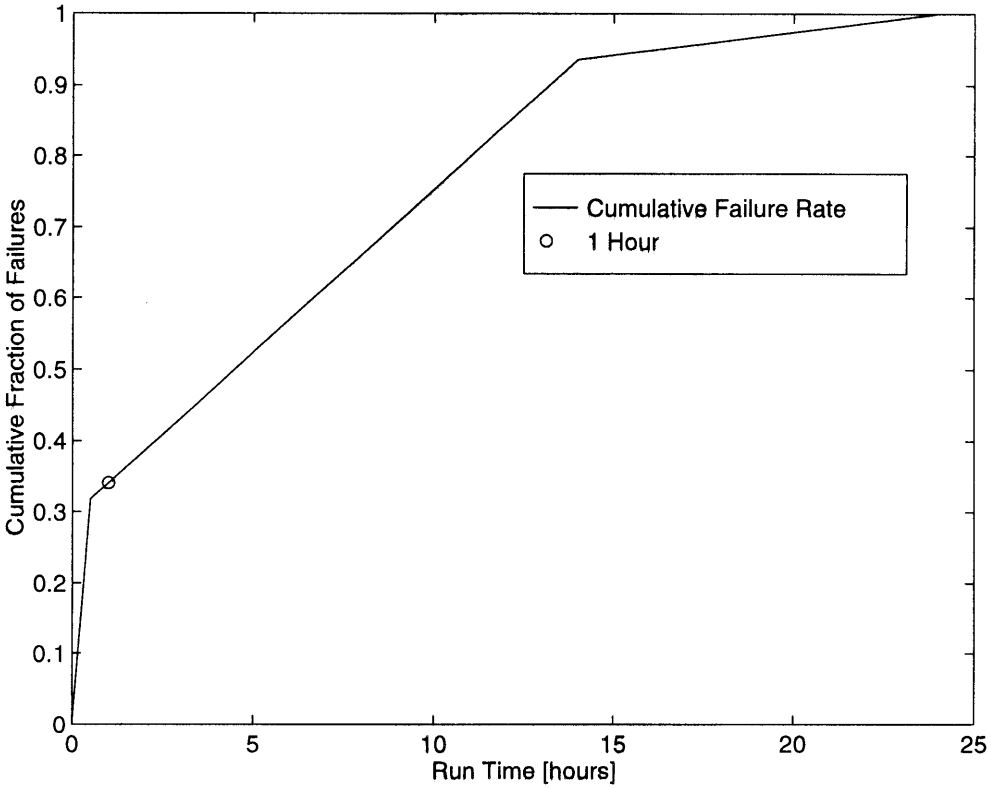


Figure 4-1: EDG Train Failure Rate with Time

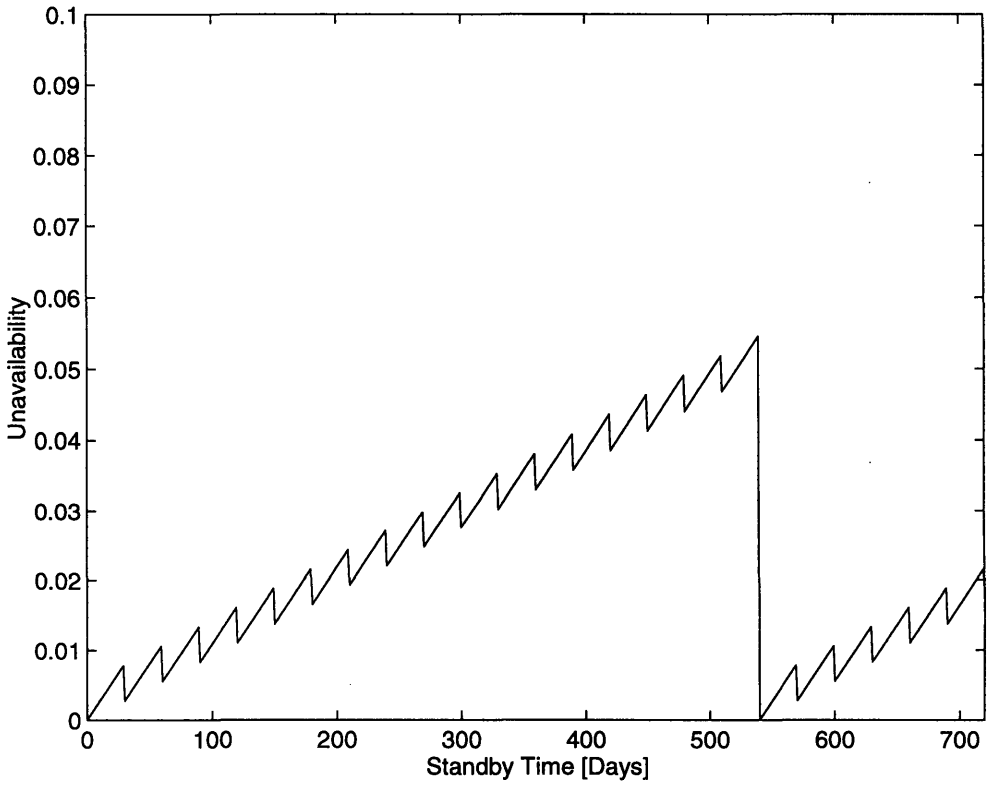


Figure 4-2: Unavailability of an EDG Train Showing Effects of Monthly and Cyclic Testing

$n = 18$, $\lambda_C = 0.033/yr$ or 3.77 E-06/hr, and $\lambda = 0.097/yr$ or 1.1 E-05/hr are used. The cycle time is, as defined in Equation 2.10, is calculated in Equation 4.3.

$$t_C = t_S + \tau + f_R \cdot t_R = 737 hours \tag{4.3}$$

Equation 4.2 yields a value of $\langle Q \rangle = 0.034$ over the eighteen month cycle between twenty-four-hour diesel tests. This corresponds to a reliability of 96.6%, which is acceptable by the standards of the Technical Specifications. However, 60% of the observed unreliability is due to the failure of monthly tests to test all failure modes. This is where room for improvement exists.

4.5 Summary

Current monitoring of the two EDG trains includes electrical performance warnings for the generator segment of the EDG, with the only alert specific to the diesel engine itself being a fuel tank level warning (part of a support system). No significant trending of EDG system performance is available. Other instrumentation can shut down a diesel under adverse conditions to prevent further damage, but offers no preventive maintenance opportunities.

Current surveillance and testing procedures stipulate a monthly one-hour run, and a twenty-four-hour run during each refueling outage. The monthly one-hour runs are not sufficient to completely reset the unavailability to zero. Vendor recommended maintenance includes a highly intrusive inspection and tear-down during refueling outage which can be replaced through increased monitoring.

Chapter 5

Failure Data

5.1 Introduction

To develop a monitoring system for the EDG and its support systems, the major EDG failure modes must be identified. The basic model of the EDG failure modes is taken from the MP-3 PRA. The fault tree is analyzed using minimal cutsets to identify the major contributors to the EDG failure rate. However, most of the EDG support systems are grouped together with the diesel engine as the "EDG supercomponent." In order to separate the failures of the EDG from the support systems, data from four sources are used. The data used come from the INEL report *Emergency Diesel Generator Power System Reliability 1987-1993* [5], the SwRI report *Surveillance, Monitoring, and Diagnostic Techniques to Improve Diesel Generator Reliability* [4], the Nuclear Plant Reliability Data System [6], and from U.S. Navy EDG reliability studies [7]. When each data source is presented, the scope of failures considered is discussed, as are discrepancies between the reporting requirements for the different sources.

The data sources used have significantly different sample sizes, and the fault tree uses rates, not absolute numbers of failures. In order to unify the data presentation, all data are normalized and presented as a percentage of failures which have been observed.

5.2 Fault Trees

The full fault trees for one EDG train at MP-3 are presented in Appendix A, along with a list of all basic events and a risk ranking of the minimal cutsets. The major EDG failure rate contributors are found and ranked, using minimal cutsets.

The top event of the fault tree is "Failure to Provide Power to Bus Via Diesel Generator A." The top event failure rate is calculated to be $\lambda = 0.097$ per year, or just under a 10% chance of failure per year. The first level of contributors to this failure rate are service water failures (36%); failure of the output breaker to close, which includes failure of the EDG to start and run (24%); failure of EDG ventilation (22%); EDG unavailability due to maintenance or testing (11%); and an assortment of smaller failures, totaling 7%. The failure of the fuel oil system, for example, only contributes 0.5% to the EDG failure rate.

The EDG fault tree consists of 121 basic events, most of which are used several times each through a network of nearly 100 logical operators. For such a complex system, the use of minimal cutsets (MCS) is the most efficient way to analyze the fault tree. Commercial software packages for handling fault trees can automatically generate lists of minimal cutsets. Part of this list of MCS is included in Appendix A, Table A.2.

Some of the minimal cutsets (such as MCS_1 through MCS_9 in Table A.2) are single event cutsets, like the alternator in the headlight example. The failure of any one of these components fails the entire EDG system. For these components, the Fussell-Vesely value is simply the failure rate of that component, divided by the total failure rate, 0.097 per year. Any component which is a minimal cutset by itself cannot participate in any other cutset. For example, the combined failure of the alternator and one headlight is a redundant case; the failure of the alternator is enough to fail the entire system on its own.

Components which are not minimal cutsets by themselves can participate in several cutsets, slightly complicating the Fussell-Vesely calculations, as shown in Equation 2.5. As an example, the event "Service Water Pump SWP1A OOS (Out of

Service) for Maintenance," number 103 on the list of basic events in Table A.1, participates in four of the minimal cutsets in Table A.2: MCS_{10}, MCS_{86}, MCS_{96}, and MCS_{97}. The failure rates for these cutsets are $P_{MCS_{10}} = 1.54E-03$ per year, $P_{MCS_{86}} = 6.75E-06$ per year, $P_{MCS_{96}} = 4.22E-06$ per year, and $P_{MCS_{97}} = 4.09E-06$ per year. The Fussell-Vesely value for the service water pump out of service failure is

$$FV_{103} = \frac{P_{MCS_{10}} + P_{MCS_{86}} + P_{MCS_{96}} + P_{MCS_{97}}}{\lambda}, \tag{5.1}$$

or,

$$FV_{103} = \frac{(1.54E-03) + (6.75E-06) + (4.22E-06) + (4.09E-06)}{0.097} = 0.016. \tag{5.2}$$

This calculation can be repeated for each basic event. The twenty basic events with the highest Fussell-Vesely values are ranked in Table 5.1. The events for which monitoring is proposed in the work reported here are also indicated. Table A.1 in Appendix A lists the Fussell-Vesely values for all basic failure events.

Each of the events listed in Table 5.1 participates in single-event cutsets except for events 11, 12, and 103. The probability of a single event cutset is the same as the probability of that single event. For the single-event cutsets, the Fussell-Vesely value is the same as the percent contribution of that basic event to the top event probability. For example, event 10, listed in Table 5.1, has a Fussell-Vesely value of 0.294. This means that these service water pump failures cause 29.4% of the EDG system failures.

For events which participate in multiple-event cutsets, the contribution of that event to the top event probability is more complicated. For events 11, 12, and 103, treating these events as though they were single-event cutsets would increase their individual contributions because they can occur together in the same cutsets. This would incorporate a certain amount of "double counting," and thus simply totaling the three Fussell-Vesely values would overstate their actual contributions. By adding the probabilities of the *cutsets* in which these events participate, the total percentage

Event #	Event Name	Description	FV	Monitor?
10	%SWP3IPMACFN	SW Pumps	0.294	Y
39	ACADG3EGSANN	EDG FTS	0.172	Y
38	ACADG3EGSAAQ	EDG MOOS	0.116	Y
25	ACABKLSHEDNN	Load Shed	0.050	N
40	ACADMDM20ANN	Damper	0.042	Y
41	ACADMDM20CNN	Damper	0.042	Y
42	ACADMDM23ANN	Damper	0.042	Y
43	ACADMDM26AFF	Damper	0.042	Y
12	%SWP3ISW1CFN	SW Pump	0.029	Y
13	ACAAVAV39ANN	Valve	0.021	N
81	HVADAAD23ANN	Damper	0.017	Y
103	SWAP3SWP1AAQ	SW Pump MOOS	0.016	Y
11	%SWP3ISW1AFN	SW Pump	0.014	Y
69	ACCDG3EGSXNN	EDGs CCF	0.012	Y
17	ACABK34C1TNN	Breaker	0.010	N
31	ACACP27R56FF	Contact Pair	0.009	N
33	ACACP62V13FF	Contact Pair	0.009	N
34	ACACP62W15FF	Contact Pair	0.009	N
36	ACACPCA1B1FF	Contact Pair	0.009	N
37	ACACPCC1D1FF	Contact Pair	0.009	N

Table 5.1: Fussell-Vesely Risk Importance Values for Risk Sensitive Components

contribution of events 11, 12, and 103 is found to be 0.044, or 4.4%.

The events listed in Table 5.1 can be further condensed into groupings by EDG support system. By totalling the contributions of all service water pump events, events 10, 11, 12, and 103, the total contribution of service water pump failures to the EDG failure to start is found to be 0.338, or 33.8%. Similarly, the EDG supercomponent contribution, found by totalling the contributions of events 38, 39, and 69, is 0.3, or 30%. Ventilation dampers failures, events 40 through 43 and 81, total 18.5%. Power output and sequencer failures, events 17 and 25, total 6%, contact pair closure (instrumentation) failures, events 31, 33, 34, 36, and 37, total 4.5%. Service water valve failures, event 13, contribute 2.1%. Collectively, these top twenty events contribute 94.9% of EDG system failure risk.

The EDG failures include those of all the support systems described in Chapter 3. The use of EDG supercomponent failure data allows the further resolution of EDG failures.

5.3 Idaho National Engineering Laboratory Analyses

As a part of the licensing requirements of nuclear power plants, all utilities are required to submit a Licensee Event Report to the NRC after any failure of any safety-related plant system. The utilities are only required to submit LERs when such a system or component fails to carry out its intended function. For a standby system such as the EDG, failures to perform in an actual emergency demand or in a test conducted to satisfy Technical Specifications must be reported as LERs. Any failures which are detected and repaired while the system is in a standby mode need not be reported.

The INEL report *Emergency Diesel Generator Power System Reliability 1987-1993* [5] uses EDG-related LERs reported between January 1987 and December 1993. A total of 353 EDG-related records were analyzed, using only the data from plants reporting under the directions of Regulatory Guide 1.108. An additional 92 failures

were listed for cases not encompassed by RG 1.108. These records do not include any failures reported for one-hour run-time, monthly surveillance tests. As is described in Section 4.4, the monthly tests do not accurately simulate actual EDG demands. For this reason, the failure rates presented only focus upon actual EDG demands and upon the more realistic twenty-four-hour tests performed during refueling outages. Appendix B lists the plants which were considered in the INEL study, with details regarding the EDG systems used at each plant.

The data as presented in the INEL report are presented numerically in Table 5.2, and the non-RG 1.108 data are presented in Table 5.3. These two sets are summed graphically as a bar chart in Figure 5-1. All percentages presented are percentages of the *total* failure rate for the EDG train. For example, the fuel oil system accounts for 26.3% of all failures from RG1.108-reporting plants. This is the sum of the contributions of the governor (14.4%), fuel leaks (3.4%), and all other fuel oil problems (8.5%).

Table B.2 in Appendix B lists the reactors for which data were assessed in the INEL study, as well as in the SwRI report [4] and in the NPRDS database. The EDG systems at each reactor, as well as the EDG manufacturers, are listed where available.

These data demonstrate that electrical and instrumentation systems cause the greatest number of EDG failures. The fuel system is also a major contributor to the failure rate. Most of these fuel system failures are attributable to problems with the engine governors, which are primarily mechanical. Digital governors are available today, but are not frequently used on nuclear power plant EDGs. The mechanical diesel engine itself only contributes about five percent of the total failure rate.

5.4 Southwest Research Institute

The data used in the report *Surveillance, Monitoring, and Diagnostic Techniques to Improve Diesel Generator Reliability* [4] are taken from Licensee Event Reports, as are the INEL report data. The SwRI report uses LERs reported between January 1968 and September 1982. A total of 689 records were analyzed. The data are presented

System	Subsystem	Failures
I&C	**Total**	**26.3%**
	Trips	20.7%
	Other	5.6%
Fuel	**Total**	**26.3%**
	Governor	14.4%
	Leaks	3.4%
	Other	8.5%
Electrical	**Total**	**24.1%**
	Voltage Regulator	15.6%
	Output Breaker	5.1%
	Sequencer	1.7%
	Generator	1.1%
	Other	0.6%
Cooling Water	**Total**	**7.4%**
Diesel Engine	**Total**	**5.7%**
Lube Oil	**Total**	**5.1%**
Air Start	**Total**	**4.8%**
Ventilation	**Total**	**0.3%**

Table 5.2: INEL Data for Cases Covered by RG 1.108

System	Subsystem	Failures
I&C	**Total**	**44.6%**
	Trips	6.5%
	Other	38.1%
Fuel	**Total**	**19.6%**
	Governor	10.9%
	Leaks	1.1%
	Other	7.6%
Electrical	**Total**	**17.4%**
	Voltage Regulator	5.4%
	Output Breaker	5.4%
	Sequencer	2.2%
	Generator	1.1%
	Other	3.3%
Cooling Water	**Total**	**8.7%**
Diesel Engine	**Total**	**2.2%**
Lube Oil	**Total**	**2.2%**
Air Start	**Total**	**3.1%**
Ventilation	**Total**	**2.2%**

Table 5.3: INEL Data for Cases not Covered by RG 1.108

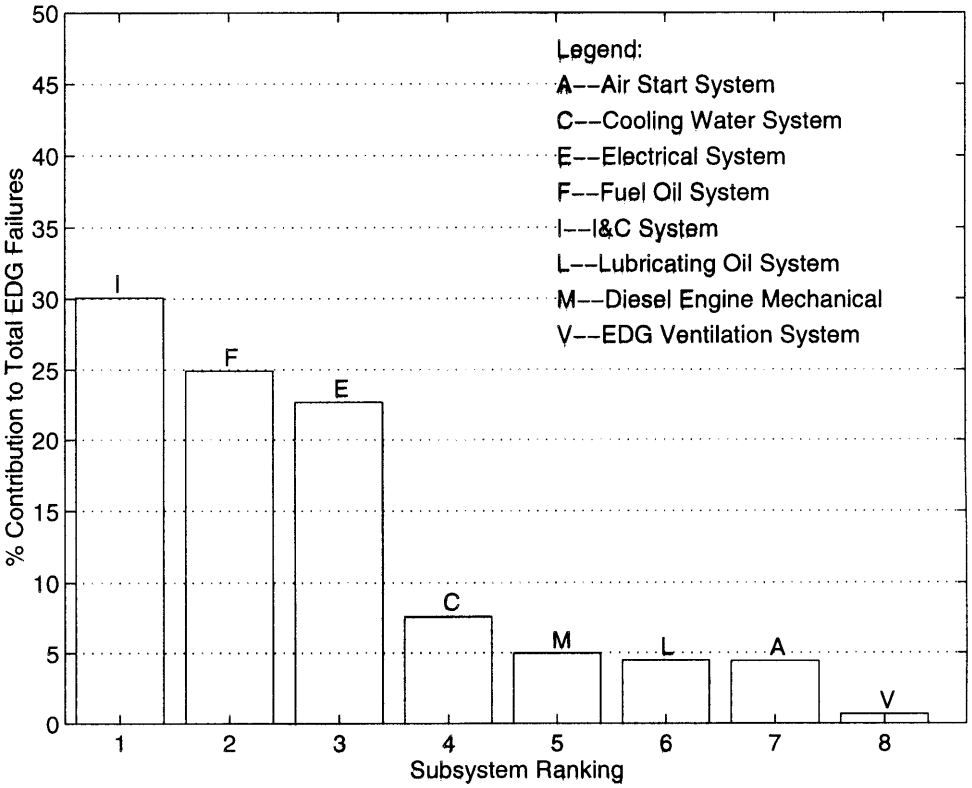


Figure 5-1: INEL EDG Failure Cause Data

numerically in Table 5.4, and as a bar chart in Figure 5-2. Appendix B shows the EDG systems in use at the plants considered in the SwRI study.

The data presented in the SwRI report are broken down into significant categories, allowing the isolation of rotating equipment, such as pumps, compressors, and motors, as well as failures due to leakage problems. No EDG ventilation system failures were identified and isolated in the SwRI report. In the INEL report, these accounted for less than 1% of all failures, so this omission is not necessarily significant.

The data presented in the SwRI report coincide well with the data from the INEL report. Both show very similar values for fuel oil, electrical, cooling water, lubricating oil, and EDG ventilation systems. The SwRI data report about one-half the frequency of instrumentation failures, but double the frequency of motor failures, and triple the frequency of starting air failures. While it is possible that the rate of air system failures has fallen somewhat, it is unlikely that mechanical engine failures and instrumentation failures have changed by so much. This suggests a difference in the reporting and analysis methods of the two reports, but it is not a significant issue. Both reports show that instrumentation and control systems are clearly problematic, while the mechanical engine is fairly stable.

5.5 U.S. Navy EDG Experience

The operational data gathered for the U.S. Navy report *CVN-68 Class Emergency Diesel Generator (EDG) Reliability and Availability* [7] cover the seven CVN-68 Class nuclear-powered aircraft carriers, each of which has four EDGs. These data are for the period January 1990 to August 1996. A total of 57 failures were observed in this period across the fleet of twenty-eight EDGs. Twenty of the fifty-seven failures are indicated as being from abnormal conditions. The ten cylinder liner/piston failures and the ten cooling water pump failures are the subjects of current redesign efforts on the part of the Navy.

The data presented in this report do not indicate failures of ventilation systems or of instrumentation & control systems. The peculiarities of ship-bound EDGs and

System	Subsystem	Failures
Fuel	**Total**	**23.9%**
	Governor	16.0%
	Leaks	2.9%
	Other	5.0%
Electrical	**Total**	**20.7%**
	Sequencer	6.0%
	Generator	5.2%
	Voltage Regulator	4.8%
	Output Breaker	3.0%
	Other	1.6%
I&C	**Total**	**14.4%**
	Trips	3.8%
	Other	7.5%
Air Start	**Total**	**13.8%**
	Moisture, Rust	3.5%
	Valves	3.5%
	Compressors/Motors	3.3%
	Leaks	2.6%
	Other	0.9%
Diesel Engine	**Total**	**10.3%**
	Turbochargers	3.6%
	Mechanical	2.8%
	Fuel Injectors	2.2%
	Exhaust	1.7%
Cooling Water	**Total**	**8.9%**
	Leaks	5.1%
	Pumps/Motors	2.0%
	Other	1.7%
Lube Oil	**Total**	**8.0%**
	Leaks	3.0%
	Pumps/Motors	1.0%
	Other	3.9%
Ventilation	**Total**	**0.0%**

Table 5.4: SwRI EDG Failure Data

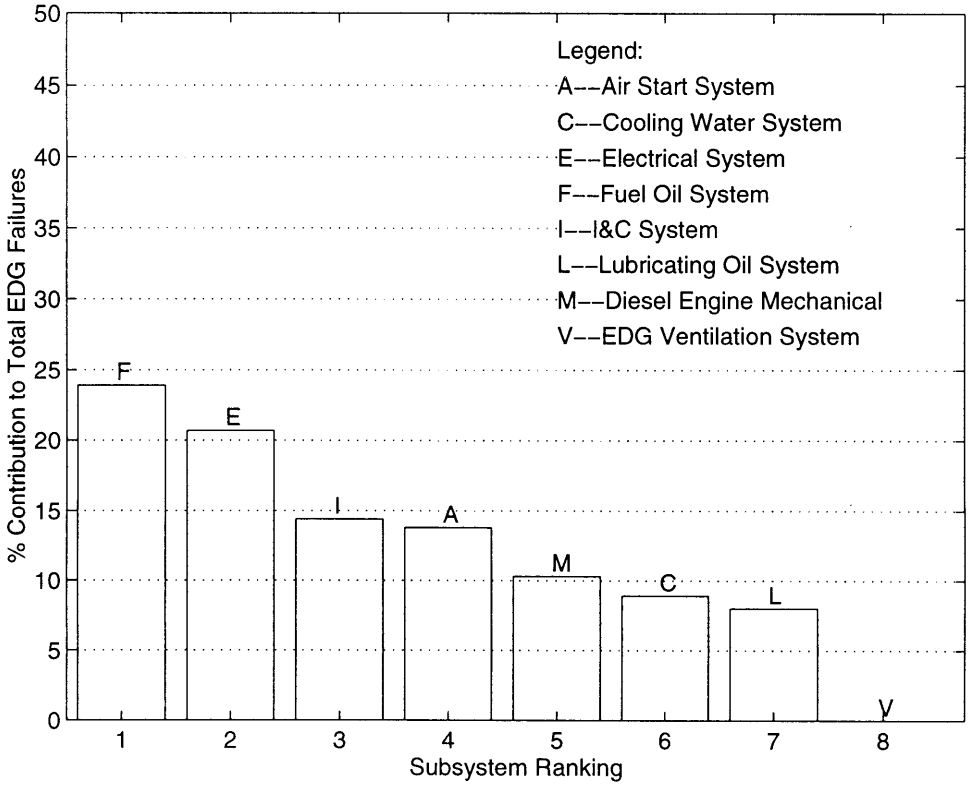


Figure 5-2: SwRI EDG Failure Data

System	Subsystem	Failures
Diesel Engine	**Total**	**36.8%**
	Piston/Cylinder Liners	17.5%
	Other Mechanical	10.5%
	Turbochargers	7.0%
	Fuel Injectors	1.8%
Fuel	**Total**	**24.6%**
	Governor	22.8%
	Fuel Lines	1.8%
Cooling Water	**Total**	**19.3%**
	Pumps/Motors	17.5%
	Other	1.8%
Start Motor	**Total**	**7.0%**
Lube Oil	**Total**	**7.0%**
	Pumps/Motors	7.0%
Electrical	**Total**	**5.3%**
	Voltage Regulator	5.3%
I&C	**Total**	**0.0%**
Ventilation	**Total**	**0.0%**

Table 5.5: U.S. Navy EDG Failure Data for CVN-68 Nuclear-Powered Aircraft Carriers

their support systems could explain the absence of ventilation system-related failures, but failures of instrumentation and control systems are most likely reported elsewhere.

These data are presented numerically in Table 5.5 and graphically in Figure 5-3.

The results for the Navy diesels are markedly different from those of the Licensee Event Reports. In the Naval example, the diesel itself is the largest contributor to the failure rate, followed by fuel and cooling systems. Electrical systems have a very small failure rate, and instrumentation systems are not presented. The starting system, the lubricating oil system, and the fuel oil system show reasonable agreement. Two particular failures which have affected the Naval EDGs are a propensity for cylinder liner and piston failures in EDGs from one particular supplier, and problems with cooling water pumps. Both of these failures, totalling thirty-six percent of the EDG failures, are currently the cause for component redesign. It should also be noted that governor problems are significant for the Naval EDGs as well, typically due to the

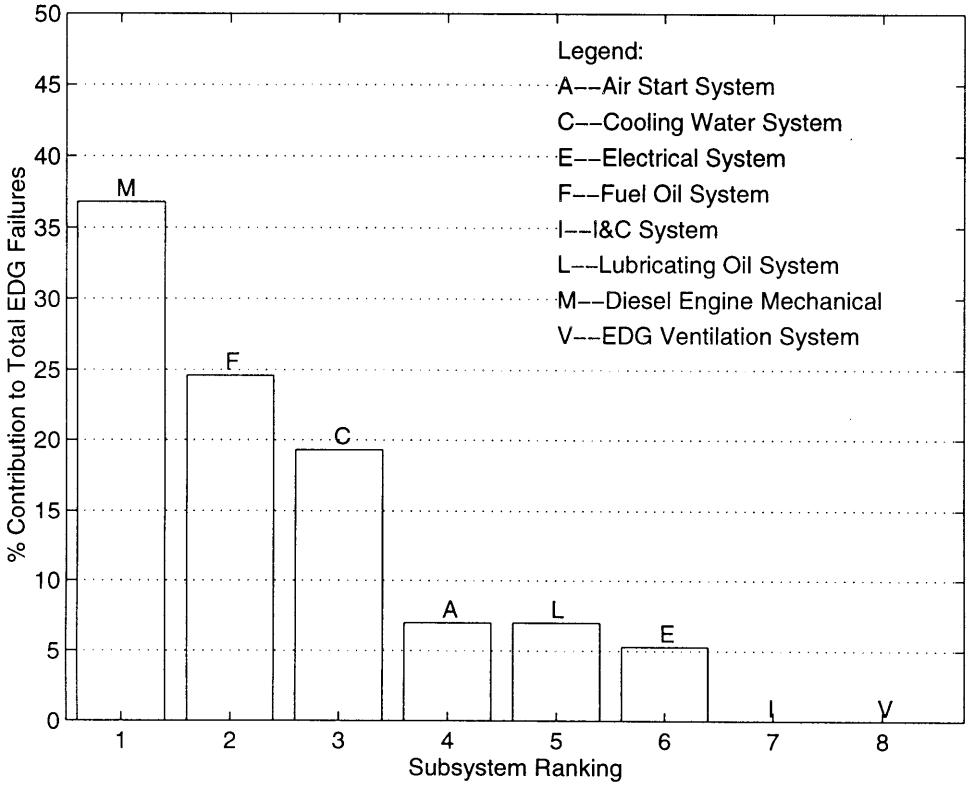


Figure 5-3: U.S. Navy EDG Failure Data for CVN-68 Nuclear-Powered Aircraft Carriers

same types of mechanical Woodward governors [35]. Finally, failures are not always defined consistently, in that some "failures" are defined as the existence of noticeable wear rather than the inability to function.

5.6 Nuclear Plant Reliability Data System

The data available from the Nuclear Plant Reliability Data System are different from the data available from Licensee Event Reports. NPRDS [6] is a database maintained by the Institute of Nuclear Power Operations (INPO), an organization made up largely of U.S. nuclear power utilities. The information reported for the NPRDS database is for the benefit of other utilities which are members. Adverse reports do not necessarily describe events which pose a safety threat to the nuclear power plants.

Utilities only submit Licensee Event Reports to the NRC when required by regulations; the required submissions describe failures of the system to perform when demanded. However, most of the component or system failures which occur are detected *before* an actual demand is made upon the standby system, and are corrected prior to any in-service demands. As a result, there are many more failures reported in the NPRDS database than in LERs.

The data analyzed in the work reported here include those of the EDG and of its support systems. In order to maintain similarity with the systems in use at the reference plants, Seabrook and Millstone 3, data were used only for Pressurized Water Reactors (PWRs), which include those of both Westinghouse and Combustion Engineering design. Events which occurred between January 1990 and January 1997 were included. A total of 3182 records were analyzed, 2539 addressing the air start, cooling water, fuel oil, and lubricating oil systems, and the remaining 643 covering the diesel engine and its remaining components, such as fuel injectors and turbochargers. Appendix B lists the EDG system details for the plants considered in the NPRDS database.

The nature of failures exhibited while in a standby mode is different from those which occur while running the EDGs. Thus, the nature of the NPRDS data is different

from that of the LER reports. The electrical output system, such as the voltage regulators and sequencer, are only monitored while the EDG is running. Similarly, no false trips occur while the diesel is not running; the only instrumentation and control failures observed are component failures to actuate pumps, compressors, and valves as demanded while in standby status. EDG building ventilation is also only actuated when the temperature of the diesel engine itself indicates that it is in use. As a result, the only failures observed during standby are failures of the fuel oil, lubricating oil, starting air, and cooling water systems, as well as some failures of the EDG itself, and associated instrumentation and control failures.

Due to the large amount of data available and the unique nature of the source, each support system is presented separately and in greater detail. Table 5.6 details failure contributions of the air starting system, Table 5.7 describes instrumentation and control failures, Table 5.8 shows the causes of lubricating oil system failures, Table 5.9 lists the causes of fuel oil system failures, Table 5.10 gives cooling water system failures, and Table 5.11 includes all other mechanical engine failures; any failures classified in NPRDS as engine failures but which described support system leakage were listed appropriately with the applicable support system. Due to the large contribution of leakage and of moisture, rust, and other contamination problems, these have been listed below as "System" failures, and the specific components which were afflicted are listed as "Components."

A graphical summary of the data for these six systems is presented in Figure 5-4.

The data gathered from the NPRDS database indicate that the most frequent failure mode observed during standby is leakage of starting air components. Some losses are inevitable in high pressure systems, and the failure to make up these losses indicates various other components' problems. Since the starting air system is in a state of maintaining a high pressure, leaks are frequently discovered.

Instrumentation makes up a significant portion of EDG repairs during standby. Typically, these are failures of mechanical and electro-mechanical relays, breakers, and contact pairs to operate the EDG support systems as demanded. The high rate of these failures recorded in the SwRI report had prompted the authors of that study

Air Start System	**Total System Failure Percentage**	**46.9%**
System	**Component**	**Failures**
Leakage	**Total**	**22.9%**
	Valves	11.4%
	Compressors	8.8%
	Engine	2.0%
	Other	0.7%
Compressors/Motors	**Total**	**10.3%**
	Gaskets	2.4%
	Air Dryer	2.2%
	Unloader	2.0%
	Lube Oil	1.9%
	Other	1.8%
Valves	**Total**	**9.2%**
Moisture & Rust	**Total**	**4.0%**
Other	**Total**	**0.5%**

Table 5.6: NPRDS Air Start System Failure Data

I&C System	**Total System Failure Percentage**	**17.3%**
System	**Component**	**Failures**
Start Air	Total	5.1%
Cooling Water	Total	5.0%
Lube Oil	Total	3.9%
Fuel Oil	Total	2.6%
Engine	Total	0.7%

Table 5.7: NPRDS Instrumentation & Control Failure Data

Lubricating Oil System	**Total System Failure Percentage**	**11.9%**
System	**Component**	**Failures**
Leakage	**Total**	**9.5%**
	Engine	5.8%
	Pumps	1.9%
	Valves	0.6%
	Heat Exchangers	0.5%
	Other	0.7%
Pumps/Motors	**Total**	**1.5%**
Valves	**Total**	**0.5%**
Other	**Total**	**0.4%**

Table 5.8: NPRDS Lubricating Oil System Failure Data

Fuel Oil System	**Total System Failure Percentage**	**10.1%**
System	**Component**	**Failures**
Leakage	**Total**	**7.9%**
	Engine	4.9%
	Valves	1.7%
	Pumps	0.8%
	Other	0.5%
Valves	**Total**	**1.0%**
Pumps/Motors	**Total**	**1.0%**
Other	**Total**	**0.2%**

Table 5.9: NPRDS Fuel Oil System Failure Data

Cooling Water System	Total System Failure Percentage	9.4%
System	**Component**	**Failures**
Leakage	**Total**	**6.9%**
	Engine	2.4%
	Heat Exchanger	1.9%
	Pumps	1.4%
	Valves	0.9%
	Other	0.3%
Heaters	**Total**	**1.1%**
Valves	**Total**	**0.7%**
Pumps/Motors	**Total**	**0.6%**
Other	**Total**	**0.1%**

Table 5.10: NPRDS Cooling Water System Failure Data

Diesel Mechanical	Total System Failure Percentage	4.6%
System	**Component**	**Failures**
Injectors & Pumps	Total	1.1%
Maintenance Errors	Total	1.0%
Turbocharger	Total	0.7%
Air Distributor	Total	0.6%
Other	Total	1.2%

Table 5.11: NPRDS Diesel Engine Mechanical Failure Data

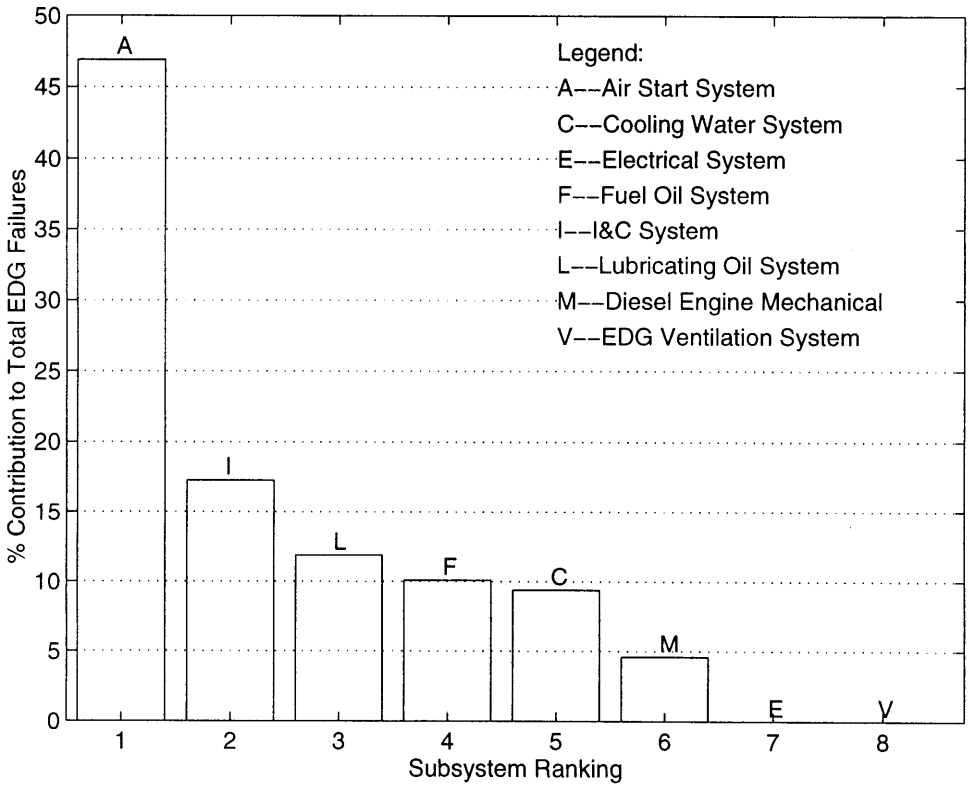


Figure 5-4: NPRDS EDG Failure Data

to recommend replacement of these mechanically-based logic devices with digital or other electronic logical systems. They reported that the contacts and moving breaker switches often failed to operate due to dirty contacts or obstructions preventing correct closure. The NPRDS data support that analysis.

Both the fuel oil and lubricating oil systems contribute equally to the EDG failure rate, and both are dominated by leakage problems. In each case, rotating machinery such as pumps and associated motors contribute a small but serious number of failures to the EDG unavailability. Similarly to the start air system, these systems all contain sufficient fluid volumes to operate as required with small leaks present. However, the failure of pumps and compressors can significantly affect system reliability as a measure of redundancy is eliminated, and repair times can be long. Data for the cooling water system demonstrate similar concerns.

Finally, the diesels themselves contribute few failures while in standby status. Most failures of the diesels are discovered during or immediately after test runs. Engine mounted fuel-delivery systems, including fuel injectors and fuel injector pumps, are the most important individual contributors. This is typically due to wearout which leads to leakage or degraded performance of the diesel. Maintenance errors were also significantly large contributors to the EDG failure rate. In particular, there were several reports of fuel rack problems, including painting over of moving parts, failure to lubricate moving parts, and even restrictions of motion from leaving masking tape on the racks, which had been used to prevent more painting problems.

5.7 Summary

The fault tree for the EDG system indicates that service water pumps contribute 33.8% of the EDG system failures, the EDG supercomponent contributes 30%, and EDG building ventilation dampers contribute 18.5%. Data are used to refine the supercomponent failures into specific support system failures.

Table 5.12 summarizes the failure rates by system for each data source considered. The INEL and SwRI reports demonstrate significant agreement, as is expected, since

they use similar data sets. The Navy data are only significantly different in their high frequency of internal engine failures. The NPRDS data indicate a definite tendency in plants for operational practices to identify system leaks before they can affect the EDGs in operation.

The data gathered from the above sources indicate several definite areas where diesel engines are failure prone. In particular, while running, the electrical and fuel systems (especially the governor) are highly problematic. Instrumentation failures are common both while operating and in standby. A significant number of starting air failures are eliminated by inspection and observation while in standby; as such, the EDG failure rate during operation due to failures of the starting air system is small. One particular component of interest in the air system is the air dryer. Air dryer failures, while infrequent, can effectively render both air start trains of an EDG inoperable, as the whole system must be isolated in order to prevent moisture from entering the diesel, and to prevent any leaking dessicants from clogging air distributor valves at the EDG. As such, while it is a small contributor to the overall failure rate, it is a significant failure mode in terms of consequence and repair time.

For cooling water and lubricating oil systems, leakage is the major concern, and the time required to diagnose, repair, or replace rotating machinery such as pumps and motors makes them a concern as well.

The diesel engine itself is limited primarily by the systems which support it. However, any failure of the diesel engine is a serious concern, as it eliminates half of the emergency power supply, and typically has a long repair time. The data from the Navy EDGs also demonstrate that the diesels are not fault proof, and that significant failure trends can exist by manufacturer or application. The authors of the INEL report took this possibility into consideration, but did not find any significant trends.

Discussions with personnel from the Navy [35], from Millstone 3 [8], and from INEL [33] suggest that the failures, as presented here, are very close to those experienced on a plant-by-plant or engine-by-engine basis. The components which these experts have further identified as being most problematic were turbochargers, voltage

System	Source			
	INEL	SwRI	U.S. Navy	NPRDS
I&C	30.1%	14.4%	0%	17.3%
Fuel Oil	24.9%	23.9%	24.6%	10.1%
Electrical	22.7%	20.8%	5.3%	0%
Cooling Water	7.6%	8.9%	19.3%	9.4%
Engine Mechanical	4.9%	10.3%	36.8%	4.6%
Lube Oil	4.5%	8%	7%	11.9%
Air Start	4.5%	13.8%	7%	46.9%
Ventilation	0.7%	0%	0%	0%

Table 5.12: Summary of EDG Failure Data by Source and EDG System

regulators, sequencers, governors, and fuel injectors.

Chapter 6

Proposed Monitoring

6.1 Introduction

On the basis of the data gathered from Licensee Event Reports, from the NPRDS database, and from U.S. Navy EDG reports, and from analysis of the fault tree for the MP-3 EDG, monitoring to help reduce EDG failure rates can be proposed. Some of this monitoring also stresses the elimination of ineffective tests or maintenance of the EDGs.

All proposed monitoring is summarized in Table 6.1. From the PRA assessment of the EDGs, the major contributors to EDG failures are the service water pumps, the EDG supercomponent, ventilation dampers, the sequencer and output breaker, contact pairs, and service water connection valves. In the interest of gaining the greatest benefit with the smallest feasible set of instrumentation, the service water pumps, the EDG supercomponent, and the ventilation dampers are proposed to be monitored. These components are not only the most significant risk contributors, but also are predominantly mechanical systems, which lend themselves to predictive monitoring and preventive maintenance.

The monitoring system used requires the definition of a baseline set of EDG operating parameters, against which performance can be compared. Through the use of expert elicitations specific to the various systems to be instrumented, criteria for identifying pending failures can be developed. As an example, a service water pump

would have a rated pressure gain associated with it; if the outlet pressure produced, which is monitored and trended, falls below an expert-defined level, the pump would be a candidate for early replacement. This distinguishes a monitoring system from an alarm system, which would give no indications of degrading performance until the component is on the brink of failure or has failed.

6.2 Instrumentation & Controls, and Electrical Power Output

Although these systems are significant failure contributors, as shown in the data from the INEL report, the SwRI report, and the NPRDS database, no monitoring for the instrumentation, controls, and electrical power output systems are to be proposed here.

The capability for the monitoring of the status of many power output components is already nominally in place, as is suggested in Table 4.1. Additionally, while instrumentation to indicate that these electrical systems have failed is available, little monitoring technology is available which could predict their failures. Thus their preventive maintenance benefits are unattainable. Instrumentation & control system failures, such as involving the contact pairs from the minimal cutset analysis, while not currently instrumented, fall into the same category, as no predictive benefits could be realized.

As an alternative to instrumentation for these electrical failures, the types of failures which occur suggest that some control and electrical power system redesign could be beneficial. The authors of the SwRI report conclude that the replacement of older electromechanical components such as relays and breakers with newer solid-state components could reduce the failure rate in several ways [4]. Solid-state components are less likely to "fail to close" as they do not have moving parts. Contamination and rusting problems are non-existent, and vibration failures are also less likely. Perhaps most significantly, installing solid-state components in a manner such that they can

be self-tested independently of EDG starts could allow for significant reliability improvements. As with any new system, a certain degree of infant mortality is to be expected, so a new system may not perform flawlessly initially; other possible failure modes include electronic interference and noise, or failures of the logical systems to perform correctly.

It is difficult to use instrumentation to monitor other instruments, such as those used to "trip" the diesels under adverse conditions. The best method available to make reported instrumentation more reliable, as with any other component which can be used in parallel, is to add redundancy, in the form of logical voting systems [36]. Voting systems, such as "two-out-of-three" voting, require that three independent sensors be used, and that a particular signal, such as high temperature, be reported on at least two of them for the diesel to trip.

The number of failures of instrumentation systems is a particular concern as additional sensing systems are being proposed here. The use of redundant sensors is advisable in order to improve the reliability of the results. Also, the monitors proposed for use can be used to trend data, not only to report a high or low condition. As such, both sudden and gradual changes in monitoring accuracy can be detected by referencing a redundant sensor.

6.3 EDG Supercomponent Monitoring

The EDG supercomponent, as defined in the PRA, includes the mechanical diesel engine, the fuel oil system from the day tank to the engine, the cooling water system between the plant-wide service water system and the engine, the lubricating oil system, the starting air system, and the turbocharger or supercharger. Monitoring of the EDG events from the PRA analysis includes instrumentation of each of these support systems.

6.3.1 Diesel Engine

Monitoring of the mechanical diesel engine is most readily accomplished with three inter-related methods, vibration analysis, engine oil chemical analysis, and whole-engine analysis. Engine analyzers are commercially available from many sources, including some of the manufacturers which provide EDGs for use in nuclear power plants; companies such as General Electric, Ingersoll-Rand, AlliedSignal, EG & G, and Snap-On also produce engine analyzers. The basic functions of engine analyzers are to monitor the pressures, temperatures, and vibrations of the diesel engine power cylinders. These variables allow diagnosis of degradations of valves, fuel injectors, seals, and piston rings, as well as general diagnosis of the health of the EDG. The crankshaft and fuel rack positions are typically monitored, and other vibration monitoring data can be available as well.

In the particular case of Millstone 3, the engine analyzer of interest is the Recip-Trap analyzer, made by Beta Monitors & Controls, Limited, a division of Liberty Technologies, Inc. The Recip-Trap analyzer provides all the above functions, and it performs trending of critical engine parameters, as well as maintaining a baseline of data against which later performance is gauged. Other analytical tools offered typically include tools for recognizing crosstalk between sensors. As an example of crosstalk, a scored cylinder liner in cylinder number two could cause an anomalous vibration pattern which is detected and reported by vibration sensors in cylinders 1, 2, and 3. Analysis tools available with some engine analyzers can help to isolate the root cause from these various reported signals, and indicate the true nature of the problem.

Similar instrumentation by EDG is in use by the Navy, in the aforementioned ICAS (Integrated Condition Assessment System). The ICAS offers performance analysis such as thermodynamic, heat transfer, mechanical efficiency, and fuel consumption calculations, as well as component-specific assessments. Vibration monitoring is used, dynamic analysis of cylinder performance is conducted, and engine oil is analyzed on-line.

Engine oil analysis can be performed in two ways, on-line and off-line. The ICAS system uses on-line monitors, which assess oil conditions as the oil flows through the system, but off-line monitoring, currently in use as described in the Technical Specifications, works well without additional sensors. Off-line monitoring is conducted by taking an oil sample off-site for chemical analysis. On-line analysis allows for a more immediate awareness of potential problems. Detection of metal particles, fuel oil, water, or combustion products in the lubricating oil indicates problems in the diesel engine, including wear of components, bearing failures, and leaking seals.

Vibration analysis can also be used to verify the condition of bearings, the crankshaft, and other moving parts within the engine, by mounting accelerometers in various locations. By performing spectral analysis on vibration patterns recorded from bearings, problems can not only be identified, but even located (inner race, outer race, rollers) without physically examining the bearing. Several nuclear power plants are currently engaged in research projects assessing the effects of using these vibratory diagnostic techniques.

Through the use of these indicators, the overall health of the diesel engine can be accurately assessed, without using intrusive and destructive teardown inspections. We anticipate that many typical failures of engine components can be predicted with these instruments in place.

6.3.2 Fuel Oil System

The data presented above indicate that the two primary failure modes associated with the fuel oil system are leakage during standby, and governor failures while running. Governor failures can be categorized with instrumentation and power output failures, as components in need of some redesign. Governors are similar devices which perform functions much better suited to digital or electronic governors. There has been some degree of interest expressed within the Navy [35], by the authors of the INEL report [33], and within the diesel industry in general [34] [37] in using digital governors to replace the mechanical governors currently in use. Many of the same companies which offer engine analyzers have developed digital governors in lieu of developing

instrumentation packages to monitor them. However, as a means of monitoring the logical output of the mechanical governors, most engine analyzers include fuel rack position indicators; both mechanical and digital governors can be assessed for proper operation in this manner.

Leakage of the fuel oil system can primarily be assessed in two ways, by monitoring fuel usage and losses, and by monitoring fuel line pressures. Fuel consumption by the engine is a factor which can be determined using engine analysis. By monitoring fuel tank levels, any fuel level decrease greater than consumption would indicate a loss. If the fuel system pressure is found to be low, it indicates that fuel is leaking, or that the fuel pumps are not operating as required.

Leakage can be accounted for with instrumentation, but, as with cooling water and lubricating oil, fuel oil leaks are likely to be discovered through observation by operators. This instrumentation can assist in verifying that a leak may be present.

6.3.3 Cooling Water System

The cooling water system primarily suffers from leakage problems. In the case of the Navy, a propensity for cooling water pump failures is also observed. As cooling water is constantly circulated through the EDG, monitoring of pumps can indicate declining performance that could require maintenance. Pressure transducers and vibration sensors would best indicate the principle problems afflicting pumps, namely degradation of the bearings or other moving parts, and failures of pumps to produce their rated pressure gain.

As in the case of the fuel oil, leakage can be detected by lower than expected pressures, and by loss of water volume. We do not anticipate that any cooling water will be "consumed" by the engine, so any deviation in the observed fluid level would indicate losses to leakage, or potentially, gains from other system fluids, including raw plant-wide service water.

In order to monitor the thermodynamic efficiency of the engine and the cooling system effectiveness, many engine analyzers also include temperature sensors for the cooling water both before entering the engine and after leaving it, prior to cooling in

the heat exchanger.

6.3.4 Lubricating Oil System

The lubricating oil is primarily subject to two failure modes, leakage and pump failures. As with cooling water and fuel oil, pumps can be monitored with pressure transducers and with vibration sensors.

Leakage of lubricating oil can also be monitored by verifying volume levels and by using pressure transducers to verify system pressure. A typical EDG start can consume small amounts of oil, such that a definite declining trend in oil volume is expected, but at a fairly constant rate. Any larger deviations could indicate leakage.

As is previously discussed, the lubricating oil is analyzed to determine the physical condition of the diesel engines. Oil temperatures entering and exiting the engine are also typically monitored by an engine analysis program to verify the efficiency of the engine and of the lubricating oil cooler.

6.3.5 Starting Air System

The starting air system is primarily affected by leakage problems and compressor failures. There is also a tendency for failures of the air drying system, which can disable the EDG.

Leakage is a more significant problem for the air system, since an air leak is not usually visually identified, as an external oil or water leak can be. However, the air start system operates at a high enough pressure that pressure transducers can readily be used to report system pressure decreases. Most leakage is currently detected by frequent self-starting of the compressors, actuated to return pressure to required levels. Online pressure sensors would allow better warning of leaking components.

Compressors are subject to the same typical failure modes as pumps, namely bearing or other component wearout, and leakage or failure to provide the rated pressure. Pressure transducers can be used to verify the head gain across the compressor, and vibration sensors can be used to warn of bearing failures.

Air dryers are used with air compressors to remove harmful moisture from the starting air. The air dryers have a very low failure rate, but almost all air dryer failures reported in the NPRDS database effectively disabled the entire EDG train. In the event of an air dryer failure, the starting air system affected is typically isolated to prevent corrosive damage to the EDG start motor. Another typical failure mode for the air dryers is a loss of the dessicant used to absorb moisture. This dessicant can be forced out of saturated air dryers, and can clog critical air distributor valves which supply starting air to the EDG. As either of these failure modes have the capability to disable the starting air system, instrumentation specific to air moisture content (relative humidity) may be called for on a plant-by-plant basis.

6.3.6 Turbochargers and Superchargers

Very little failure data have been available for turbochargers and superchargers, except for brief references in the SwRI report and references made by engineers working in this field. The failure modes most common to these chargers are bearing failures and lubrication failures, as with all other rotating equipment. The use of vibration sensors can help to reduce these charger failures. In order to evaluate the performance of the turbocharger or supercharger, inlet and outlet air temperatures may also be monitored. Some engine analyzers include this instrumentation with a basic package. Chargers which use intercoolers (cooling systems for the combustion air, used because cooler air has higher density, increasing the mass of oxygen available to support combustion) are particularly good candidates for temperature sensors.

As the function of a turbocharger or supercharger is basically the same as that of an air compressor, monitoring of the pressure gain across the charger, or boost, is also recommended.

6.4 Other Fault Tree Systems

The PRA analysis treats the role of the EDG building ventilation separately from the rest of the EDG support systems, and the plant-wide service water system is not

treated as a part of the EDG train. However, both of these systems have significant risk contributions, greater than that of the failure of the diesel engine itself.

6.4.1 Plant-Wide Service Water System

The plant-wide service water system interfaces with the EDG cooling water system in two ways. First, a motor-operated valve is opened when necessary to allow service water to flow to the heat exchanger. This valve is expected to open whenever the EDG is operating. Second, two service water pumps provide a flow of water to the heat exchanger to cool the EDG cooling water.

The failure rate for the valve is low, and adds little to the failure rate of the EDG. However, failure of the service water pumps contributes more than a third of the EDG system failure rate. As with the other rotary equipment described above, the service water pumps should be instrumented with pressure transducers in order to verify the performance of the pumps, and with vibration sensors to predict the wearout of internal components.

6.4.2 EDG Building Ventilation System

The EDG building ventilation system is responsible for controlling the room temperature, providing combustion air to the EDG, and removing exhaust gases. As such, dampers which close off the air flow to the room are critical to the proper operating temperature of the generator, and for supplying fresh air to the diesel engine. These dampers are designed to fault to the "open" position in the event of a failure, but they can also fail to open. As such, both the dampers and motors which operate them are candidates for vibration monitoring to help predict failures. Blowers used to promote circulation, like other rotating equipment, are subject to moving component failures, detectable with vibration sensors, and to failures to provide flow, analogous to the failure of a pump to provide a pressure head, which can be detected with air flow sensors.

6.5 Summary

The diesel engine supercomponent is a complex combination of rotating equipment and fluid delivery systems. As such, monitoring of leakage of these systems is critical for maintaining proper operating condition. The internal condition of rotating equipment, not as easily observed as leakage problems, are best instrumented with vibration sensors to predict failures of moving components, and with performance monitors for the output of the pumps, compressors, and blowers.

Within the diesel engine, the performance of the supporting components can best be monitored and predicted by measuring critical internal combustion parameters such as cylinder temperature, pressure, and vibration. Other sensors are also used to monitor the position of critical components such as the fuel rack and crankshaft, such that the overall performance of the EDG can be trended.

The plant-wide service water system and EDG building ventilation are also critical to EDG performance, and, as such, are instrumented similarly for rotating equipment and leakage failures.

The monitoring proposed is summarized in Table 6.1. The proposed monitoring is described by system and component or failure mode. The monitoring which is included with an engine analyzer such as the Recip-Trap analyzer is indicated as well.

System	Component or Failure Mode	Monitored Parameter	Engine Analyzer?
Engine	Cylinder	Pressure	Yes
		Exhaust Temperature	Yes
		Vibration	Yes
	Fuel Rack	Position	Yes
	Crankshaft	Position	Yes
	Bearings	Vibration	Some
		Temperature	Some
Fuel Oil	Tanks	Level	No
	Fuel Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
Cooling Water	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
	Coolant to Engine	Temperature	Some
	Coolant from Engine	Temperature	Some
Lubricating Oil	Oil	Chemical Analysis	Some
	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
	Oil to Engine	Temperature	Some
	Oil from Engine	Temperature	Some
Starting Air	System	Pressure	No
	Compressor	Differential Pressure	No
		Vibration	No
	Air Dryer		No
			No
Turbocharger or Supercharger	Boost	Differential Pressure	No
	Intercooler	Inlet Temperature	Some
		Outlet Temperature	Some
	Charger	Vibration	No
Service Water	Pumps	Differential Pressure	No
		Vibration	No
Ventilation	Blowers	Air Flow	No
		Vibration	No
	Dampers	Vibration	No

Table 6.1: Proposed Component, Failure Mode, and Monitoring Variables

Chapter 7

Net Benefit Assessment

7.1 Introduction

In order to fully evaluate the effectiveness of the proposed monitoring system, it is necessary to examine the use of such a system on a trial basis. In order to justify such a demonstration, an estimate is made here of the effects that monitoring can have upon risk levels for the EDG system, and thus, upon the core damage risk (CDF). A sample method used to assess the benefits gained is discussed first, then applied to this specific example. The reduction in costs associated with such a system is also estimated. This estimate includes reducing unnecessary testing and maintenance procedures, the reduction in repair and maintenance costs offered by preventive maintenance, and the cost outlay for a monitoring system.

In order to evaluate the effects of monitoring, the reduction of the EDG failure rate is calculated. This reduced rate is then used to justify an increase in the EDG surveillance interval and a change of the surveillance test duration. The calculation shown here is illustrative. A more accurate estimate, using the method shown here would be needed in practice.

7.2 Effects of Monitoring on EDG Failure Rate

In order to estimate the effects of monitoring upon the EDG failure rate, use of the proposed monitoring system must be translated into a change in the failure rates for the EDG basic events. Sensitivity analysis is then used to evaluate the effect of these basic event changes on the EDG failure rate.

The proposed monitoring system reduces the event frequency or probability for four groups of basic events: 1) failures of EDG building ventilation dampers to close, 2) failure of the EDG supercomponent to start or run, 3) failure of the EDG supercomponent to be available due to maintenance or testing, and 4) failure of service water pumps. The "EDG supercomponent" includes the diesel engine and all of the support systems described in Chapter 3. Proposed monitoring for the EDG supercomponent includes all the proposed monitoring except that for the service water pumps and EDG building ventilation dampers.

We use sensitivity analysis in order to assess the effects of monitoring upon the EDG system failure rate. Table 7.1 lists the twenty-one basic events which are affected by the proposed monitoring system, grouped as service water failures, EDG supercomponent failures, and EDG building ventilation failures.

In order to evaluate the reduction of the EDG system failure rate, the fault tree top event failure probability value is recalculated using new values for the twenty-one events listed in Table 7.1. In a sensitivity analysis, the failure rates for these basic events listed were reduced by 25%, 50%, 75%, and 100%, respectively, then the results of these reductions were plotted with a least-squares best-fit line in Figure 7-1. For example, with an expected basic event reduction of 50%, the EDG system failure rate would decrease by 38.6%, from 0.097 per year to 0.059 per year.

For the purpose of comparison, two other sets of calculations are plotted in Figure 7-1. For one set, the proposed monitoring would have to be expanded to include all rotating equipment and all system valves, essentially including every non-electrical component in the EDG system, encompassing a total of fifty-seven basic events. With thirty-six additional sensors, and, again, with the basic event probability reduction

System Grouping	Basic Event Number	Description
Service Water Pumps	10	(INIT) CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAILS TO RUN
	11	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN
	12	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN
	103	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE
	104	SERVICE WATER PUMP SWP1A FAILS TO RUN
	105	SERVICE WATER PUMP SWP1A FAILS TO START ON DEMAND
	106	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE
	107	SERVICE WATER PUMP SWP1A FAILS TO RUN
	108	SERVICE WATER PUMP SWP1A FAILS TO START ON DEMAND
	118	CCF OF ALL 4 SERVICE WATER PUMPS TO START
	119	CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAIL TO RUN
	120	CCF TO START OF SW PUMPS 'A' AND 'C'
EDG Supercomponent	38	DIESEL GENERATOR A UNAVAILABLE DUE TO TEST OR MAINTENANCE
	39	DIESEL GENERATOR A FAILS TO START ON DEMAND (INCLUDES FAILURE TO RUN)
	69	CCF OF DGs TO START ON DEMAND (INCLUDES FAILURE TO RUN)
EDG Building Ventilation Dampers	40	OUTLET DAMPER 20A FAILS TO OPEN
	41	OUTLET DAMPER 20C FAILS TO OPEN
	42	INLET DAMPER 23A FAILS TO OPEN
	43	RECIRC DAMPER 26A FAILS TO CLOSE
	81	AIR OPERATED DAMPER *23A FAILS TO OPEN
	85	CCF - AIR OPERATED DAMPERS *23A AND *23B FAIL TO OPEN

Table 7.1: Basic Events Affected by Proposed Monitoring System

of 50%, there is only a 41.6% reduction in the EDG system failure rate, from 0.097 per year to 0.057 per year. This is only 3% more with thirty-six additional sensors.

The second set of comparative data shows a reduction of the failure rate of the 116 physical basic events in the fault tree. (Three events, summer operation, and pump train 'A' or 'C' in the lead, do not have *failure* rates, but have probability values used to describe operating conditions. Instrumentation is also not applicable to two other events, a human error failure rate, and the rate of the loss of offsite power. These five events are not included in the "best case" analysis.) This set is not realistic or feasible for a monitoring system, but it defines the maximum amount of benefit possible. As would be expected, reducing all basic event frequencies by 50% reduces the EDG failure rate by 50%, from 0.097 per year to 0.048 per year.

Figure 7-2 shows the effect on both the EDG failure rate and the core damage frequency of increasing the number of sensors, or the number of basic events monitored. The data plotted represent a 50% reduction of the basic event probability values for monitored events. The failure rates in Figure 7-2 are presented as relative failure rates, such that both the EDG failure rate and the CDF are on the same scale. The effect of EDG failure rate reduction on the CDF assumes that the EDG contributes 33% of the CDF risk [27]. It is seen that the relative failure rate is insensitive to additional monitoring once the twenty most important events have been instrumented for on-line monitoring.

Figure 7-3 shows the effects of implementing the proposed monitoring system without changing the test frequency or duration. This figure does not show outage times due to testing or maintenance. The current testing procedures include a one hour test per month, a twenty-four-hour test at the end of the eighteen month cycle, and an average repair time per monthly test of 6.06 hours [21]. With monitoring, the average unavailability, $\langle Q \rangle$, as calculated with Equation 2.13, is reduced from 0.0385 to 0.0313, an 18.7% reduction.

A 50% reduction in basic event failure rates has been assumed for these estimates. In order to assess better what the actual reduction rate is, experimentation on a trial diesel engine is required. However, the presented range of values of failure frequency

reduction, from 25% to 75%, occurring as a result of monitoring, is not unreasonable. A rough, conservative estimate of the expected reliability improvements can be made by considering how the monitoring works, and how it could fail to predict failures.

As is discussed in Chapter 8, failures of the monitoring system take three forms: 1) failure to report a correct signal, 2) failure of the component model to predict pending failures, and 3) failure of the component in a manner not described by the model. Examples of each of these forms of failures in fuel oil system monitoring could include: failure to report the fuel pump vibration accurately; failure of the fuel pump due to worn bearings without showing the expected vibration patterns; and failure of the fuel pump due to contamination from the fuel tanks. The first case would be an instrumentation failure, the second a failure of the model to predict the vibration patterns that would indicate a pending failure, and the third would be a failure that can not be predicted with the instrumentation proposed for the fuel oil system.

If, in this example, 80% of the failures were of types which the monitoring system can predict, and if expert opinions suggest that 80% of these modeled failures can be detected early, then even with instruments which are only 80% accurate, 50% of all failures could be predicted before they were to occur. This result corresponds to a reduction of the basic event failure rates by 50%. This is a conservative reduction estimate, as most failures are indeed of types assessed with the proposed monitors, and few failures are anticipated which would occur without any warning. Sensors are also expected to be significantly more than 80% reliable. The use of redundant sensors would further improve reliability, as in a two-out-of-three voting system, using 80% reliable sensors, could be combined for a system with 96% reliability.

7.3 Changes to Test Duration and Frequency

7.3.1 Introduction

The current standards for the EDG surveillance intervals and test durations are established in the Technical Specifications. The surveillance intervals were not defined

using an estimate of the EDG failure rate. Rather, the required intervals imply a maximum acceptable failure rate. By reducing the failure rate of the EDGs with monitoring, new, longer surveillance intervals can be justified. The justification for the duration of the currently required tests was based upon EDG manufacturer recommendations. As is previously discussed, the diesel engine usage at nuclear power plants is quite different from and less demanding than the usage for which the engines were designed, and which provided the experience base for the vendor recommendations. Nuclear plant service includes frequent, fast starts of the EDGs relative to the short running periods. The engines were designed for rare, slow starts and long-term operation. Using the failure information discussed above, new test durations are also proposed.

7.3.2 The Revised Required Test Duration

In the example of the Fairbanks Morse Company, the maker of the Colt-Pielstick diesel engines, a one-hour test duration was recommended for the Technical Specifications. According to the Colt maintenance recommendations, one hour is the time required for temperatures in the diesel engine to stop increasing, and for a steady-state temperature to be achieved. However, as analysis in Chapter 4 suggests, a one hour test run is only 60% efficient for demonstrating engine reliability. Only 34.5% of failures can be examined with a one hour run, as was demonstrated in the INEL report [5]. The steady-state condition for some critical failure modes, such as vibration failures, is not reached in one hour, but finally approached in fourteen hours.

In contrast, the twenty-four-hour run is nearly 100% effective at testing all of the EDG failure modes and resetting the EDG unavailability to zero. Also, these tests best simulate actual demand conditions. However, testing for the full twenty-four hours may not prove to be necessary.

By further examining Figure 4-1, it can be observed that after fourteen hours of running, about 95% of failure modes for a twenty-four-hour run have been interrogated. After fourteen hours of running, the additional reduction in the EDG system failure rate, about 0.5% per hour, may not be sufficient to warrant testing for another

ten hours. However, the twenty-four-hour runs, conducted during refueling outages, are very efficient at verifying the diesels' ability to perform under the likely operating conditions of the EDGs.

As such, the proposal of the work reported here is that the required test duration be increased from one hour to twenty-four hours. In order to compensate for this increase in running time of the EDGs and for the increase of unavailability due to testing, the frequency of EDG tests is proposed to be reduced from once per month to once every twelve months. The discussion of the surveillance interval change continues in the next section.

7.3.3 Test Frequency

We propose to use the monitoring-based reduced EDG failure rate defined above in order to justify reducing the EDG surveillance interval without increasing the average unavailability of the EDG system. Also, a reduction in test frequency would help to alleviate EDG unavailability increases due to the increased test duration, or "maintenance out of service" (MOOS) time.

For the purposes of comparison, the availability gains that can be realized with the proposed monitoring are evaluated in three ways. First, the reduction of the failure rate for affected basic events is assumed to be 50%. With this assumed reduction, the effects of increasing the testing interval and increasing the test duration are examined. Second, a target testing interval and a target test duration are varied in order to find the minimum acceptable basic event failure reduction. Third, the test frequency and the failure rate reduction can be adjusted to achieve a desired target average unavailability.

Without the use of monitoring, the use of twenty-four-hour tests can improve EDG availability, as the EDG unreliability is reset to a value of zero after each test. The effects of the non-zero reset at the end of the one-hour tests are obvious in Figure 7-3 in the previous section, as the lower points on the "sawtooth" pattern rise exponentially with time.

Equation 7.1 is used to find the longest surveillance interval, t_S, which does not

increase the average unavailability, $\langle Q \rangle$. Using a test duration of $\tau = 24$ hours, the current EDG failure rate of $\lambda = 0.097$ per year, the average repair time $t_R f_R = 6.06$ hours, and the current unavailability of $\langle Q \rangle = 0.0385$, the maximum allowable surveillance interval, t_S is 6100 hours, or 8.4 months. Figure 7-4 compares the current testing with a twenty-four-hour run once every eight months. For a test interval of eight months, the average unavailability is reduced slightly, from 0.0385 to 0.0373, a 3% reduction, using the relationship

$$\langle Q \rangle = \frac{\frac{1}{2}\lambda t_S^2 + \tau + t_R \cdot f_R}{t_S + \tau + t_R \cdot f_R}. \tag{7.1}$$

By including the proposed monitoring with the extended test duration, the surveillance interval can be further extended. Using Equation 7.1 again, with the reduced EDG failure rate of $\lambda = 0.059$ per year (reduced due to monitoring), the surveillance interval, t_S, can be extended to 14.6 months. Figure 7-5 shows the effects of both using monitoring and extending the test interval to twelve months with the use of longer tests. The average unavailability is reduced from the current value of 0.0385 to 0.0328, a 15% reduction.

The effects of changing the test duration and frequency and adding monitoring are compared in Table 7.2, showing the *combined* effects of these three changes. This table shows the average unavailability $\langle Q \rangle$, the testing length τ, and testing interval t_S used, and the failure rate λ and effectiveness of tests (% recovery) assumed.

	$\langle Q \rangle$	t_S	τ	λ	% Recovery
Current Methods	0.0385	1 month	1 hour	0.0968	66%
Monitoring	0.0313	1 month	1 hour	0.0594	66%
Testing Changes	0.0373	12 months	24 hours	0.0968	100%
Proposed Changes	0.0328	12 months	24 hours	0.0594	100%

Table 7.2: Effects of Monitoring, Testing Changes, and Combined Proposed Changes on EDG Average Unavailability

The second method of evaluating the monitoring method is to set a target surveillance interval and test duration, then finding the smallest basic event reduction (pre-

viously assumed to be 50%) which would reduce unavailability. Using Equation 7.1 with $\tau = 24$ hours and $t_S = 12$ months $= 8760$ hours, a maximum allowable value for λ, the failure rate, can be found. In order to achieve these target testing conditions without increasing unavailability, the value of λ must be less than 0.0704 per year. From Figure 7-1, in order to obtain a failure rate less than 0.0704 with the proposed monitoring system, the probabilities of the basic events must be reduced by 35% or more.

The third method of evaluating the monitoring method or the changes to the testing procedures is to set a target unavailability, and then to find the test interval or failure rate reduction which satisfies the goal in Equation 7.1.

7.3.4 Recovery from Extended Testing

The major drawback to extending the test duration is its contribution to the EDG unavailability due to the EDG being unavailable during testing. The EDG is deemed to be unavailable when any maintenance or testing is being carried out. In order to rectify this problem, we propose that a mechanism be considered to allow an EDG under testing to become available upon demand. During testing, the EDG is operated as it would be in hot standby mode, without system loads supported by the generator. We propose that if the EDG unavailability due to maintenance is found to be unacceptably large, then the necessary steps must be taken to allow a switch of the operating EDG to a mode synchronized with the emergency plant loads. The EPRI ALWR Project reports [13] include data on both the failure to recover an EDG which is unavailable due to any testing or maintenance, as well as the failure to recover an EDG which is not undergoing maintenance, but which failed to start upon demand.

The failure rates defined for an EDG in any stage of maintenance or testing outage are excessively large for evaluating the recovery from testing. These failure rates, 1.0 within 40 minutes, 0.9 within two hours, 0.8 within four hours, and 0.7 within eight hours, are reasonable for assessing the failure to recover an EDG with equipment failures or in a teardown repair state, but are excessively high for EDGs which are operational, but off-line for testing. These values are sufficiently large to represent

the time required to complete repair work on a malfunctioning EDG, but excessive for describing the unavailability due to testing of an EDG which is demonstrated to be operable.

Classifying the diesel under testing as an operable, but currently unavailable system, the ALWR Project failure rates for recovery, as defined for "DG Actuation," of 0.04 within 70 minutes, 0.03 within twelve hours, and 0.001 within one day [13], are more realistic for representing a restart attempt [38]. This recovery is similar to the single test specified in the Technical Specifications, which includes a requirement for restarting the EDGs within five minutes of being shut down. In the event of an actual demand, the twenty-four-hour tests can reasonably be terminated as necessary. Possible modifications to the sequencer system could allow an automated transition of a running EDG from test mode to demanded operation, thereby further reducing the disadvantages of extended testing. Doing any of these things would greatly reduce the contribution to EDG unavailability due to testing for long durations.

7.3.5 Testing of Support Systems

An additional reduction of EDG system unavailability could be realized with the continued, but restricted, use of monthly surveillance tests. Table 4.8 lists the basic events for which the failure probabilities are at least partially reset towards zero values by monthly tests. All but two of the basic events listed are support system failures. As an additional method of reducing EDG unavailability, the testing of EDG support systems without running the diesel engine can be considered.

With relatively minor modifications, the air start system, the fuel oil transfer system, the cooling and service water systems, the lubricating oil system, and the EDG building ventilation system can be tested without requiring the EDG to start [39]. The systems which interface with the EDG most directly, the fuel injectors, governors, fuel racks, turbochargers, and air start motors could not readily be tested without starting the EDG.

7.3.6 Summary

We propose to use a reduction of the EDG failure rate to extend the surveillance interval from one month to twelve months, while increasing the test duration from one hour to twenty-four hours. With a 50% reduction in basic event failure rates in monitored components, the average EDG unavailability would be reduced by 15%.

The assumed effectiveness of the monitoring system for reducing the EDG failure rate is rather conservative; we anticipate that the rate of failures for the monitoring system will be small, such that the benefits presented here can readily be achieved; further experimentation is required to obtain more exact results. However, further safety gains can be made, as necessary, with modifications to the sequencing system, such that testing does not make an EDG completely unavailable. Further small modifications to various EDG support systems could allow their continued monthly surveillance, though the estimates presented here do not indicate that need.

7.4 Cost Reductions Due to Proposed Changes

7.4.1 Reduced Costs

Cost reductions are anticipated in two ways. First, the use of an effective monitoring system can allow the elimination of intrusive and expensive teardown inspections during refueling outages. Second, the advantages of predictive monitoring and preventive maintenance should decrease time lost to unavailability while decreasing diagnosis and repair costs. The costs of implementing a monitoring system are expected to be less than these cost savings.

The first method of cost reduction is observed by eliminating the intrusive teardown inspections during refueling outages. This topic is explored more fully in Utton's research, but is presented here briefly [2].

The largest cost contributor during refueling outages is the cost of downtime, or of purchasing replacement power. Using the example of the three NUSCO Millstone plants, replacement power costs between twenty-five and thirty million dollars per

month, or about one million dollars per day. Millstone 3 accounts for 43% of the 2680 MWe (megawatts-electric) output of the three plants, so the cost of replacement power for Millstone 3 outages are typically about $430,000 per day. At Millstone-3, removal of the EDG teardowns from the refueling outage would reduce the outage length by two to three days per diesel, for a total replacement power savings of $1.7 million to $2.6 million, every eighteen months, or about $1.1 million to $1.7 million per year [38].

The other two large cost contributors during refueling outages are labor and EDG vendor support. For a typical refueling inspection, Coltec (Fairbanks-Morse) support adds about $150,000 to the total cost. Labor for the diesel teardowns, between 250 and 280 man-hours, totals roughly $15,000 per outage [8] [38].

The total costs associated with the refueling outage inspections are about $1.89 million to $2.75 million per refueling outage, or $1.26 million to $1.83 million per year.

The second contributor to cost reductions is the use of preventive maintenance to schedule repair work better and to anticipate serious failures before they occur. The amount of cost savings that this action will generate depends entirely upon the effectiveness of the monitoring system as found through experimentation.

Report NUREG/CR-5994 indicates that there are real, achievable, safety and cost improvements available with preventive maintenance. The switch from purely corrective maintenance to preventive maintenance is already well under way; currently, two-thirds of maintenance out of service time is used for preventive maintenance, while only one-third of maintenance time is spent on corrective maintenance [21]. However, much of this preventive maintenance is being performed blindly, following a fixed schedule for component replacement or adjustment. We expect that any monitoring which can identify potential failures will reduce these costs and unavailabilities further.

The SwRI report similarly suggests that significant cost savings can be realized through the use of preventive maintenance practices, and that troubleshooting, data trending, and analysis time and costs could be reduced with a monitoring system

[4]. The authors also indicate that monitoring systems have an excellent track record in reducing costs and improving reliability in other maintenance-intensive industries, such as chemical processing industries, manufacturing, and other diesel engine uses.

7.4.2 Added Costs

The implementation of a complex monitoring system will cause power plants to incur new expenses. Generally, there will be development costs for a new system, implementation costs for procuring and installing a system, analysis costs for creating a data baseline for comparisons, and training costs for EDG operators. These new costs are expected to be offset by delayed reductions in other maintenance costs and repair time and materials.

The SwRI report, *Surveillance, Monitoring, and Diagnostic Techniques to Improve Diesel Generator Reliability* [4], offers an analysis of the costs to develop an intensive monitoring system for an EDG. This analysis includes factors of hardware development and installation in both the EDG room and the control room, as well as the development of software for monitoring, trending analysis, and diagnostic purposes.

The 1988 estimate for the cost of the first prototype system is about $927,000, a breakdown of which is presented in Table 7.3. Subsequent installations at other plants, assuming negligible differences, would be reduced to $241,000. Each additional EDG at a plant with monitoring in place would add about $148,000 to the total cost. These costs are also itemized in Table 7.3. However, the monitoring encompassed by the SwRI system is significantly more intensive than that proposed here. While costs would be anticipated to have increased in the nine years since this study, the advancement of technology over the same period can be expected to help offset this increase.

7.5 Summary

The benefits to be realized from the proposed monitoring system include both unavailability and cost reductions. Monitoring of a small set of EDG components can

Stage	Type or Location	Initial Install Costs	Subsequent Install Costs	Additional EDG Costs
System Development	**Total**	**$247,152**	**$21,378**	**$0**
Hardware	EDG Room	$40,329	$40,329	$40,329
	Control Room	$23,088	$23,088	$0
	Total	**$63,417**	**$63,417**	**$40,329**
Installation	EDG Room	$173,347	$132,473	$105,578
	Control Room	$19,247	$19,247	$0
	Total	**$192,594**	**$151,720**	**$105,578**
Software	Monitoring	$98,014	$0	$0
	Trend Analysis	$73,220	$0	$0
	Diagnostic	$252,462	$4,257	$2,000
	Total	**$423,696**	**$4,257**	**$2,000**
Total	**Total**	**$926,859**	**$240,772**	**$147,907**

Table 7.3: SwRI Estimated Monitoring Costs

significantly reduce the failure rate of the EDG, and can help to eliminate unnecessary and often destructive repair work during refueling outages. The reduced EDG failure rate is used to justify an extended surveillance interval and test duration for the EDG, which further reduces the EDG unavailability, by means of testing more efficiently. The cost savings obtained from the elimination of the refueling outage inspections are sufficient to recover the expense of adding the proposed monitoring system; cost reductions incurred with the successful use of preventive maintenance, and resulting from reduced diagnosis and repair times can be applied to furthering safety improvements in other areas of nuclear power plants.

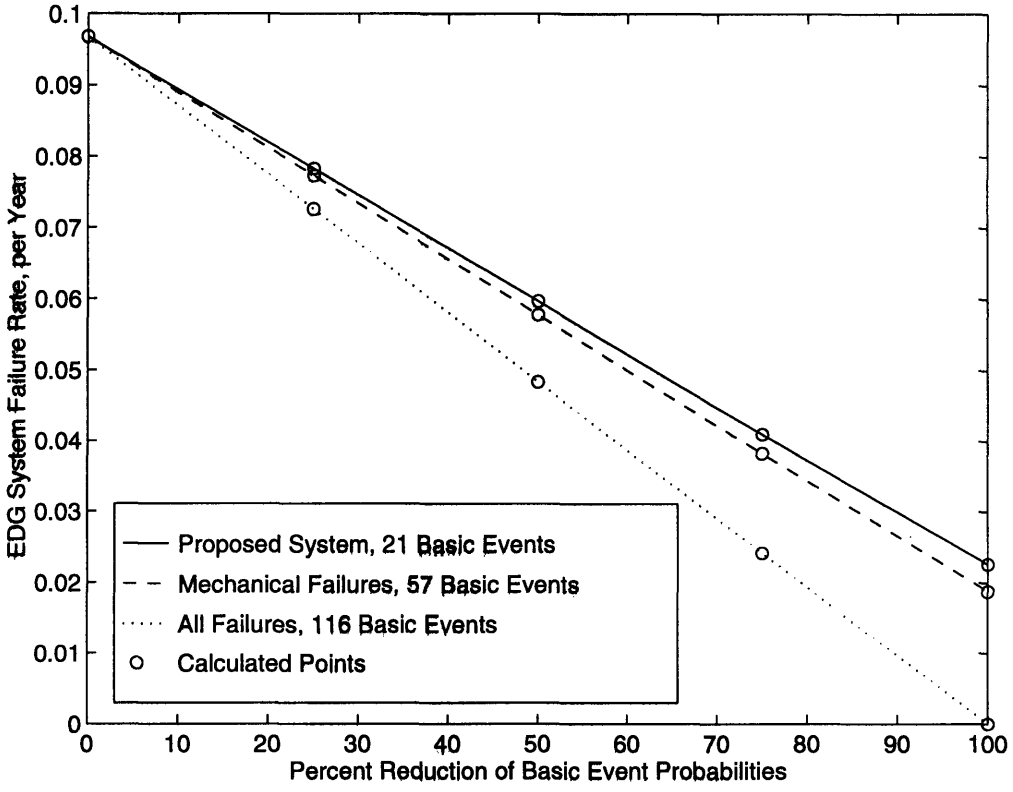


Figure 7-1: Effect of Basic Event Failure Frequency Reduction upon Diesel Failure Rate

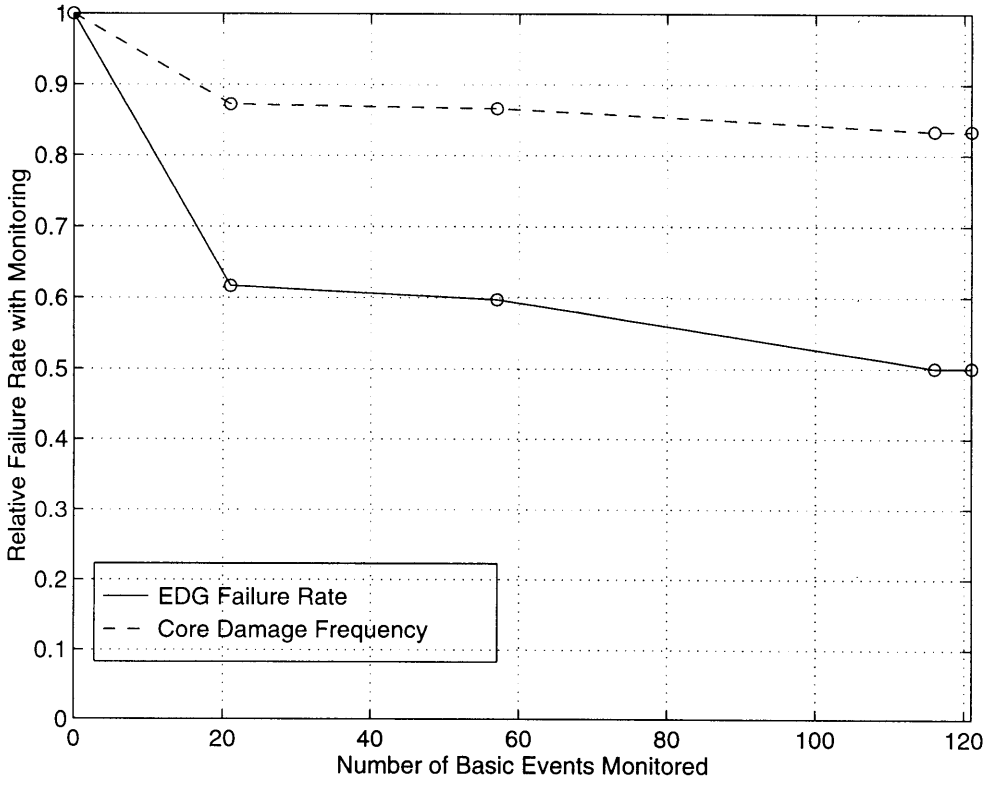


Figure 7-2: Effect of the Number of Monitored Basic Events upon the CDF and the EDG Failure Rate

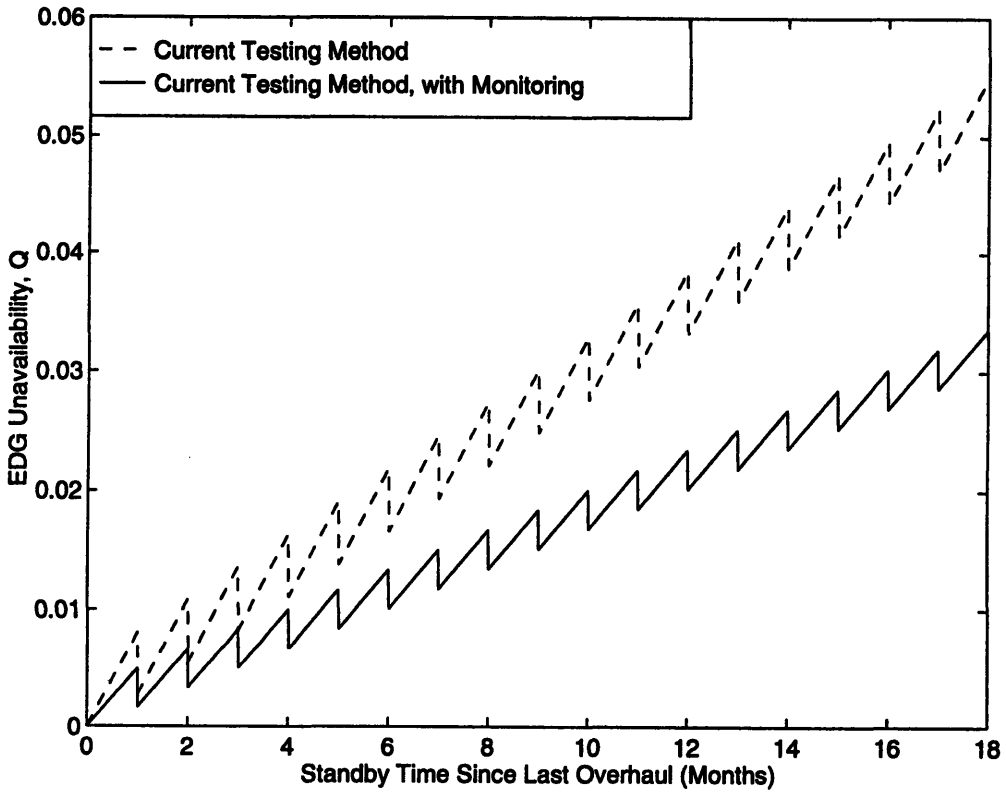


Figure 7-3: Effects of Monitoring upon EDG Unavailability, Contrasting Current Testing Methods and Testing Combined with Monitoring

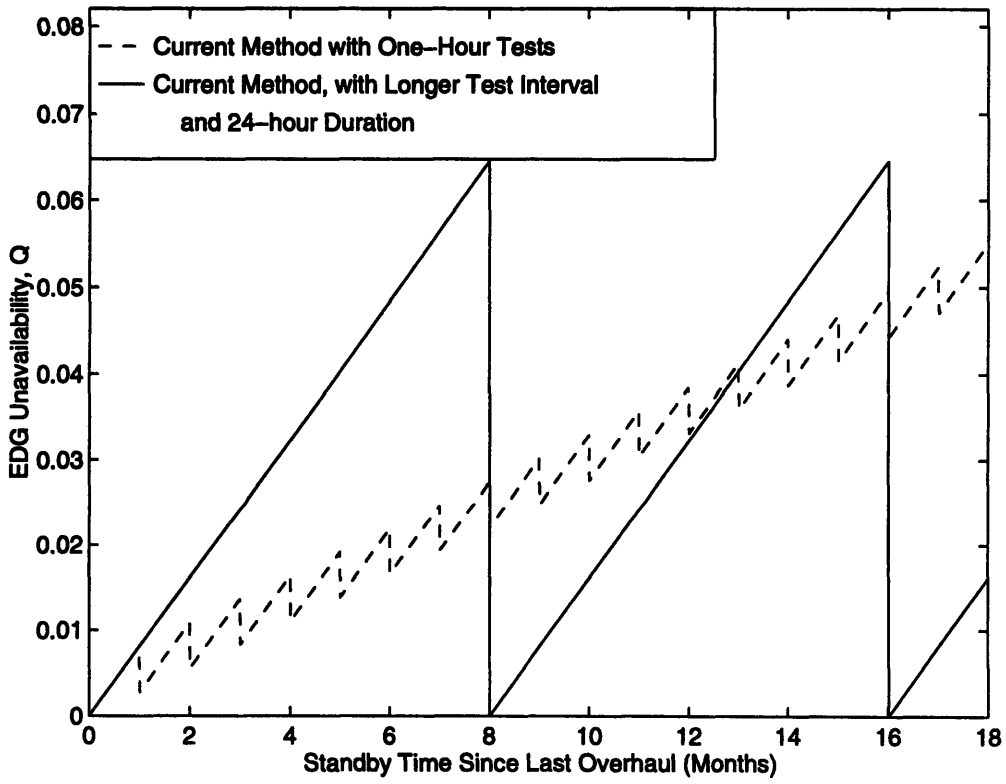


Figure 7-4: Effects of Increased Test Intervals and Test Duration upon EDG Unavailability Compared to Results with Current Testing Methods

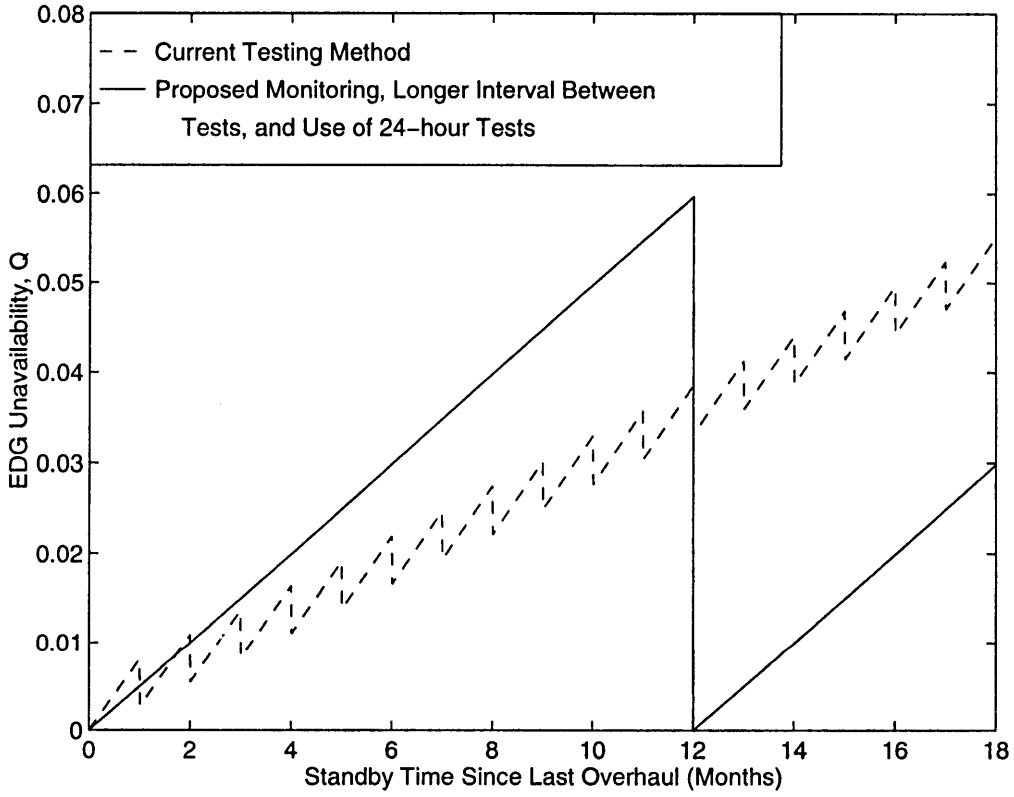


Figure 7-5: Effects upon EDG Unavailability of Proposed Monitoring and Testing Changes, Compared to Results of Current Testing Methods

Chapter 8

Risk Assessment

8.1 Introduction

Before NRC approval of any proposed changes is granted, it is necessary to demonstrate that the proposed changes will not increase the risk level at the plant, and that preferably, the changes will lower the risk level.

The reduction of risk levels with the use of monitoring is demonstrated first by satisfying the recommendations of Draft Guide DG-1065, *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications* [22]. These recommendations include the satisfaction of defense-in-depth principles and the maintenance of current levels of availability. Demonstration that the proposed monitoring systems and other proposed changes to testing intervals and duration increase safety levels have been made previously, and demonstration that no significant new failure modes are caused by the monitoring system are offered below.

8.2 Changes to Technical Specifications

The NRC draft guide DG-1065, *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications* [22], is used here to verify that the proposed changes to the Technical Specifications can be accepted by the NRC.

The guide offers a four-element approach for the implementation of risk-based

changes to technical specifications, as follows.

"Element 1: Define the proposed Technical Specification change" requires the clear definition of all Specifications which are to be affected by the proposed changes. In this particular case, the changes proposed affect surveillance requirements 3.8.1.2 through 3.8.1.20, as defined in Table 4.3.

"Element 2: Conduct engineering evaluations" includes the failure assessments performed in this report, as well as the trial basis implementation and expert elicitations used to produce baseline standards. This element will be completed when an accurate assessment of the availability gains due to basic event rate reduction is obtained.

"Element 3: Develop implementation and performance monitoring strategies" will partially be satisfied by the experimentation described in Element 2. Further evaluation of the effectiveness of the monitoring system to predict failures may be required by the NRC for full approval.

"Element 4: Document evaluations and submit request" is the final stage of utility application for changes to the licensing basis. The work proposed above will have to be conducted while complying with current Technical Specifications, so only the predictive capabilities of the monitoring system can be tested, while the benefits of surveillance interval and duration changes will have to be assessed through engineering evaluations and not experimentation.

The five key principles proposed in the guide to describe the review process are that the proposed change meets current regulations for safety, that defense-in-depth is maintained, that sufficient safety margins are maintained, that proposed changes do not increase risks to public health and safety, and that the performance of these new changes is monitored, such that uncertainties in modeling and analysis can be addressed.

As the analysis of the benefits of the monitoring system have discussed, the proposed changes can only improve safety levels. Significant benefits are expected, while

only negligible disadvantages are anticipated, as is discussed in the next section. The current compliance with defense-in-depth principles is not changed, as no equipment is being removed from service, and all redundancy is maintained or improved, as with sensing systems. Further, proposed changes to the governing, electrical, and controls systems can significantly improve the availability of the critical EDG system. Clearly, no new risks are posed to the reactor or the public. Finally, the last principle, of continued monitoring, is the very nature of the proposed system. By trending collected data, the performance of the EDG, its support systems, and its new monitoring system are continually updated and revised.

The draft guide DG-1065 offers a roadmap, as discussed here, for verifying, as the NRC will, that any proposed changes will not pose safety risks. This report, when combined with an experimental implementation of the sensing system, can be used to satisfy NRC concerns prior to approval of the proposed changes.

8.3 Added Risks

The use of an instrumentation and monitoring system can expose the EDG to two new types of failures. The monitoring system can fail to predict failures, and the monitoring system can create new failure modes.

8.3.1 Failure of the Monitoring System

The failure of the monitoring system can occur in three ways. The sensors may fail to report correctly on operating conditions, components may fail without exceeding the warning criteria set in the failure model, and components may fail in ways that the monitoring system cannot assess. Each of these failure modes is discussed below.

The first potential failure mode for the monitoring system is a failure of the sensors to accurately report operating conditions. This failure mode should typically be a small contributor to the overall failure rate for the monitoring system. Most industrial-grade instruments available today meet or exceed 99% reliability, provided they are used as designed. Sample failure rates for some pressure and temperature

sensors are offered in the Advanced Light Water Reactor reports [13]. Typical values for these failures are 6.0 E-6 per hour for a flow transmitter, 5.0 E-6 for a pressure transmitter or level transmitter, and 1.0 E-6 for a temperature transmitter.

We propose that current standards used by the NRC and the utilities in formulating licensing bases be employed in selecting appropriate sensors. In the Final Safety Analysis Report for the Millstone-3 plant [30], reference standards such as *Criteria for Protection Systems for Nuclear Power Plants*, IEEE Standard 279 [40]; *Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*, IEEE Standard 338 [41]; and *Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations*, IEEE Standard 336 [42] are applied for initial sensor system designs, and would be similarly applicable for such changes to the design basis.

The failure of the sensors to report accurately includes false reports of negative conditions when none are present (this is the typical mode of current EDG trip failures) and failing to report a negative condition when one is present. The former is less of a concern, as a sensor can be self-tested, and traditional means can be used to assess the performance of the EDG component in question; as these sensors are not capable of tripping the EDG, a false negative signal would not disable the system without human interaction.

The failure to report a negative signal is of greater concern, as no indication is given that there may be a problem. To prevent these failures, highly reliable sensors must be used, and redundancy, or voting systems, should be employed [36].

The second monitoring system failure mode is the failure of a component without exceeding warning criteria used in the failure model. The failure model is not as easily optimized as a sensing system; it is formulated by combining the operating baseline for an EDG with evaluations from component experts. As such, the level of reliability is restricted. Generally, an arbitrarily accurate model can be created, but excessively high accuracy will be overly restrictive, suggesting the need for frequent replacement of components which may be quite far from failure. This failure mode

will be explored most effectively with experimentation on EDG failure modes. Additionally, the accuracy of the model can be specified during experimentation to give the desired total accuracy of the entire monitoring system.

The final failure mode of the monitoring system is the failure of a monitored component by a mode not interrogated with current sensors. The effects of these component failure modes can be reduced by either expanding the set of sensors utilized, or by testing these components to verify their availability. As is discussed above, the proposed monitoring approach utilizes a small set of sensors, designed for detecting the largest contributors to the EDG failure rate. As such, it interrogates failure modes accounting for nearly 95% of all risks, and it is anticipated that any additional expansion of the monitoring system would have a very poor return for the effort. As such, testing is the only effective means of identifying these failure modes. While the data presented above show that the surveillance interval can be extended to more than one year, it is advisable to restrict the interval to twelve months; this decreases the interval between tests which could reveal failures not addressed by the monitoring system. Similarly, the monthly surveillance test proposed for the EDG support systems helps to reduce the contributions of these modes to the overall EDG failure rate by increasing the test frequency.

8.3.2 Failure of the EDG Due to Monitoring

The use of a monitoring system can also cause new failure modes for the EDG system. The potential for failures is assessed generally by separating all proposed sensors into functional groups: vibration sensors; flow, pressure, and fluid temperature sensors; level sensors; and cylinder pressure sensors. The risk contribution of each of these groups is evaluated separately.

Vibration sensors are typically small, fully-enclosed sensors which are externally applied to stationary casings of moving parts. As such, they can rarely affect performance of the component in question. Vibration sensors, such as accelerometers, are typically held onto the component in question magnetically or using adhesives. In the event of a failure of the adhesion, an accelerometer could conceivably fall into

some moving component, but such a failure mode can be adequately prevented during installation if it is anticipated.

Flow, pressure, and temperature sensors for fluid systems are typically susceptible for causing two types of failure modes: contamination and leakage. Any opening of a closed, purified system, such as the fuel or lubricating oil, cooling water, or starting air systems, is subject to these failure modes. In order to reduce these contributors, design steps are necessary to verify the application of each sensor used, and to follow the design basis installation procedures used in the initial EDG instrumentation. As there are currently similar sensors utilized for EDGs, we expect that leakage and contamination concerns are small; for example, no such failure modes due to trip sensors are indicated in fault trees or the industrial data.

Level sensors, provided they are used within their design specifications, are not subject to any significant failure modes which could affect EDG performance. Level switches used currently to actuate fuel transfer pumps are subject to failures to start the pumps, but not to failure modes which directly incapacitate the train.

The most significant monitoring system failure contributors for the EDGs are the cylinder pressure sensors. These pressure sensors are subject to severe operating conditions, including high pressures, corrosive fluids, high temperatures, and combustion conditions. Additionally, any structural failure of these sensors could readily incapacitate the mechanical diesel engine, as any debris deposited inside the power cylinders would almost certainly cause internal damage. The reliability of these sensors is verified by the vendor for the engine analyzer, but periodic replacement or examination of the pressure sensors may be found to be necessary, and would not typically make an EDG unavailable for a significant period of time; vendor recommedations would indicate any required maintenance procedures. It should be noted that these sensors are designed with this application, and often higher pressures and temperatures, in mind. Provided that these sensors comply with all relevant standards, the contribution of sensors to the EDG failure rate should be exceedingly small.

8.4 Summary

The draft version of the new NRC tool for evaluating proposed changes to Technical Specifications, utilizing risk-based analyses, shows the concerns the NRC has for safety factors and defense-in-depth. The analysis of the failure modes encompassed by the proposed changes shows that safety levels of the EDG can be significantly improved with negligibly few new EDG failure modes. The defense-in-depth is not jeopardized, but improved, as is public safety and EDG system reliability. Weaknesses of the monitoring system are presented, and methods for minimizing their effects have been proposed. Of particular concern, relevant standards regarding the application of sensors to the EDG system have been proposed to comply with the original licensing basis.

Chapter 9

Recommendations

9.1 Introduction

This chapter summarizes the proposed recommendations made throughout this report. We propose a monitoring system for use, on an initial trial basis to verify the predicted results experimentally. Using the reduced failure rate found with the use of the monitoring system, we propose changes to the Technical Specifications of a plant, including the testing interval and the test duration. We further recommend changes regarding the replacement of particularly troublesome components and systems, such as the mechanical governors and the electro-mechanical logic networks which make up the electrical and controls systems. We recommend the use of expert elicitations for the creation of warning criteria in the failure mode models, but not for the evaluation of the effectiveness of monitoring. We also recommend that efforts be made to improve vibration analysis methods, which are critical to the success of the proposed monitoring system.

9.2 Proposed Monitoring

We propose to use performance monitoring for the EDG system to improve reliability and availability. From the failure data in Chapter 5, we recommend new instrumentation on the diesel engine, the service water pumps, and the EDG building ventilation

dampers. The proposed monitoring is summarized in Table 6.1, and is repeated in Table 9.1. Twenty-one of the 121 EDG fault tree basic events are involved in this monitoring. This monitoring system covers 94.9% of all EDG system failures; with a 50% reduction in the basic event rate for these twenty-one events, the failure rate of the EDG system can be reduced from 0.097 per year to 0.059 per year, a 41.6% reduction.

9.3 Trial Basis

We propose the implementation the above recommended monitoring system on a trial basis to verify how effectively basic event rates can be reduced. For much of the above analysis, a 50% reduction of basic event rates has been assumed. Figure 7-1, repeated in Figure 9-1, shows the effect of reducing basic event rates on the EDG system failure rate. Experimentation will allow an accurate assessment of where on the line in Figure 9-1 this system lies.

9.4 Changes to Technical Specifications

Using the above reduced failure rates, and considering the efficacy of monthly surveillance tests as described in Table 4.8, three changes to the Technical Specifications are proposed: elimination of the teardown inspections during refueling outages, extension of the surveillance interval from one month to twelve months, and increasing the test run time for surveillance tests from one hour to twenty-four hours. Table 7.2, repeated below as Table 9.2, summarizes the effects of these changes on EDG unavailability.

The teardown inspections conducted during refueling outages have been described in Chapter 4 as excessively intrusive with little benefit realized. The monitoring system proposed here allows for the more complete and thorough examination of the same failure modes, without any of the disadvantages associated with rebuilding the EDG. We recommend the elimination of this unnecessary test.

With the reduced failure rate, as estimated above, and considering the ineffectiveness of the monthly surveillance tests, we propose to extend the surveillance interval from one month to twelve months. This change can reduce EDG unavailability, even without the benefits of monitoring, as illustrated in Figure 7-4. With the proposed extended test length included in combination with a monitoring system, the unavailability can be reduced significantly still further.

Considering the inefficacy of the monthly one-hour tests as compared to the twenty-four-hour tests, we propose to extend surveillance tests from one hour to twenty-four hours. By reducing the frequency of surveillance tests by one-sixth, the EDG time out of service due to the longer tests only makes a small contribution to EDG unavailability. This contribution is offset by the efficiency of twenty-four-hour tests for reducing the EDG unavailability, as is demonstrated in Figures 7-4 and 7-5, with monitoring. Figure 7-5 is repeated below, as Figure 9-2.

The cumulative effect of making these Technical Specification changes reduces average EDG unavailability by about 15%, as suggested by Table 7.2, but the emphasis in making these proposals is on minimizing the unnecessary testing and maintenance procedures. Significant cost savings are also outlined in Chapter 7.

9.5 Digital Governors and Improved Electrical and Controls Systems

The mechanical governors and electro-mechanical components of the electrical power output and instrumentation & controls systems are difficult to monitor, but are problematical. As such, we recommend that some redesign and replacement for these components be considered. The Southwest Research Institute and Idaho National Engineering Laboratory reports [4] [5] include similar recommendations, and similar problems are reported by various sources in the diesel engine industry [8] [33] [34] [35] [37].

Use of digital governors and solid-state logical components for controls systems and

electrical output would allow better surveillance, reduced vibration and contamination failures, and improved reliability. The development of sufficient instrumentation to similarly reduce these failure modes would be a serious undertaking with little real benefit assured.

9.6 Expert Elicitations

With the creation of baselines for the operating conditions for the monitored and trended EDG parameters, expert elicitations will be required to create a set of warning criteria. Experts on each component being monitored can be used to indicate how the monitored parameters should change from the baseline values prior to different failure modes. By reducing the role of elicitations from estimating the overall effectiveness of the monitoring system to giving engineering analysis on performance parameters, a much higher degree of accuracy is anticipated.

9.7 Review of Prelubrication Requirement

In the course of the data analysis for this report, two particular failure modes were discovered, which were not included in any available failure analysis, both regarding failures of opposed-piston diesel engines, due to prelubrication. One failure was observed in the U.S. Navy [35], where leaking upper seals allowed lubricating oil to drip into the combustion chamber and fill it. When the entire cylinder was filled and an EDG start was attempted, the lubricating oil acted as a hydraulic lock, preventing the EDG from starting, failing the system. Further review of this peculiar failure mode located another example, known to the EDG manufacturer, Fairbanks-Morse/Colt. In *Enhancement of On-Site Emergency Diesel Generator Reliability*, NUREG/CR-0660 [43], a failure due to prelubrication was identified. Like the Navy failure, lubricating oil in an opposed-piston engine leaked past the upper seals, into the combustion chamber. However, in this case, the pistons were in the outer positions, leaving the exhaust ports open (see Figure 3.4). The lubricating oil flowed through the outlets

into the exhaust headers, where it was ignited from the heat of the next EDG start. In the Navy case, the pistons were in the inner positions, covering the inlet and outlet ports (see Figure 3.4), such that the oil collected.

With the reduction of the number of starts from twelve per year to two per year, the starting-related wear which prompted the prelubrication requirement [18] should be greatly reduced. As such, the current application of prelubrication for the opposed-piston engines should be reconsidered.

In the Fairbanks Morse/Colt case, the manufacturers reiterated that their recommendation was for two to three minutes of prelubrication prior to starting, as compared to the then-standard fifteen to thirty minute prelubrication period; sufficient lubricant volume to cause these failures should not have accumulated in that time frame. Contrary to these recommendations, current procedures include prelubrication at all times, possibly exposing the EDGs to serious failure modes with little proven need.

System	Component or Failure Mode	Monitored Parameter	Engine Analyzer?
Engine	Cylinder	Pressure	Yes
		Exhaust Temperature	Yes
		Vibration	Yes
	Fuel Rack	Position	Yes
	Crankshaft	Position	Yes
	Bearings	Vibration	Some
		Temperature	Some
Fuel Oil	Tanks	Level	No
	Fuel Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
Cooling Water	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
	Coolant to Engine	Temperature	Some
	Coolant from Engine	Temperature	Some
Lubricating Oil	Oil	Chemical Analysis	Some
	Tanks	Level	No
	Lines	Pressure	No
	Pumps	Differential Pressure	No
		Vibration	No
	Oil to Engine	Temperature	Some
	Oil from Engine	Temperature	Some
Starting Air	System	Pressure	No
	Compressor	Differential Pressure	No
		Vibration	No
	Air Dryer		No
			No
Turbocharger or Supercharger	Boost	Differential Pressure	No
	Intercooler	Inlet Temperature	Some
		Outlet Temperature	Some
	Charger	Vibration	No
Service Water	Pumps	Differential Pressure	No
		Vibration	No
Ventilation	Blowers	Air Flow	No
		Vibration	No
	Dampers	Vibration	No

Table 9.1: Proposed Component, Failure Mode, and Monitoring Variables

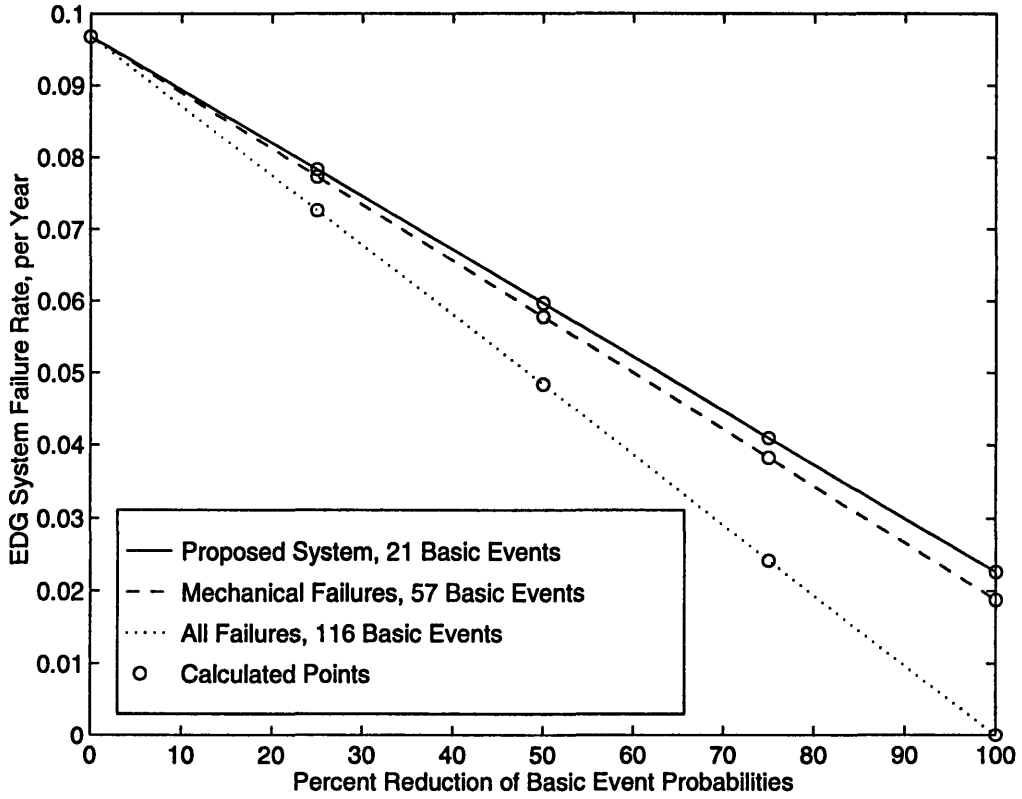


Figure 9-1: Effect of Monitoring-Based Basic Event Failure Frequency Reduction upon Diesel Failure Rate

	$\langle Q \rangle$	t_S	τ	λ	% Recovery
Current Methods	0.0385	1 month	1 hour	0.0968	66%
Monitoring	0.0313	1 month	1 hour	0.0594	66%
Testing Changes	0.0373	12 months	24 hours	0.0968	100%
Proposed Changes	0.0328	12 months	24 hours	0.0594	100%

Table 9.2: Effects of Monitoring, Testing Changes, and Combined Proposed Changes on EDG Average Unavailability

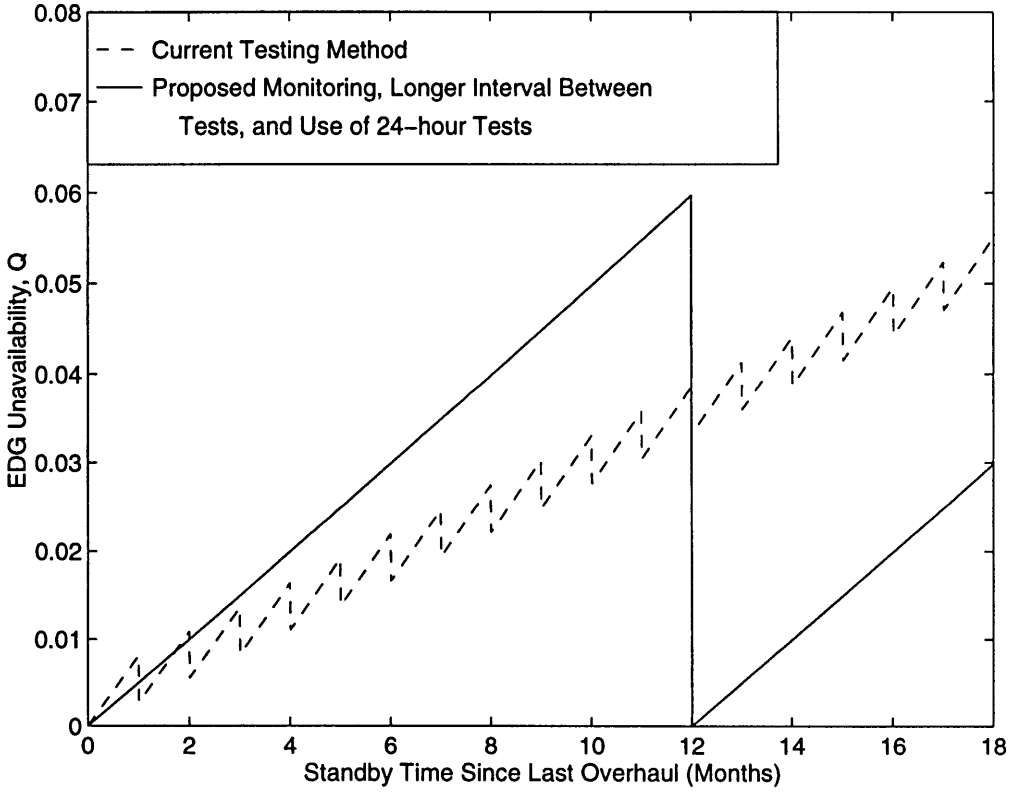


Figure 9-2: Effects upon EDG Unavailability of Proposed Monitoring and Testing Changes as Compared to Results of Current Testing Methods

Chapter 10

Conclusion

The work reported here demonstrates the significance of the emergency diesel generators for nuclear power plant safety. Using industry data and probabilistic risk assessment, this report proposes the application of a monitoring system to the emergency diesel generator system. This proposal includes monitoring and trending of the performance of service water pumps, EDG building ventilation dampers, and whole-engine analysis of the mechanical diesel engine. Additionally, instrumentation of EDG support components, including fuel oil, lubricating oil, cooling water, and starting air system rotating machinery and system leakage is proposed.

With instrumentation for sensing twenty-one of the 121 basic events in the EDG fault tree, the proposed monitoring system monitors 94.9% of the contributors to the EDG failure risk. With a 50% reduction in these twenty-one basic event failure rates, the EDG system failure rate is reduced by 41.6%, from 0.097 per year to 0.059 per year.

With capture of the reduced EDG system failure rate due to the monitoring system, we propose to extend the EDG surveillance interval from one month to twelve months, to lengthen the running tests from one hour to twenty-four hours, and to eliminate the tear-down inspections conducted during refueling outages. This optimization of the maintenance procedures helps to reduce unnecessary costs without jeopardizing EDG system or plant safety. With the EDG failure rate reduction and proposed changes to the testing procedure, the average EDG unavailability can be

reduced by 15% while attempting to maximize the surveillance interval.

Cursory cost estimates suggest the possibility of annual cost savings of $1.26 million to $1.83 million, just from the elimination of the tear-down inspections during refueling outages. Using SwRI estimates, a one-time development cost for a monitoring system would approach $1 million, but subsequent installations at plants with two EDGs would cost about $389,000. The typical savings anticipated with monitoring and preventive maintenance, reduced failures, reduced diagnosis and repair times and costs, and the ability to schedule preventive maintenance, would all result in savings above and beyond those already listed.

The total effectiveness of the monitoring system for reducing EDG system failure rates and unavailability, and the total cost savings which can be realized, can not be fully determined without the application of such a monitoring system on a trial basis. The work reported here demonstrates the feasible gains which can be realized, and proposes a method for evaluating the efficacy of the system as realized through experimentation.

Further recommendations proposed here include some redesign of the governor, of the electrical power output system, and of the instrumentation and controls system. By replacing these older mechanical and electro-mechanical components with solid-state or digital systems, higher reliability and independent testing can be realized.

Reconsideration of the prelubrication requirement is also suggested for opposed-piston diesel engines, as the need for this practice is reduced with fewer starts, and serious failure modes can be caused by this practice.

With these proposals, significant safety and cost benefits can be realized by nuclear power utilities. Unnecessary and unfounded regulations can be replaced for the greater good of the industry and public safety, and the nuclear power industry can continue to compete in a deregulated industry.

References

[1] *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* WASH-1400, NUREG-75/014, October 1975.

[2] Utton, Shantel. *Study of the Nuclear Regulatory Commission's Required Refueling Outage Inspection of Nuclear Utility Emergency Diesel Generators.* MIT Report No. MIT-ANP-TR-057.

[3] Millstone 3 Probabilistic Risk Assessment, Northeast Utilities Services Company.

[4] Driscoll, G.D., et al., *Surveillance, Monitoring, and Diagnostic Techniques to Improve Diesel Generator Reliability.* Southwest Research Institute, EPRI Report NP-5924, July 1988.

[5] Grant, G.M., et al., *Emergency Diesel Generator Power System Reliability: 1987-1993.* INEL-95/0035, February 1996.

[6] *Nuclear Plant Reliability Data System.* Institute of Nuclear Power Operations, Atlanta, GA.

[7] Grotsky, Peter. *CVN-68 Class Emergency Diesel Generator (EDG) Reliability and Availability.* U.S. Navy Report, 9233 Ser. 03X3/331, October 1996.

[8] Personal Communication: Shanahan, Brian E. Millstone-3 EDG Engineer, 1996, 1997.

[9] *Severe Accident Risks: Assessment for Five U.S. Nuclear Power Plants: Final Summary.* NUREG-1150, December 1990.

[10] Battle, R.E. and D.J. Campbell, *Reliability of Emergency AC Power Systems at Nuclear Power Plants.* NUREG/CR-2989, July 1983.

[11] Battle, R.E. *Emergency Diesel Generator Operating Experience, 1981-1983.* NUREG/CR-4347, December 1985.

[12] *Analysis of Core Damage Failure from Internal Events.* NUREG/CR-4550, (Volume 1, Rev. 1) January 1990, (Volume 2) April 1989, (Volume 3, Rev. 1) April

1990, (Volume 4, Rev. 1) December 1990, (Volume 5, Rev. 1) April 1990, (Volume 6) April 1987, (Volume 7, Rev. 1) May 1990.

[13] *Advanced Light Water Reactor Utility Requirements Document.* Volumes I, II, and III. EPRI Report NP-6780-L, September 1990.

[14] NRC Regulatory Guide 1.108. *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power System at Nuclear Power Plants.* Rev. 1, August 1977.

[15] Baranowsky, P.W. *Evaluation of Station Blackout Accidents at Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-44, Draft Report for Comment.* NRC Report NUREG-1032, NTIS, 1985.

[16] U.S. Nuclear Regulatory Commission, 10CFR50.63, *Loss of All Alternating Current Power*, Proposed Rule, April 1992.

[17] NRC Regulatory Guide 1.155. *Station Blackout.* August 1988.

[18] NRC Generic Letter 84-15, *Proposed Staff Actions to Improve and Maintain Diesel Generator Reliability.* July, 1984.

[19] NRC Regulatory Guide 1.9. *Selection, Design, Qualification, and Testing of Emergency Diesel Generator Units Used as Class 1E Onsite Electric Power System at Nuclear Power Plants.* Rev. 3, July 1993.

[20] IEEE Standard 387, *IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations*, 1995.

[21] Samanta, P. et al. *Emergency Diesel Generator: Maintenance and Failure Unavailability, and Their Risk Impacts.* NUREG/CR-5994, November 1994.

[22] *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications.* NRC Draft Guide DG-1065, Rev. 5, February 1997.

[23] Abdelkader, Sarah. MIT Report No. MIT-ANP-TR-058.

[24] NUREG-0600. *Investigation into the March 28, 1979 Three Mile Island Accident by Office of Inspection and Enforcement.* August 1979.

[25] Apostolakis, G.E. *A Commentary on Model Uncertainty.* Proceedings of Workshop on Model Uncertainty: Its Characterization and Quantification. A. Mosleh, N. Siu, C. Smidts, and C. Lui, Eds. October 1993.

[26] Kumamoto, H. and E.J. Henley. *Probabilistic Risk Assessment and Management for Engineers and Scientists.* IEEE Press, 1996.

[27] Masui, Hideki. *Quantitative Methodology for Surveillance Interval Extension at Nuclear Power Plants.* S.M. Thesis, Massachusetts Institute of Technology, June 1996.

[28] Apostolakis, G. and T.L. Chu. "The Unavailability of Systems Under Periodic Test and Maintenance." *Nuclear Technology*, August 1980.

[29] *Seabrook Station Probabilistic Safety Assessment*, Seabrook Nuclear Power Plant, Northeast Utilities Services Company, August 1982.

[30] "Final Safety Analysis Report, Millstone Unit 3 Nuclear Power Plant", Docket Number 50-423, NUREG-1350, *NRC Information Digest*, 1997.

[31] *Standard Technical Specifications, Westinghouse Plants.* NUREG-1431, September 1992.

[32] Kates, E.J. and W.E. Luck. *Diesel and High Compression Gas Engines.* American Technical Publishers, 1974.

[33] Personal Communication: Grant, G.L. Idaho National Engineering Laboratory, 1996.

[34] Billig, R.G. and A.D. Gillette. *A Results Oriented Maintenance Approach for Nuclear Emergency Diesel Generators.* SAE (Society of Automotive Engineers) Paper No. 941810, September 1994.

[35] Personal Communication: Grotsky, Peter. U.S. Navy, Naval Sea Systems, 1996.

[36] Cluley, J.C. *Reliability in Instrumentation and Control.* Institute of Measurement and Control, 1993.

[37] Ryan, W.P. et al. *Application of a Digital Speed Governing System for Nuclear Emergency Diesel Generators.* SAE Paper No. 932443, September 1993.

[38] Personal Communication: Labrecque, Richard C. Millstone-3 Probabilistic Risk Assessment, 1996, 1997.

[39] Personal Communication: Stadnick, Stephen. Millstone-2 EDG Engineer, 1997.

[40] IEEE Standard 279. *Criteria for Protection Systems for Nuclear Power Plants*, 1971.

[41] IEEE Standard 338. *Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*, 1971.

[42] IEEE Standard 336. *Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations*, 1971.

[43] Boner, Gerald L. and Harvey W. Hanners. *Enhancement of On-Site Emergency Diesel Generator Reliability*, NUREG/CR-0660, University of Dayton Research Institute, February 1979.

Appendix A

Millstone 3 PRA

The following material is a summary of the fault tree information used in the Probabilistic Risk Assessment of the Northeast Utilities Services Company Millstone 3 plant [3].

Table A.1 includes a listing of the basic events which are used in the MP-3 fault tree. Any event code marked with a "%" is considered an initiating event, meaning it falls outside the EDG boundary. However, the key role that these events play in determining EDG availability require their inclusion.

Table A.2 includes a partial listing of the minimal cutsets for the MP-3 fault tree. Each cutset listing is numbered, and lists the individual names and contributions of each contributing basic event.

Figure A.1 includes the fault tree for MP-3. The basic events are identified by event codes and descriptions from Table A.1. Fault tree pages A-1 and S-1 contain many significant details, and are presented first. The remaining fault tree pages are presented in alphanumeric order.

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
1	%DCBCI301AFN	BATTERY CHARGER 1 FAILS DURING OPERATION	7.000e-06	H	8760	6.132e-02	0.000e+00
2	%DCBKI301ANF	DC PANEL 301A-1 BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.520e-06	H	8760	1.332e-02	0.000e+00
3	%DCBK1A301NF	DC PANEL 301A-1 BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.520e-06	H	8760	1.332e-02	0.000e+00
4	%DCBSI301AFN	METAL ENCLOSED DC BUS 301A1 BUS-TO-GROUND SHORT	2.000e-07	H	8760	1.752e-03	0.000e+00
5	%LOOP	LOSS OF OFFSITE POWER	1.000e+00	N/A	0.041	4.100e-02	1.602e-03
6	%SWEJEXJ1AFN	(INIT) EXPANSION JOINT EXJ1A RUPTURES	8.480e-08	H	8760	7.428e-04	1.534e-05
7	%SWEJEXJ1CFN	(INIT) EXPANSION JOINT EXJ1C RUPTURES	8.480e-08	H	8760	7.428e-04	5.861e-05
8	%SWMVI102AFN	(INIT) MOTOR OPERATED VALVE V102A FAILS TO REMAIN OPEN	1.400e-07	H	8760	1.226e-03	2.574e-05
9	%SWMVI102CFN	(INIT) MOTOR OPERATED VALVE V102C FAILS TO REMAIN OPEN	1.400e-07	H	8760	1.226e-03	1.121e-04
10	%SWP3IPMACFN	(INIT) CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAILS TO RUN	3.200e-05	H	876	2.803e-02	2.945e-01
11	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.200e-05	H	8760	2.803e-01	1.412e-02
12	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.200e-05	H	8760	2.803e-01	2.897e-02
13	ACAAVAV39ANN	SERVICE WATER OUTLET VALVE AOV39A FAILS TO OPEN ON DEMAND	2.000e-03	N	1	2.000e-03	2.101e-02
14	ACABK32T12NF	BUS FEED BREAKER 32T1-2 FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
15	ACABK32T42NF	BUS FEED BREAKER 32T4-2 FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
16	ACABK32T62NF	BUS FEED BREAKER 32T6-2 FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
17	ACABK34C1TNN	34A TO 34C BUS TIE BREAKER 34C-1T-2 FAILS TO OPEN ON DEMAND	1.580e-04	N	6	9.480e-04	9.958e-03
18	ACABK34C32NF	BUS FEED BREAKER 34C3-2 FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
19	ACABK42P1AFF	TRANSFER PUMP *P1A '42 BREAKER' FAILS TO CLOSE	3.380e-04	N	1	3.380e-04	0.000e+00
20	ACABK42P1CFF	TRANSFER PUMP *P1C '42 BREAKER' FAILS TO CLOSE	3.380e-04	N	1	3.380e-04	0.000e+00
21	ACABKESWGANF	BUS FEED BREAKER TO 34C AUX CIRCUIT FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
22	ACABKF1A42FF	'42 BREAKER' FOR *FN1A FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	3.550e-03
23	ACABKF1C42FF	'42 BREAKER' FOR *FN1C FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	3.550e-03

Table A.1: Basic Events

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
24	ACABKG14U2FF	DIESEL GENERATOR A OUTPUT BREAKER FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	3.550e-03
25	ACABKLSHEDNN	FAILURE TO SHED MAJOR EQUIPMENT LOADS (BREAKERS FAIL TO OPEN)	1.580e-04	N	30	4.740e-03	4.979e-02
26	ACABSBS32TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (BUS 32T)	2.000e-07	H	24	4.800e-06	5.042e-05
27	ACABSBS34CFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (BUS 34C)	2.000e-07	H	24	4.800e-06	5.042e-05
28	ACABSM321TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (MCC 32-1T)	2.000e-07	H	24	4.800e-06	5.042e-05
29	ACABSM325TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (MCC 32-5T)	2.000e-07	H	24	4.800e-06	5.042e-05
30	ACABSVIAC1FN	METAL ENCLOSED BUS VIAC-1 BUS-TO-GROUND SHORT	2.000e-07	H	24	4.800e-06	5.042e-05
31	ACACP27R56FF	CONTACT PAIR 27R56 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	8.508e-03
32	ACACP27Y12FF	CONTACT PAIR 27Y12 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	0.000e+00
33	ACACP62V13FF	CONTACT PAIR 62V13 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	8.508e-03
34	ACACP62W15FF	CONTACT PAIR 62W15 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	8.508e-03
35	ACACP62Y62FF	CONTACT PAIR 62Y62 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	0.000e+00
36	ACACPCA1B1FF	CONTACT PAIR 3A-3EGS*EG-A CA1-CB1 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	8.508e-03
37	ACACPCC1D1FF	CONTACT PAIR 3A-3EGS*EG-A CC1-CD1 FAILS TO CLOSE	1.350e-04	N	6	8.100e-04	8.508e-03
38	ACADG3EGSAAQ	DIESEL GENERATOR A UNAVAILABLE DUE TO TEST OR MAINTENANCE	1.100e-02	N	1	1.100e-02	1.155e-01
39	ACADG3EGSANN	DIESEL GENERATOR A FAILS TO START ON DEMAND (INCLUDES FAILURE TO RUN)	1.640e-02	N	1	1.640e-02	1.723e-01
40	ACADMDM20ANN	OUTLET DAMPER 20A FAILS TO OPEN	4.000e-03	N	1	4.000e-03	4.202e-02
41	ACADMDM20CNN	OUTLET DAMPER 20C FAILS TO OPEN	4.000e-03	N	1	4.000e-03	4.202e-02
42	ACADMDM23ANN	INLET DAMPER 23A FAILS TO OPEN	4.000e-03	N	1	4.000e-03	4.202e-02
43	ACADMDM26AFF	RECIRC DAMPER 26A FAILS TO CLOSE	4.000e-03	N	1	4.000e-03	4.202e-02
44	ACAESEGLSANN	EDG LOAD SEQUENCER 'A' FAILS ON DEMAND	1.000e+00	N/A	0.000758	7.580e-04	7.962e-03
45	ACAFNVFN1AFN	FAN UNIT *FN1A FAILS TO RUN	7.890e-06	H	24	1.894e-04	1.989e-03

Table A.1: Basic Events (cont'd.)

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
46	ACAFNVFN1ANN	FAN UNIT *FN1A FAILS TO START	4.840e-04	N	1	4.840e-04	5.084e-03
47	ACAFNVFN1ANQ	FAN UNIT *FN1A OUT OF SERVICE FOR MAINTENANCE	5.660e-04	N	1	5.660e-04	5.945e-03
48	ACAFNVFN1CFN	FAN UNIT *FN1C FAILS TO RUN	7.890e-06	H	24	1.894e-04	1.989e-03
49	ACAFNVFN1CNN	FAN UNIT *FN1C FAILS TO START	4.840e-04	N	1	4.840e-04	5.084e-03
50	ACAFNVFN1CNQ	FAN UNIT *FN1C OUT OF SERVICE FOR MAINTENANCE	5.660e-04	N	1	5.660e-04	5.945e-03
51	ACAFUVIAC1NF	FUSE VIAC1 FAILS TO REMAIN CLOSED	5.000e-07	H	24	1.200e-05	1.261e-04
52	ACAININV1AFN	DC TO AC POWER INVERTER-1 FAILS DURING OPERATION	2.000e-05	H	24	4.800e-04	5.042e-03
53	ACALSLS40ANN	LEVEL SWITCH LS40A FAILS TO OPERATE (LOW DAY TANK LEVEL)	1.000e-05	N	1	1.000e-05	0.000e+00
54	ACALSLS41ANN	LEVEL SWITCH LS41A FAILS TO OPERATE (LOW-LOW DAY TANK LEVEL)	1.000e-05	N	1	1.000e-05	0.000e+00
55	ACAPMEFP1AFN	FUEL OIL TRANSFER PUMP *P1A FAILS TO RUN	2.500e-05	H	24	6.000e-04	1.261e-05
56	ACAPMEFP1ANN	FUEL OIL TRANSFER PUMP *P1A FAILS TO START	2.000e-03	N	1	2.000e-03	5.462e-05
57	ACAPMEFP1CFN	FUEL OIL TRANSFER PUMP *P1C FAILS TO RUN	2.500e-05	H	24	6.000e-04	1.261e-05
58	ACAPMEFP1CNN	FUEL OIL TRANSFER PUMP *P1C FAILS TO START	2.000e-03	N	1	2.000e-03	5.462e-05
59	ACARCR27Y2NN	RELAY COIL 27Y2 FAILS TO ENERGIZE	1.000e-04	N	6	6.000e-04	0.000e+00
60	ACARCRC27RNN	RELAY COIL 27R FAILS TO DEENERGIZE	1.000e-04	N	6	6.000e-04	6.303e-03
61	ACARCRC62VNN	RELAY COIL 62V FAILS TO ENERGIZE	1.000e-04	N	6	6.000e-04	6.303e-03
62	ACARCRC62WNN	RELAY COIL 62W FAILS TO ENERGIZE	1.000e-04	N	6	6.000e-04	6.303e-03
63	ACARCRC62YNN	RELAY COIL 62Y FAILS TO ENERGIZE	1.000e-04	N	6	6.000e-04	0.000e+00
64	ACATKFTK1ATN	FUEL OIL STORAGE TANK TK1A RUPTURES	1.000e-07	H	24	2.400e-06	2.521e-05
65	ACATKFTK2ATN	FUEL OIL DAY TANK TK2A RUPTURES	1.000e-07	H	24	2.400e-06	2.521e-05
66	ACATR4C31XFN	TRANSFORMER 34C3-1X FAILS TO OPERATE	1.200e-06	H	24	2.880e-05	3.025e-04
67	ACATSTS32ANN	TEMPERATURE SWITCH TS32A FAILS TO OPERATE	2.000e-04	N	1	2.000e-04	2.101e-03
68	ACCAVV39ABNN	CCF - SW AIR OPERATED VALVES *39A,B FAIL TO OPEN ON DEMAND	2.000e-03	N	0.068	1.360e-04	1.429e-03
69	ACCDG3EGSXNN	CCF OF DGs TO START ON DEMAND (INCLUDES FAILURE TO RUN)	1.640e-02	N	0.068	1.115e-03	1.171e-02

Table A.1: Basic Events (cont'd.)

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
70	ACCPMFP1ACFN	COMMON CAUSE FAILURE TO RUN OF TRANSFER PUMPS *P1A AND *P1C	2.500e-05	H	2.4	6.000e-05	6.303e-04
71	ACCPMFP1ACNN	COMMON CAUSE FAILURE TO START OF TRANSFER PUMPS *P1A AND *P1C	2.000e-03	N	0.1	2.000e-04	2.101e-03
72	DCABK31A1ANF	DC PANEL 301A-1A BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
73	DCABK31A1BNF	DC PANEL 301A-1B BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
74	DCABKA1301NF	DC PANEL 301A-1 BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
75	DCABKINV1ANF	DC BUS 301A-1 FEED BREAKER TO INV1 FAILS TO REMAIN CLOSED	1.520e-06	H	24	3.648e-05	3.832e-04
76	DCABS301A1FN	METAL ENCLOSED DC BUS-TO-GROUND SHORT (DC PANEL 301A-1)	2.000e-07	H	24	4.800e-06	5.042e-05
77	DCABS301AAFN	METAL ENCLOSED DC BUS 301A-1A BUS-TO-GROUND SHORT	2.000e-07	H	24	4.800e-06	5.042e-05
78	DCABS301ABFN	METAL ENCLOSED DC BUS 301A-1B BUS-TO-GROUND SHORT	2.000e-07	H	24	4.800e-06	5.042e-05
79	DCABT301A1FN	STORAGE BATTERY 301A-1 FAILS TO PROVIDE OUTPUT ON DEMAND	5.000e-04	N	1	5.000e-04	5.252e-03
80	HVABK42F2AFF	'42 BREAKER' FOR VENTILATION UNIT HVY*FN2A FAILS TO CLOSE	3.380e-04	N	1	3.380e-04	2.814e-03
81	HVADAAD23ANN	AIR OPERATED DAMPER *23A FAILS TO OPEN	2.000e-03	N	1	2.000e-03	1.662e-02
82	HVAFNEFN2AFN	VENTILATION UNIT HVY*FN2A FAILS TO RUN	7.890e-06	H	24	1.894e-04	1.989e-03
83	HVAFNEFN2ANN	VENTILATION UNIT HVY*FN2A FAILS TO START	4.840e-04	N	1	4.840e-04	4.021e-03
84	HVATSTS60ANN	TEMPERATURE SWITCH TS60A FAILS TO OPERATE	2.000e-04	N	1	2.000e-04	1.662e-03
85	HVCDAD23ABNN	CCF - AIR OPERATED DAMPERS *23A AND *23B FAIL TO OPEN	2.000e-03	N	0.068	1.360e-04	1.130e-03
86	HVCFNFN2ABFN	CCF - VENTILATION UNITS HVY*FN2A, FN2B FAIL TO RUN	7.890e-06	H	2.4	1.894e-05	1.989e-04
87	HVCFNFN2ABNN	CCF - VENTILATION UNITS HVY*FN2A, FN2B FAIL TO START	4.840e-04	N	0.1	4.840e-05	4.021e-04
88	NOTSUMMER	NOT SUMMER OPERATION	1.000e+00	N/A	0.75	7.500e-01	0.000e+00
89	SWABKBKP1AFF	PUMP SWP*P1A START CIRCUIT BREAKER FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	4.979e-04
90	SWABKBKP1CFF	PUMP SWP*P1C START CIRCUIT BREAKER FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	4.979e-04
91	SWABKV102AFF	BUS FEED BREAKER FOR V102A FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	4.979e-04

Table A.1: Basic Events (cont'd.)

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
92	SWABKV102CFF	BUS FEED BREAKER FOR V102C FAILS TO CLOSE ON DEMAND	3.380e-04	N	1	3.380e-04	4.979e-04
93	SWACP52A34FF	PUMP 'A' CONTACT PAIR 52S 53-54 FAILS TO CLOSE	1.350e-04	N	132	1.782e-02	0.000e+00
94	SWACP52C34FF	PUMP 'C' CONTACT PAIR 52S 53-54 FAILS TO CLOSE	1.350e-04	N	132	1.782e-02	0.000e+00
95	SWACP63X12FF	LOW HEADER PRESSURE CONTACT PAIR 63X12 FAILS TO CLOSE	1.350e-04	N	132	1.782e-02	3.345e-04
96	SWACP63X56FF	LOW HEADER PRESSURE CONTACT PAIR 63X56 FAILS TO CLOSE	1.350e-04	N	132	1.782e-02	3.345e-04
97	SWACVCV768NN	PUMP 'C' LUBRICATION FAILS (CHECK VALVE -768 FAILS TO OPEN)	2.000e-04	N	1	2.000e-04	2.941e-04
98	SWACVCV769NN	PUMP 'A' LUBRICATION FAILS (CHECK VALVE -769 FAILS TO OPEN)	2.000e-04	N	1	2.000e-04	2.941e-04
99	SWACVP1AV7NN	CHECK VALVE P1A*V7 FAILS TO OPEN ON DEMAND	2.000e-04	N	1	2.000e-04	2.941e-04
100	SWACVP1CV5NN	CHECK VALVE P1C*V5 FAILS TO OPEN ON DEMAND	2.000e-04	N	1	2.000e-04	2.941e-04
101	SWAMVV102ANN	MOTOR OPERATED VALVE V102A FAILS TO OPEN ON DEMAND	4.000e-03	N	1	4.000e-03	5.951e-03
102	SWAMVV102CNN	MOTOR OPERATED VALVE V102C FAILS TO OPEN ON DEMAND	4.000e-03	N	1	4.000e-03	5.950e-03
103	SWAP3SWP1AAQ	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE	1.100e-02	N	1	1.100e-02	1.634e-02
104	SWAP3SWP1AFN	SERVICE WATER PUMP SWP1A FAILS TO RUN	3.200e-05	H	24	7.680e-04	1.329e-03
105	SWAP3SWP1ANN	SERVICE WATER PUMP SWP1A FAILS TO START ON DEMAND	2.400e-03	N	1	2.400e-03	3.545e-03
106	SWAP3SWP1CCQ	SERVICE WATER PUMP SWP1C OOS FOR MAINTENANCE	9.000e-04	N	1	9.000e-04	1.324e-03
107	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.200e-05	H	24	7.680e-04	1.373e-03
108	SWAP3SWP1CNN	SERVICE WATER PUMP SWP1C FAILS TO START ON DEMAND	2.400e-03	N	1	2.400e-03	3.529e-03
109	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD	1.000e+00	N/A	0.5	5.000e-01	1.435e-02
110	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD	1.000e+00	N/A	0.5	5.000e-01	2.938e-02
111	SWAPSPS27ANN	PRESSURE SWITCH PS27A FAILS TO OPERATE	2.000e-04	N	132	2.640e-02	9.895e-04
112	SWCCV5AND7NN	CCF OF CHECK VALVES V5 AND V7 FAILS TO OPEN ON DEMAND	2.000e-04	N	0.068	1.360e-05	0.000e+00
113	SWCCV76869NN	COMMON CAUSE FAILURE OF LUBE LINE CHECK VALVES V768 AND V769 TO CLOSE	2.000e-04	N	0.068	1.360e-05	0.000e+00

Table A.1: Basic Events (cont'd.)

Event #	Basic Event Code	Description	Rate	Unit	Exposure	Probability	Fussell-Vesely
114	SWCCVL4OF4NN	CCF OF ALL 4 LUBE LINE CHECK VALVES TO OPEN	2.000e-04	N	0.00029	5.800e-08	0.000e+00
115	SWCCVV4OF4NN	CCF OF ALL 4 DISCHARGE CHECK VALVES TO OPEN	2.000e-04	N	0.00029	5.800e-08	0.000e+00
116	SWCMV102ACNN	CCF OF MOTOR OPERATED VALVES 102A AND 102C FAILS TO OPEN ON DEMAND	4.000e-03	N	0.068	2.720e-04	1.176e-04
117	SWCMVV4OF4NN	CCF OF ALL 4 DISCHARGE MOTOR OPERATED VALVES TO OPEN	4.000e-03	N	0.00029	1.160e-06	0.000e+00
118	SWCP3P4OF4NN	CCF OF ALL 4 SERVICE WATER PUMPS TO START	2.400e-03	N	0.0022	5.280e-06	0.000e+00
119	SWCP3PMPACFN	CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAIL TO RUN	3.200e-05	H	2.4	7.680e-05	8.067e-04
120	SWCP3PMPACNN	CCF TO START OF SW PUMPS 'A' AND 'C'	2.400e-03	N	0.1	2.400e-04	1.034e-04
121	SWXP3SWP1XNX	OPERATOR FAILS TO START FOLLOW PUMP	1.000e+00	N	0.01	1.000e-02	1.303e-03

Table A.1: Basic Events (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
1	%SWP3IPMACFN	(INIT) CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAILS TO RUN	3.20e-05	8.76e+02	2.80e-02	2.80e-02
2	ACADG3EGSANN	DIESEL GENERATOR A FAILS TO START ON DEMAND (INCLUDES FAILURE TO RUN)	1.64e-02	1.00e+00	1.64e-02	1.64e-02
3	ACADG3EGSAAQ	DIESEL GENERATOR A UNAVAILABLE DUE TO TEST OR MAINTENANCE	1.10e-02	1.00e+00	1.10e-02	1.10e-02
4	ACABKLSHEDNN	FAILURE TO SHED MAJOR EQUIPMENT LOADS (BREAKERS FAIL TO OPEN)	1.58e-04	3.00e+01	4.74e-03	4.74e-03
5	ACADMDM23ANN	INLET DAMPER 23A FAILS TO OPEN	4.00e-03	1.00e+00	4.00e-03	4.00e-03
6	ACADMDM20ANN	OUTLET DAMPER 20A FAILS TO OPEN	4.00e-03	1.00e+00	4.00e-03	4.00e-03
7	ACADMDM20CNN	OUTLET DAMPER 20C FAILS TO OPEN	4.00e-03	1.00e+00	4.00e-03	4.00e-03
8	ACADMDM26AFF	RECIRC DAMPER 26A FAILS TO CLOSE	4.00e-03	1.00e+00	4.00e-03	4.00e-03
9	ACAAVAV39ANN	SERVICE WATER OUTLET VALVE AOV39A FAILS TO OPEN ON DEMAND	2.00e-03	1.00e+00	2.00e-03	2.00e-03
10	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	1.54e-03
	SWAP3SWP1AAQ	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE	1.10e-02	1.00e+00	1.10e-02	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
11	HVADAAD23ANN	AIR OPERATED DAMPER *23A FAILS TO OPEN	2.00e-03	1.00e+00	2.00e-03	1.50e-03
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	
12	ACCDG3EGSXNN	CCF OF DGs TO START ON DEMAND (INCLUDES FAILURE TO RUN)	1.64e-02	6.80e-02	1.12e-03	1.12e-03
13	ACABK34C1TNN	34A TO 34C BUS TIE BREAKER 34C-1T-2 FAILS TO OPEN ON DEMAND	1.58e-04	6.00e+00	9.48e-04	9.48e-04
14	ACACP62W15FF	CONTACT PAIR 62W15 FAILS TO CLOSE	1.35e-04	6.00e+00	8.10e-04	8.10e-04
15	ACACP27R56FF	CONTACT PAIR 27R56 FAILS TO CLOSE	1.35e-04	6.00e+00	8.10e-04	8.10e-04
16	ACACP62V13FF	CONTACT PAIR 62V13 FAILS TO CLOSE	1.35e-04	6.00e+00	8.10e-04	8.10e-04
17	ACACPCC1D1FF	CONTACT PAIR 3A-3EGS*EG-A CC1-CD1 FAILS TO CLOSE	1.35e-04	6.00e+00	8.10e-04	8.10e-04

Table A.2: Minimal Cutsets

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
18	ACACPCA1B1FF	CONTACT PAIR 3A-3EGS*EG-A CA1-CB1 FAILS TO CLOSE	1.35e-04	6.00e+00	8.10e-04	8.10e-04
19	ACAESEGLSANN	EDG LOAD SEQUENCER 'A' FAILS ON DEMAND		7.58e-04	7.58e-04	7.58e-04
20	ACARCRC62WNN	RELAY COIL 62W FAILS TO ENERGIZE	1.00e-04	6.00e+00	6.00e-04	6.00e-04
21	ACARCRC27RNN	RELAY COIL 27R FAILS TO DEENERGIZE	1.00e-04	6.00e+00	6.00e-04	6.00e-04
22	ACARCRC62VNN	RELAY COIL 62V FAILS TO ENERGIZE	1.00e-04	6.00e+00	6.00e-04	6.00e-04
23	ACAFNVFN1CNQ	FAN UNIT *FN1C OUT OF SERVICE FOR MAINTENANCE	5.66e-04	1.00e+00	5.66e-04	5.66e-04
24	ACAFNVFN1ANQ	FAN UNIT *FN1A OUT OF SERVICE FOR MAINTENANCE	5.66e-04	1.00e+00	5.66e-04	5.66e-04
25	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	5.61e-04
	SWAMVV102ANN	MOTOR OPERATED VALVE V102A FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
26	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	5.61e-04
	SWAMVV102CNN	MOTOR OPERATED VALVE V102C FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
27	DCABT301A1FN	STORAGE BATTERY 301A-1 FAILS TO PROVIDE OUTPUT ON DEMAND	5.00e-04	1.00e+00	5.00e-04	5.00e-04
28	ACAFNVFN1CNN	FAN UNIT *FN1C FAILS TO START	4.84e-04	1.00e+00	4.84e-04	4.84e-04
29	ACAFNVFN1ANN	FAN UNIT *FN1A FAILS TO START	4.84e-04	1.00e+00	4.84e-04	4.84e-04
30	ACAININV1AFN	DC TO AC POWER INVERTER-1 FAILS DURING OPERATION	2.00e-05	2.40e+01	4.80e-04	4.80e-04
31	HVAFNEFN2ANN	VENTILATION UNIT HVY*FN2A FAILS TO START	4.84e-04	1.00e+00	4.84e-04	3.63e-04
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	
32	ACABKG14U2FF	DIESEL GENERATOR A OUTPUT BREAKER FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	3.38e-04
33	ACABKF1C42FF	'42 BREAKER' FOR *FN1C FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	3.38e-04
34	ACABKF1A42FF	'42 BREAKER' FOR *FN1A FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	3.38e-04
35	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	3.36e-04
	SWAP3SWP1CNN	SERVICE WATER PUMP SWP1C FAILS TO START ON DEMAND	2.40e-03	1.00e+00	2.40e-03	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
36	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	3.36e-04
	SWAP3SWP1ANN	SERVICE WATER PUMP SWP1A FAILS TO START ON DEMAND	2.40e-03	1.00e+00	2.40e-03	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
37	HVABK42F2AFF	'42 BREAKER' FOR VENTILATION UNIT HVY*FN2A FAILS TO CLOSE	3.38e-04	1.00e+00	3.38e-04	2.54e-04
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	
38	ACCPMFP1ACNN	COMMON CAUSE FAILURE TO START OF TRANSFER PUMPS *P1A AND *P1C	2.00e-03	1.00e-01	2.00e-04	2.00e-04
39	ACATSTS32ANN	TEMPERATURE SWITCH TS32A FAILS TO OPERATE	2.00e-04	1.00e+00	2.00e-04	2.00e-04
40	HVAFNEFN2AFN	VENTILATION UNIT HVY*FN2A FAILS TO RUN	7.89e-06	2.40e+01	1.89e-04	1.89e-04
41	ACAFNVFN1CFN	FAN UNIT *FN1C FAILS TO RUN	7.89e-06	2.40e+01	1.89e-04	1.89e-04
42	ACAFNVFN1AFN	FAN UNIT *FN1A FAILS TO RUN	7.89e-06	2.40e+01	1.89e-04	1.89e-04
43	HVATSTS60ANN	TEMPERATURE SWITCH TS60A FAILS TO OPERATE	2.00e-04	1.00e+00	2.00e-04	1.50e-04
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	
44	ACCAVV39ABNN	CCF - SW AIR OPERATED VALVES *39A,B FAIL TO OPEN ON DEMAND	2.00e-03	6.80e-02	1.36e-04	1.36e-04
45	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	1.26e-04
	SWAP3SWP1CCQ	SERVICE WATER PUMP SWP1C OOS FOR MAINTENANCE	9.00e-04	1.00e+00	9.00e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
46	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	1.08e-04
	SWAP3SWP1AFN	SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
47	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	1.08e-04
	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
48	HVCDAD23ABNN	CCF - AIR OPERATED DAMPERS *23A AND *23B FAIL TO OPEN	2.00e-03	6.80e-02	1.36e-04	1.02e-04
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
49	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	8.20e-05
	HVADAAD23ANN	AIR OPERATED DAMPER *23A FAILS TO OPEN	2.00e-03	1.00e+00	2.00e-03	
50	SWCP3PMPACFN	CCF OF SERVICE WATER PUMPS 'A' AND 'C' FAIL TO RUN	3.20e-05	2.40e+00	7.68e-05	7.68e-05
51	ACCPMFP1ACFN	COMMON CAUSE FAILURE TO RUN OF TRANSFER PUMPS *P1A AND *P1C	2.50e-05	2.40e+00	6.00e-05	6.00e-05
52	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	4.74e-05
	SWABKV102CFF	BUS FEED BREAKER FOR V102C FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
53	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	4.74e-05
	SWABKBKP1AFF	PUMP SWP*P1A START CIRCUIT BREAKER FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
54	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	4.74e-05
	SWABKV102AFF	BUS FEED BREAKER FOR V102A FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
55	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	4.74e-05
	SWABKBKP1CFF	PUMP SWP*P1C START CIRCUIT BREAKER FAILS TO CLOSE ON DEMAND	3.38e-04	1.00e+00	3.38e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
56	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	3.70e-05
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
	SWAPSPS27ANN	PRESSURE SWITCH PS27A FAILS TO OPERATE	2.00e-04	1.32e+02	2.64e-02	
	SWXP3SWP1XNX	OPERATOR FAILS TO START FOLLOW PUMP		1.00e-02	1.00e-02	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
57	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	3.70e-05
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
	SWAPSPS27ANN	PRESSURE SWITCH PS27A FAILS TO OPERATE	2.00e-04	1.32e+02	2.64e-02	
	SWXP3SWP1XNX	OPERATOR FAILS TO START FOLLOW PUMP		1.00e-02	1.00e-02	
58	DCABK31A1BNF	DC PANEL 301A-1B BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
59	ACABK32T62NF	BUS FEED BREAKER 32T6-2 FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
60	DCABK31A1ANF	DC PANEL 301A-1A BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
61	ACABK34C32NF	BUS FEED BREAKER 34C3-2 FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
62	ACABK32T12NF	BUS FEED BREAKER 32T1-2 FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
63	DCABKA1301NF	DC PANEL 301A-1 BUS FEED BREAKER FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
64	DCABKINV1ANF	DC BUS 301A-1 FEED BREAKER TO INV1 FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
65	ACABKESWGANF	BUS FEED BREAKER TO 34C AUX CIRCUIT FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
66	ACABK32T42NF	BUS FEED BREAKER 32T4-2 FAILS TO REMAIN CLOSED	1.52e-06	2.40e+01	3.65e-05	3.65e-05
67	HVCFNFN2ABNN	CCF - VENTILATION UNITS HVY*FN2A, FN2B FAIL TO START	4.84e-04	1.00e-01	4.84e-05	3.63e-05
	NOTSUMMER	NOT SUMMER OPERATION		7.50e-01	7.50e-01	
68	ACATR4C31XFN	TRANSFORMER 34C3-1X FAILS TO OPERATE	1.20e-06	2.40e+01	2.88e-05	2.88e-05
69	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.80e-05
	SWACVP1CV5NN	CHECK VALVE P1C*V5 FAILS TO OPEN ON DEMAND	2.00e-04	1.00e+00	2.00e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
70	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.80e-05
	SWACVCV769NN	PUMP 'A' LUBRICATION FAILS (CHECK VALVE -769 FAILS TO OPEN)	2.00e-04	1.00e+00	2.00e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
71	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.80e-05
	SWACVP1AV7NN	CHECK VALVE P1A*V7 FAILS TO OPEN ON DEMAND	2.00e-04	1.00e+00	2.00e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
72	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.80e-05
	SWACVCV768NN	PUMP 'C' LUBRICATION FAILS (CHECK VALVE -768 FAILS TO OPEN)	2.00e-04	1.00e+00	2.00e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
73	%SWP3ISW1CFN	(INIT) SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.50e-05
	SWACP63X12FF	LOW HEADER PRESSURE CONTACT PAIR 63X12 FAILS TO CLOSE	1.35e-04	1.32e+02	1.78e-02	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
	SWXP3SWP1XNX	OPERATOR FAILS TO START FOLLOW PUMP		1.00e-02	1.00e-02	
74	%SWP3ISW1AFN	(INIT) SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	8.76e+03	2.80e-01	2.50e-05
	SWACP63X56FF	LOW HEADER PRESSURE CONTACT PAIR 63X56 FAILS TO CLOSE	1.35e-04	1.32e+02	1.78e-02	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
	SWXP3SWP1XNX	OPERATOR FAILS TO START FOLLOW PUMP		1.00e-02	1.00e-02	
75	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	1.98e-05
	HVAFNEFN2ANN	VENTILATION UNIT HVY*FN2A FAILS TO START	4.84e-04	1.00e+00	4.84e-04	
76	HVCFNFN2ABFN	CCF - VENTILATION UNITS HVY*FN2A, FN2B FAIL TO RUN	7.89e-06	2.40e+00	1.89e-05	1.89e-05
77	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	1.39e-05
	HVABK42F2AFF	'42 BREAKER' FOR VENTILATION UNIT HVY*FN2A FAILS TO CLOSE	3.38e-04	1.00e+00	3.38e-04	
78	ACAFUVIAC1NF	FUSE VIAC1 FAILS TO REMAIN CLOSED	5.00e-07	2.40e+01	1.20e-05	1.20e-05
79	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	1.12e-05
	SWCMV102ACNN	CCF OF MOTOR OPERATED VALVES 102A AND 102C FAILS TO OPEN ON DEMAND	4.00e-03	6.80e-02	2.72e-04	
80	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	1.01e-05
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
	SWAPSPS27ANN	PRESSURE SWITCH PS27A FAILS TO OPERATE	2.00e-04	1.32e+02	2.64e-02	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
81	SWAP3SWP1AFN	SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	1.01e-05
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
	SWAPSPS27ANN	PRESSURE SWITCH PS27A FAILS TO OPERATE	2.00e-04	1.32e+02	2.64e-02	
82	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	9.84e-06
	SWCP3PMPACNN	CCF TO START OF SW PUMPS 'A' AND 'C'	2.40e-03	1.00e-01	2.40e-04	
83	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	8.20e-06
	HVATSTS60ANN	TEMPERATURE SWITCH TS60A FAILS TO OPERATE	2.00e-04	1.00e+00	2.00e-04	
84	SWACP63X12FF	LOW HEADER PRESSURE CONTACT PAIR 63X12 FAILS TO CLOSE	1.35e-04	1.32e+02	1.78e-02	6.84e-06
	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
85	SWACP63X56FF	LOW HEADER PRESSURE CONTACT PAIR 63X56 FAILS TO CLOSE	1.35e-04	1.32e+02	1.78e-02	6.84e-06
	SWAP3SWP1AFN	SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
86	%SWMVI102CFN	(INIT) MOTOR OPERATED VALVE V102C FAILS TO REMAIN OPEN	1.40e-07	8.76e+03	1.23e-03	6.75e-06
	SWAP3SWP1AAQ	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE	1.10e-02	1.00e+00	1.10e-02	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
87	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	5.58e-06
	HVCDAD23ABNN	CCF - AIR OPERATED DAMPERS *23A AND *23B FAIL TO OPEN	2.00e-03	6.80e-02	1.36e-04	
88	ACABSBS32TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (BUS 32T)	2.00e-07	2.40e+01	4.80e-06	4.80e-06
89	DCABS301A1FN	METAL ENCLOSED DC BUS-TO-GROUND SHORT (DC PANEL 301A-1)	2.00e-07	2.40e+01	4.80e-06	4.80e-06
90	DCABS301ABFN	METAL ENCLOSED DC BUS 301A-1B BUS-TO-GROUND SHORT	2.00e-07	2.40e+01	4.80e-06	4.80e-06
91	DCABS301AAFN	METAL ENCLOSED DC BUS 301A-1A BUS-TO-GROUND SHORT	2.00e-07	2.40e+01	4.80e-06	4.80e-06
92	ACABSM321TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (MCC 32-1T)	2.00e-07	2.40e+01	4.80e-06	4.80e-06
93	ACABSBS34CFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (BUS 34C)	2.00e-07	2.40e+01	4.80e-06	4.80e-06
94	ACABSM325TFN	METAL ENCLOSED AC BUS-TO-GROUND SHORT (MCC 32-5T)	2.00e-07	2.40e+01	4.80e-06	4.80e-06

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
95	ACABSVIAC1FN	METAL ENCLOSED BUS VIAC-1 BUS-TO-GROUND SHORT	2.00e-07	2.40e+01	4.80e-06	4.80e-06
96	SWAP3SWP1AAQ	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE	1.10e-02	1.00e+00	1.10e-02	4.22e-06
	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
97	%SWEJEXJ1CFN	(INIT) EXPANSION JOINT EXJ1C RUPTURES	8.48e-08	8.76e+03	7.43e-04	4.09e-06
	SWAP3SWP1AAQ	SERVICE WATER PUMP SWP1A OOS FOR MAINTENANCE	1.10e-02	1.00e+00	1.10e-02	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
98	ACAPMEFP1ANN	FUEL OIL TRANSFER PUMP *P1A FAILS TO START	2.00e-03	1.00e+00	2.00e-03	4.00e-06
	ACAPMEFP1CNN	FUEL OIL TRANSFER PUMP *P1C FAILS TO START	2.00e-03	1.00e+00	2.00e-03	
99	%SWMVI102CFN	(INIT) MOTOR OPERATED VALVE V102C FAILS TO REMAIN OPEN	1.40e-07	8.76e+03	1.23e-03	2.45e-06
	SWAMVV102ANN	MOTOR OPERATED VALVE V102A FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
100	%SWMVI102AFN	(INIT) MOTOR OPERATED VALVE V102A FAILS TO REMAIN OPEN	1.40e-07	8.76e+03	1.23e-03	2.45e-06
	SWAMVV102CNN	MOTOR OPERATED VALVE V102C FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
101	ACATKFTK2ATN	FUEL OIL DAY TANK TK2A RUPTURES	1.00e-07	2.40e+01	2.40e-06	2.40e-06
102	ACATKFTK1ATN	FUEL OIL STORAGE TANK TK1A RUPTURES	1.00e-07	2.40e+01	2.40e-06	2.40e-06
103	%LOOP	LOSS OF OFFSITE POWER		4.10e-02	4.10e-02	1.98e-06
	HVCFNFN2ABNN	CCF - VENTILATION UNITS HVY*FN2A, FN2B FAIL TO START	4.84e-04	1.00e-01	4.84e-05	
104	SWAMVV102ANN	MOTOR OPERATED VALVE V102A FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	1.54e-06
	SWAP3SWP1CFN	SERVICE WATER PUMP SWP1C FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
105	SWAMVV102CNN	MOTOR OPERATED VALVE V102C FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	1.54e-06
	SWAP3SWP1AFN	SERVICE WATER PUMP SWP1A FAILS TO RUN	3.20e-05	2.40e+01	7.68e-04	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	

Table A.2: Minimal Cutsets (cont'd.)

#	Basic Events	Description	Rate	Exposure	B. E. Prob.	MCS Prob.
106	%SWEJEXJ1AFN	(INIT) EXPANSION JOINT EXJ1A RUPTURES	8.48e-08	8.76e+03	7.43e-04	1.49e-06
	SWAMVV102CNN	MOTOR OPERATED VALVE V102C FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPALEAD	SERVICE WATER TRAIN 'A' PUMP 'A' IN LEAD		5.00e-01	5.00e-01	
107	%SWEJEXJ1CFN	(INIT) EXPANSION JOINT EXJ1C RUPTURES	8.48e-08	8.76e+03	7.43e-04	1.49e-06
	SWAMVV102ANN	MOTOR OPERATED VALVE V102A FAILS TO OPEN ON DEMAND	4.00e-03	1.00e+00	4.00e-03	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	
108	%SWMVI102CFN	(INIT) MOTOR OPERATED VALVE V102C FAILS TO REMAIN OPEN	1.40e-07	8.76e+03	1.23e-03	1.47e-06
	SWAP3SWP1ANN	SERVICE WATER PUMP SWP1A FAILS TO START ON DEMAND	2.40e-03	1.00e+00	2.40e-03	
	SWAPCLEAD	SERVICE WATER TRAIN 'A' PUMP 'C' IN LEAD		5.00e-01	5.00e-01	

Table A.2: Minimal Cutsets (cont'd.)

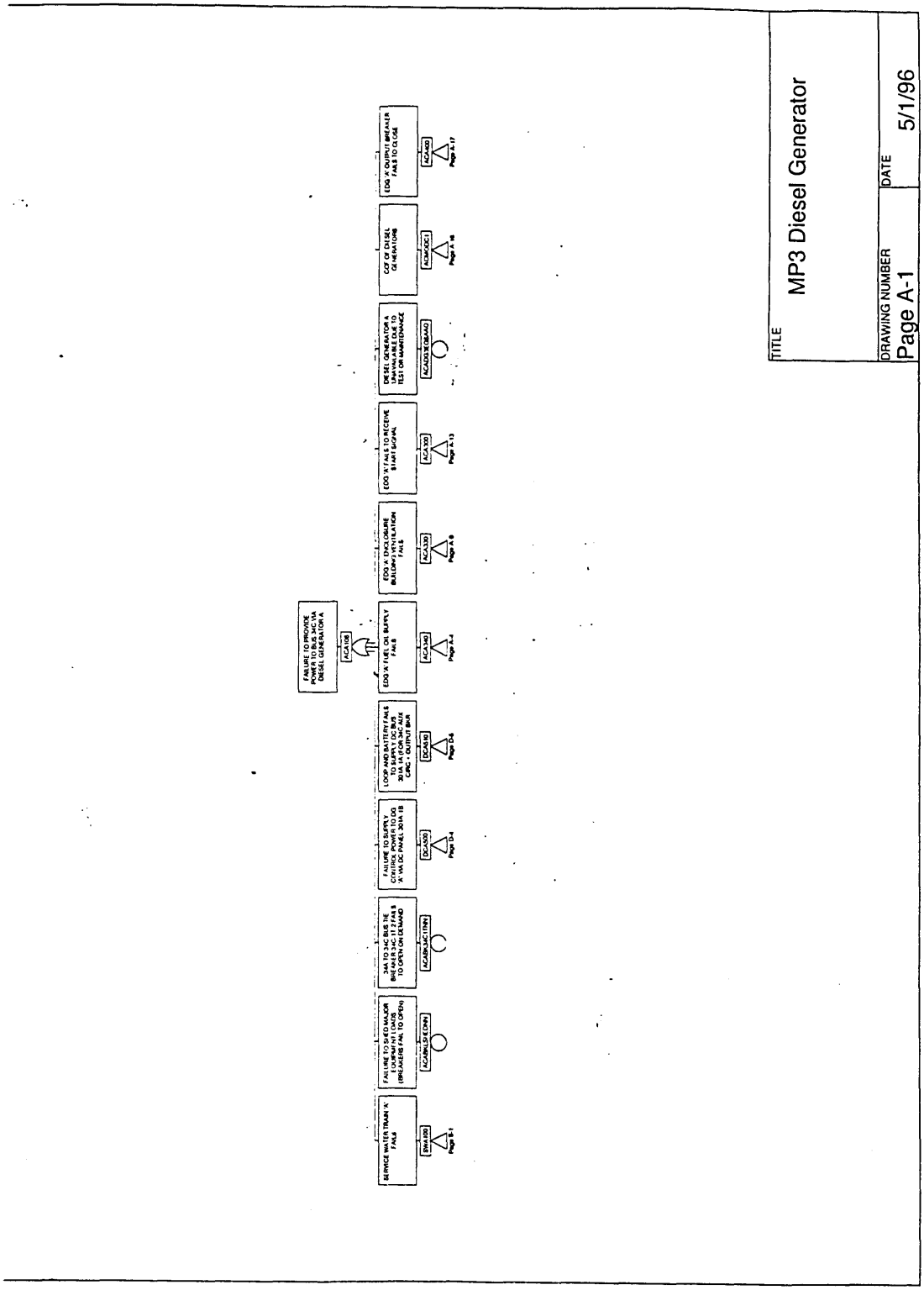


Figure A.1: Millstone 3 EDG Fault Tree

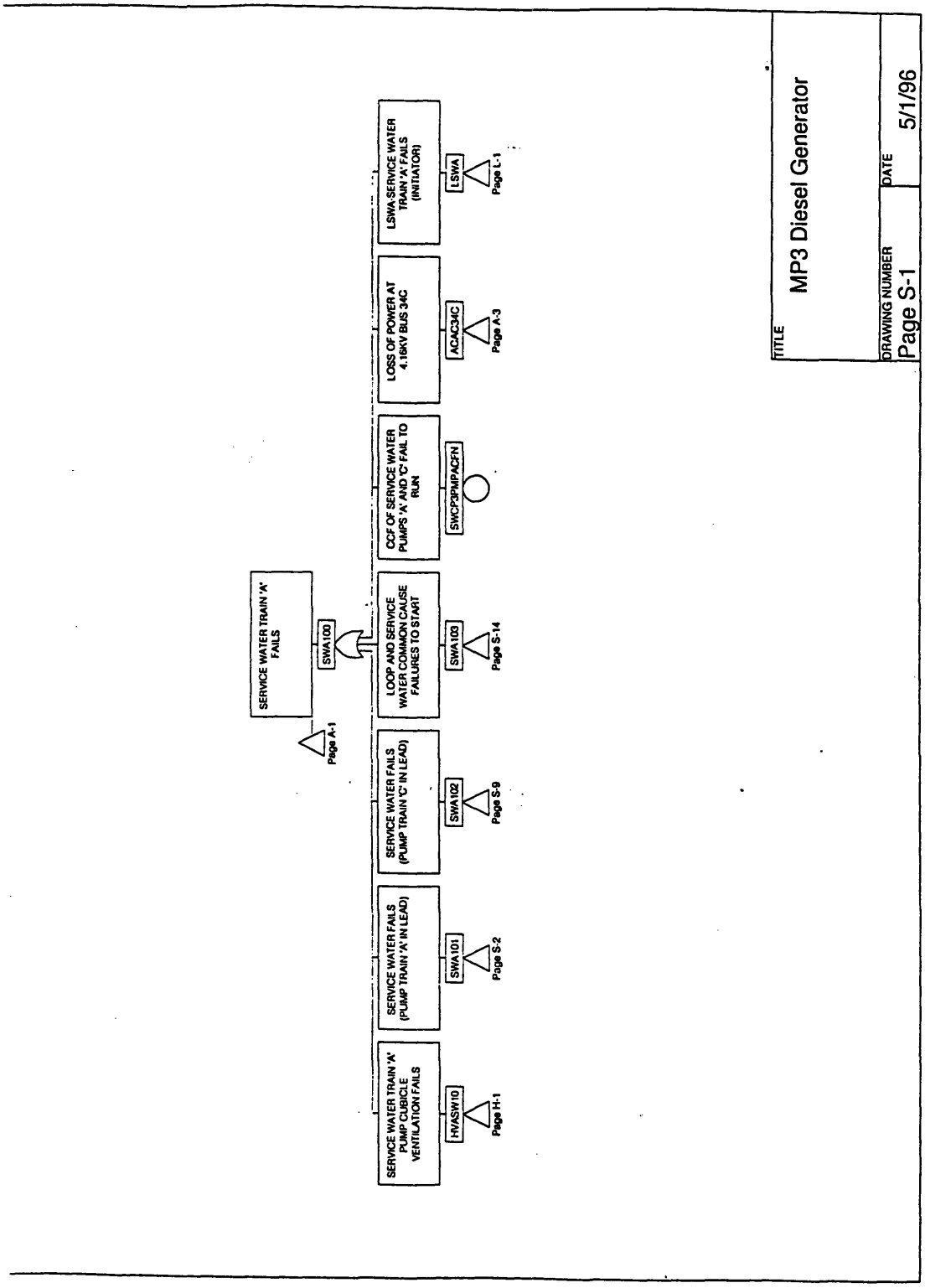
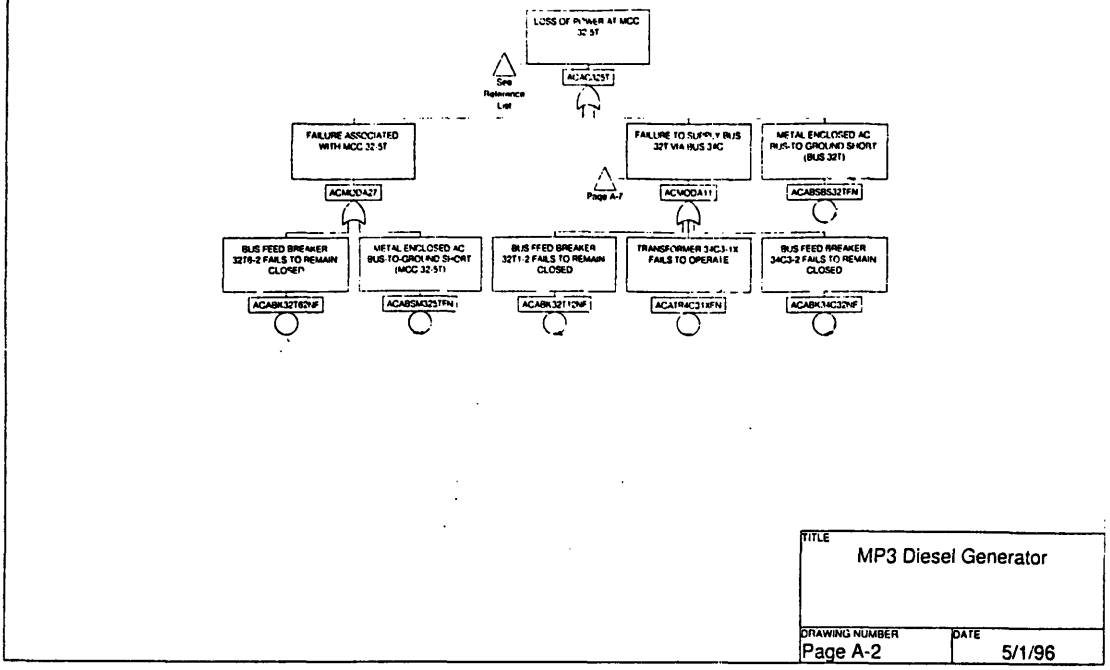


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



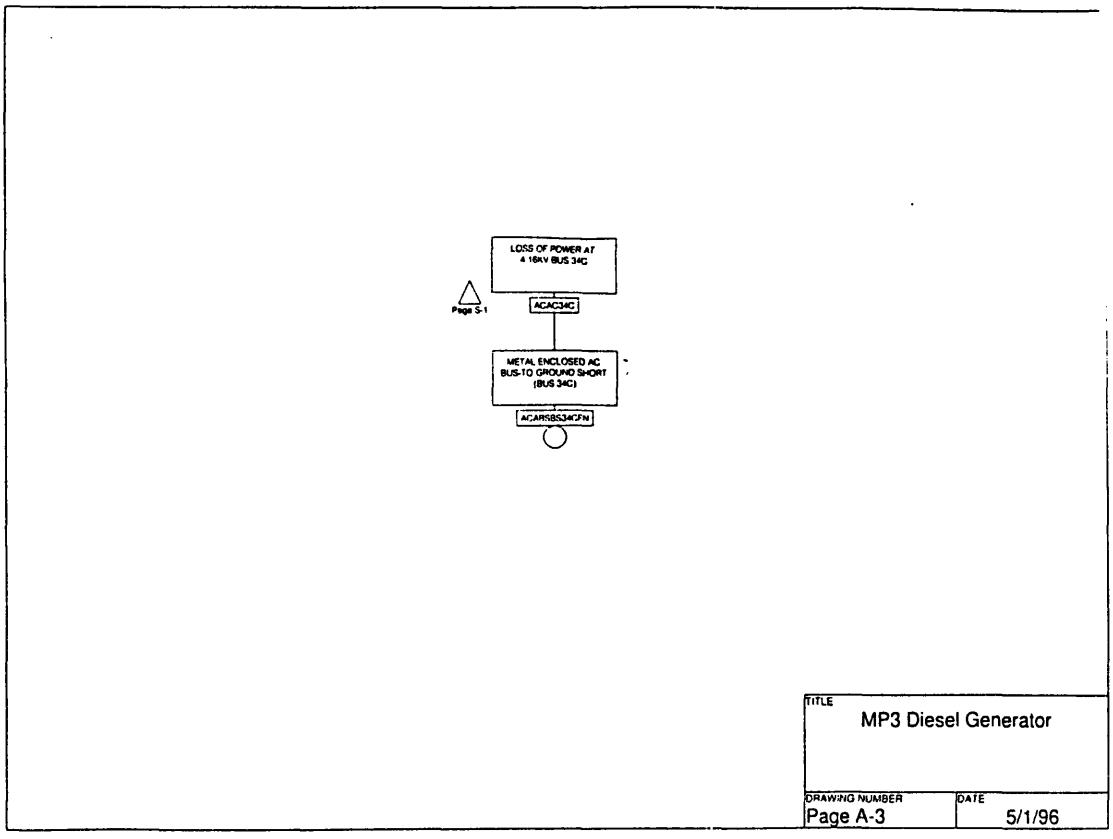
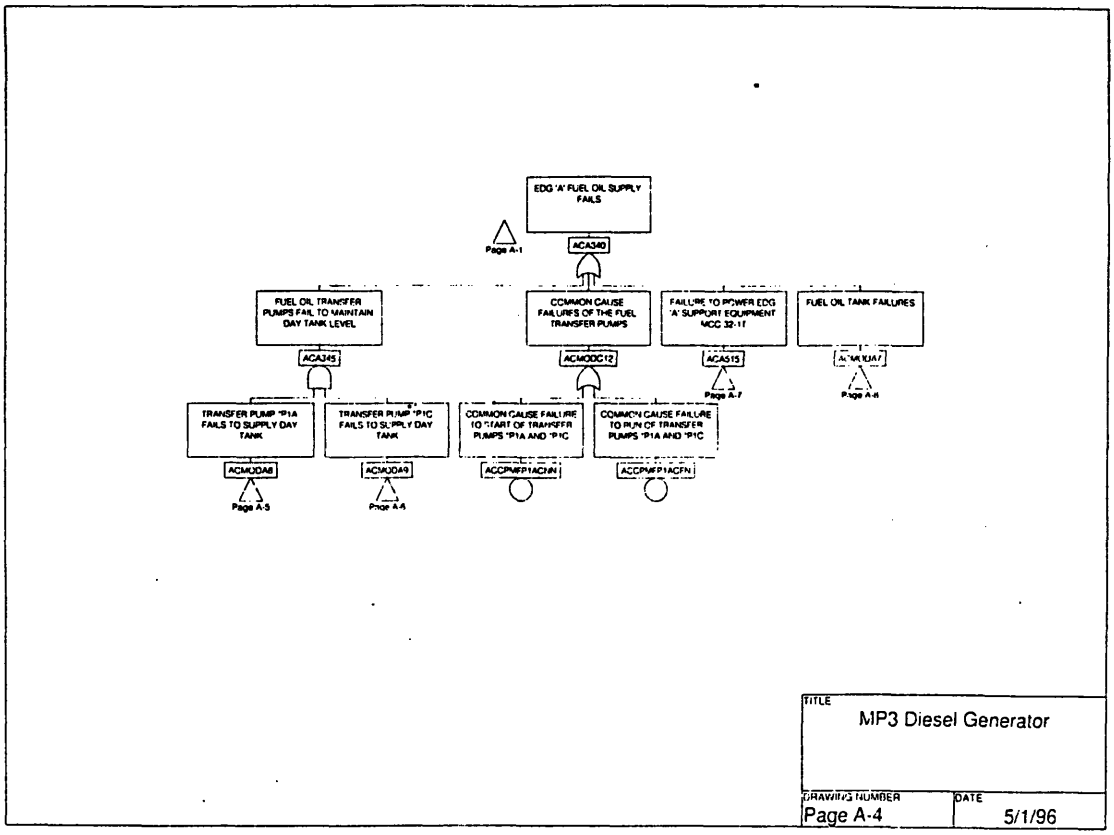


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



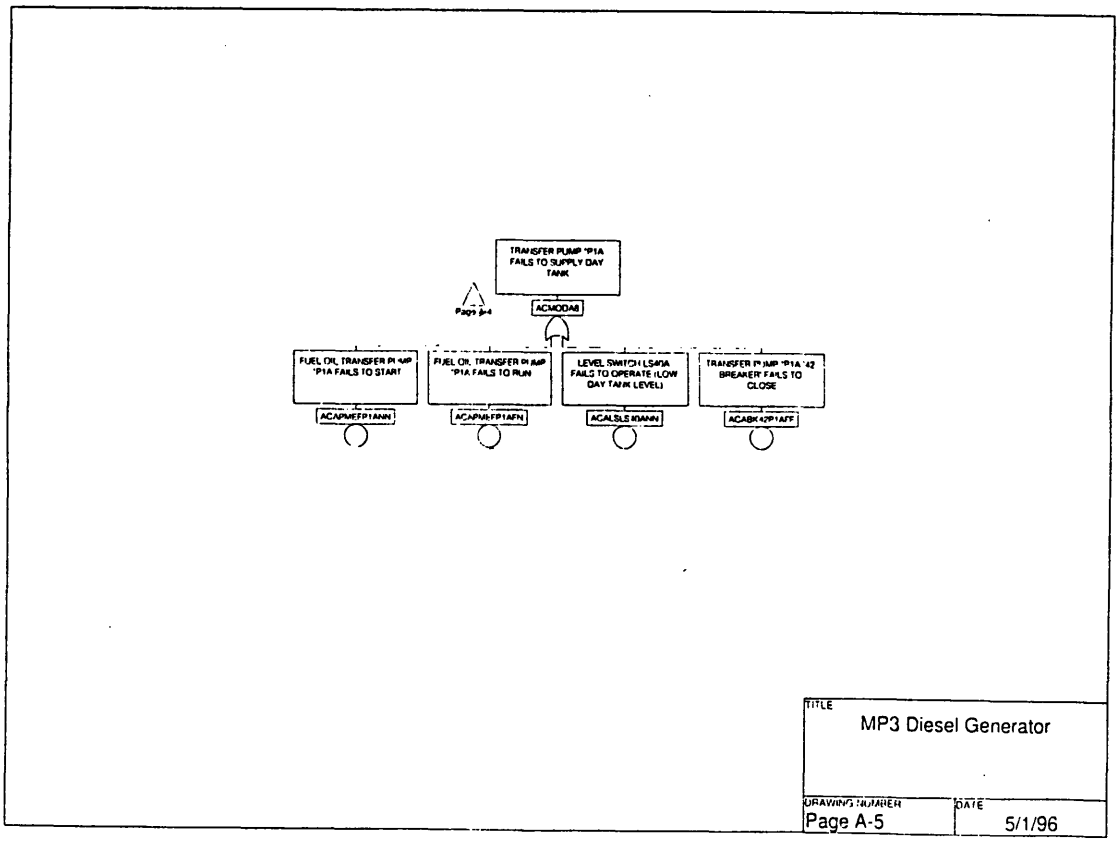
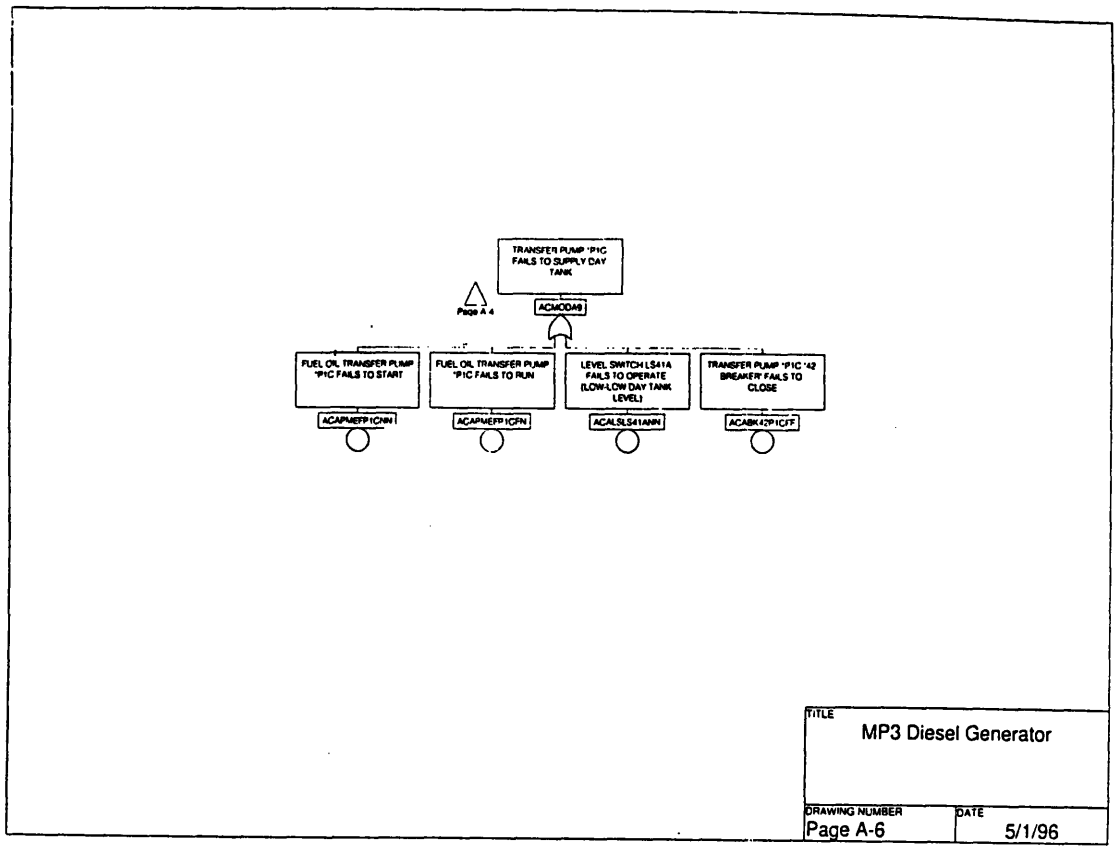


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



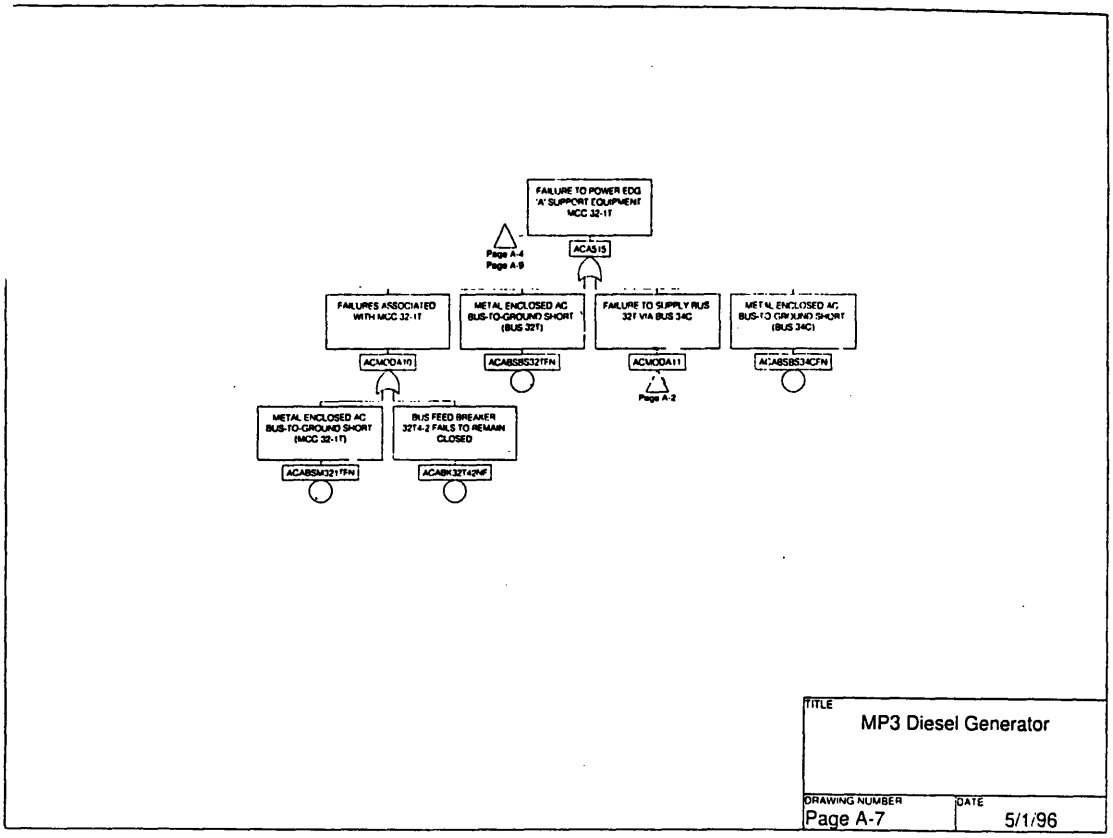
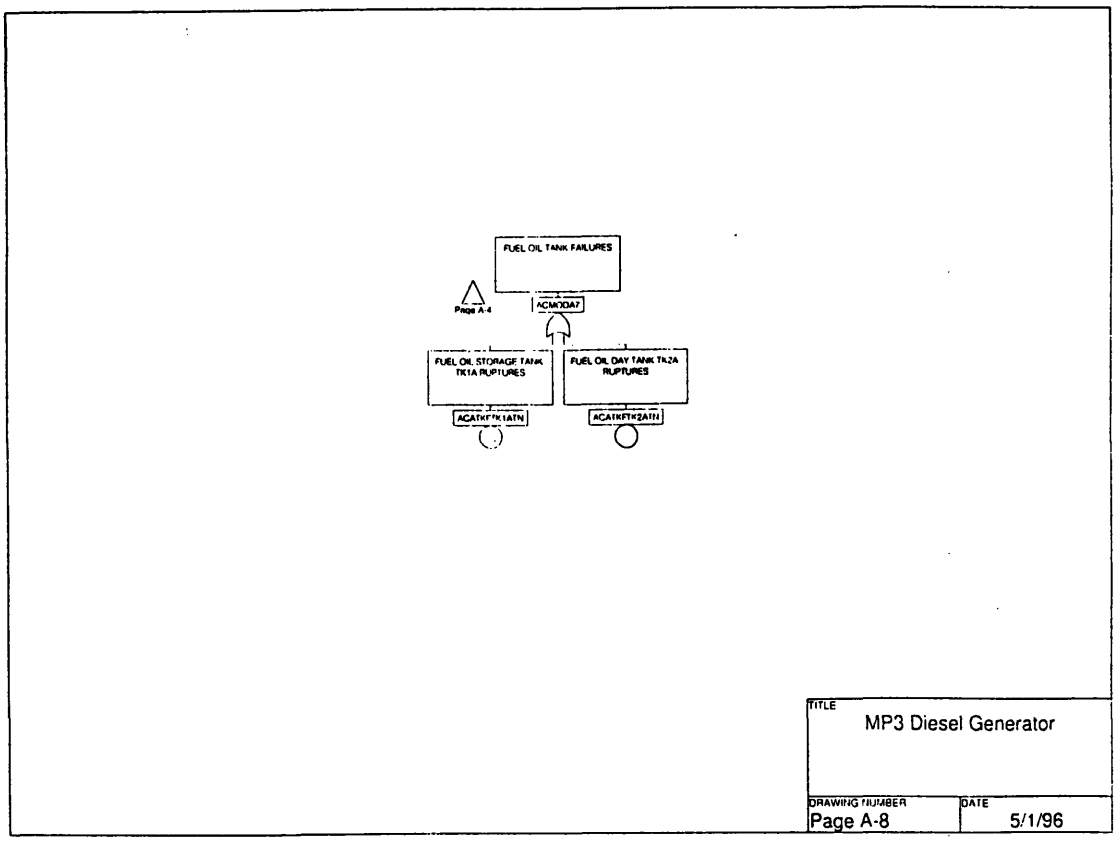


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



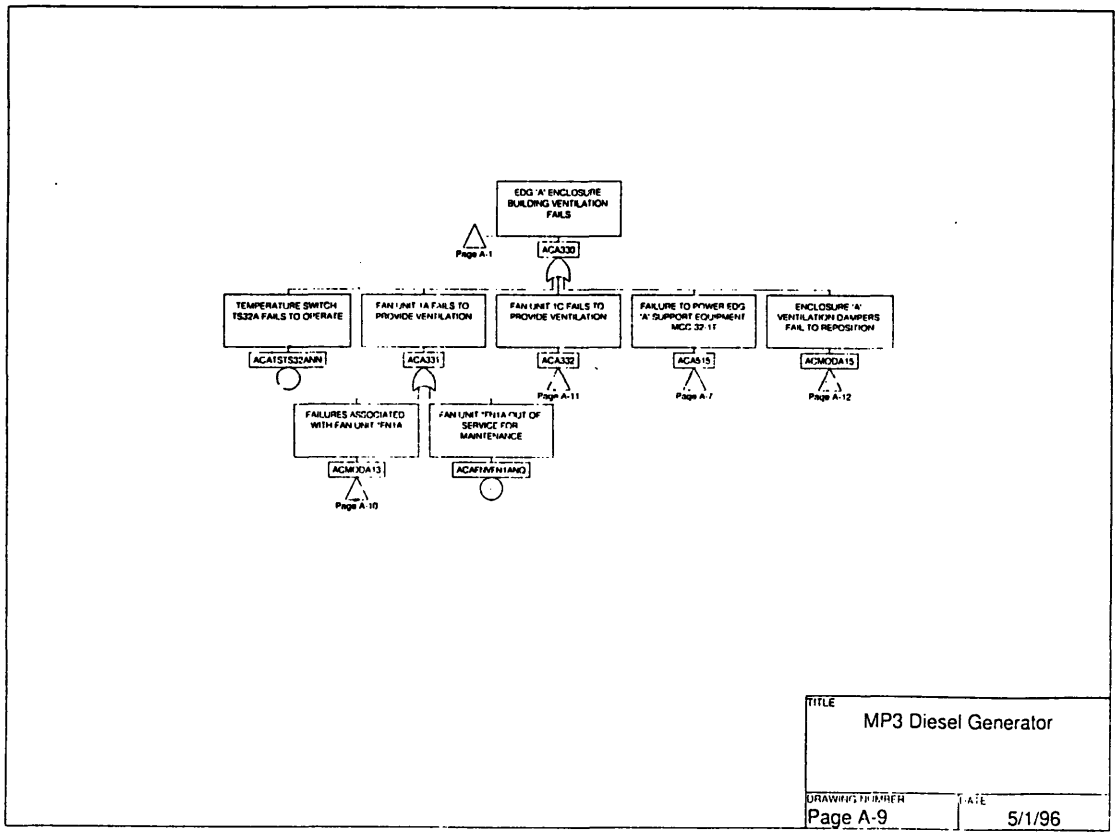
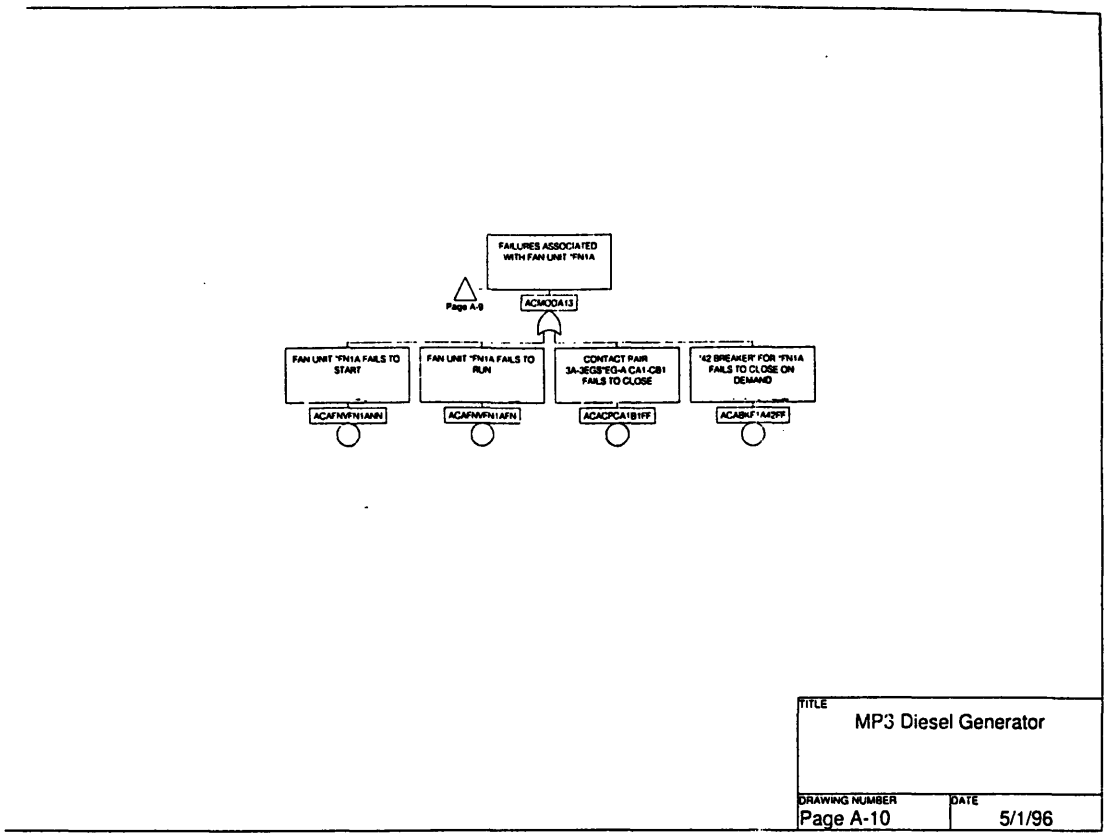


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



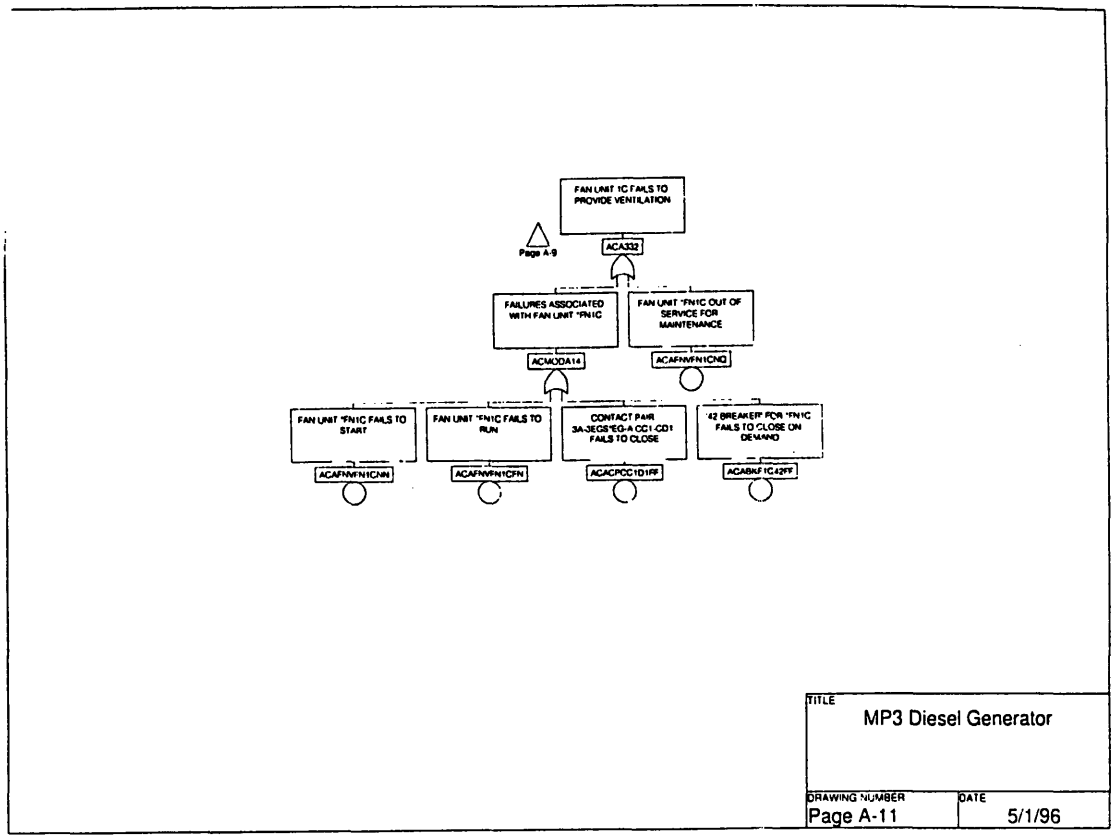
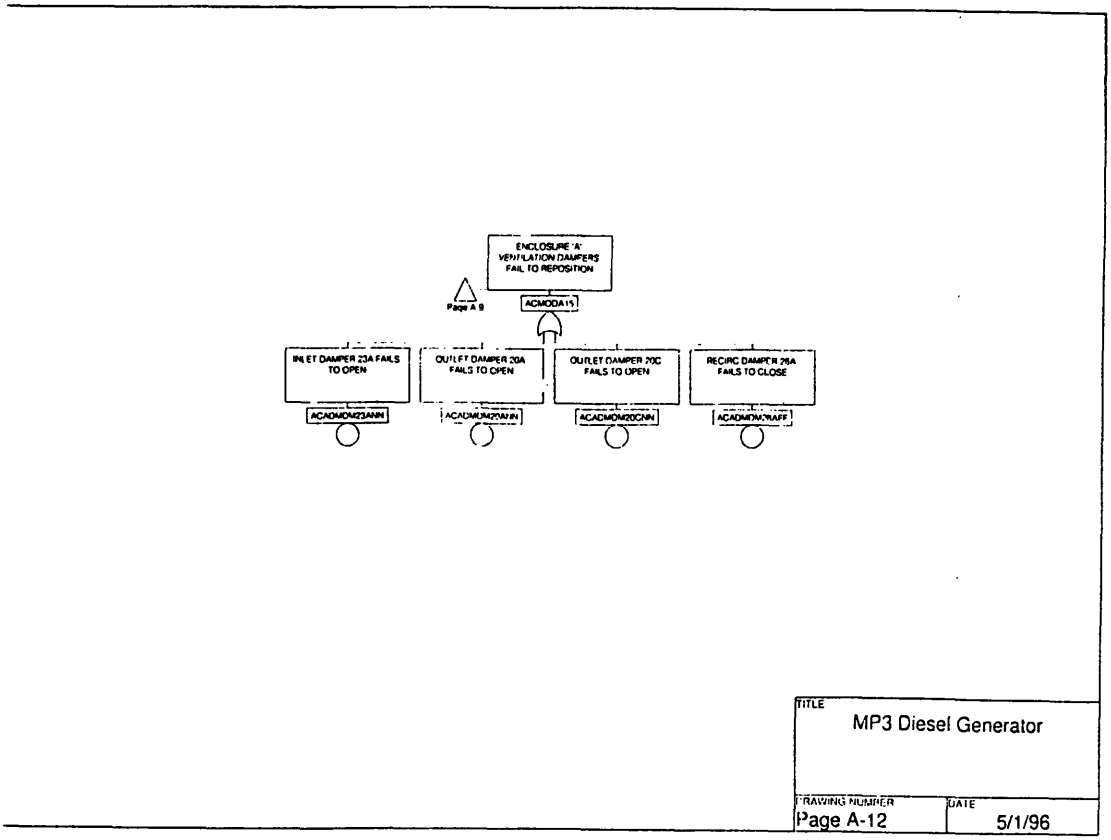


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



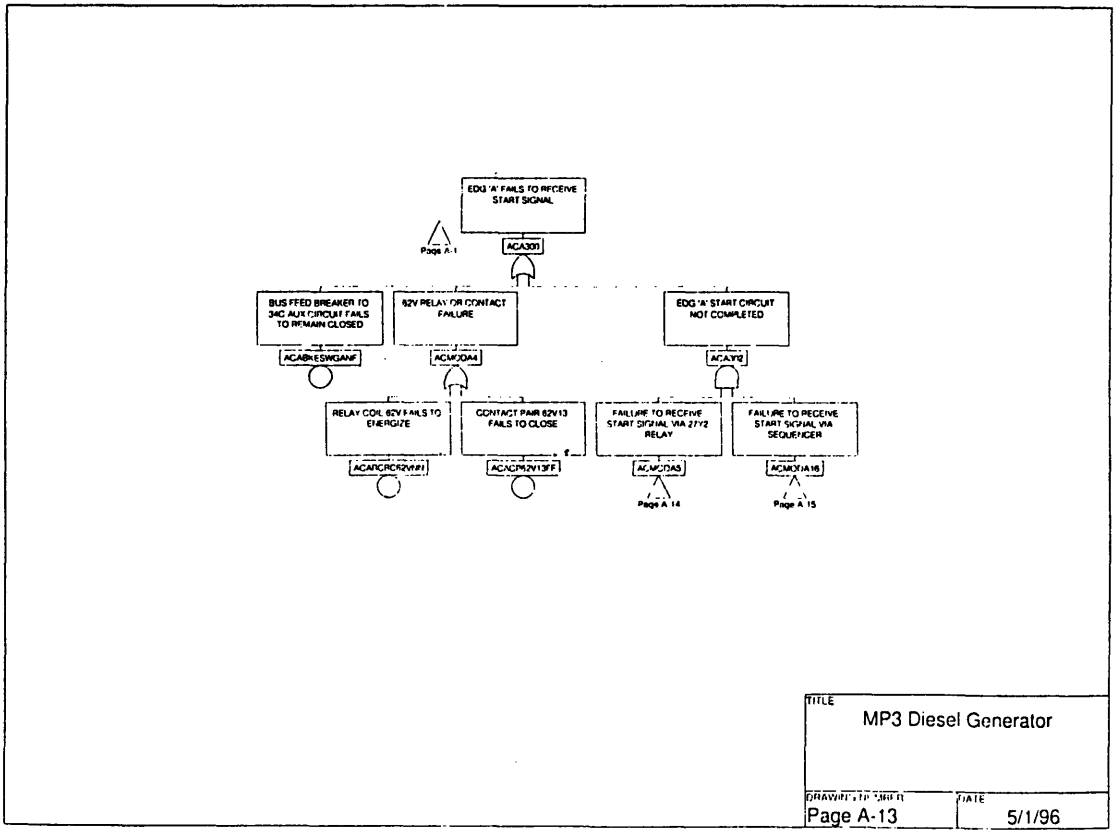
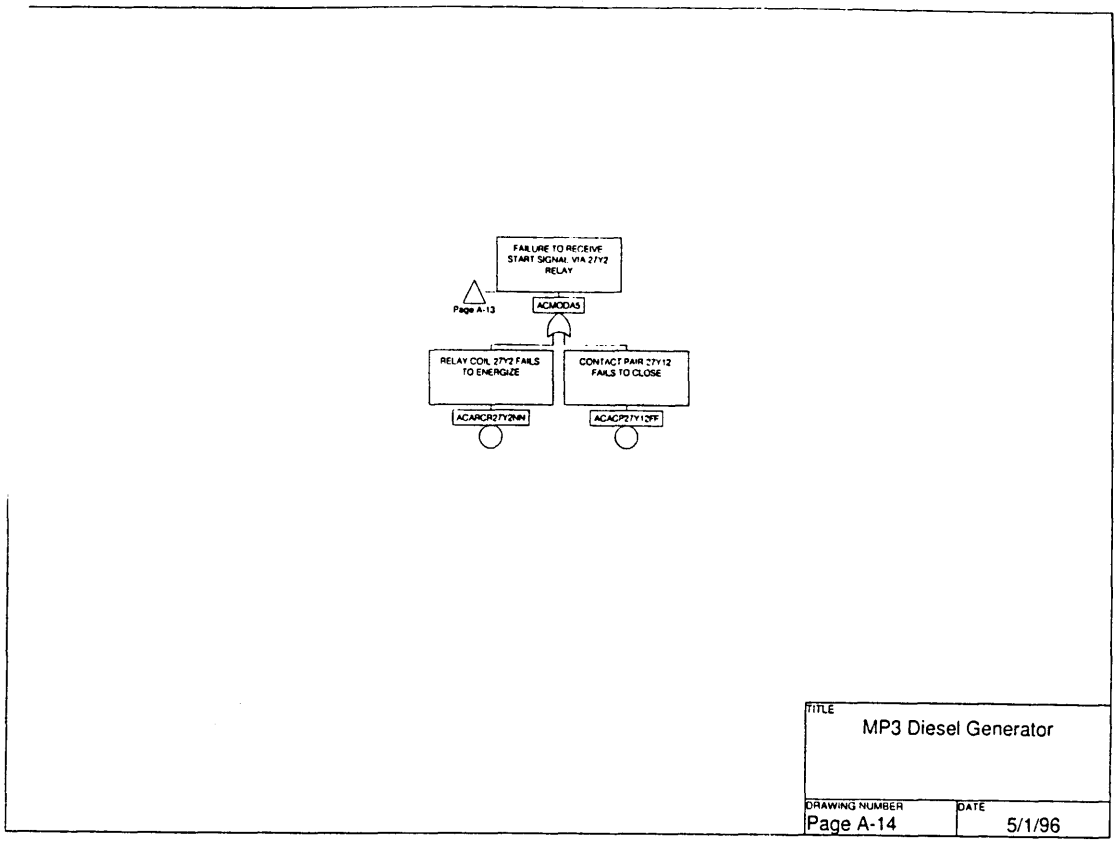


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



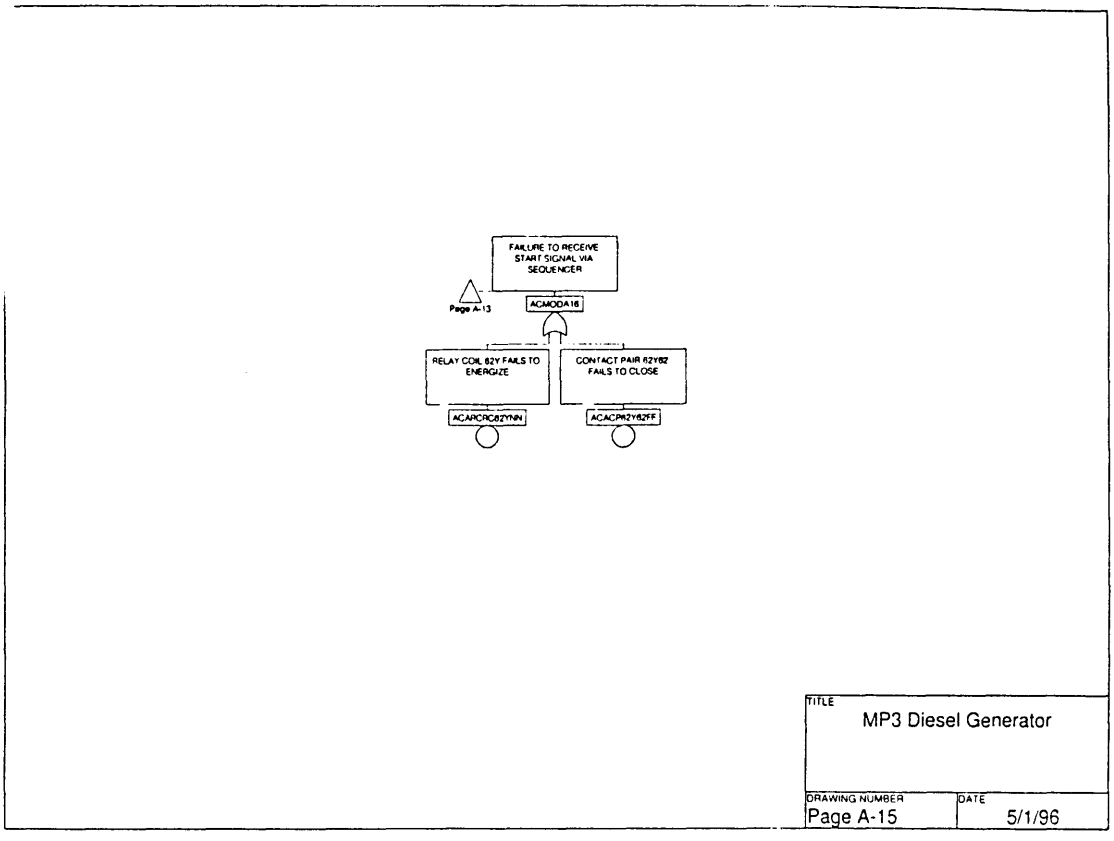
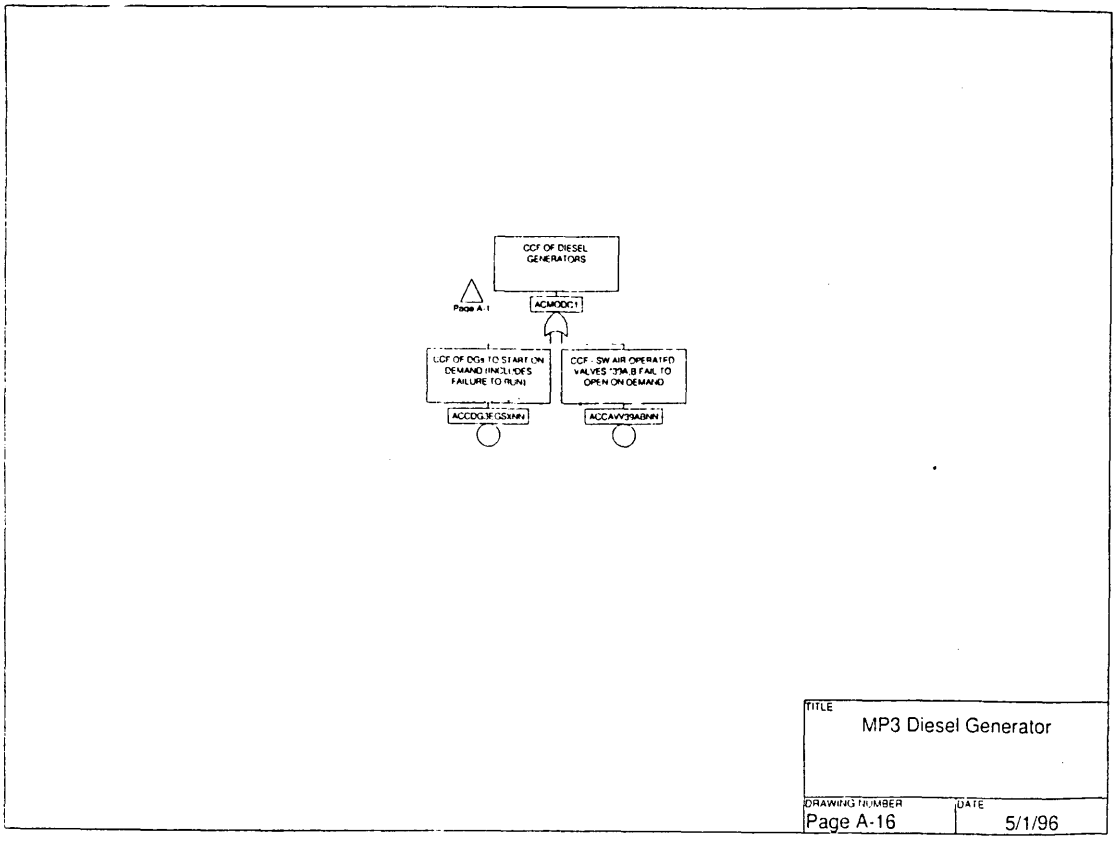


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



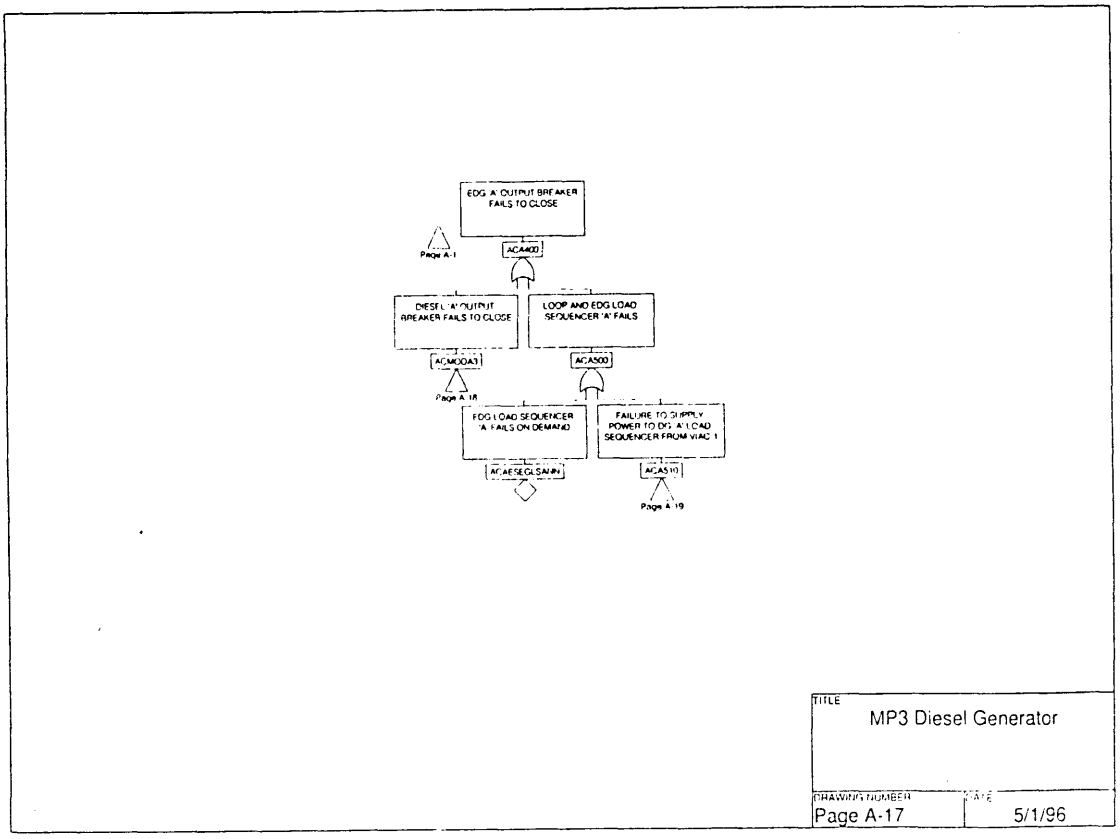
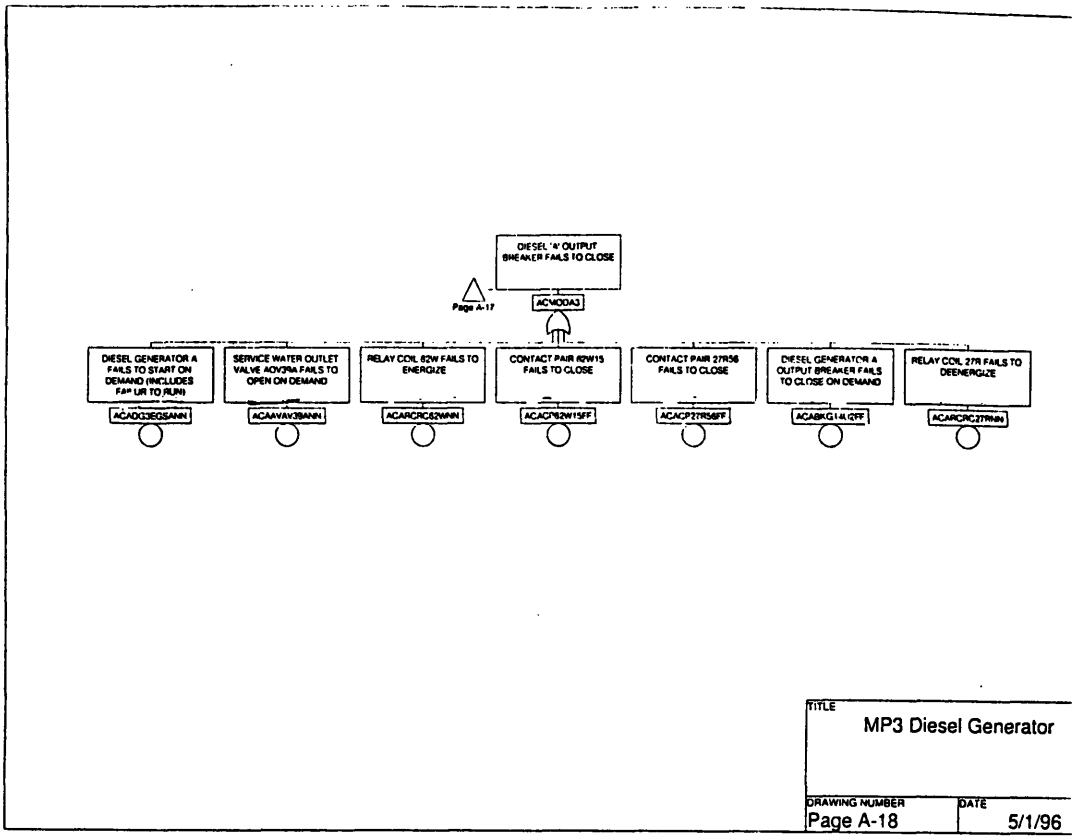


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



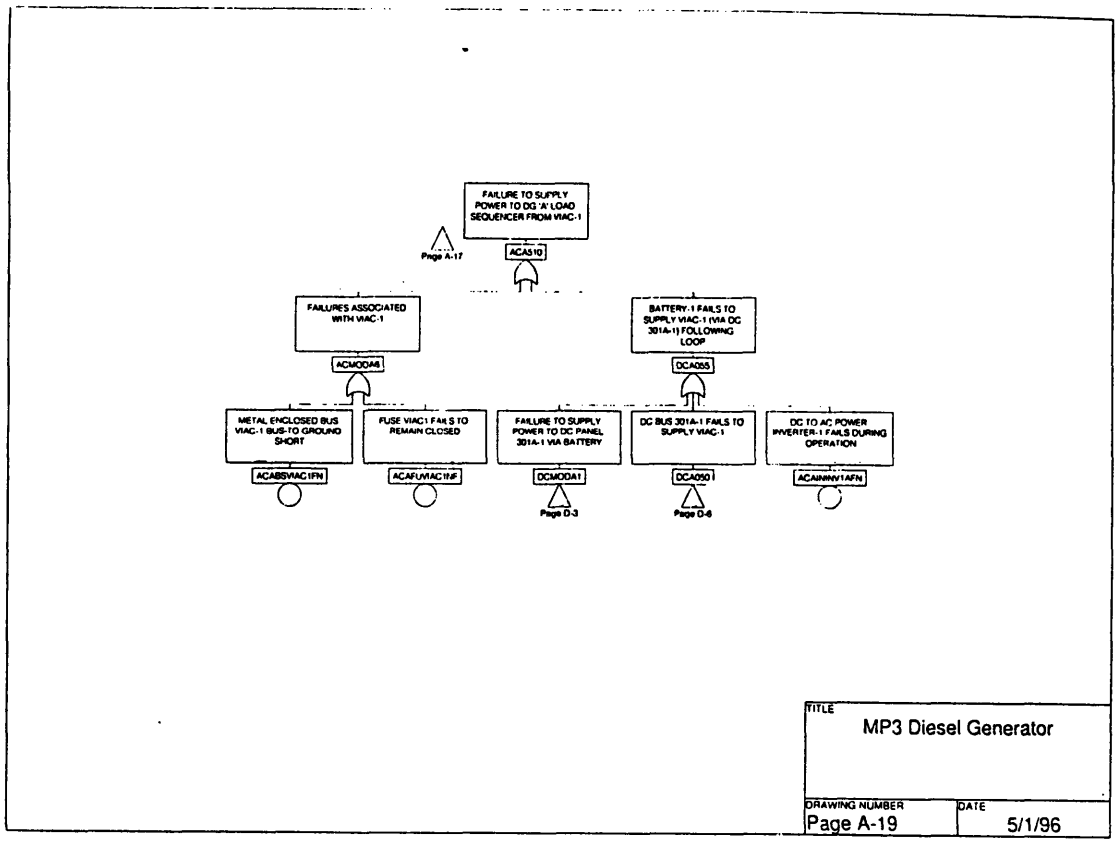
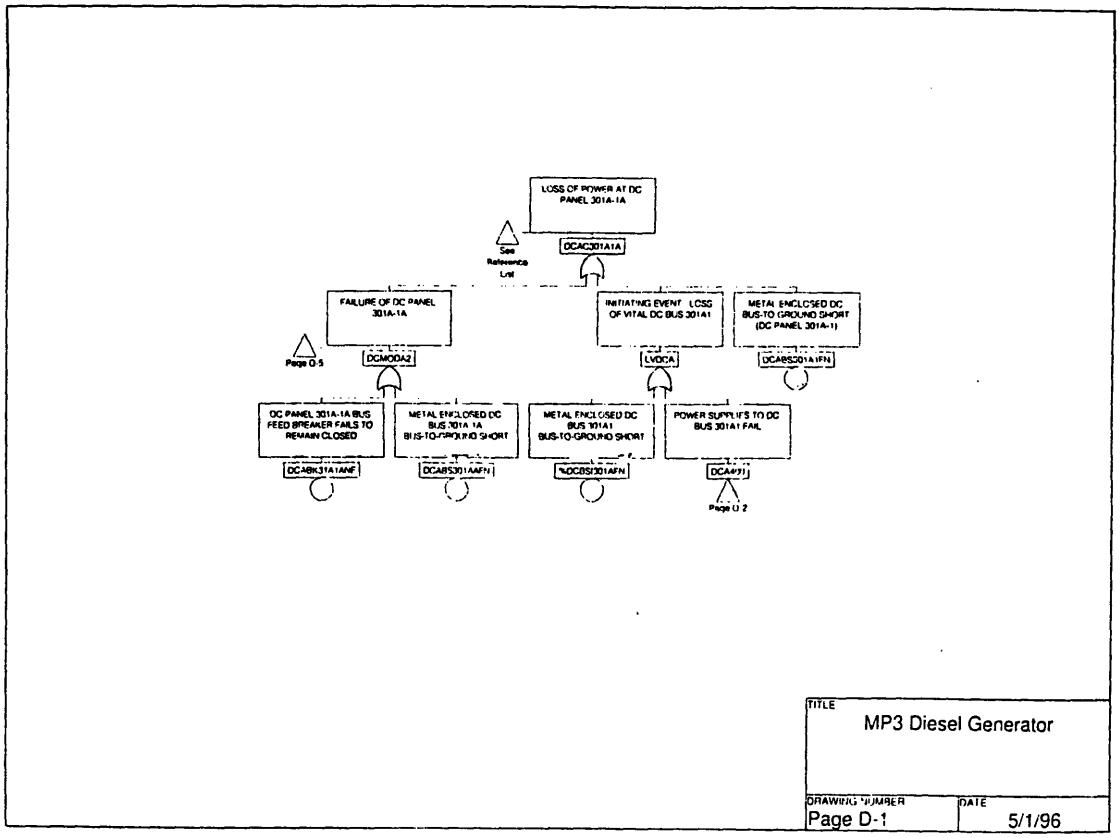


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



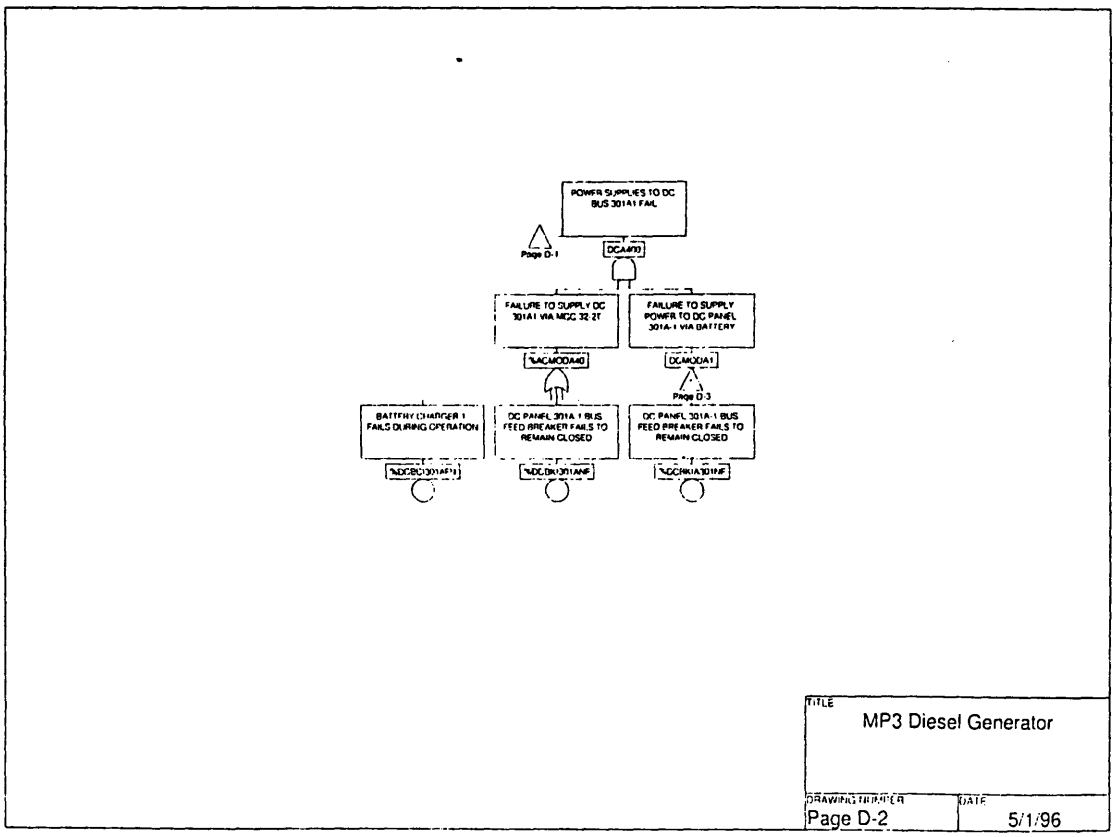
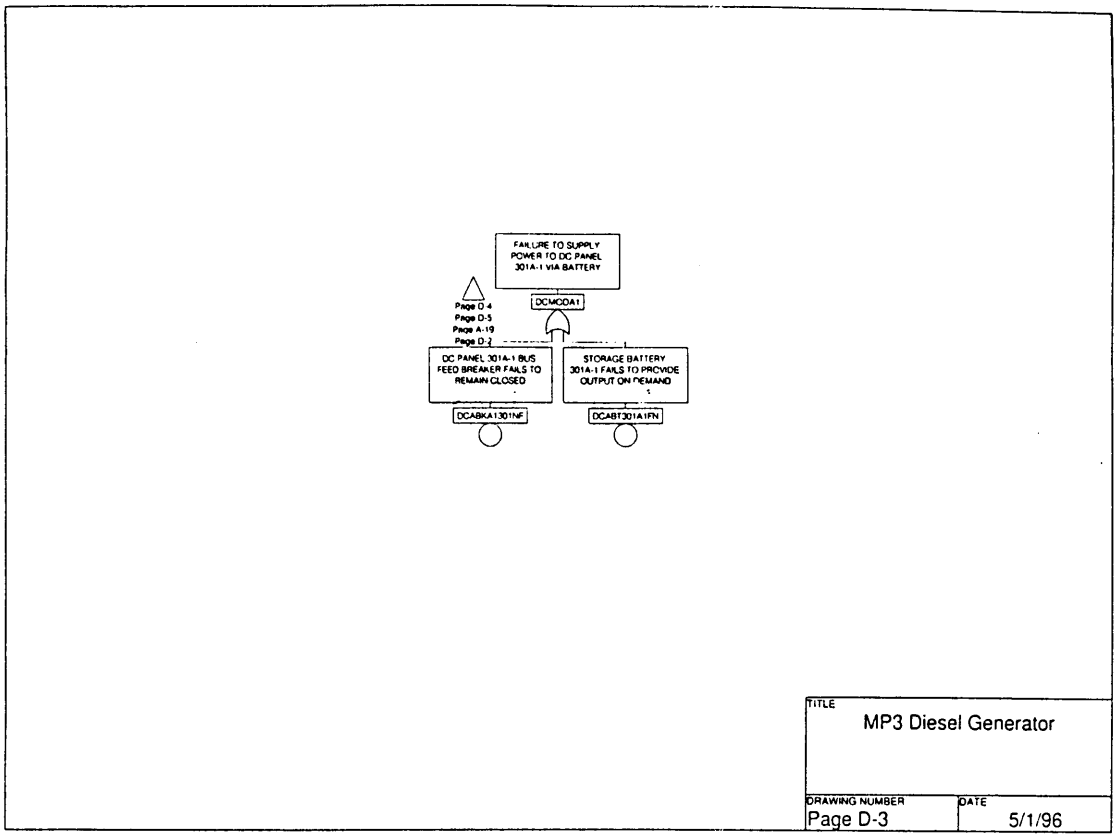


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



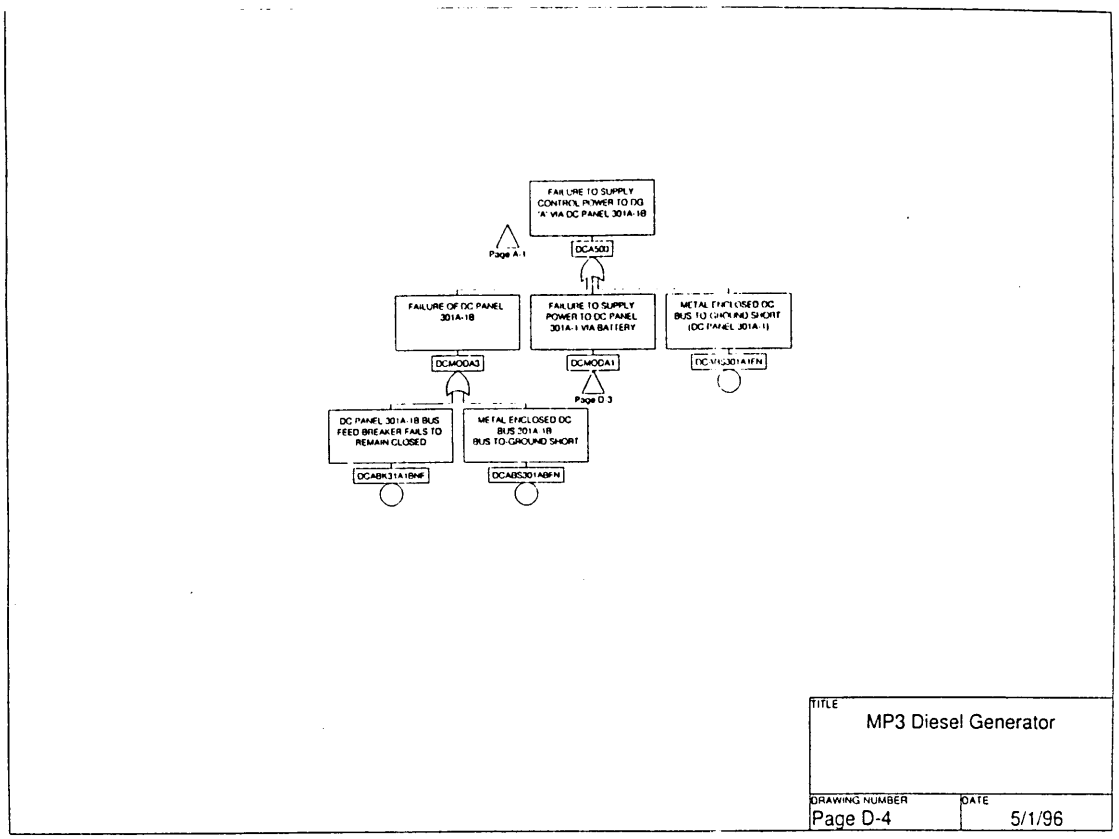
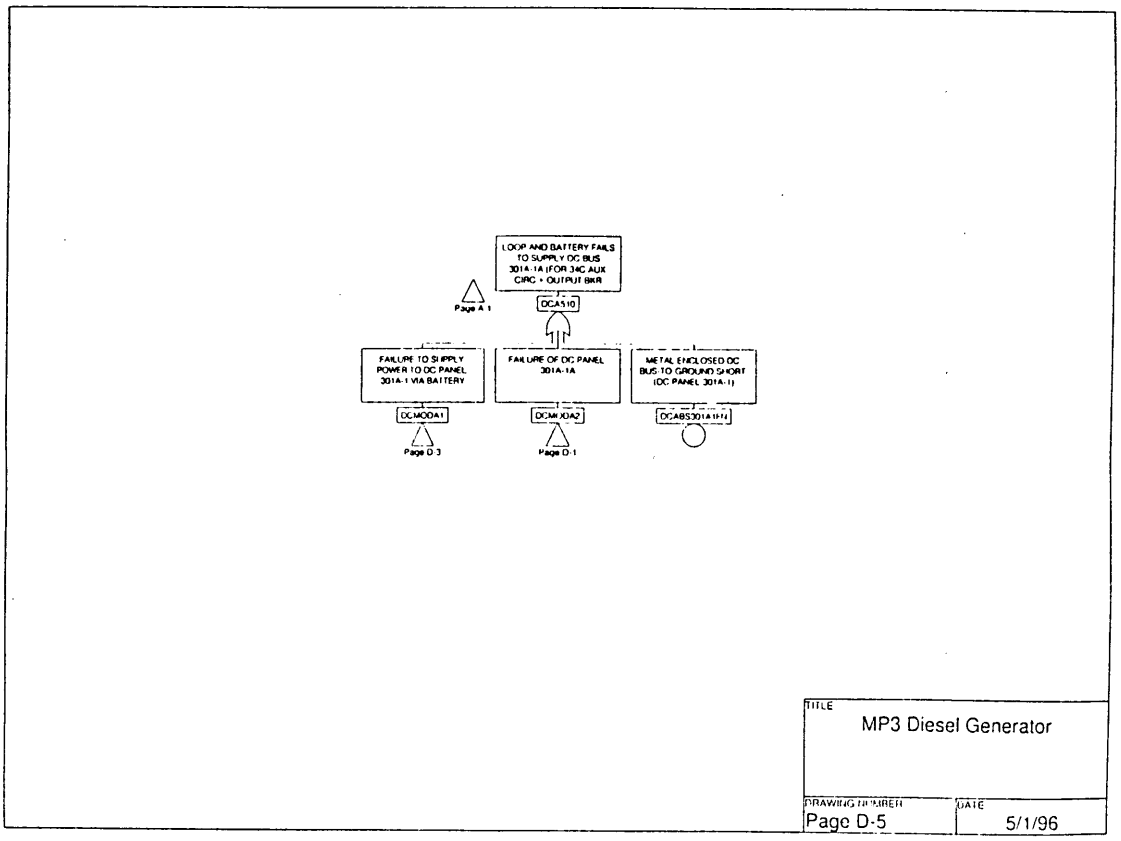


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



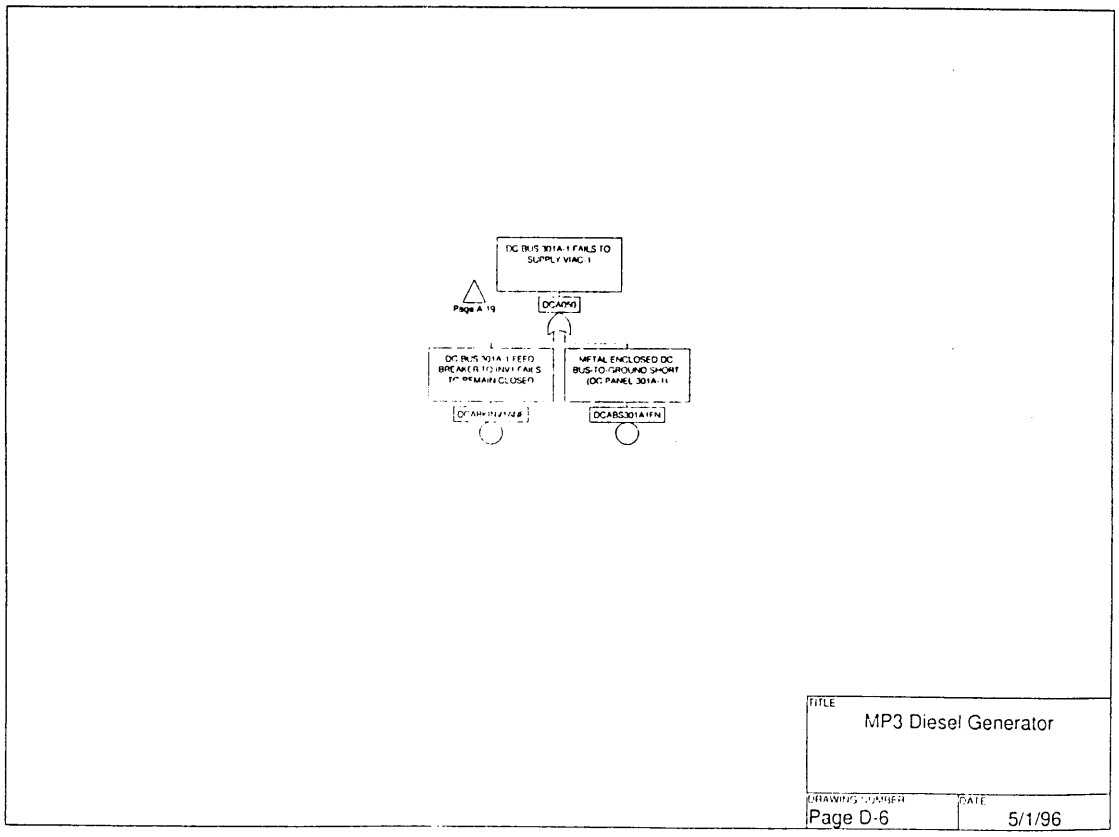
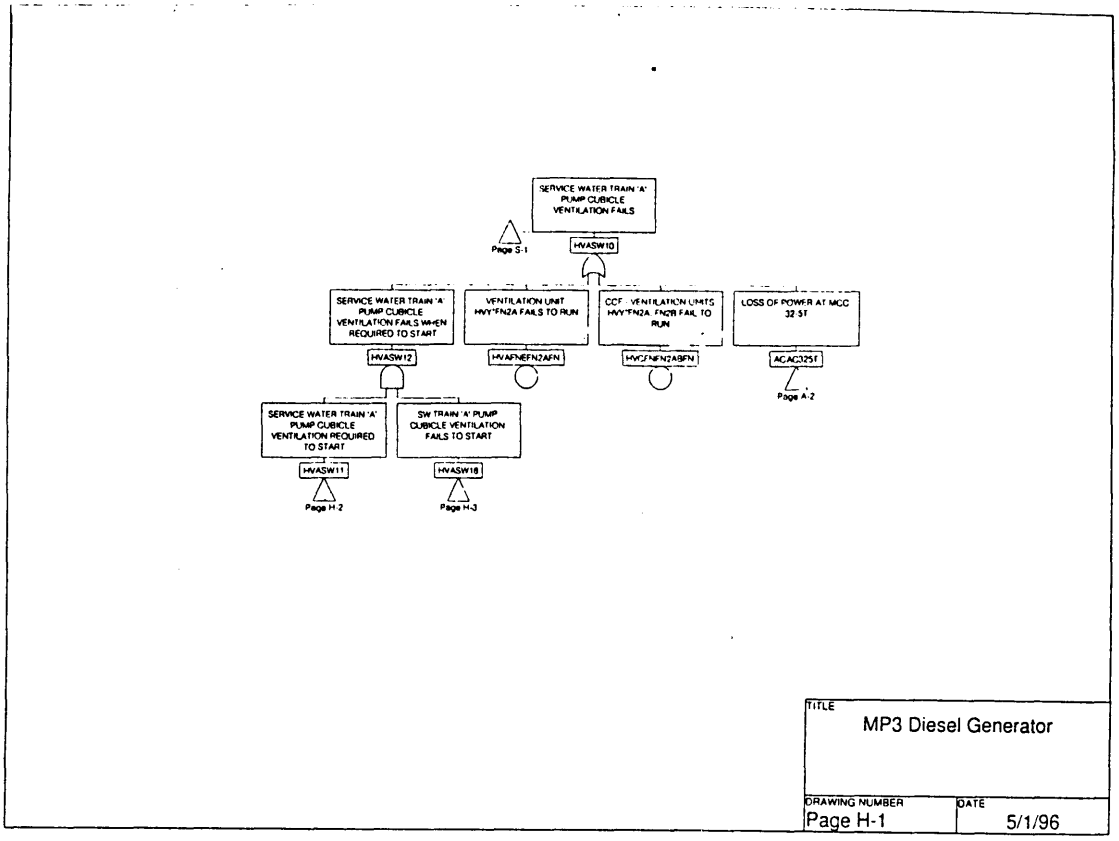


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



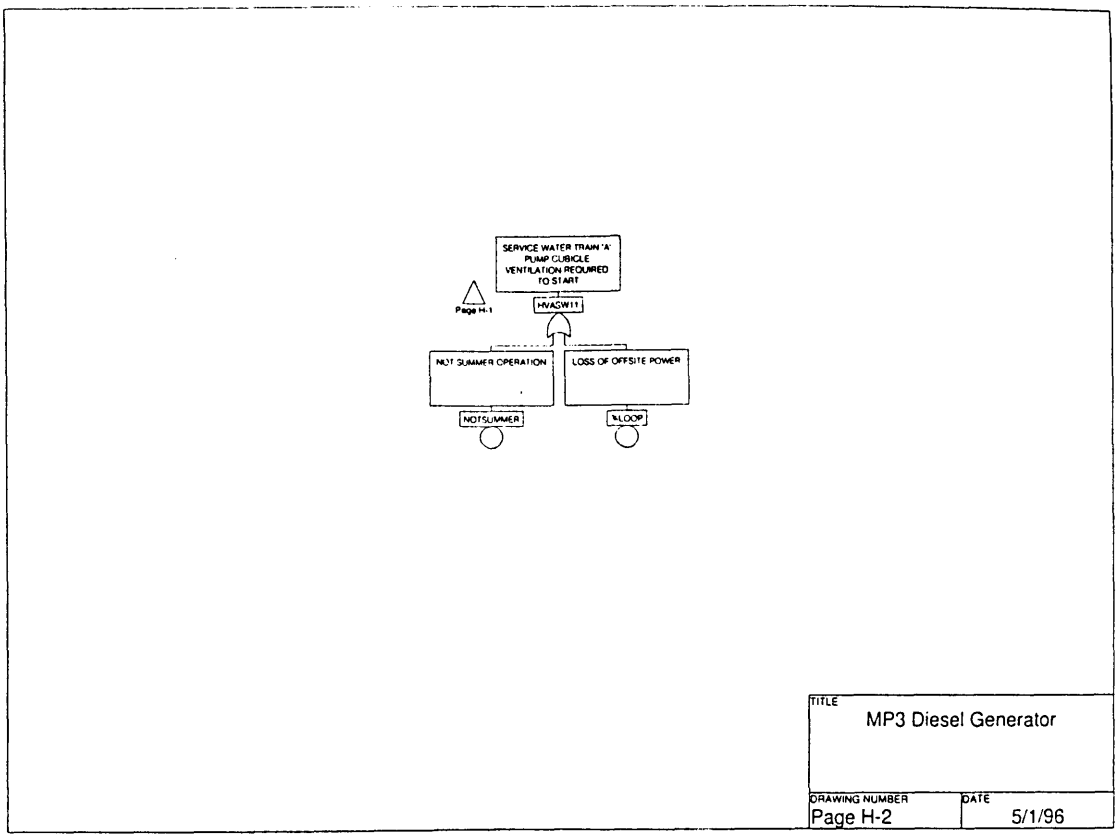
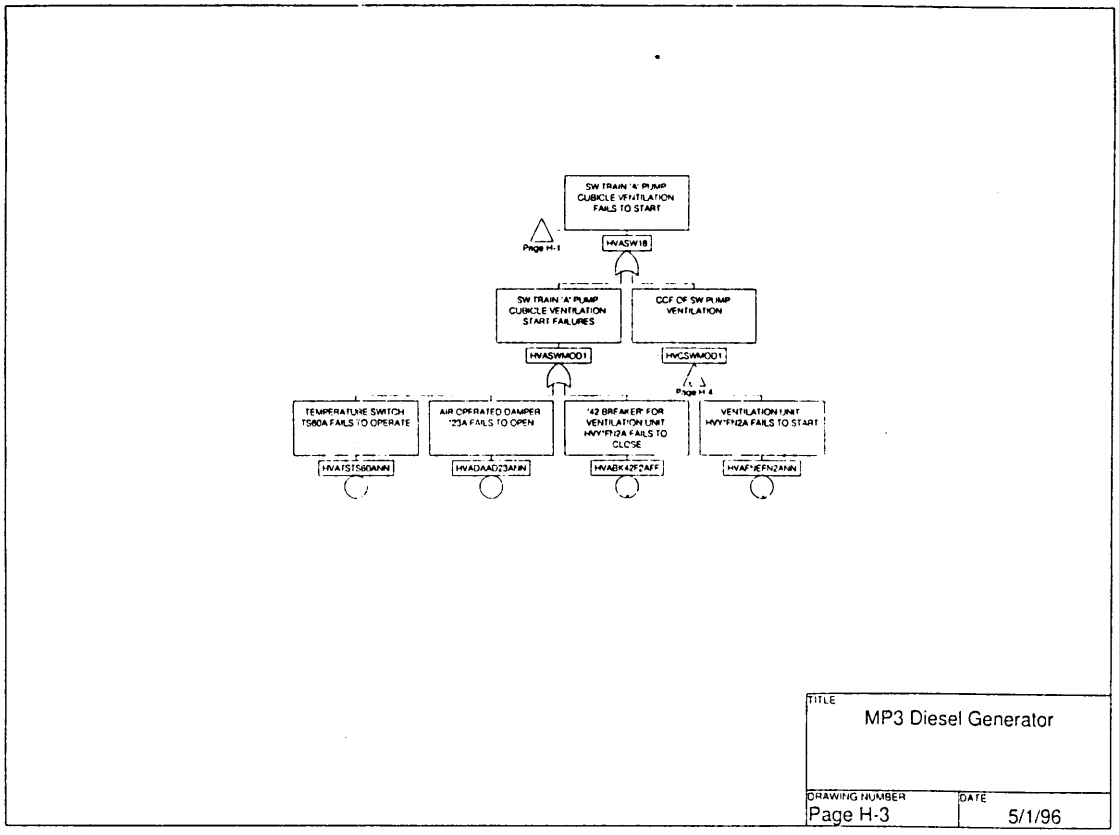


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



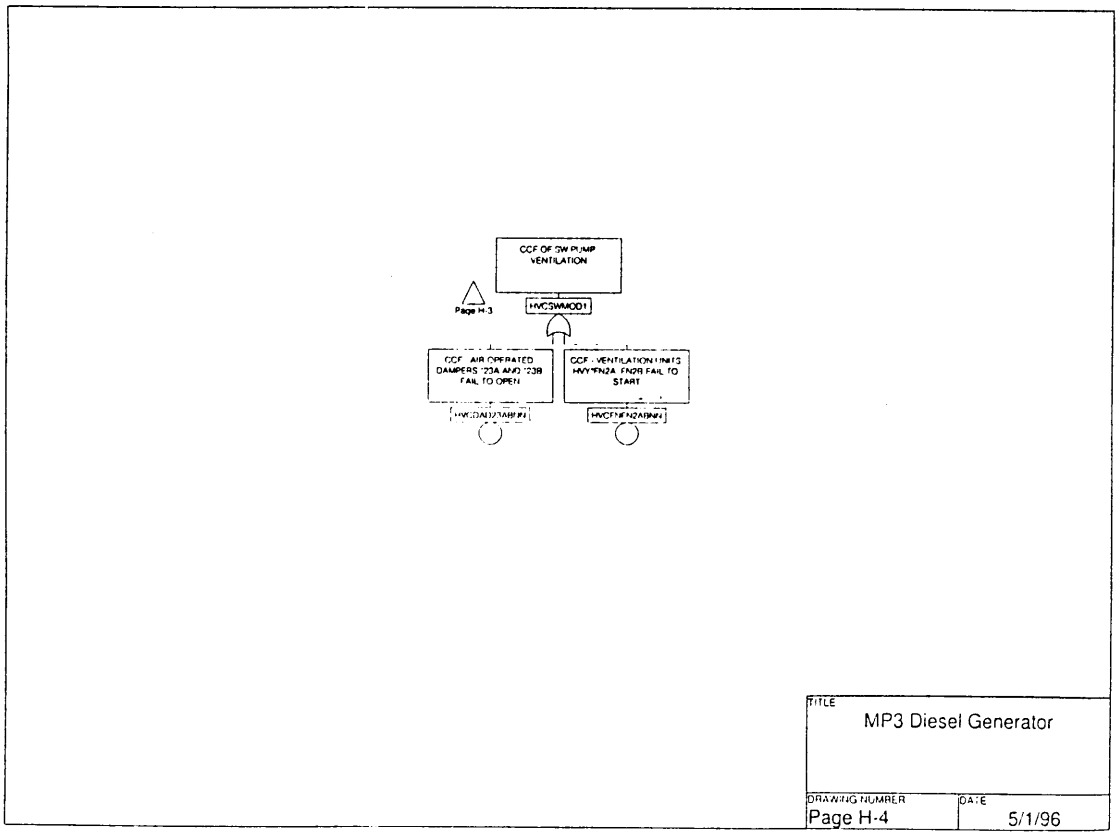
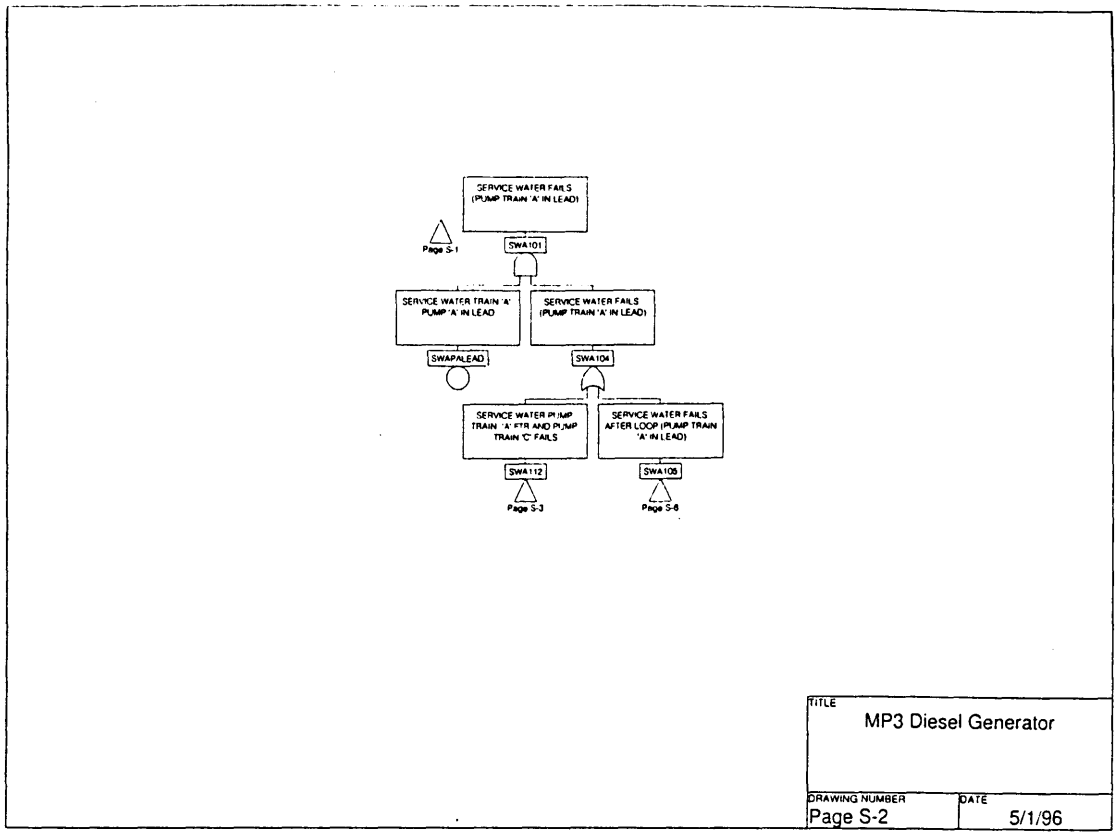


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



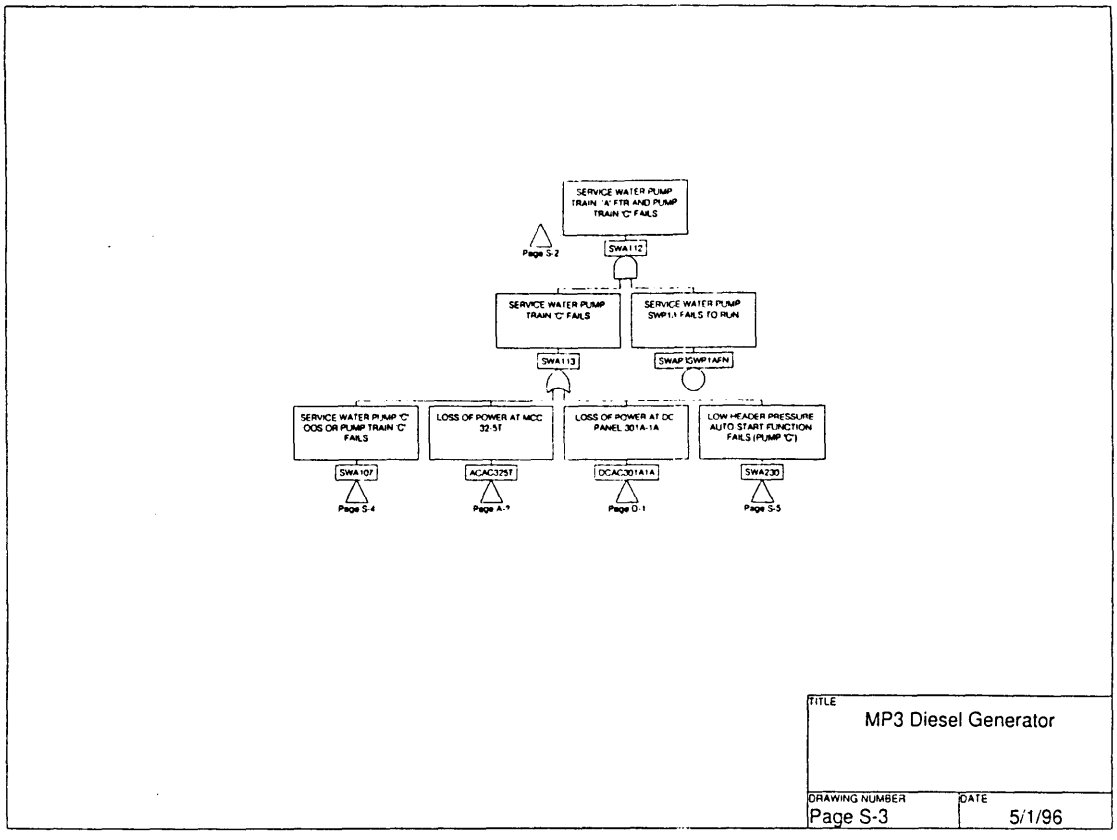
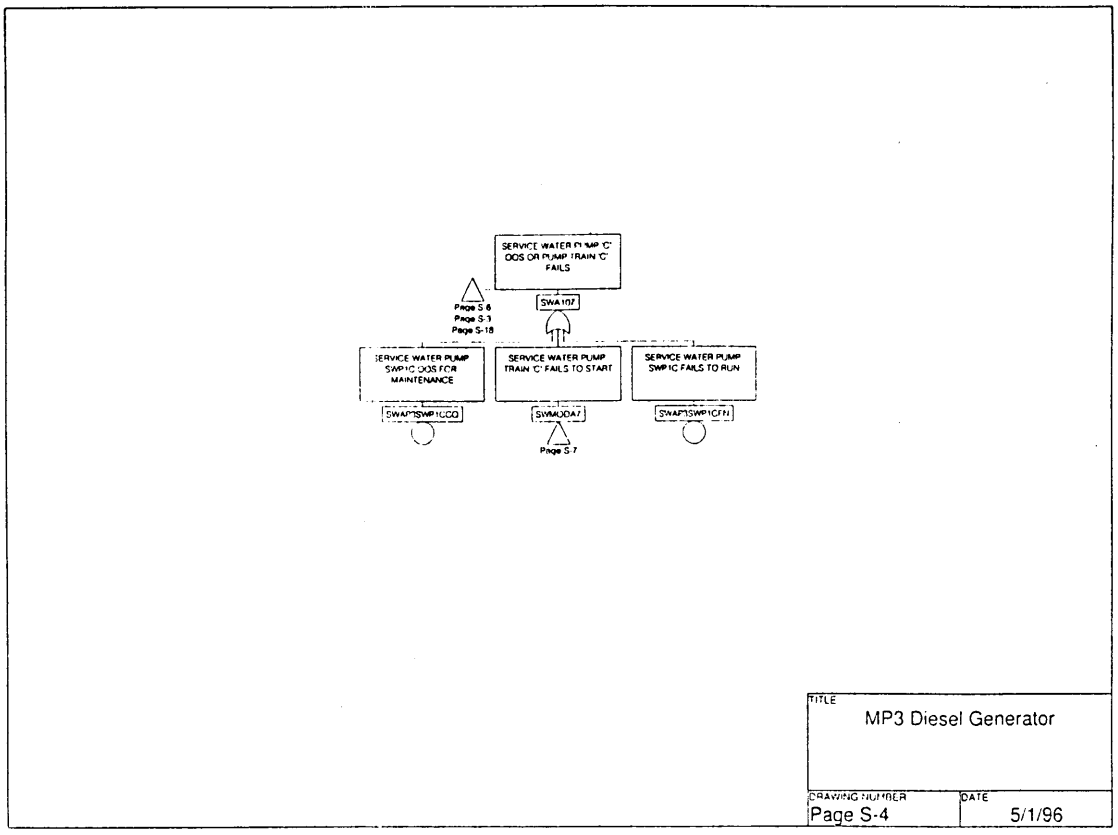


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



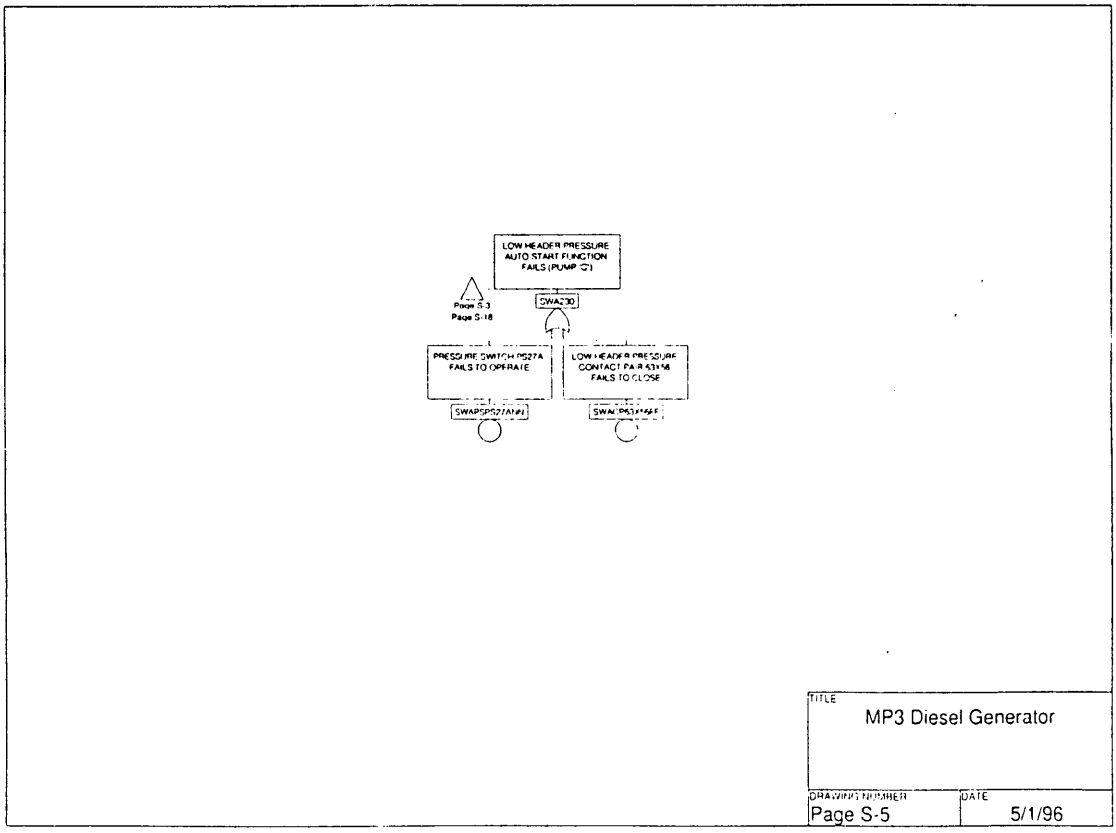
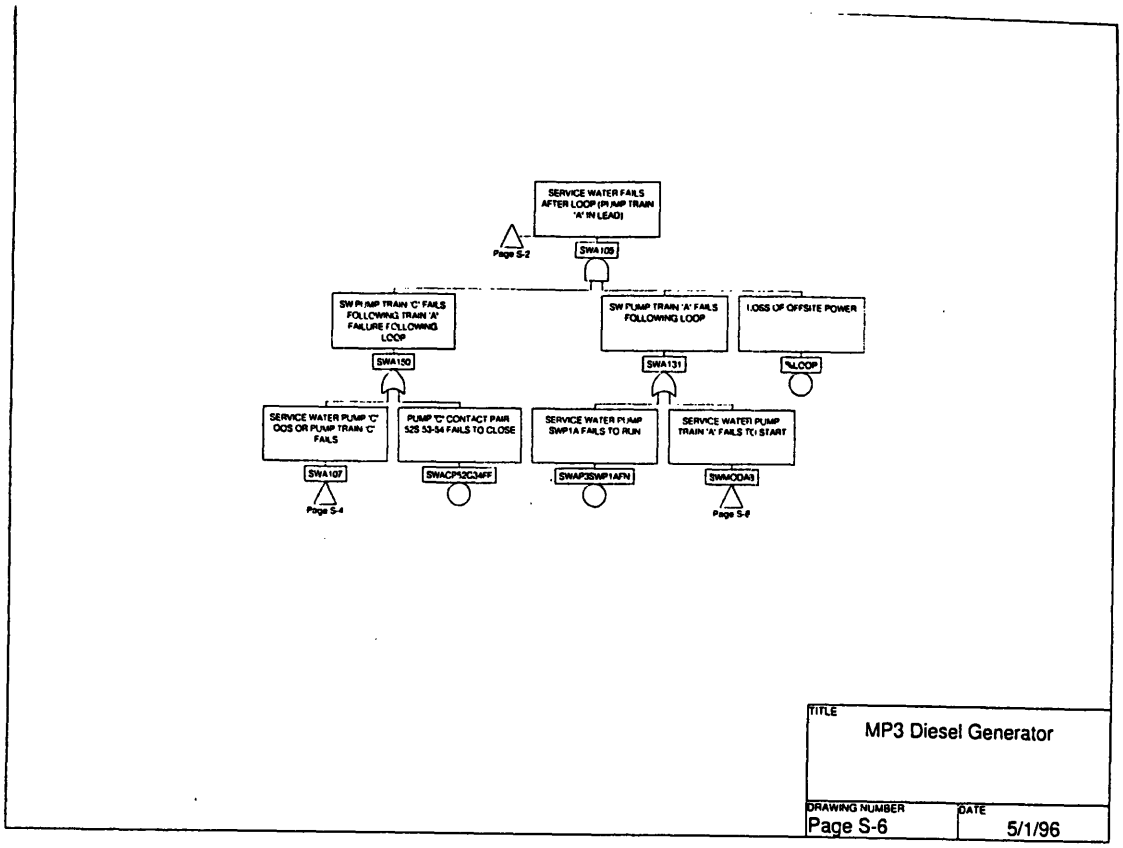


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



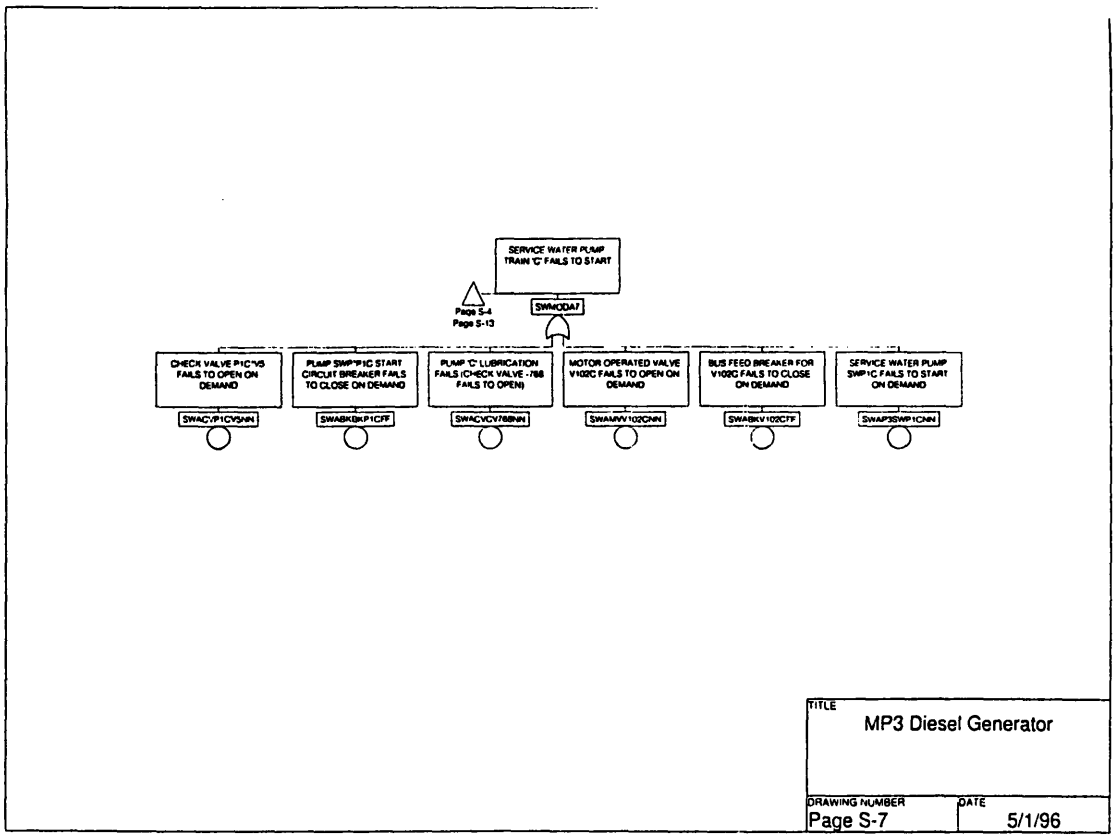
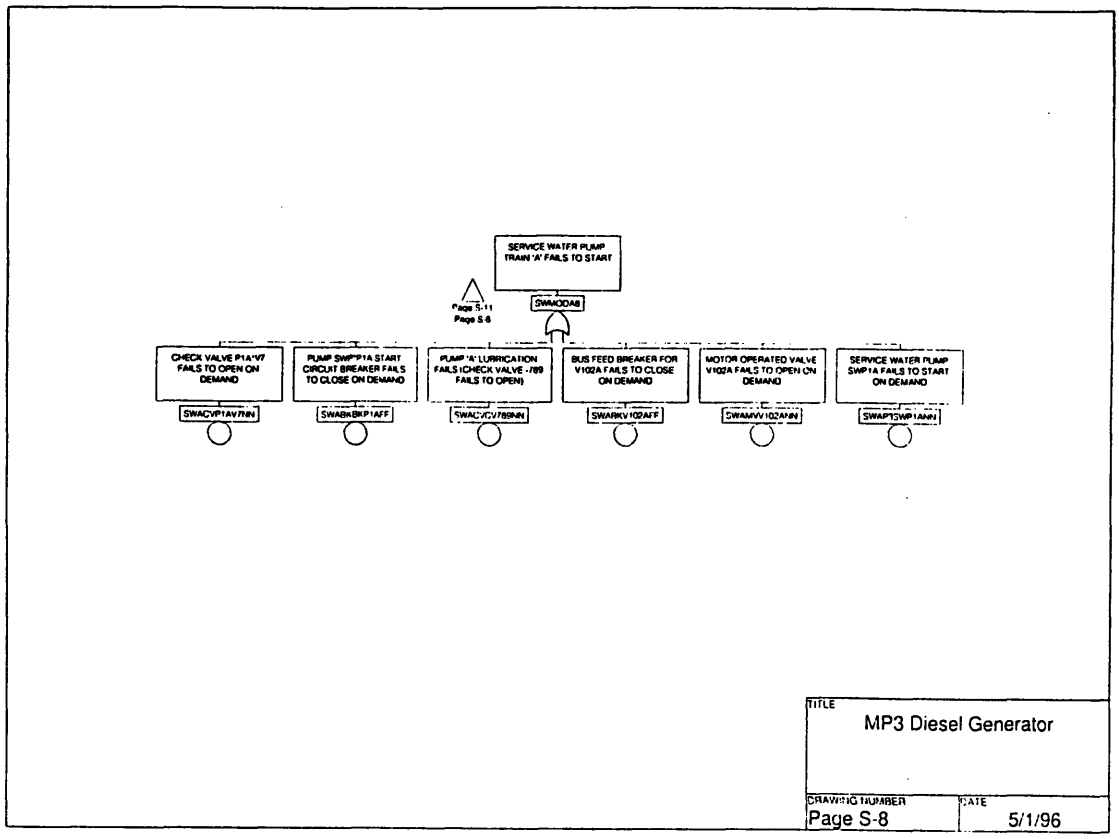


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



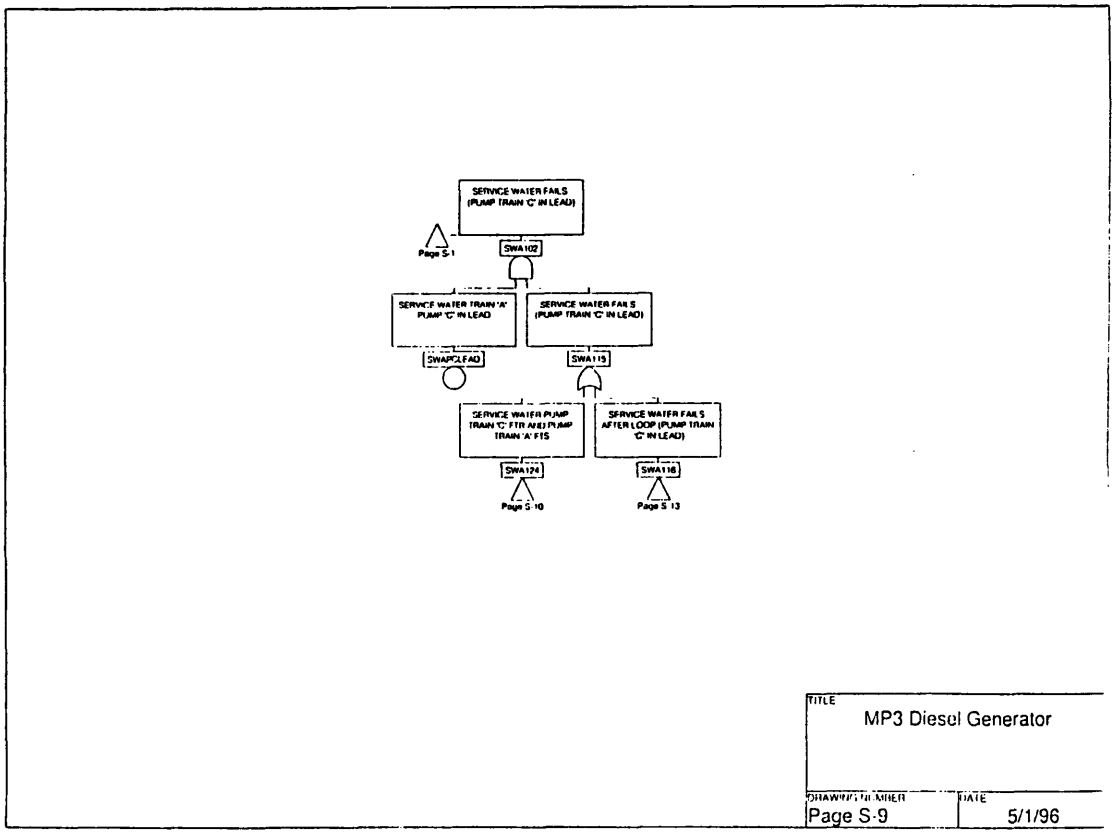
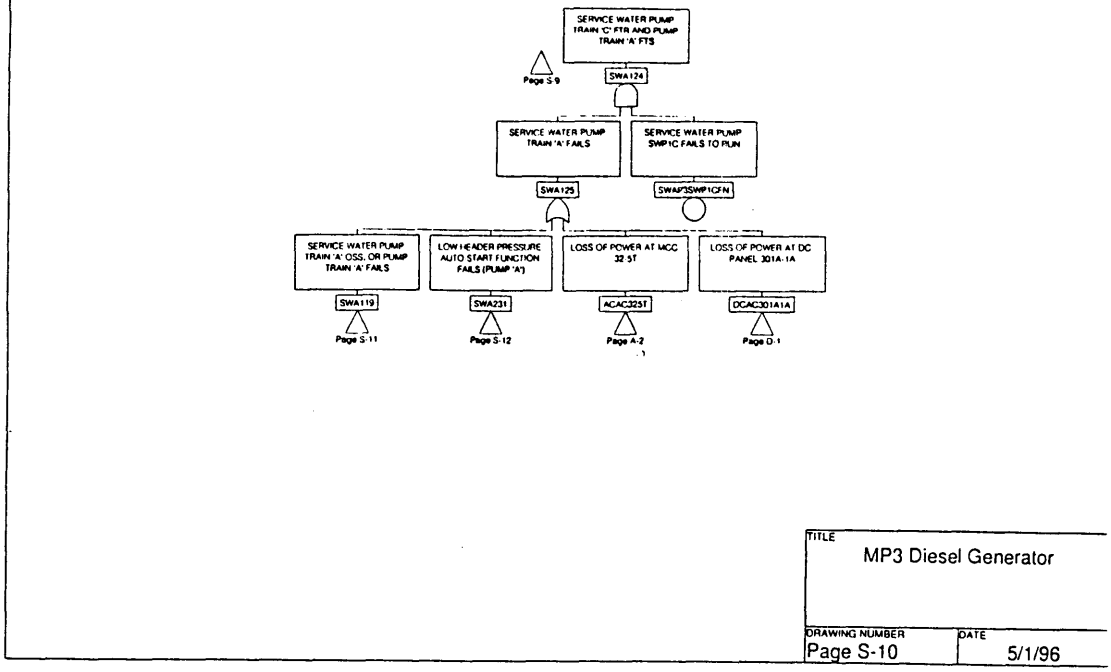


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



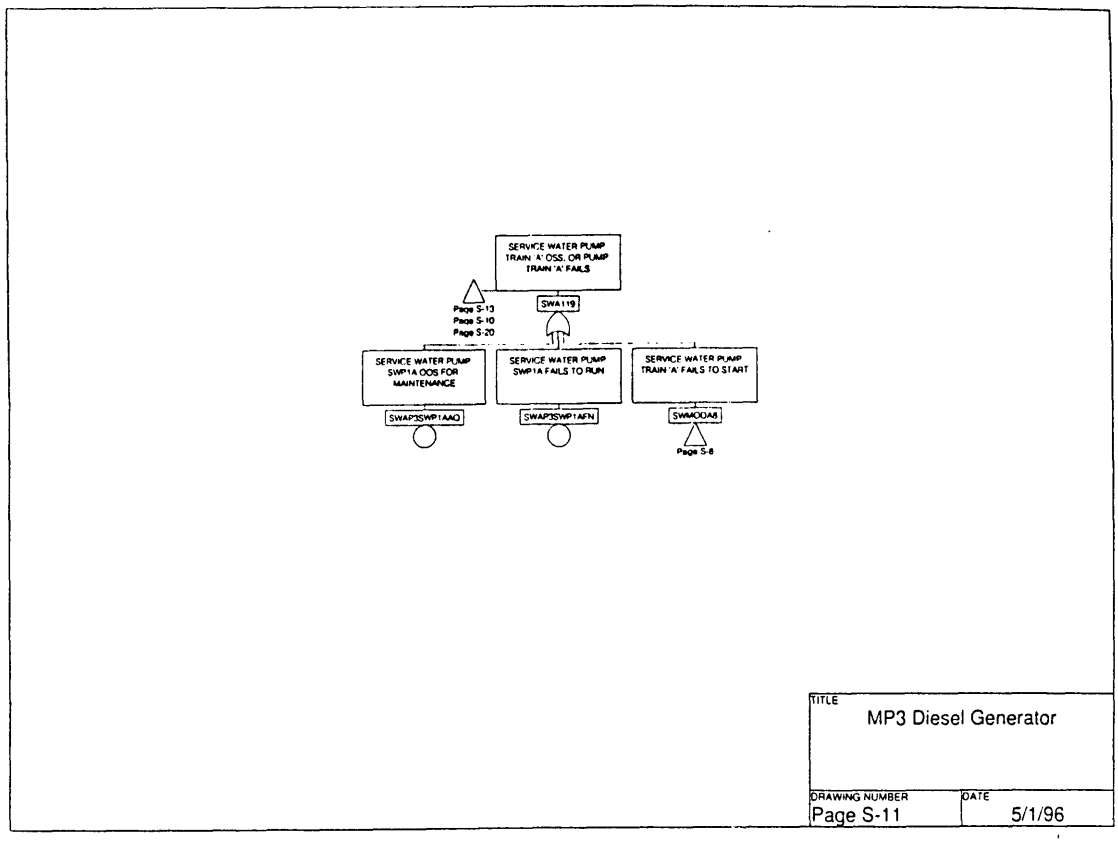
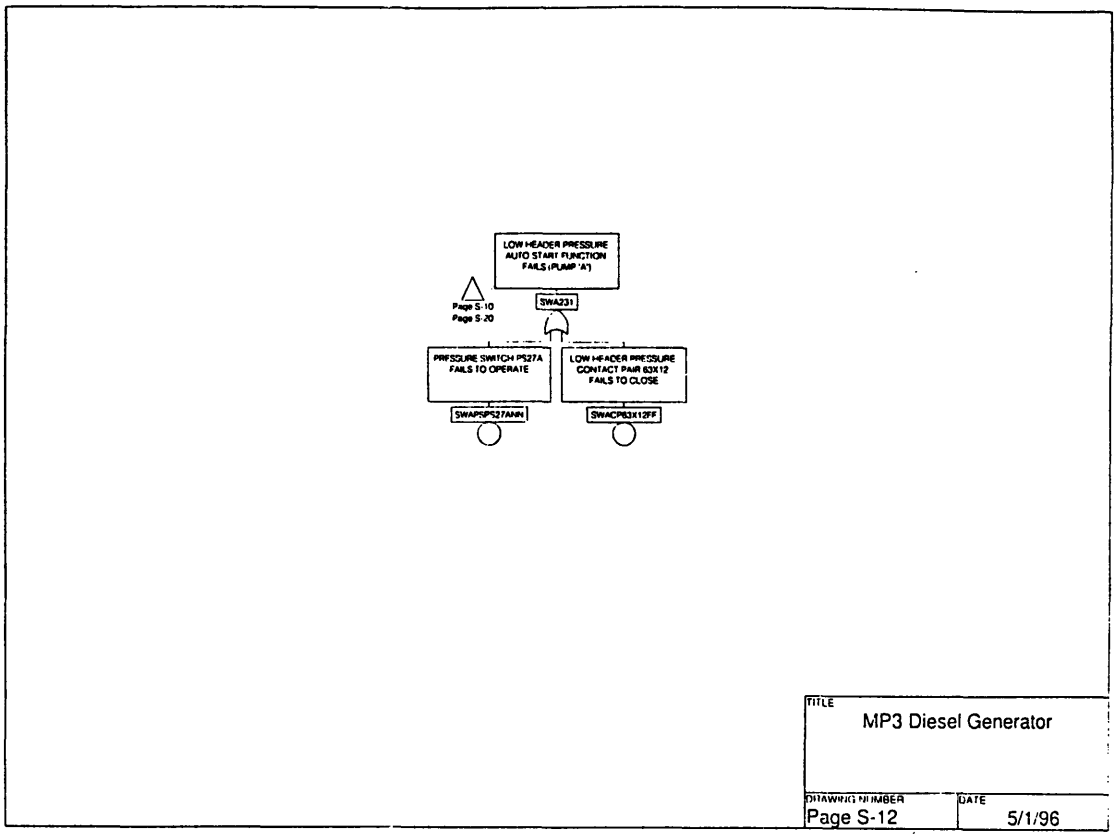


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



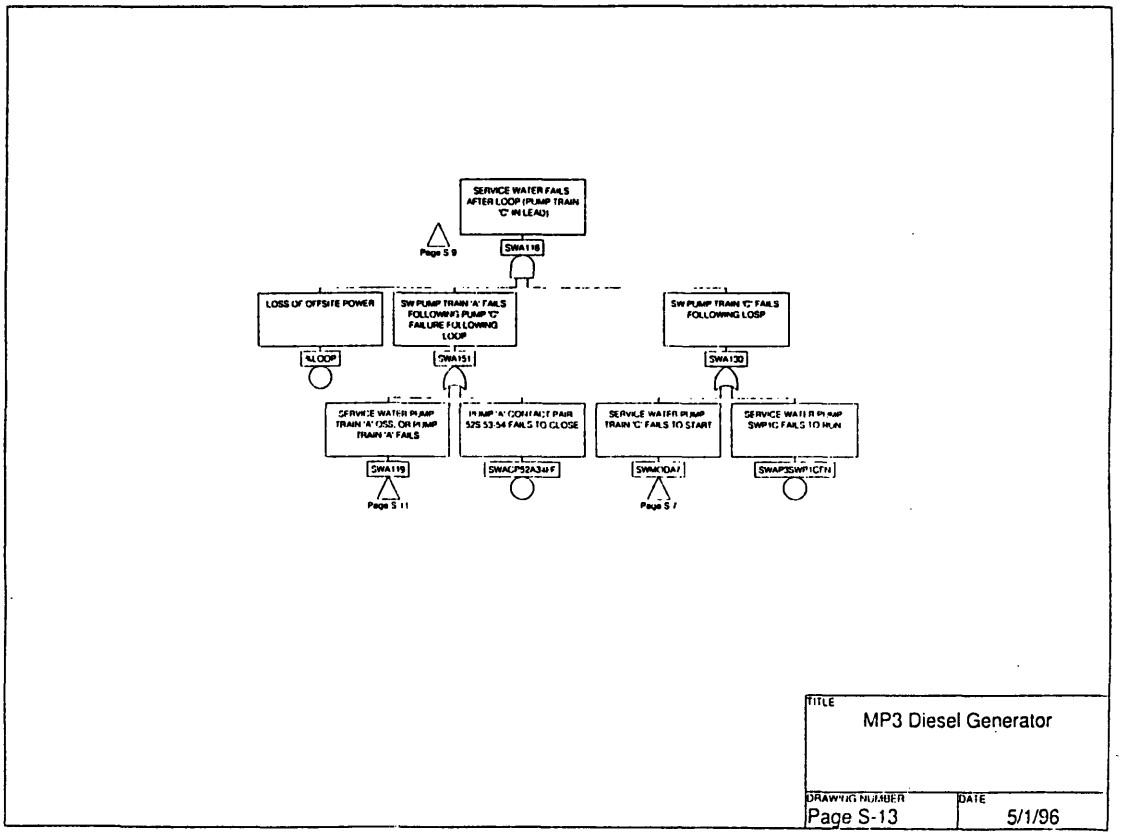
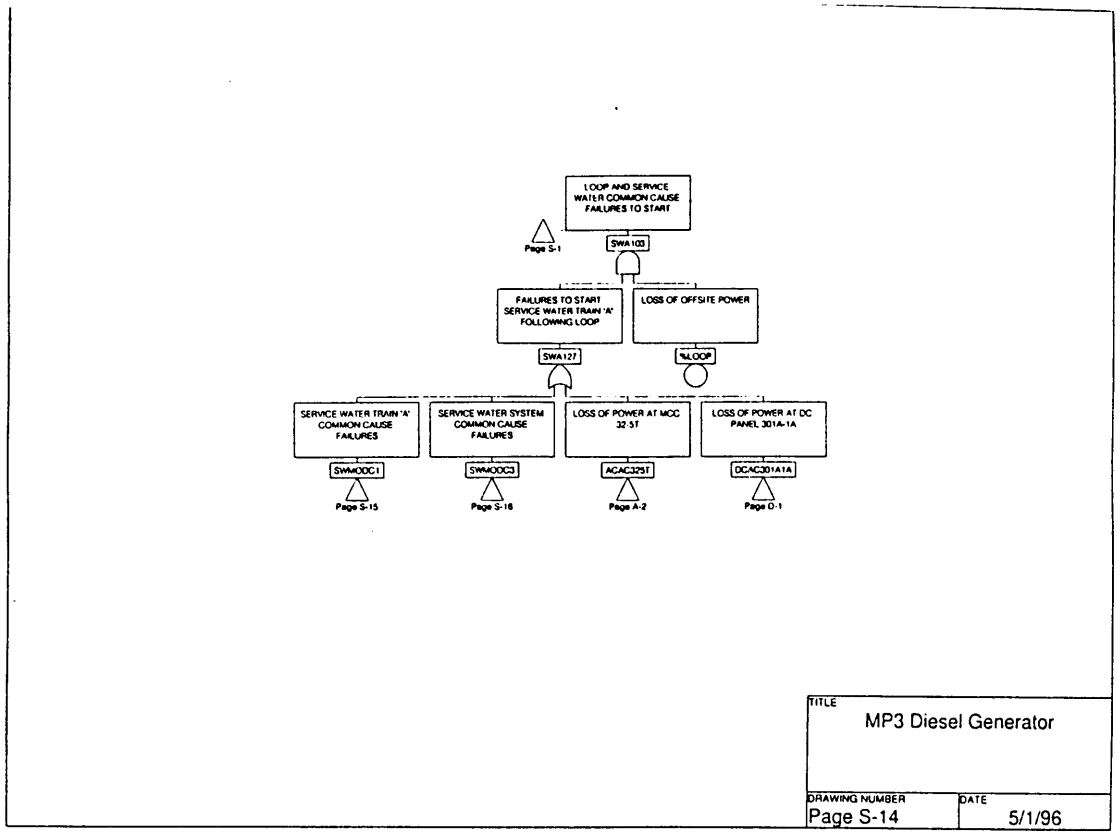


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



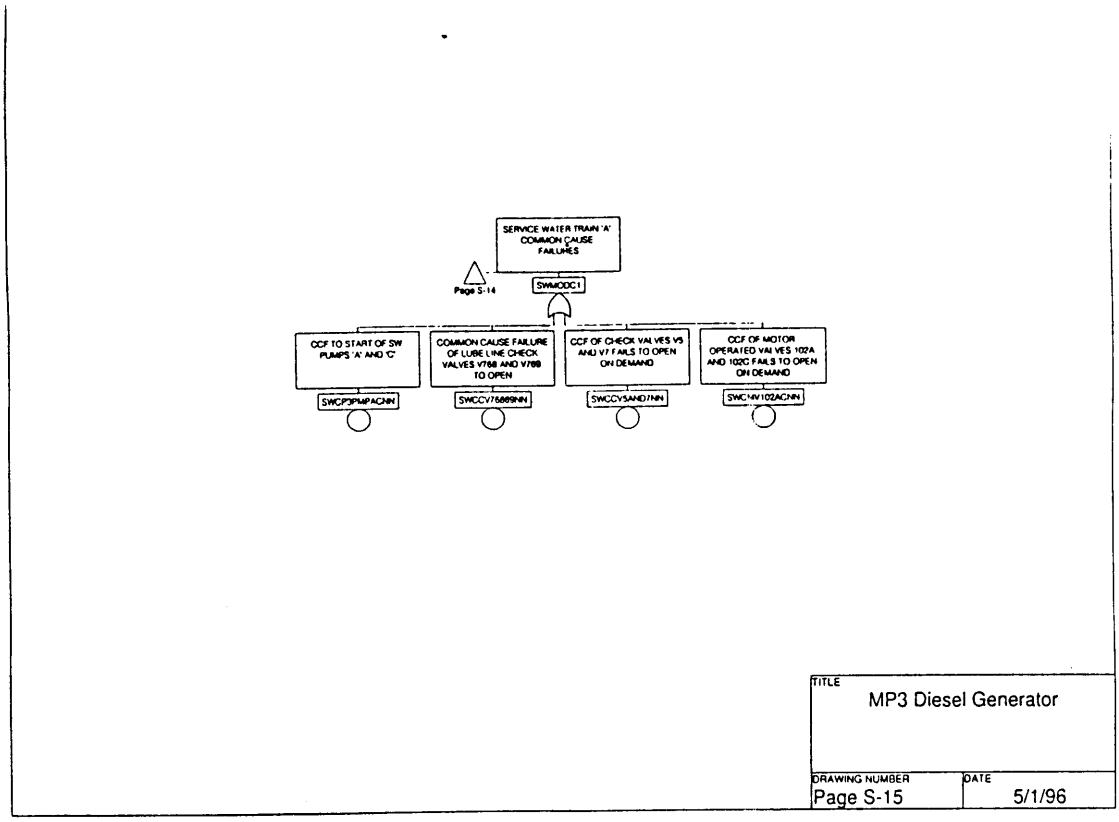
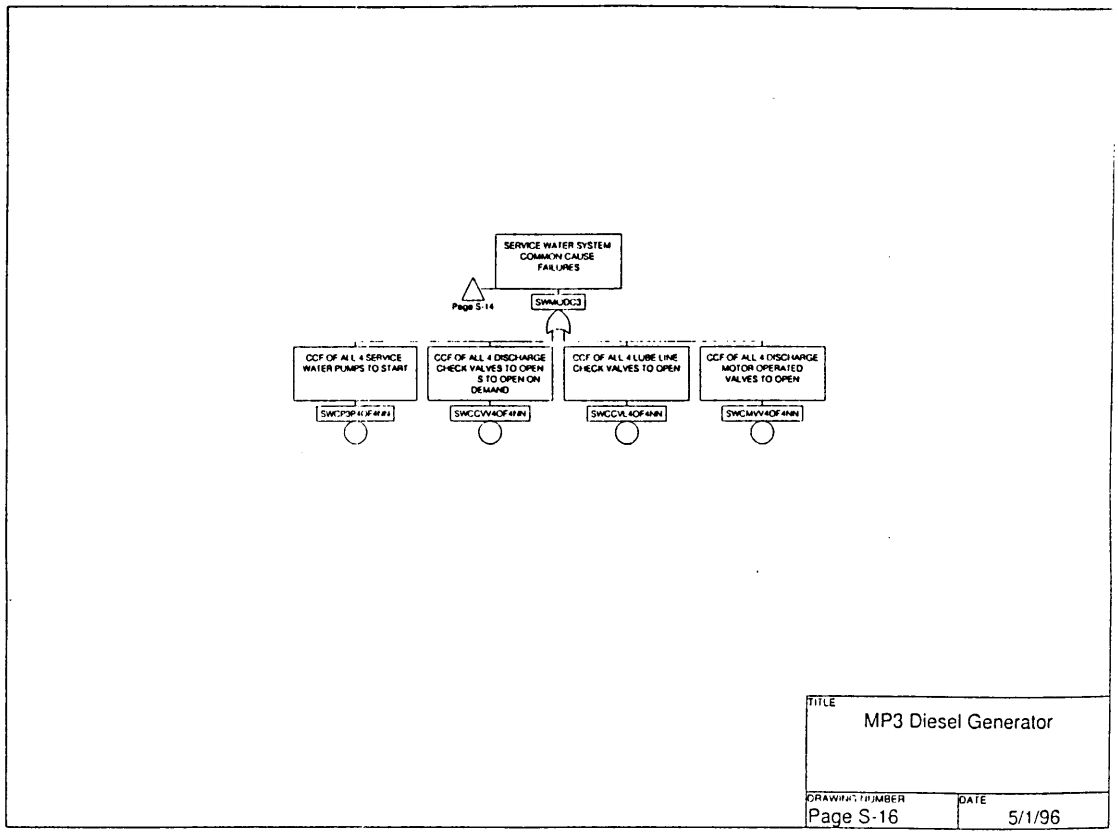


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



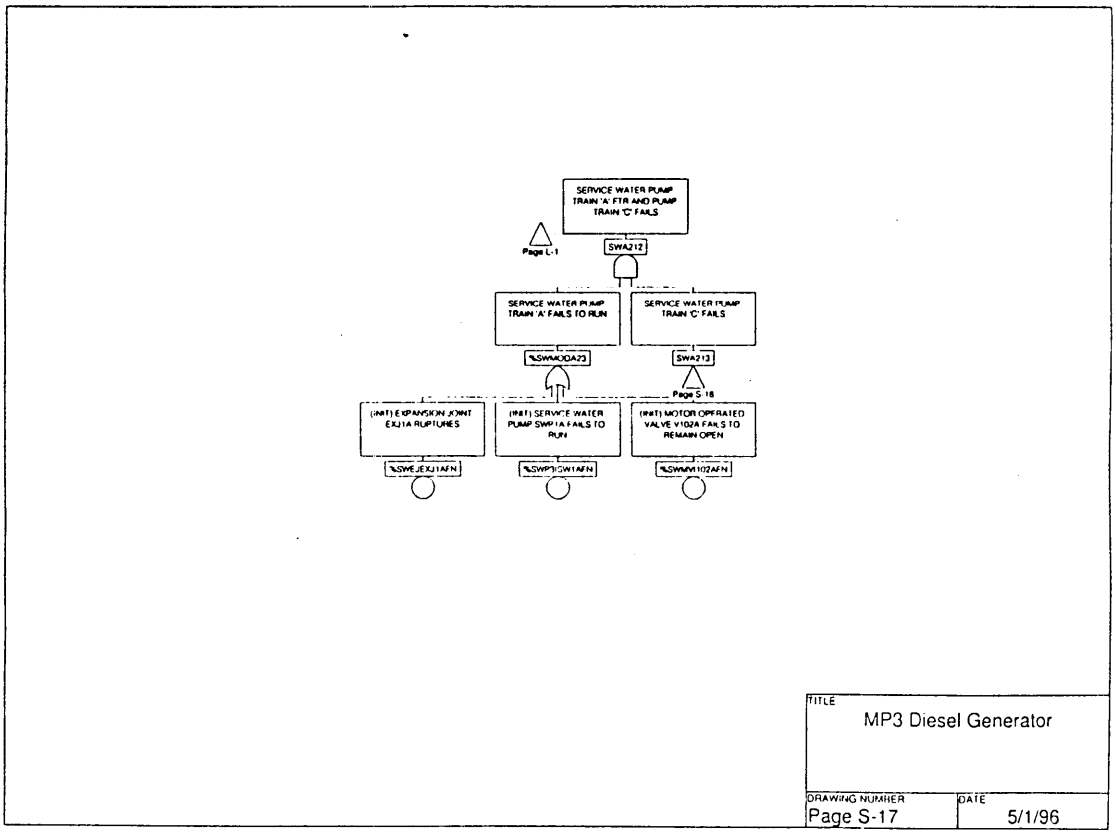
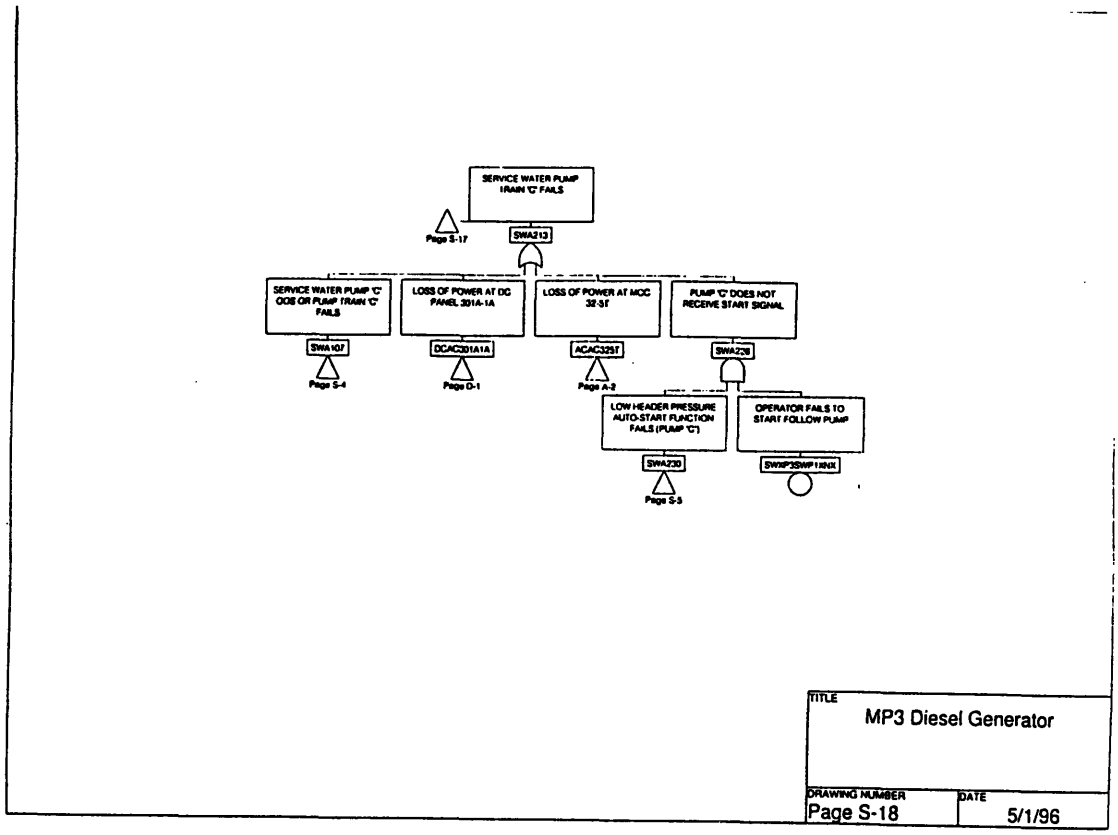


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



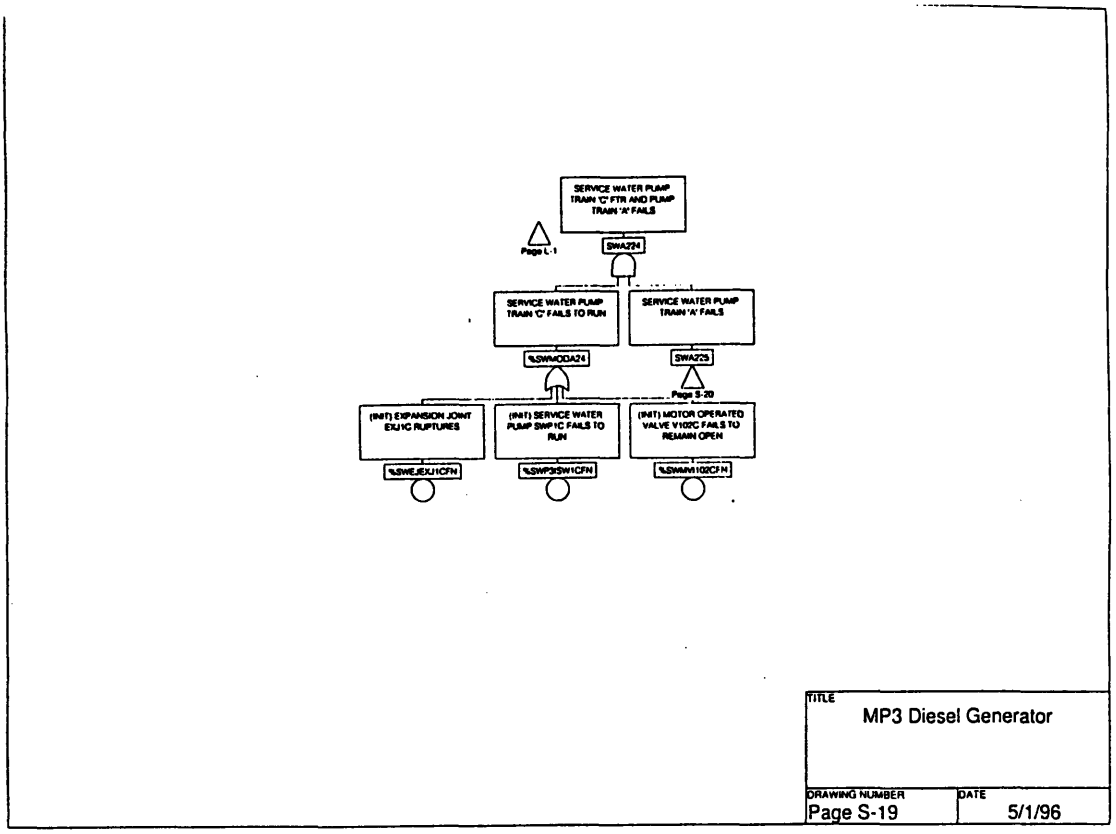
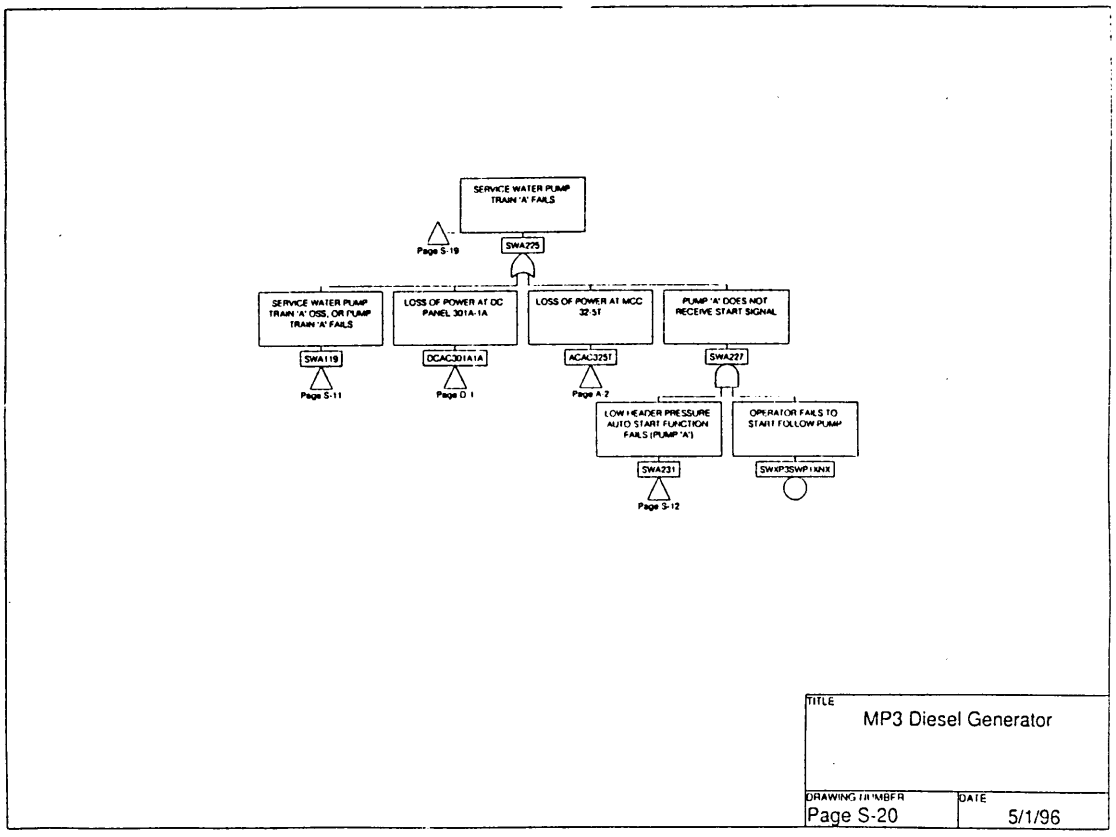


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)



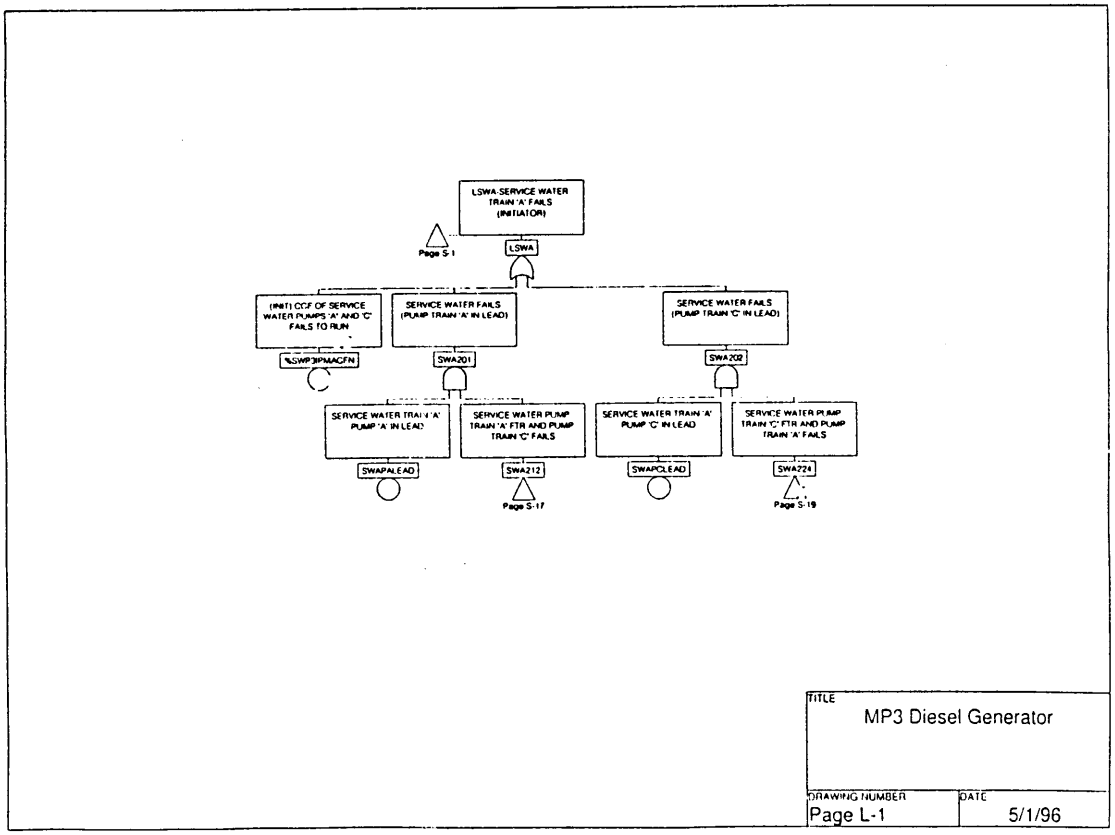


Figure A.1: Millstone 3 EDG Fault Tree (cont'd)

Appendix B

List of Reactors Considered, with EDG Information

Table B.2 below lists the nuclear power plants in the United States along with information regarding the EDG systems in use at each plant and the manufacturers of these EDG units. For each data source used in the work reported here, the plants for which failures were assessed are indicated. Additionally, notes are included for other points of interest. Table B.1 provides a key for the acronyms used in Table B.2.

Types:	BWR	Boiling Water Reactors
	PWR	Pressurized Water Reactors
Reactors:	B&W	Babcock & Wilcox (BWR)
	CE	Combustion Engineering (PWR)
	GE	General Electric (BWR)
	W	Westinghouse (PWR)
EDGs:	AP	ALCO Power (GE of England)
	CAT	Caterpillar
	CB	Cooper Bessemer
	EM	Electro Motive (General Motors)
	FC	Fairbanks Morse/Colt
	NM	Nordberg Manuf.
	TD	Transamerica Delaval
	WC	Worthington Corp.
†	Swing EDGs	Shares with Prior Plant
‡	Oconee 1, 2, 3	Use Hydroelectric Power for Emergency

Table B.1: Key to Reactor EDG Information

Plant Name	Utility Company	Type	Reactor Manuf.	EDG Manuf.	# of EDGs	# Swing	INEL	SwRI	NPRDS	Notes
Arkansas 1	Entergy Operations Inc.	BWR	B&W	EM	2	0	Y	Y	N	
Arkansas2	Entergy Operations Inc.	PWR	CE	FC	2	0	Y	Y	Y	
Beaver Valley 1	Duquesne Light Co.	PWR	W	EM	2	0	Y	Y	Y	
Beaver Valley 2	Duquesne Light Co.	PWR	W	FC	2	0	Y	N	Y	Commenced 11/87
Big Rock Point 1	Consumers Power Co.	BWR	GE	CAT	1	0	N	Y	N	
Braidwood 1	Commonwealth Edison Co.	PWR	W	CB	2	0	Y	N	Y	Commenced 7/88
Braidwood 2	Commonwealth Edison Co.	PWR	W	CB	2	0	Y	N	Y	Commenced 10/88
Browns Ferry 1	Tennessee Valley Authority	BWR	GE	EM	0	4	N	Y	N	
Browns Ferry 2	Tennessee Valley Authority	BWR	GE	EM	0	4	Y	Y	N	
Browns Ferry 3	Tennessee Valley Authority	BWR	GE	EM	4	0	N	Y	N	
Brunswick 1	Carolina Power & Light Co.	BWR	GE	NM	2	0	Y	Y	N	
Brunswick 2	Carolina Power & Light Co.	BWR	GE	NM	2	0	Y	Y	N	
Byron 1	Commonwealth Edison Co.	PWR	W	CB	2	0	Y	N	Y	Commenced 9/85
Byron 2	Commonwealth Edison Co.	PWR	W	CB	2	0	Y	N	Y	Commenced 8/87
Callaway 1	Union Electric Co.	PWR	W	FC	2	0	Y	N	Y	Commenced 4/85
Calvert Cliffs 1	Baltimore Gas & Electric Co.	PWR	CE	FC	1	1	Y	Y	Y	
Calvert Cliffs 2	Baltimore Gas & Electric Co.	PWR	CE	FC	1	†	Y	Y	Y	
Catawba 1	Duke Power Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 6/85
Catawba 2	Duke Power Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 8/86
Clinton 1	Illinois Power Co.	BWR	GE	EM	2	0	Y	N	N	Commenced 11/87
Comanche Peak 1	Texas Utilities Electric Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 8/90
Comanche Peak 2	Texas Utilities Electric Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 8/93
Cook 1	Indiana & Michigan Elec. Co.	PWR	W	WC	2	0	Y	Y	Y	

Table B.2: Reactors with EDG Information

Plant Name	Utility Company	Type	Reactor Manuf.	EDG Manuf.	# of EDGs	# Swing	INEL	SwRI	NPRDS	Notes
Cook 2	Indiana & Michigan Elec. Co.	PWR	W	WC	2	0	Y	Y	Y	
Cooper Station	Nebraska Public Power District	BWR	GE	CB	2	0	Y	Y	N	
Crystal River 3	Florida Power Corp.	BWR	B&W	FC	2	0	Y	Y	N	
Davis-Besse 1	Toledo Edison Co.	BWR	B&W	EM	2	0	Y	Y	N	
Diablo Canyon 1	Pacific Gas & Electric Co.	PWR	W	AP	2	1	Y	N	Y	Commenced 5/85
Diablo Canyon 2	Pacific Gas & Electric Co.	PWR	W	AP	2	†	Y	N	Y	Commenced 3/86
Dresden 2	Commonwealth Edison Co.	BWR	GE	EM	1	1	Y	Y	N	
Dresden 3	Commonwealth Edison Co.	BWR	GE	EM	1	†	Y	Y	N	
Duane Arnold	IES Utilities Inc.	BWR	GE	FC	2	0	Y	Y	N	
Farley 1	Southern Nuclear Operating Co.	PWR	W	FC	2	1	Y	Y	Y	
Farley 2	Southern Nuclear Operating Co.	PWR	W	FC	2	†	Y	Y	Y	
Fermi 2	Detroit Edison Co.	BWR	GE	FC	4	0	Y	N	N	Commenced 1/88
Fitzpatrick	Power Authority of the State of NY	BWR	GE	EM	4	0	Y	Y	N	
Fort Calhoun 1	Omaha Public Power District	PWR	CE	EM	2	0	Y	Y	Y	
Ginna 1	Rochester Gas & Electric Corp.	PWR	W	AP	2	0	Y	Y	Y	
Grand Gulf 1	Entergy Operation, Inc.	BWR	GE	TD	2	0	Y	N	N	Commenced 7/85
Haddam Neck	Conn. Yankeee Atomic Power Co.	PWR	W	EM	2	0	Y	Y	Y	Shut Down 1996
Harris 1	Carolina Power & Light Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 5/87
Hatch 1	Southern Nuclear Operating Co.	BWR	GE	FC	2	1	Y	Y	N	
Hatch 2	Southern Nuclear Operating Co.	BWR	GE	FC	2	†	Y	Y	N	
Hope Creek 1	Public Service Electric & Gas Co.	BWR	GE	FC	4	0	Y	N	N	Commenced 12/86
Indian Point 2	Consolidated Edison Co.	PWR	W	AP	3	0	Y	Y	Y	
Indian Point 3	Power Authority of the State of NY	PWR	W	AP	3	0	Y	Y	Y	

Table B.2: Reactors with EDG Information (cont'd.)

Plant Name	Utility Company	Type	Reactor Manuf.	EDG Manuf.	# of EDGs	# Swing	INEL	SwRI	NPRDS	Notes
Kewaunee 1	Wisconsin Public Service Corp.	PWR	W	EM	2	0	Y	Y	Y	
LaSalle 1	Commonwealth Edison Co.	BWR	GE	EM	1	1	Y	N	N	Commenced 1/84
LaSalle 2	Commonwealth Edison Co.	BWR	GE	EM	1	†	Y	N	N	Commenced 10/84
Limerick 1	Philadelphia Electric Co.	BWR	GE	FC	4	0	Y	N	N	Commenced 2/86
Limerick 2	Philadelphia Electric Co.	BWR	GE	FC	4	0	Y	N	N	Commenced 1/90
Maine Yankee	Maine Yankee Atomic Power Co.	PWR	CE	EM	2	0	Y	Y	Y	
McGuire 1	Duke Power Co.	PWR	W	NM	2	0	Y	Y	Y	
McGuire 2	Duke Power Co.	PWR	W	NM	2	0	Y	N	Y	Commenced 3/84
Millstone 1	Northeast Nuclear Energy Co.	BWR	GE	FC	1	0	Y	Y	N	
Millstone 2	Northeast Nuclear Energy Co.	PWR	CE	FC	2	0	Y	Y	Y	
Millstone 3	Northeast Nuclear Energy Co.	PWR	W	FC	2	0	Y	N	Y	Commenced 4/86
Monticello	Northern States Power Co.	BWR	GE	EM	2	0	Y	Y	N	
Nine Mile Point 1	Niagara Mohawk Power Corp.	BWR	GE	EM	2	0	Y	Y	N	
Nine Mile Point 2	Niagara Mohawk Power Corp.	BWR	GE	CB	2	0	Y	N	N	Commenced 3/88
North Anna 1	Virginia Electric & Power Co.	PWR	W	FC	2	0	Y	Y	Y	
North Anna 2	Virginia Electric & Power Co.	PWR	W	FC	2	0	Y	Y	Y	
Oconee 1	Duke Power Co.	BWR	B&W	‡	‡	‡	N	N	N	
Oconee 2	Duke Power Co.	BWR	B&W	‡	‡	‡	N	N	N	
Oconee 3	Duke Power Co.	BWR	B&W	‡	‡	‡	N	N	N	
Oyster Creek 1	GPU Nuclear Corp.	BWR	GE	EM	2	0	Y	Y	N	
Palisades	Consumers Power Co.	PWR	CE	AP	2	0	Y	Y	Y	
Palo Verde 1	Arizona Public Service Co.	PWR	CE	CB	2	0	Y	N	Y	Commenced 1/86

Table B.2: Reactors with EDG Information (cont'd.)

Plant Name	Utility Company	Type	Reactor Manuf.	EDG Manuf.	# of EDGs	# Swing	INEL	SwRI	NPRDS	Notes
Palo Verde 2	Arizona Public Service Co.	PWR	CE	CB	2	0	Y	N	Y	Commenced 9/86
Palo Verde 3	Arizona Public Service Co.	PWR	CE	CB	2	0	Y	N	Y	Commenced 1/88
Peach Bottom 2	PECO	BWR	GE	FC	0	4	Y	Y	N	
Peach Bottom 3	PECO	BWR	GE	FC	0	†	Y	Y	N	
Perry 1	Cleveland Electric Illuminating Co.	BWR	GE	TD	2	0	Y	N	N	Commenced 11/87
Pilgrim 1	Boston Edison Co.	BWR	GE	AP	2	0	Y	Y	N	
Point Beach 1	Wisconsin Electric Power Co.	PWR	W	EM	0	2	Y	Y	Y	
Point Beach 2	Wisconsin Electric Power Co.	PWR	W	EM	0	†	Y	Y	Y	
Prairie Island 1	Northern States Power Co.	PWR	W	FC	2	0	Y	Y	Y	
Prairie Island 2	Northern States Power Co.	PWR	W	CL	2	0	Y	Y	Y	
Quad Cities 1	Commonwealth Edison Co.	BWR	GE	EM	1	1	Y	Y	N	
Quad Cities 2	Commonwealth Edison Co.	BWR	GE	EM	1	†	Y	Y	N	
Rancho Seco 1	Sacramento Municipal Utilities District	PWR	B&W	EM	4	0	Y	Y	N	Shut Down 1989
River Bend 1	Entergy Operations, Inc.	BWR	GE	TD	2	0	Y	N	N	Commenced 6/86
Robinson 2	Carolina Power & Light Co.	PWR	W	FC	2	0	Y	Y	Y	
Salem 1	Public Service Electric & Gas Co.	PWR	W	AP	3	0	Y	Y	Y	
Salem 2	Public Service Electric & Gas Co.	PWR	W	AP	3	0	Y	Y	Y	
San Onofre 1	Southern California Edison Co.	PWR	W	TD	2	0	Y	Y	Y	Shut Down 1992
San Onofre 2	Southern California Edison Co.	PWR	CE	EM	2	0	Y	N	Y	Commenced 8/83
San Onofre 3	Southern California Edison Co.	PWR	CE	EM	2	0	Y	N	Y	Commenced 4/84
Seabrook 1	North Atlantic Energy Service Corp.	PWR	W	FC	2	0	Y	N	Y	Commenced 8/90
Sequoyah 1	Tennessee Valley Authority	PWR	W	EM	2	0	Y	Y	Y	
Sequoyah 2	Tennessee Valley Authority	PWR	W	EM	2	0	Y	Y	Y	
South Texas 1	Houston Lighting and Power Co.	PWR	W	CB	3	0	Y	N	Y	Commenced 8/88

Table B.2: Reactors with EDG Information (cont'd.)

Plant Name	Utility Company	Type	Reactor Manuf.	EDG Manuf.	# of EDGs	# Swing	INEL	SwRI	NPRDS	Notes
South Texas 2	Houston Lighting and Power Co.	PWR	W	CB	3	0	Y	N	Y	Commenced 6/89
St. Lucie 1	Florida Power & Light Co.	PWR	CE	EM	2	0	Y	Y	Y	
St. Lucie 2	Florida Power & Light Co.	PWR	CE	EM	2	0	Y	N	Y	Commenced 8/83
Summer 1	South Carolina Electric & Gas Co.	PWR	W	FC	2	0	Y	N	Y	Commenced 1/84
Surry 1	Virginia Electric & Power Co.	PWR	W	EM	1	1	Y	Y	Y	
Surry 2	Virginia Electric & Power Co.	PWR	W	EM	1	†	Y	Y	Y	
Susquehanna 1	Pennsylvania Power & Light Co.	BWR	GE	CB	0	5	Y	N	N	Commenced 6/83
Susquehanna 2	Pennsylvania Power & Light Co.	BWR	GE	CB	0	†	Y	N	N	Commenced 2/85
Three Mile Island 1	GPU Nuclear Co.	BWR	B&W	FC	2	0	Y	Y	N	
Trojan	Portland General Electric Co.	PWR	W	EM	2	0	Y	Y	Y	Shut Down 1992
Turkey Point 3	Florida Power & Light Co.	PWR	W	EM	2	0	Y	Y	Y	
Turkey Point 4	Florida Power & Light Co.	PWR	W	EM	2	0	Y	Y	Y	
Vermont Yankee	Vermont Yankee Nuclear Power Corp.	BWR	GE	FC	2	0	Y	Y	N	
Vogtle 1	Southern Nuclear Operating Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 6/87
Vogtle 2	Southern Nuclear Operating Co.	PWR	W	TD	2	0	Y	N	Y	Commenced 5/89
Wash. Nuclear 2	Wash. Public Power Supply System	BWR	GE	EM	2	0	Y	Y	N	
Waterford 3	Entergy Operations, Inc.	PWR	CE	CB	2	0	Y	N	Y	Commenced 9/85
Watts Bar 1	Tennessee Valley Authority	PWR	W	N/A	N/A	N/A	N	Y	Y	Commenced 1996
Wolf Creek 1	Wolf Creek Nuclear Operating Corp.	PWR	W	FC	2	0	Y	N	Y	Commenced 9/85
Yankee-Rowe 1	Yankee Atomic Electric Co.	PWR	W	EM	3	0	Y	Y	Y	Shut Down 1991
Zion 1	Commonwealth Edison Co.	PWR	W	CB	2	1	Y	Y	Y	
Zion 2	Commonwealth Edison Co.	PWR	W	CB	2	†	Y	Y	Y	

Table B.2: Reactors with EDG Information (cont'd.)