A RELIABILITY PROGRAM
FOR NUCLEAR POWER PLANT
EMERGENCY DIESEL GENERATORS

by

Kenneth J. Peters

Report submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

Systems Engineering

APPROVED:

B. S. Blanchard, Chairman

P. T. Kemmerling

K. L. Werner

August, 1990

Blacksburg, Virginia

c.2

LD
5655
V851
1990
P473
c.2

A RELIABILITY PROGRAM
FOR NUCLEAR POWER PLANT
EMERGENCY DIESEL GENERATORS

by

Kenneth J. Peters

Committee Chairman: B. S. Blanchard
Systems Engineering

(ABSTRACT)

This report demonstrates the use of MIL-STD-785B, Military Standard - Reliability Program for Systems and Equipment Development and Production. A reliability program is developed for nuclear power plant Emergency Diesel Generators in accordance with MIL-STD-785B requirements. The United States Nuclear Regulatory Commission has stated that a diesel generator reliability program is necessary to resolve outstanding safety issues. The plan proposed uses the Indian Point 3 Nuclear Power Plant Emergency Diesel Generator configuration for illustration purposes.

TABLE OF CONTENTS

List of Tables v

List of Figures vi

Chapter

1. INTRODUCTION 1

The Indian Point 3 Nuclear Power Plant 3

Objective 7

Identification of Need.....11

2. PROGRAM SURVEILLANCE AND CONTROL.....20

Reliability Program Plan 21

Control of Subcontractors and Suppliers.....39

Program Reviews.....41

Failure Reporting, Analysis, and Corrective Action System.....44

Failure Review Board.....54

3. DESIGN AND EVALUATION.....56

Reliability Modeling.....57

Reliability Allocation.....66

Reliability Predictions.....68

Failure Modes, Effects, and Criticality Analysis..74

Sneak Circuit Analysis.....88

Electronic Parts/Circuits Tolerance Analysis.....90

Parts Program.....92

Reliability Critical Items.....95

Life Criteria.....97

Table of Contents (Continued)

4. DEVELOPMENT AND PRODUCTION TESTING.....108

Environmental Stress Screening (ESS).....110

Reliability Development/Growth Test (RDGT) Program.....113

Reliability Qualification Test (RQT) Program.....115

Production Reliability Acceptance Test (PRAT) Program.....118

5. SUMMARY AND CONCLUSIONS.....120

WORKS CITED.....123

APPENDIX.....125

List of Abbreviations.....126

VITA.....127

LIST OF TABLES

Table

1. Identification of Reliability Program Tasks.....24
2. Reliability Design Review Checklist.....29
3. Past Diesel Generator Failures.....37
4. Past Diesel Problems at the Indian Point Site.....38
5. Data Used for Failure Rate Predictions.....70
6. Failure Modes, Effects, and Criticality Analysis.....76
7. Expert Recommended Diesel Surveillance.....100
8. Detailed Maintenance Plan for IP3 Diesel Generators.103

LIST OF FIGURES

Figure

1. Simplified Indian Point 3 Electrical Distribution Schematic.....4
2. Reliability Requirements in the System Life Cycle...10
3. Life Cycle Cost Commitment.....17
4. Milestone Chart for Reliability Tasks.....26
5. Diesel Reliability Program Chain of Command.....33
6. Vendor reliability Program Chain of Command.....34
7. Failure Analysis and Root Cause Determination.....45
8. Example of Failure Analysis.....47
9. Lube Oil System Reliability Block Diagram.....59
10. Fuel Oil System Reliability Block Diagram.....60
11. Jacket Water System Reliability Block Diagram.....62
12. Starting Air System Reliability Block Diagram.....64
13. Instrumentation and Control System Functions.....65
14. Diesel System Reliability Allocation.....67
15. Reliability Qualification Testing.....116

CHAPTER 1

INTRODUCTION

Most commercial nuclear power plants in the United States use Emergency Diesel Generator (EDG) units to supply alternating current (ac) power to safety related equipment if normal plant ac power is not available. Normal plant ac power generally comes from the offsite utility distribution network, or from the plant's main generator. As the backup ac power source, EDGs must be highly reliable. A "station blackout" (SBO) would occur if there were no ac power available to operate the plant's equipment. Diesel reliability is a U.S. Nuclear Regulatory Commission (NRC) "Generic Safety Issue" which plays a large part in the NRC resolution of the SBO issue.

To support the resolution of Generic Safety Issue B-56, "Diesel Reliability," the NRC has established the need for an Emergency Diesel Generator reliability program. The NRC's position is "the reliable operation of onsite emergency ac power sources should be ensured by a reliability program designed to maintain and monitor the reliability level of each power source over time for assurance that selected reliability levels are being achieved." [1] The program the NRC desires is an ongoing reliability assessment to determine system weaknesses and take corrective actions. This program would be aimed at the Emergency Diesels already in operation at the United States'

one hundred and eight operating nuclear plants. [2] The program desired by the NRC does not seem to recognize that reliability is an inherent design characteristic. A true reliability program is one that begins at the beginning of a system's development, with the identification of a need for a system. This is not meant to imply that changes in operating and maintenance practices, or system modifications, can not enhance system performance and reliability; they can. However, the optimum time (and most cost effective) to incorporate system reliability requirements into any system or program is at the beginning of system development. The program described herein is a reliability program that begins with the identification of a need, and provides reliability requirements and tasks for each phase of system development. This reliability program is based on the requirements of MIL-STD-785B, "Military Standard - Reliability Program for Systems and Equipment Development and Production."

The Indian Point 3 Nuclear Power Plant

The Indian Point 3 Nuclear Power Plant (IP3) is owned and operated by the New York Power Authority (NYPA). NYPA is a state agency, founded in 1931 to assure that the hydroelectric resources of the St. Lawrence River were utilized for the benefit of the entire State of New York. NYPA also owns and operates the James A. Fitzpatrick (JAF) Nuclear Power Plant near Oswego, New York, adjacent to Lake Ontario.

The Indian Point site is on the east bank of the Hudson River, in Buchanan, New York, twenty four miles north of New York City. Indian Point contains three nuclear plants. Indian Point units 1 (no longer active) and 2 are owned and operated by Consolidated Edison (Con Ed). Indian Point 3 is a 965 megawatt pressurized water reactor power plant. IP3 was acquired by NYPA from Con Ed on December 31, 1975, and began commercial operation in August of 1976.

During normal plant operation at IP3, ac power is supplied to the plant's equipment through the unit auxiliary transformer. Standby power can be supplied from the Buchanan substation, by way of various lines, to the station auxiliary transformer. There are also standby gas turbine generators connected to various points of the power distribution system. Figure 1 shows a simplified schematic of the IP3 electrical distribution system.

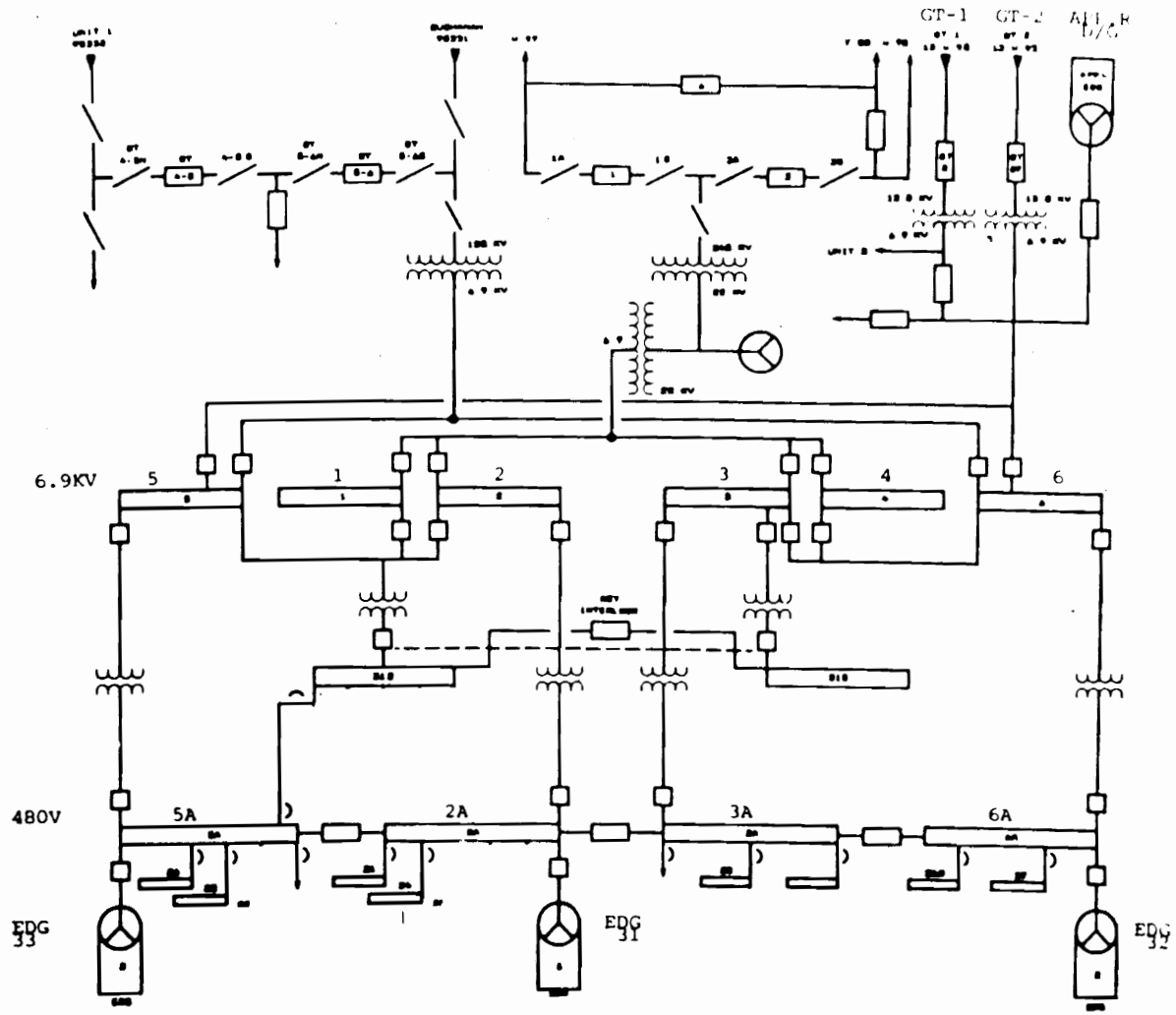


Figure 1. Simplified Indian Point 3 Electrical Distribution Schematic

If all of the standby sources of power should fail, IP3 has three emergency diesel generator sets as sources of onsite emergency power. The Emergency Diesels provide a reliable source of backup power to essential 480V bus equipment. This essential equipment includes that required for safe reactor shutdown following a loss of normal ac power and the safeguards equipment required to limit the consequences of a loss-of-coolant accident. Any two of the three Emergency Diesels are capable of allowing the plant to be controlled under the worst possible accident conditions.

Each EDG set consists of an Alco engine coupled to a Westinghouse 900 rpm, 3 phase, 60 cycle, 480 volt generator. [3] The diesels are rated at 1750 kw. [4] The diesels are located in a heated, tornado-proof, reinforced concrete building adjacent to the plant control building. There are internal walls in the diesel building to separate the three EDGs and associated circuitry from each other for fire protection.

There is an additional diesel generator onsite that consists of an Alco engine coupled to a Kato 900 rpm, 3 phase, 60 cycle, 6900 volt generator. [5] This generator was added to the site to respond to the NRC fire protection rule (10 CFR 50, Appendix R). This generator is not classified as an Emergency Diesel Generator, but would be used as an alternate ac power source in the event of a Station Blackout.

The following systems are EDG support systems:

- o Lube oil system
- o Diesel fuel oil system
- o Jacket water cooling system
- o Diesel engine starting air system
- o Instrumentation and control systems

Each EDG is automatically started by either one of two redundant air motors. Each unit has its own air receiver, with sufficient air for four starts. The diesels are equipped with water jacket and lube oil heating, and a pre-lube pump to circulate oil when the unit is not running.

Fuel oil for each EDG is stored in a 7700 gallon underground tank. In addition, each diesel has its own small fuel storage (day) tank that feeds the fuel oil pump on the engine. Each day tank is automatically filled from an underground tank when the volume reaches a predetermined level.

Each EDG is started upon: (1) initiation of safety injection operation, or (2) an undervoltage condition on its associated bus. On a bus undervoltage signal, the EDG starts, the normal bus power supply breakers open, the EDG output breaker closes, and critical reactor plant components such as auxiliary feedwater, service water, and component cooling pumps are reenergized. Each unit can be started within ten seconds and fully loaded within sixty seconds.

Objective

The objective of this report is to describe a reliability program for nuclear power plant Emergency Diesel Generators. The NRC has determined that such a program is required, in order to minimize the probability of a nuclear plant experiencing a loss of all sources of ac power. As is generally the case in the U.S. nuclear power industry, new regulatory positions and requirements are being placed on systems already in operation. However, reliability is an inherent design characteristic, and is one of the design-related specialties that must be integrated properly into the overall Systems Engineering process for system development. Systems Engineering has been defined as:

> The application of scientific and engineering efforts to (1) transform an operational need into a description of system performance parameters and a preferred system configuration through the use of an iterative process of functional analysis, synthesis, optimization, definition, design, test and evaluation; (2) integrate related technical parameters and assure capability of all physical, functional, and program interfaces in a manner that optimizes the total system definition and design; and (3) integrate reliability, maintainability, logistic support, safety, producibility, security, survivability, structural integrity, human factors, and other related specialties into the total engineering effort. [6]

This report assumes that a new nuclear power plant is being built, and the power plant construction includes the installation of an emergency diesel generator system. The reliability program developed will follow the guidelines

of MIL-STD-785B, Military Standard - Reliability Program for Systems and Equipment Development and Production, not the program format described by the NRC. The reliability program described in this report applies to each phase of the diesel system life cycle, particularly the design phases; the NRC program describes efforts that are to start in the system utilization phase. The reliability tasks of MIL-STD-785B are described in the report. These tasks are applicable to a new system undergoing development. However, the examples used to illustrate the tasks of MIL-STD-785B are based on the system configuration of IP3, a power plant that is already in operation. The calculations used to illustrate tasks like reliability prediction are based on a compilation of data reported to the NRC by a number of utilities.

MIL-STD-785B provides general requirements and specific tasks for reliability programs during equipment development, production, and initial deployment. The intent of MIL-STD-785B is to "(1) improve operational readiness and mission success of the major end-item; (2) reduce item demand for maintenance manpower and logistic support; (3) provide essential management information; and (4) hold down its own impact on overall program cost and schedule." [7]

The reliability program tasks identified by MIL-STD-785B are divided into three sections: Section 100, Program Surveillance and Control; Section 200, Design and

Evaluation; and Section 300, Development and Production Testing. Within these three sections are 18 separate tasks, numbered 101 through 304. These subtasks are used to tailor reliability requirements in the most cost effective manner that meets established program objectives. It is important to coordinate task requirements with other engineering groups, such as Logistic Support and System Safety, to minimize task duplication. [8]

Although the numbering of the tasks by MIL-STD-785B is the general progression of reliability program tasks, this order may be changed, and not all tasks delineated by MIL-STD-785B will be necessary for each specific application. Figure 2 presents reliability requirements as they apply to the various phases of a system life cycle. Figure 2 shows that the application of reliability efforts, like Systems Engineering efforts in general, is very iterative in nature.

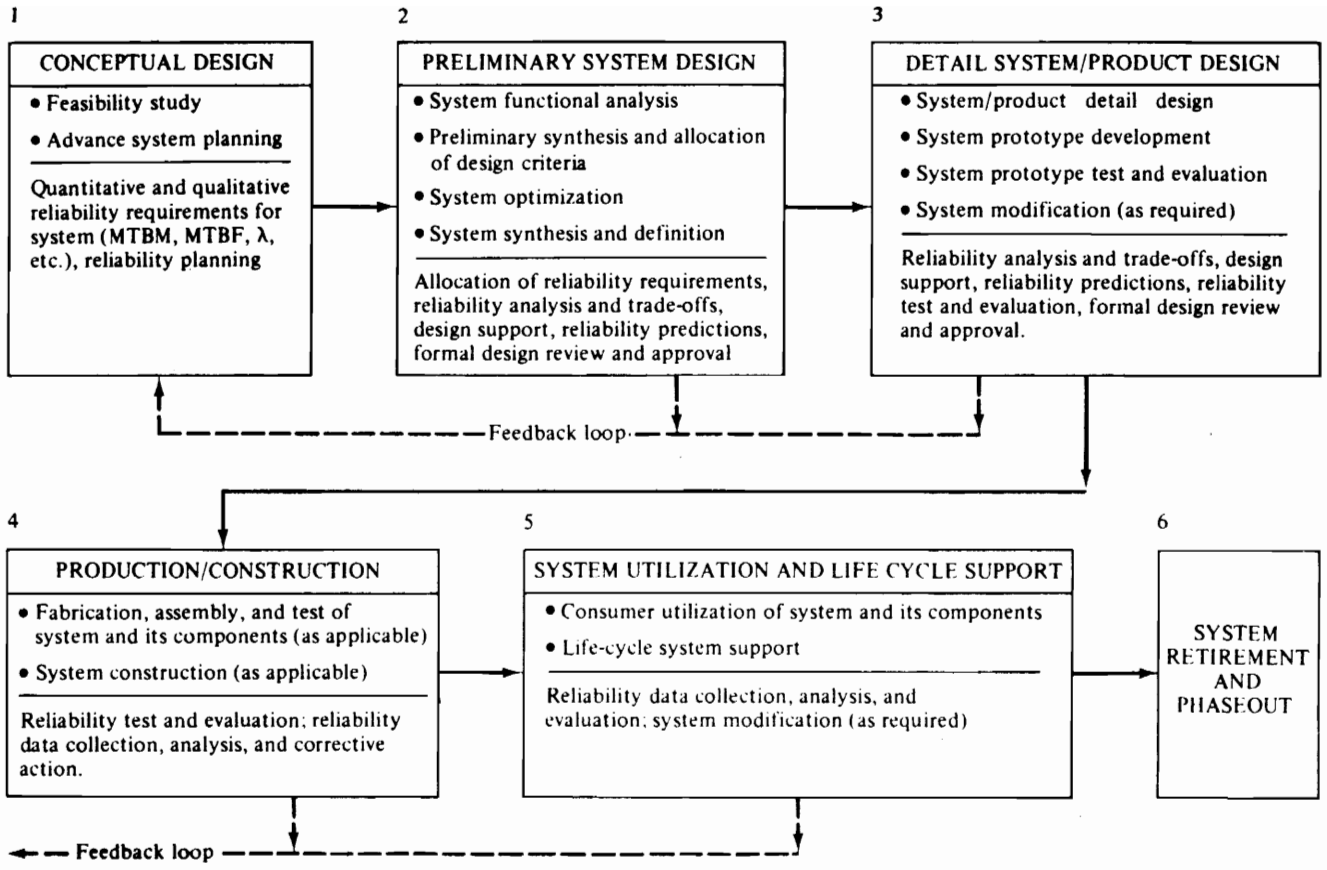


Figure 2. Reliability Requirements in the System Life Cycle

Source: Blanchard, Benjamin S., and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981, p. 325.

Identification of Need

The need for a diesel reliability program is the NRC mandate that a diesel reliability program is required. The NRC's purpose in requiring an EDG reliability program is to minimize the probability of nuclear plants experiencing a loss of all ac power. The following are the principle elements of the reliability program, as the NRC envisions the program. The elements, and the information describing each element of the program, are taken from U.S. NRC Regulatory Guide 1.9, proposed revision 3 (dated November, 1988).

Diesel generator reliability

An operational assessment of diesel generator reliability would be calculated as follows:

R = (start reliability) x (load-run reliability)

Start reliability is defined as the number of successful starts divided by the number of valid start demands. Load-run reliability is defined as the number of successful load-runs divided by the number of valid demands to load. This calculation would be performed for a period of about two years or less. This is not the definition of reliability that the program described starting in Chapter 2 uses. When the program described in Chapter 2 and following

uses the term reliability (R), this means $R = e^{-\lambda t}$ is calculated for a period of 154,800 hours, λ is the failure rate, and t is the time. In this case, R is the probability that the system will operate without a failure for the specified time (154,800 hours).

Analysis of surveillance needs

The NRC defines surveillance as all failure detection, in-plant reliability information gathering, and condition monitoring activities. The surveillance strategy for the diesels should be the result of analysis of the surveillance needs. The surveillance plan should define the parameters to be monitored, the types of surveillance to be employed, and the intervals for each type of surveillance.

Performance monitoring

A diesel generator reliability program should specify how to monitor diesel generator performance over time, using trending of operational and surveillance data. Performance monitoring should include both condition monitoring and reliability monitoring. Condition monitoring would entail tracking such data as lube oil pressure or water jacket outlet temperature. Reliability monitoring would include tracking of data such as failure modes, repair frequency, and repair times.

Maintenance program

The maintenance policy is needed for a satisfactory preventive maintenance program, an acceptable spare parts inventory, and input of necessary data into review functions such as failure analysis. Preventive maintenance should serve to reduce the number of catastrophic failures and reduce the long-term degradation of equipment caused by aging. One approach to maintenance would be a reliability centered maintenance (RCM) approach, where the maintenance performed is based on the outcome of a Failure Modes, Effects, and Criticality Analysis.

Failure analysis and root cause investigation

The diesel generator reliability program should contain a structured approach to reduce problems to correctable causes. A root cause investigation should be very methodical, to ensure the determination of a root cause which may be several layers below the visible symptoms.

Formal problem closeout

A formal problem closeout procedure is intended to ensure that effective solutions to detected problems are devised and implemented in a timely manner. The solution should correct the reliability problem without creating any

new reliability problems. The problem closeout procedure should provide for any additional monitoring activities deemed necessary.

Data collection and utilization

The reliability program should have a data gathering, storage, and retrieval system which can support all of the reliability program tasks. The data should support the assessment of the reliability programs goals and targets.

Responsibilities and management controls

The reliability program should have clear line responsibilities and management controls which identify the individual responsible for implementation and operation of the diesel generator reliability program. The implementation and operation of the reliability program should enjoy the full support of plant management.

The requirement for a diesel generator reliability program has been determined by the NRC to be a necessary part of the resolution to the issue of Station Blackout, to minimize the probability of a Station Blackout event. A Regulatory Guide (Reg. Guide) is not a regulation or rule in and of itself. It is an NRC staff accepted method for

meeting regulatory requirements. The reliability program described herein does not follow the format of Reg. Guide 1.9, but describes a different approach to an EDG reliability program. The prime objective of this report is to demonstrate the applicability of MIL-STD-785B to nuclear power plant Emergency Diesel Generators, assuming the EDG system is a new system. In order to adequately design and plan for system reliability, a reliability program similar to this must be developed for a new system or equipment, starting at the beginning of the system life cycle. This program would be one small part of the overall systems engineering process for the development of a new nuclear power plant.

At the top level of a determination to build a new nuclear power plant is a statement of need and a feasibility analysis. At the very top level of this project, the need would be a utility's need for more generating capacity. A feasibility study would include a look at all alternatives, including oil and gas fired plants, hydroelectric plants, and nuclear plants, as well as purchasing power from some other generator. Fundamental to the decision as to the type of plant to construct (or power to purchase), as it is to all aspects of systems engineering, is the life-cycle cost approach. Life-cycle cost can be thought of as "...all costs associated with the system or product as applied to the defined life cycle." [9] It is imperative that

life-cycle cost is emphasized early in the process of system development because a major portion of life-cycle costs are determined by decisions made early in system planning and design (see figure 3). While it does not seem likely given the current political atmosphere, assume that the decision is to construct a nuclear power plant. Nuclear power may be a viable option in the future, due to the need for increased generating capacity, and growing environmental concerns regarding coal-fired plants.

The next defined need, relative to electrical system design, would be the need for the power plant overall electrical system design, including allocation of reliability to various electrical distribution subsystems. Next would come the need for emergency ac power sources, which could be: emergency diesel generators, batteries with motor-generator sets, gas turbine generators, or any other type of standby power supply conceivable. Again, life-cycle cost should play a very large part in the decision-making process. The previous discussion points out the iterative nature of systems engineering efforts. For the purpose of the remainder of this report, it is assumed that diesel generators are chosen as the preferred emergency ac power source.

The primary missions of the emergency diesel generator system are to (1) provide ac power promptly to engineered

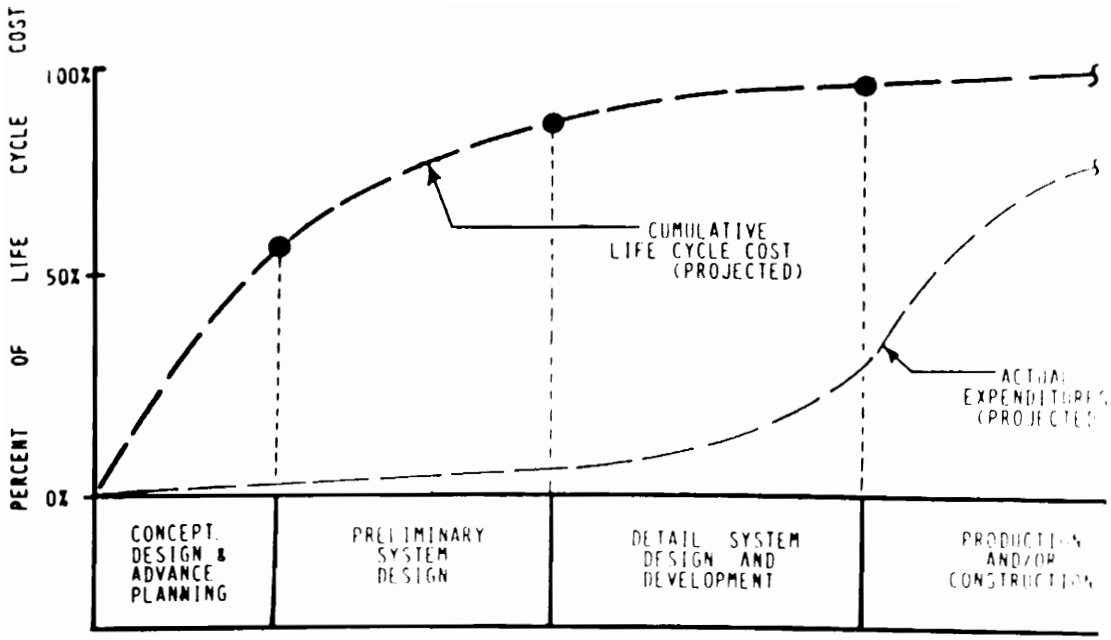


Figure 3. Life Cycle Cost Commitment

Source: ENGR 5980, Virginia Tech, class notes.

safety features should a loss of offsite power and an accident occur simultaneously, (2) supply power continuously to the equipment needed to maintain the plant in a safe condition if an extended loss of offsite power occurs, and (3) be capable of starting and accelerating a number of large motor loads in rapid succession while sustaining the loss of all or any part of such loads and maintaining voltage and frequency within acceptable limits. [10]

The following requirements come from the General Design Criteria of Title 10 of the Code of Federal Regulations, Part 50, Appendix A. Diesel Generators (DG's) should supply 480 volt, 3 phase, 60 cycle ac power to the required buses. The particular configuration specified (1 of 2, 1 of 3, etc.) should be rated for at least 4000 kw. The DG's should be capable of automatically starting and assuming full voltage and speed within ten seconds, and be fully loaded within sixty seconds. The majority of the loads will be large motors, so the DG's should have a maximum voltage reduction of 25%, and a maximum frequency reduction of 5%, when starting such motors. The DG's should be designed to be testable with the reactor plant in operation, such that an actual system demand is accurately simulated. DG instrumentation should be readily accessible and capable of being calibrated in place. All parameters monitored (voltage, frequency, operational status) and all alarm conditions (such as overspeed) shall have remote indications

in the central control room.

The reliability program that follows is based on the requirements of MIL-STD-785B. Descriptions of the diesel systems are based on the configuration of the Indian Point 3 Nuclear Power Plant. Procedures and staff structures described in the report are also based on those of IP3. Calculations used to illustrate tasks, such as the reliability predictions, are based on a compilation of data reported to the NRC by a number of utilities.

CHAPTER 2

PROGRAM SURVEILLANCE AND CONTROL

Task section 100 of MIL-STD-785B, "Program Surveillance and Control," identifies and quantifies the reliability requirements of the system. The reliability requirements must be established very early in the system acquisition process so that they may be included in the "Request for Proposal."

In determining reliability requirements it is essential to assemble mission and performance requirements (specified at the subsystem level), anticipated environments, mission reliability, and basic reliability requirements. [11] Once the system reliability has been established, this requirement is allocated among the subsystems and components. This allocation is performed using reliability block diagrams. Block diagrams are developed for each system function, and failure rates are estimated for each block; these failure rates become design goals. Failure rates can be derived from many sources, including actual experience with similar items, reliability predictions for similar items, or engineering estimates. A reliability model is developed that yields a mathematical expression for reliability of a small part of the proposed system configuration.

Reliability Program Plan

Task 101

The purpose of task 101 is to develop a reliability program plan which identifies, and ties together, all program management tasks required to accomplish program requirements. [12] The reliability program plan is a basic tool for the utility purchasing the diesel generators to manage an effective reliability program and ensure that the diesel vendor properly executes the reliability tasks required, and focuses appropriate attention on the area of system reliability.

To begin the process of developing the reliability program plan, there is a large amount of information that must go into the "Request for Proposal" in order to ensure that the vendor chosen can perform an adequate job. The five vendors with the most U.S. nuclear plant EDG experience are Alco, Cooper-Bessemer, General Motors (Electromotive Division), Colt (Fairbanks Morse Division), and Nordberg.

The diesel systems must satisfy the General Design Criteria of 10 CFR Part 50 mentioned earlier. Each individual diesel is to be designed for a mean time between failure (MTBF) of no less than 27,374 hours. The projected lifetime of the diesel system is 30 years. The diesels will be available in a standby mode approximately 215 days per year (based on a 60% capacity factor), 24 hours per day.

Reliability (R) is the probability that the diesel will operate in the intended manner and environment, with no failures for a given time period. The period, 154,800 hours, is determined by multiplication (30 yrs. x 24 hrs. x 215 days). The required MTBF is determined using the equation $R = e^{-\lambda t}$, and the fact that the MTBF equals $1/\lambda$. The MTBF of 27,374 hours (over a time period of 154,800 hours) is the standard to which the diesel system shall be designed. The diesel system shall have a mean time to repair of eight hours or less, and possess an inherent availability of at least 0.995.

Once the diesels are operational, they will normally be manually started monthly to ensure operability. Every 18 months the automatic start capability will be tested by simulating a loss of bus voltage signal. Maintenance of the diesels will include normal testing, weekly system visual inspections, and fuel, water, and oil sampling. The organizational level (onsite) maintenance will be performed by the utility maintenance department. The diesel system shall be repairable by personnel with an intermediate skill level. The diesel system should have extensive alarm and indicating features, to give the operators as much information as possible regarding system operation. Electrical equipment should use modular construction where possible. Mechanical components should use wrenchless fasteners where possible, or require standard size wrenches.

Self-test features should allow quick isolation and replacement of electrical components. Onsite maintenance will consist of testing, preventive maintenance, and corrective maintenance that does not require elaborate equipment.

Intermediate level maintenance will be performed in the machine shop. These tasks will be larger than the onsite maintenance tasks, such as replacement of individual module components. Depot level maintenance will be performed by the diesel generator vendor, and be limited to large scope jobs such as governor rebuilding, or rebuilding of the turbocharger or engine itself.

One of the most important aspects of the reliability program is the description of each specific task that will be required. The specific tasks are listed according to the phases of the system life cycle, so that it becomes evident how the reliability program fits into the total system design, construction, and utilization effort. In addition to showing how reliability tasks will be allocated to each phase of system development, the identification of reliability tasks will be the basis for determination of whether or not the vendor has complied with the terms of the contract, and scheduled milestones. Table 1 identifies the tasks required as part of the reliability program for the EDG's. Figure 4 is a milestone chart that lists all the tasks required and the schedule for completing them.

Table 1

Identification of Reliability Program Tasks

A. Conceptual Phase

A1. UTILITY: Perform needs and feasibility analyses
A2. UTILITY: Define system operational requirements
A3. UTILITY: Define system reliability requirements
A4. UTILITY: Evaluate conceptual designs. Select preferred configuration/vendor
A5. VENDOR: Establish reliability organization. Plan for reliability. Establish failure review board.
A6. UTILITY/VENDOR: Conduct formal conceptual design review.
A7. UTILITY/VENDOR: Begin to plan system testing. Test components.
A8. VENDOR: Perform failure modes, effects, and criticality analysis. Task 204.

B. Preliminary System Design Phase

B1. VENDOR: Develop reliability model. Task 201.
B2. VENDOR: Perform reliability allocation. Task 202.
B3. VENDOR: Perform reliability predictions. Task 203.
B4. VENDOR: Perform sneak circuit analysis. Task 205.
B5. UTILITY/VENDOR: Conduct preliminary design review.

C. Detail Design Phase

C1. VENDOR: Perform reliability analysis and trade-offs. Identify critical items. Task 208.
C2. VENDOR: Perform circuit tolerance analyses. Task 206.
C3. VENDOR: Construct prototype unit.
C4. VENDOR: Perform environmental stress screening of prototype. Task 301.
C5. VENDOR: Perform reliability development, growth and qualification testing of prototype. Tasks 302 and 303.
C6. UTILITY/VENDOR: Conduct detail design review.

Table 1 (Continued)

D. Production and Construction Phase

D1. VENDOR/SUBCONTRACTORS: Produce the diesel system.
D2. UTILITY: Perform installation inspections. Conduct test readiness review (with vendor).
D3. UTILITY/VENDOR: Conduct reliability acceptance test program. Task 304.
D4. UTILITY: Collect reliability data. Review test data for approval.
D5. VENDOR/SUBCONTRACTORS: Modify system as required.

E. Utilization Phase

E1. UTILITY: Operate the diesel systems.
E2. UTILITY: Maintain the diesel system. Install any required modifications (with vendor help as necessary).
E3. UTILITY: Collect reliability data.

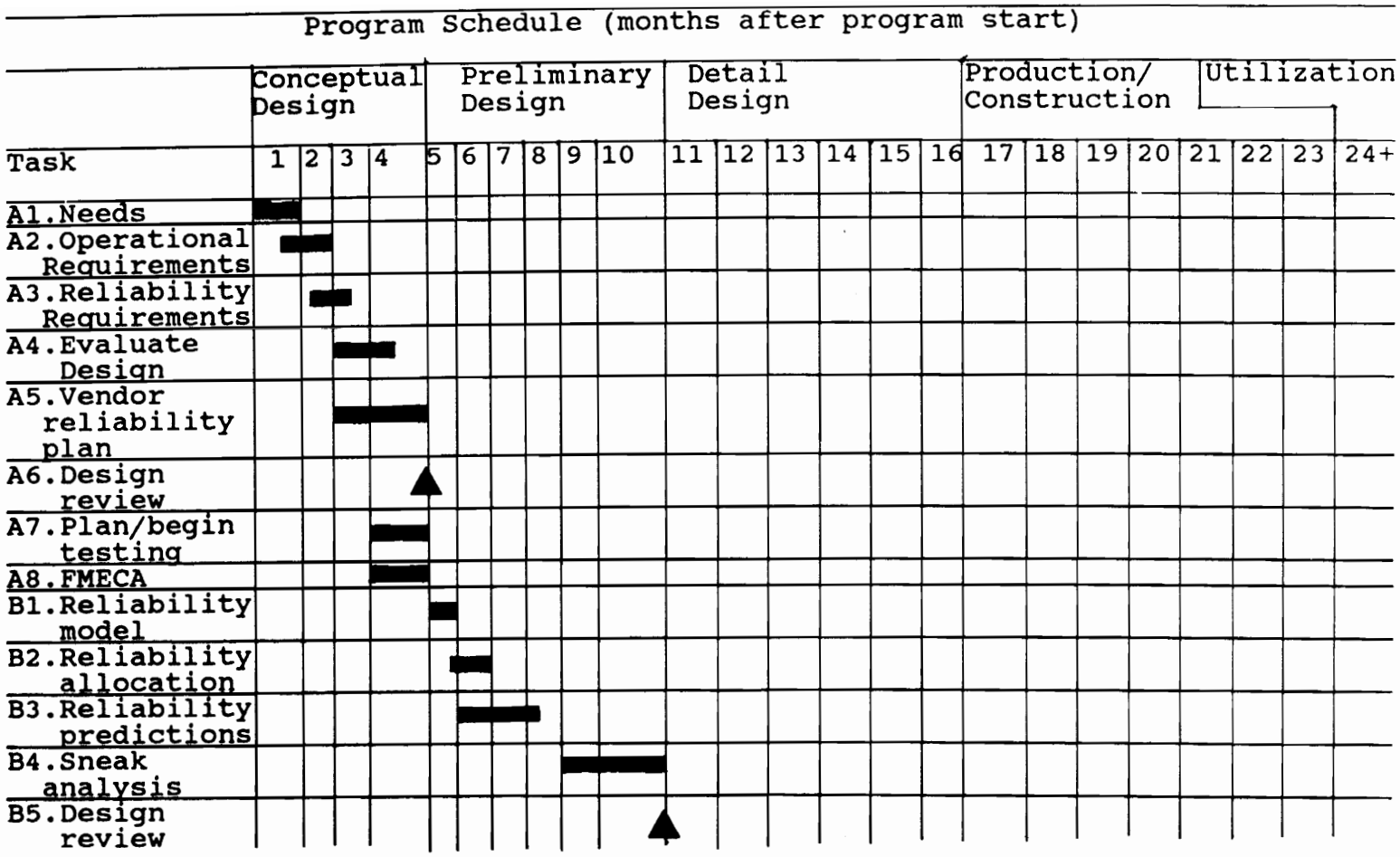


Figure 4. Milestone Chart for Reliability Tasks

Program Schedule (months after program start)

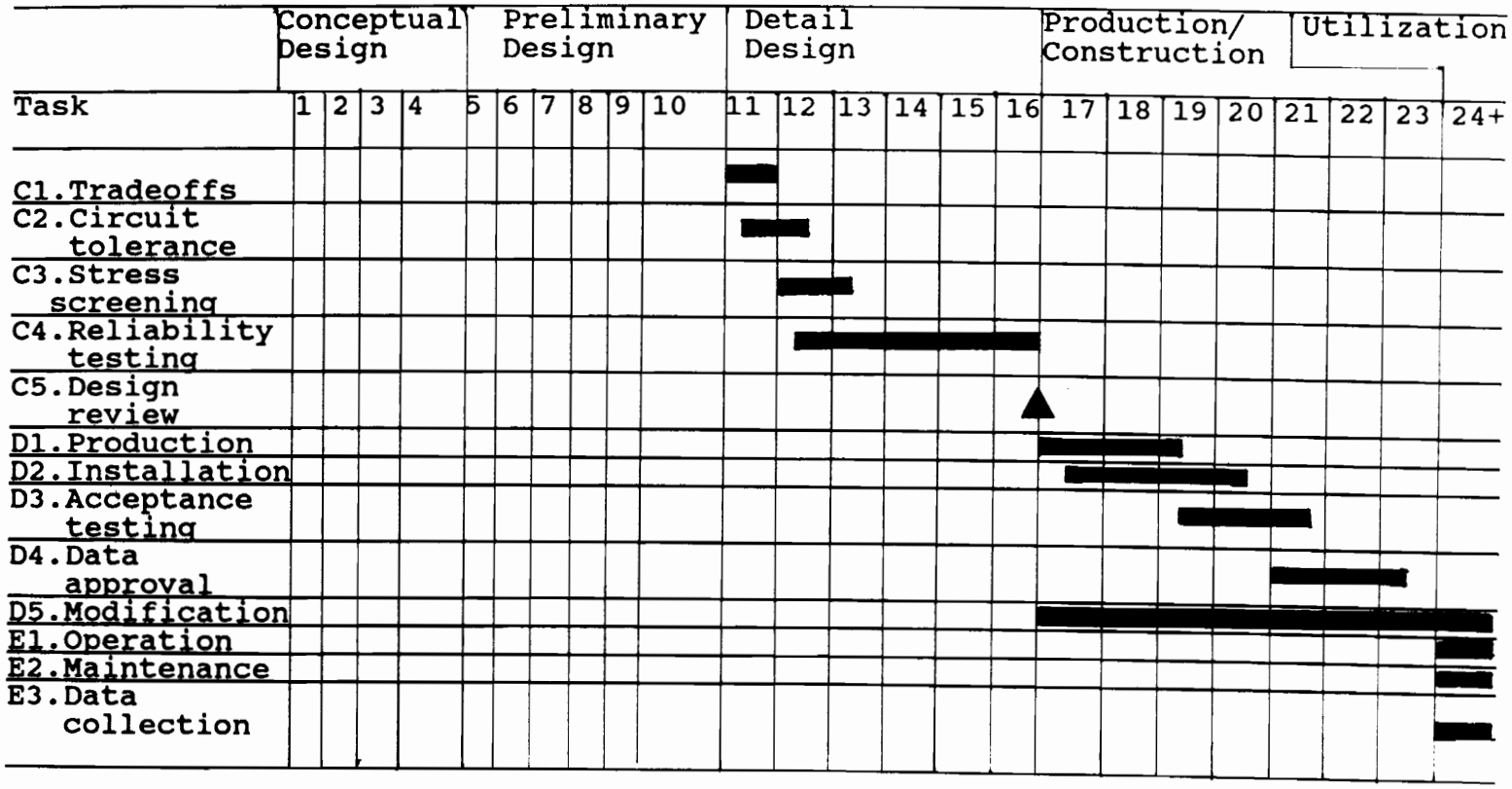


Figure 4 (Continued)

The identification of reliability program tasks and the milestone chart show design reviews at the end of the conceptual, preliminary, and detail design phases of project development. At each of these design reviews the design for reliability to date must be examined. At each design review the diesel system must be evaluated in terms of compliance with the initially specified diesel system reliability requirements. The design will be approved as is if the requirements appear to be fulfilled. Appropriate corrective actions will be instituted if the requirements are not fulfilled. To support the reliability design reviews, a checklist will be used that will include the items of Table 2. The questions asked by Table 2 do not cover all the questions pertinent to the reliability design, but they cover most of the major points necessary to assure the utility that the diesel reliability program is proceeding properly.

Another of the elements necessary for the reliability program plan is to specify the chain of command for the utility's diesel reliability program (and have the vendor specify their chain of command). The utility representative with the overall responsibility for the reliability program is the Diesel Generator System Engineer. This engineer will be the utility's liaison with the diesel generator vendor and all subcontractors. He or she will play an active role in all decisions made in each phase of the system life

Table 2

Reliability Design Review Checklist

1. Have reliability requirements (quantitative and qualitative) for the diesel generators been adequately specified?
2. Are the diesel reliability requirements compatible with other system requirements?
3. Has the diesel system design complexity been minimized?
4. Have failure modes and effects been identified?
5. Are item failure rates known?
6. Have parts with excessive failure rates been identified?
7. Has the diesel system mean life been determined?
8. Have derating factors been used where appropriate?
9. Is protection against secondary failures (resulting from primary failures) incorporated?
10. Has the use of adjustable components been minimized to the maximum extent practicable?
11. Have all critical-useful-life items been eliminated from the diesel system design?
12. Has cooling been incorporated for "hot-spots?"
13. Have all hazardous conditions been eliminated?
14. Have all reliability program requirements been met?

Source: Blanchard, Benjamin S., and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981, p. 357.

cycle. All questions from the vendor regarding the reliability program will be referred to the Diesel Generator System Engineer. Each vendor involved in the diesel system development will have one individual specified with primary responsibility for diesel reliability. These individuals will coordinate their efforts to ensure the overall reliability goal is met.

Once the diesel system reaches the post-installation test phase, the Diesel Generator System Engineer will be responsible for the compilation of all of the DG performance and maintenance data. This person will be part of the Plant Performance and Reliability group, and will be able to access the diesel data in the computer system for manipulation (the data will be accessible company wide for review). The DG system engineer will be responsible for the monthly review of all diesel data for trend analysis. The DG system engineer will be responsible for the preparation of diesel performance quarterly reports, which will be sent to all the department heads. This person will determine all required maintenance, and perform all diesel systems root cause analysis. Overall, this person is responsible for all aspects of the diesel reliability program, aside from the actual performance of operations and maintenance.

The plant maintenance staff will perform all maintenance (preventive and corrective) on the diesels, as well as local testing. Starting of the diesels from the

control room is a function of the Reactor Operators. The maintenance department may call the vendor for assistance, as needed, in performing corrective maintenance.

The plant Operational Experience Review Group and the DG system engineer will be responsible for root cause analysis, as well as for determination of appropriate re-testing and corrective action verification.

The plant Maintenance Superintendent is responsible for all maintenance department actions associated with the diesels and associated subsystems. The maintenance personnel chosen for diesel system maintenance are the Maintenance Superintendent's responsibility (which may be delegated to appropriate supervisors). The Maintenance Superintendent is responsible for ensuring that appropriate maintenance personnel receive adequate diesel system training, including periodic refresher training. It is also the Maintenance Superintendent's responsibility to ensure that information regarding problems and lessons learned (both internal and from other utilities) is routed to all maintenance personnel involved with the diesels.

The Technical Services Superintendent (TSS) is responsible for the proper functioning of the Diesel reliability program. The TSS is responsible to assure, and report to the Resident Manager, that the reliability program is adhered to, and that diesel reliability remains high. The TSS bears the primary responsibility for review of

the quarterly DG performance reports, as well as periodic reviews of all reliability program records. Any changes in the diesel reliability program require the Plant Operating Review Committee's concurrence, through the TSS. The Superintendent is also responsible for ensuring that all plant operators, Operations and Maintenance Supervisors, and affected technicians receive training regarding the implementation of the reliability program. During the design and testing phases of the project, the TSS will bear the primary responsibility for how the diesel program interfaces with other plant engineering and construction activities. The TSS will resolve any conflicts between diesel reliability and other engineering concerns, with input from the vendors, and with the concurrence of the Plant Manager.

The Quality Assurance department is required to verify the correctness of all maintenance actions. The Quality Assurance department will provide an independent audit and assessment of the diesel generator reliability program. The Quality assurance department will provide input regarding the program to the Vice President of Appraisal and Compliance.

The overall utility reporting arrangement for the diesel reliability program is shown in Figure 5. The vendor's chain of command is shown in Figure 6.

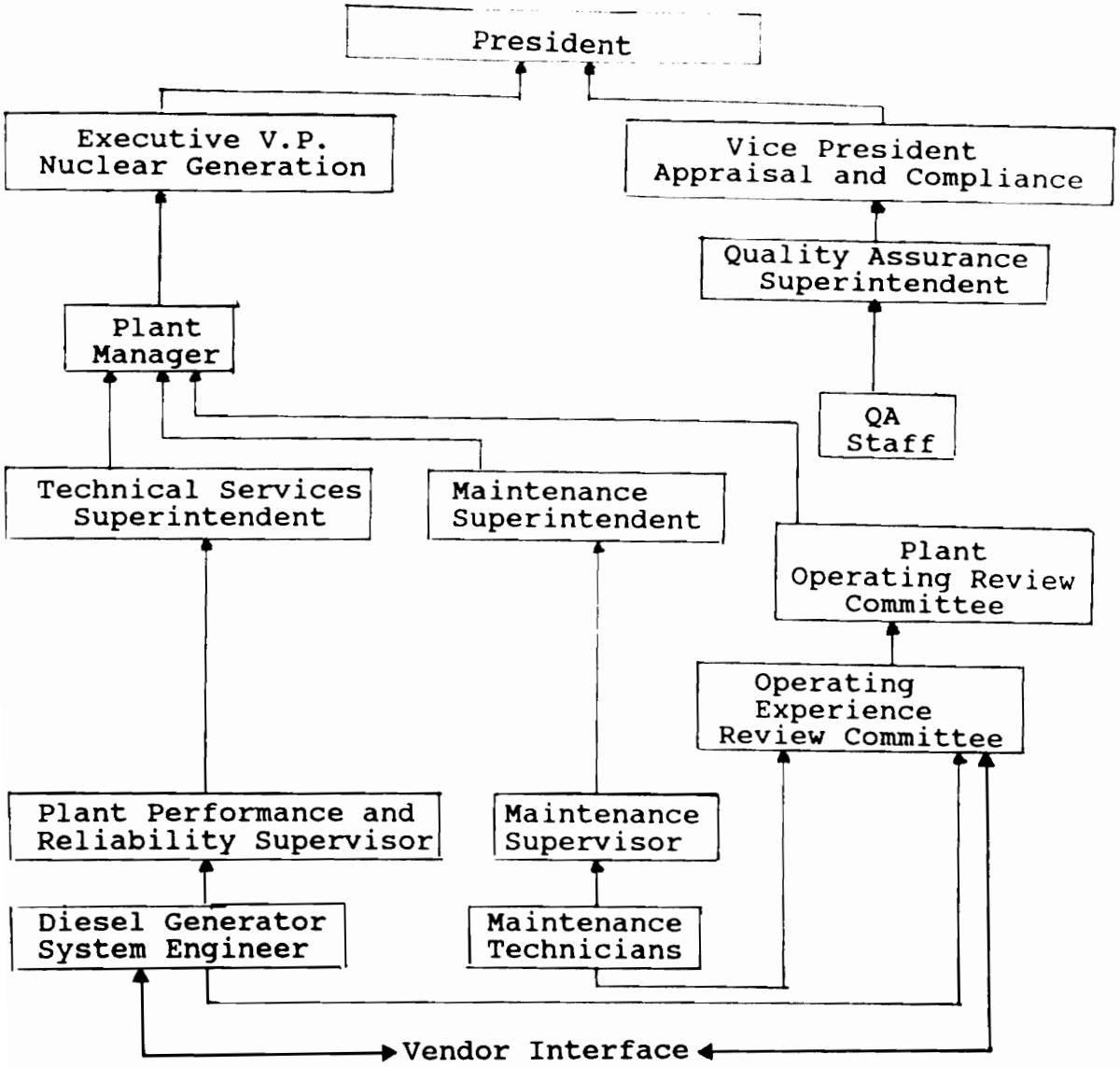


Figure 5. Diesel Reliability Program Chain of Command

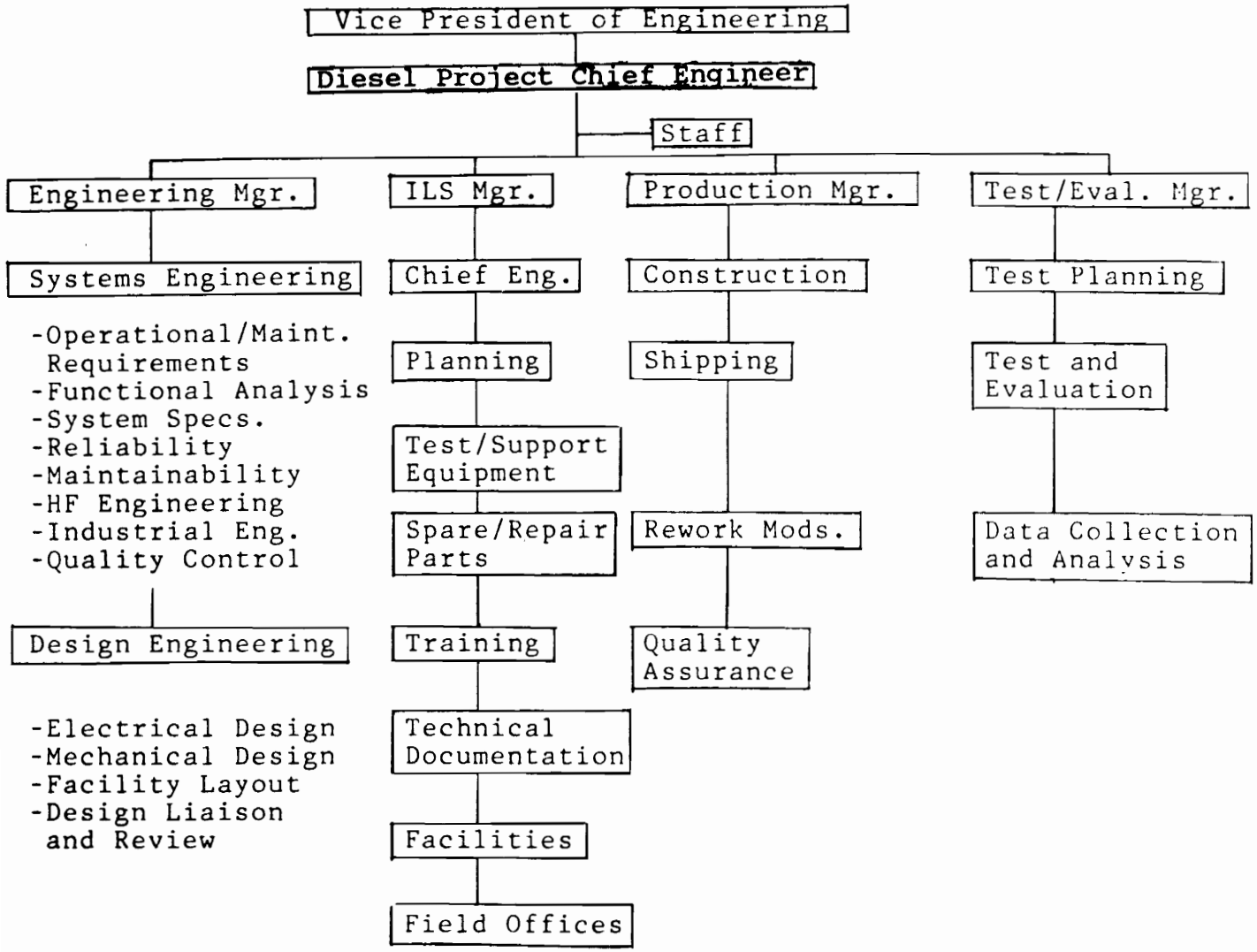


Figure 6. Vendor Reliability Program Chain of Command

The final area covered by the reliability program plan is the identification of known reliability problems. Past nuclear power plant EDG problems should be reviewed. This review would include both generic EDG problems and problems that affect only the chosen diesel vendor.

The first problem area of a generic type is diesel generator governors. Governors are a problem with all diesel vendors, because there is only one company that manufactures the governors (Woodward). Many governor problems are due to the sensitive nature of the governor adjustments, and through the introduction of air into the governor oil. The diesel vendor selected for the project will need to assure the utility that the Woodward Company has an adequate reliability program and has taken steps to correct past governor problems. Many governor problems of the past have been due to operator errors. The contract with the vendor will include a complete governor training program (including hands-on experience) for six of the utility's maintenance technicians.

Another generic area of concern is instrumentation and control system failures. Most of these failures have been due to circuit breaker and relay failures. Many of these failures have been due to poor manufacturing and construction practices. The vendor will be required to show that their reliability program addresses this area.

The next step for problem identification is to review the component failure histories of the specific diesel vendors. Table 3 shows the top five failed components for each of the five current vendors. This shows where the vendors reliability program's emphasis should be. This will also show whether or not the vendor has actively sought to correct past problems. At the time of contract award, it will be beneficial to take this problem examination one step further. Past problems should be reviewed for a representative number of power plants using the specific vendor's diesels. The vendor will be required to show documentation that past problem causes have been corrected. Table 4 shows this type of problem listing for the Indian Point site (Alco diesel generators).

Table 3

Past Diesel Generator Failures

Component	Number of failures	Rank
Alco		
Governor	19	1
Cooling system piping	9	2
Relays (switchgear) *	6	3
Turbocharger	6	4
Circuit breakers	6	5
Colt		
Governor	33	1
Relays (switchgear) *	24	2
Fuel piping	22	3
Turbocharger	21	4
Crankcase	21	5
Cooper-Bessemer		
Control air (I&C)	17	1
Governor	15	2
Fuel piping	14	3
Sensors (I&C)	11	4
Overspeed governor	11	5
General Motors		
Governor	66	1
Relays (switchgear) *	44	2
Starting motors	33	3
Turbocharger	30	4
Starting Control (I&C)	30	5
Nordberg		
Governor	4	1
Sensors (I&C)	4	2
Injector pumps	4	3
Alarms (I&C)	4	4
Cooling heat exchangers	4	5

NOTES: 1. Asterisked items (*) include both diesel and generator failures.

2. I&C = instrumentation and control

Source: NUREG/CR-5078, Volume I, "A Reliability Program for Emergency Diesel Generators at Nuclear Power Plants," U. S. Nuclear Regulatory Commission, Washington, D. C., April 1988, pp. I - 12, 13.

Table 4

Past Diesel Problems at the Indian Point Site

LER* No.	Date	Subsystem	Cause
		IP3	
80-10	6-29-80	breaker	Screw stuck in trip latch
78-23	8-29-78	fuel	Tank level control failure
76-40	11-26-76	control	Loss of speed control
76-35	10-22-76	governor	Maintenance; air in oil
76-31	9-29-76	governor	Low oil; drain not tight
76-20	6-25-76	breaker	Spurious relay operation
		IP2	
80-9	8-10-80	breaker	Defective overcurrent relay
80-2	4-9-80	engine	Timing out of specification
78-37	12-19-78	air-start	Air start motors dirty
77-29	8-29-77	cooling	Jacket water leaks
77-18	8-26-77	lube oil	Pressure switch
77-25	10-19-77	control	Terminal block short
77-20	9-14-77	exhaust	Blower motor failure
77-1	3-2-77	lube oil	Leaking pressure switch
76-27	12-12-76	lube oil	Shorted lube oil heater

* LER = Licensee Event Report (made to the NRC)

Source: NUREG/CR-2989, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1983, pp. 207-209.

Control of Subcontractors and Suppliers

Task 102

The purpose of task 102 is to provide the prime contractor with appropriate management and surveillance of subcontractor reliability programs so that program progress is verified and timely action is taken when required. [13]

The diesel generator vendor is responsible to ensure that items obtained from subcontractors will meet individual and overall system requirements. This includes all levels of subcontracted components. The diesel vendor will certify to the utility, in writing, that the subcontractors reliability and quality efforts have been audited. This certification will be made at each design review identified in Figure 4. The diesel vendor will perform reliability allocations and predictions to a level required to incorporate quantitative reliability requirements into any subcontracted equipment specifications.

The vendor will be contractually obligated to attend and participate in subcontractor design reviews. Subcontractors must notify the vendor at least six working days prior to all design reviews. The vendor in turn must notify the utility at least four working days prior to subcontractor design reviews. Utility personnel will reserve the right to attend all design reviews. Utility personnel, and vendor personnel, will also reserve the right

to inspect subcontractor's facilities with respect to the diesel-related activities.

The diesel vendor will be responsible for reviewing the subcontractor's test plans and procedures. The vendor shall furnish the subcontractors with all relevant data derived from integrated testing that is beyond the subcontractors' control. The subcontractors are responsible for providing the utility with all required technical and administrative support for their products, over the whole system life cycle. This includes having adequate provisions for a failure reporting, analysis, and corrective action system, that can be initiated by the subcontractor, vendor, or utility personnel.

As mentioned in task 101, Woodward governors have been a known problem area for nuclear plant EDG's. The diesel vendor selected will need to place special emphasis on governor reliability throughout the diesel life cycle. This includes an in-depth review of Woodward's reliability program, field checks, documentation of past problem correction, review of training and maintenance manuals, and providing assurance that Woodward has an ongoing, effective, failure review process.

Program Reviews

Task 103

The purpose of task 103 is to establish a requirement for the contractor to conduct reliability program reviews at specified points in time to assure that the reliability program is proceeding in accordance with the contractual milestones, and that the equipment reliability requirements will be achieved. [14]

Design reviews are an important management tool to evaluate program consistency and technical adequacy, including the reliability of the detail design of the selected configuration. The design reviews are major milestones as shown in the Figure 4 chart. Figure 4 shows a design review at the end of the conceptual, preliminary, and detail design phases.

At the conceptual and preliminary design reviews, all pertinent aspects of the reliability program will be discussed, including the status of: reliability modeling, allocations, and predictions, the failure mode, effects, and criticality analysis, and adherence to specified requirements. The status of the spare parts program and reliability problems are also to be included. In conducting reviews, the Table 2 checklist should be used as a starting point. Approximately three weeks prior to these design reviews as scheduled on Figure 4, the diesel vendor will

hold a similar preparatory review with all subcontractors. The utility will be given at least three days notice of this review, and will have the option of participating.

The detail design review shown on the milestone chart is also called the critical design review. This review is to determine the acceptability of the detail design (including reliability) prior to beginning production. At this point the design is essentially frozen, and manufacturing procedures, costs, and schedules are reviewed and approved. The critical design review will also use the Table 2 checklist, and will cover all items mentioned for the earlier design reviews. The critical design review should concentrate on progress since the last review, and any problems and follow-up items. Items needed to conduct the critical design review include construction drawings and parts lists, reliability and maintainability predictions, engineering test reports, the logistic support analysis, a construction and product utilization plan, and a logistic support plan. [15] The design review board will consist of the utility and subcontractor representatives, and vendor personnel with expertise in basic design, reliability, maintainability, human factors and system safety, logistic support, and quality control.

At least two weeks before the diesel system acceptance testing begins, a test readiness review will be conducted. This review will cover the testing dates, status

of reliability predictions, the test plan including prerequisites, sequencing, acceptance criteria, foreseeable problems, and the test report format. This test review will also cover the diesel system as it interfaces with the rest of the power plant, for example, how the diesels fit into the overall electrical distribution system test plan.

Failure Reporting, Analysis, and Corrective Action System Task 104

The purpose of task 104 is to establish a closed loop failure reporting system, procedures for analysis of failures to determine cause, and documentation for recording corrective action. [16] Early elimination of failure causes is a major contributor to reliability growth and attaining acceptable field reliability.

The purpose of this part of the reliability program is to ensure that the root causes of problems are corrected, not just the problem symptoms. Figure 7 shows a top level structured approach to Failure Analysis and Root Cause Determination. This approach will systematically eliminate the root causes of problems. This approach starts with failure analysis, which starts with the symptom and progresses to determination of the underlying failure. The root cause analysis attempts to go one level further and identify the cause of the underlying failure, which could be a design deficiency, or related to an operational or maintenance procedure. This approach is discussed in more detail starting on page 46. All failed parts will eventually be returned to the diesel vendor so that the vendor can perform their own analysis and provide the utility with the results.

One of the keys to a successful root cause analysis

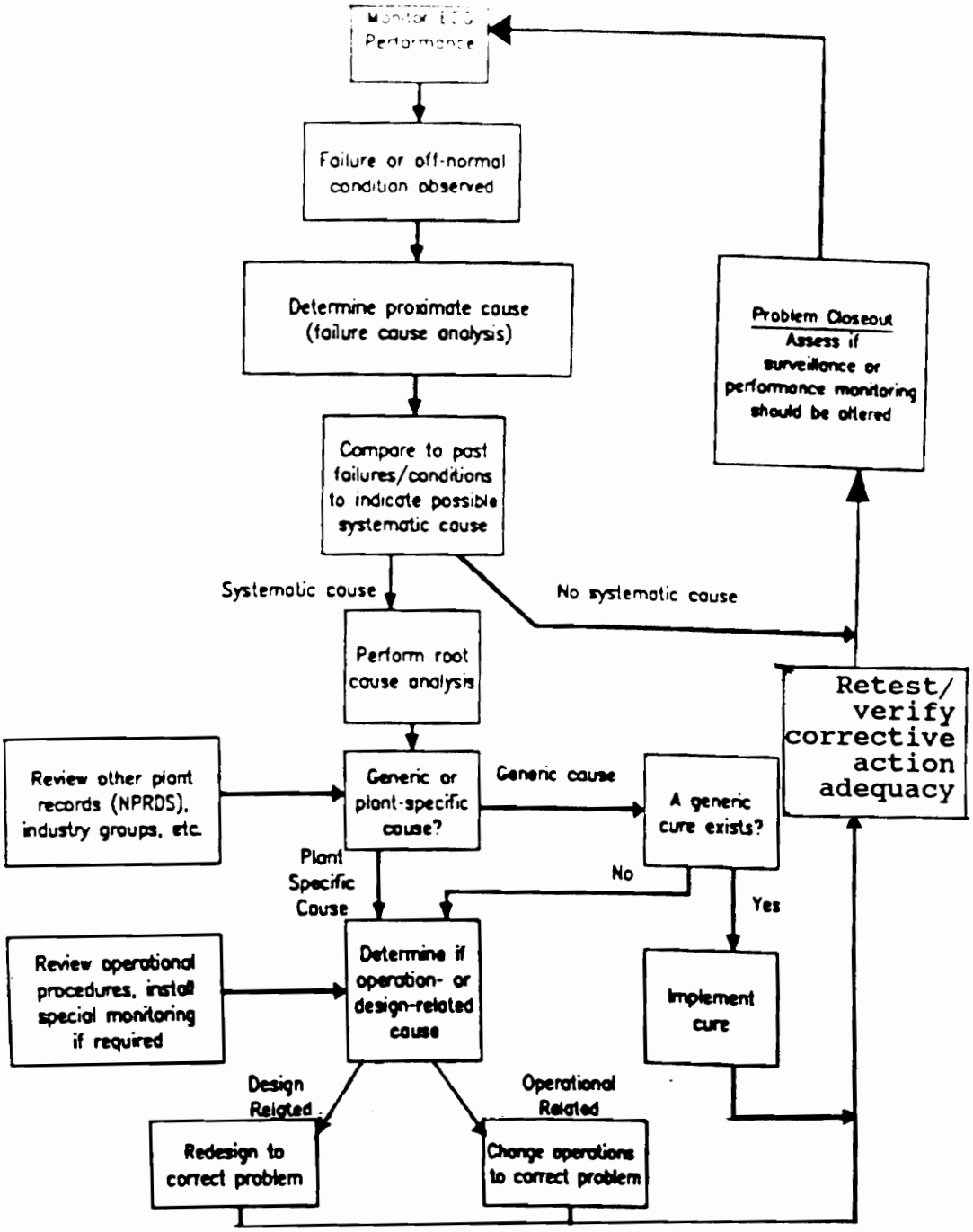


Figure 7. Failure Analysis and Root Cause Determination

Source: Proposed Revision 3 to Regulatory Guide 1.9, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., November 1988, p. 30.

program is the availability of data. This includes all maintenance data, all operational data, failure documentation (for all diesels from the same vendor), and examination of all parts removed or replaced during corrective maintenance. This information will be stored and retrieved using the site computer system. All abnormal conditions noted, as well as all failures, will be recorded in this database.

Root cause analysis often involves many disciplines, and as such a group similar to the IP3 Operational Experience Review Group (OERG) will be well suited for this task. This plan will attempt to maintain continuity in assignments, since repeated observation is a necessary ingredient to the acquisition of the expertise necessary for successful root cause analysis.

When a diesel generator failure occurs, all data pertaining to the failure (and repair if already repaired) will be provided to the Diesel Generator System Engineer by way of an incident report. The DG System Engineer will then use the data available, and in consultation with the OERG, attempt to determine the underlying cause of the failure. The results of each analysis will be relayed to the Plant Operating Review Committee (PORC), as described in the problem closeout process which follows (using the same incident report, to ensure that all information related to a specific problem is kept together). Figure 8 shows an

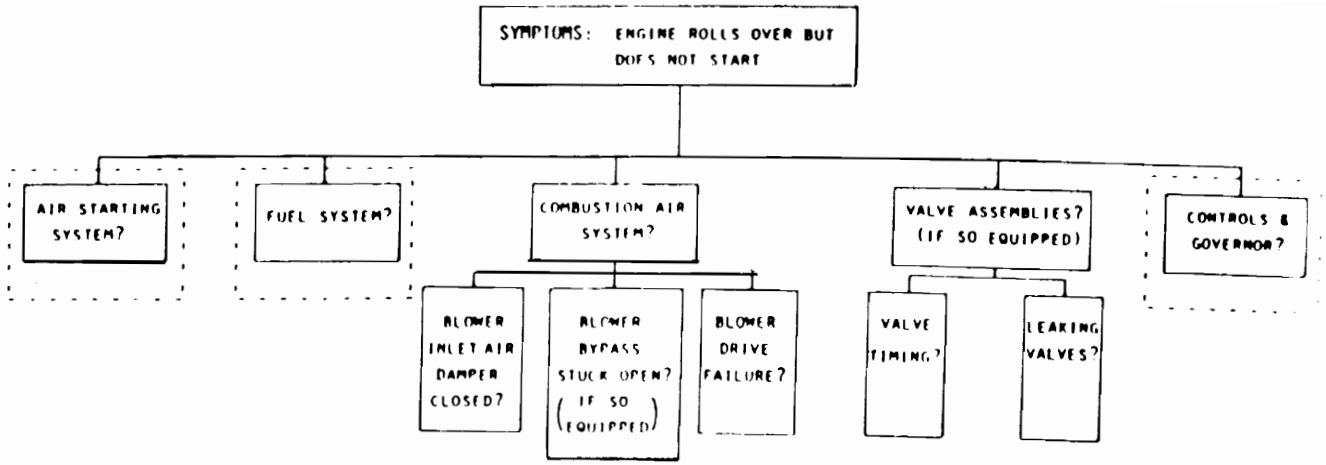


Figure 8. Example of Failure Analysis

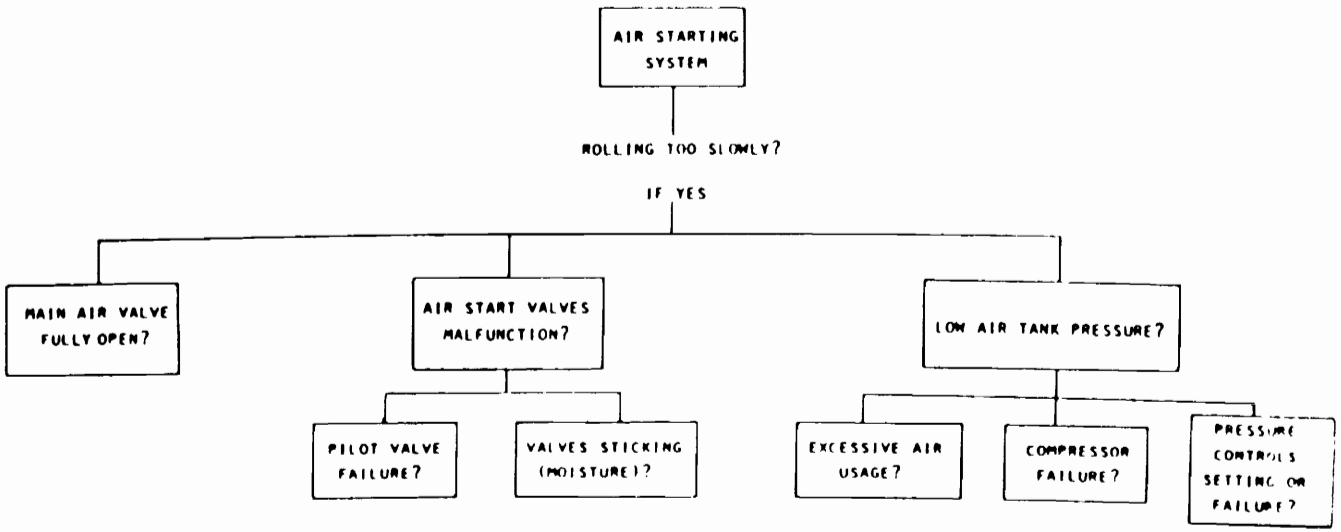


Figure 8. (Continued)

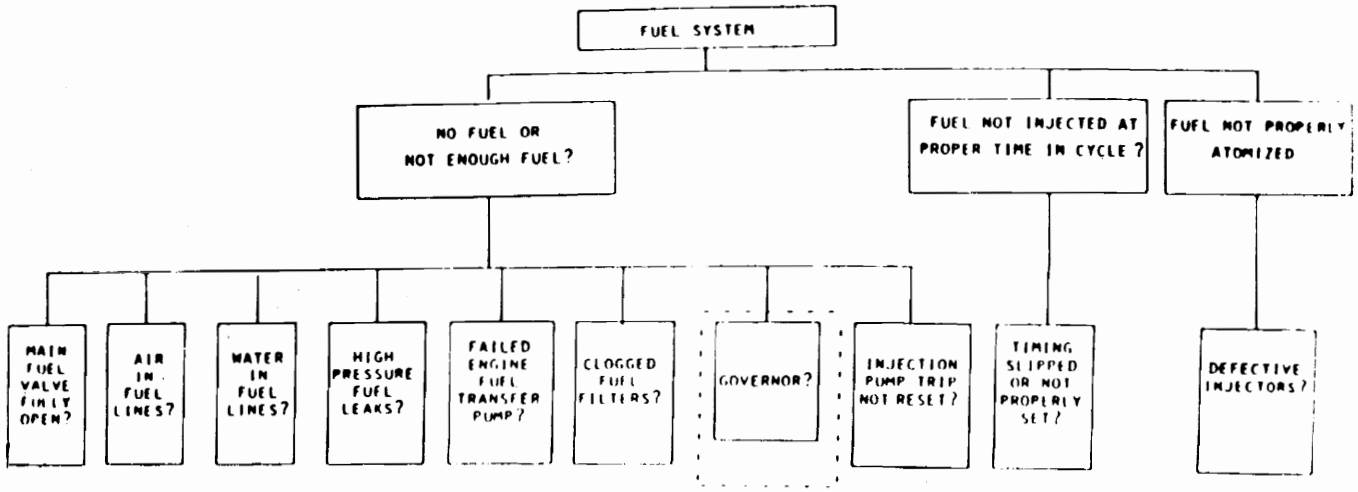


Figure 8. (Continued)

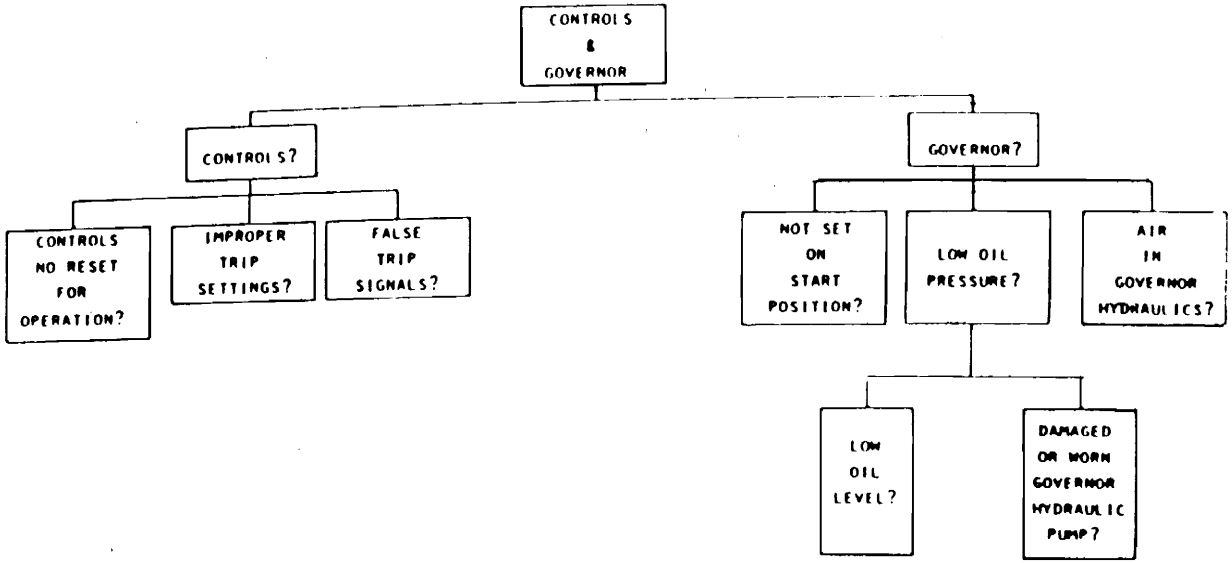


Figure 8. (Continued)

Source: NUREG/CR-5078, Volume 1, "A Reliability Program for Emergency Diesel Generators at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1988, pp. E-14, E-15, E-16, E-17.

example of the process of failure analysis. The potential causes of the diesel engine not starting are shown in this figure, and the figure takes the process down a few levels, to the level of the proximate cause. When any cause is determined to have contributed to the problem, continuing down to the root cause of the problem may require investigation several levels below the proximate cause. It is important to realize that all possible causes must be evaluated at each level, not just the first problem found. This is necessary because a contributing cause for any given failure may progress to be the primary cause of the next failure if not corrected.

The problem closeout procedure for the diesel generator reliability program will be a procedure similar to the closeout procedure currently in use for all significant safety equipment at IP3. Once a diesel generator problem or abnormality is discovered, it will be made known to the PORC. A problem will be tracked from detection, to determination of cause, to corrective action implementation, to verification of the adequacy of the corrective action. Once the corrective actions are verified to be adequate, and any long-term changes are made (e.g., changes to operational or maintenance procedures), a member of the OERG will bring the item back to the PORC, to ensure that the PORC concurs that the problem has been adequately resolved and can be closed out. Closeout will not occur (the item will remain

on the follow-up list) until the adequacy of all corrective actions has been verified.

The corrective action adequacy verification (or re-test) is the key element to problem closeout. For example, if a modification is made to the diesel system, the system must be tested and determined to be operable. It must then be determined that the modification corrected the problem it was designed to correct, and that the system reliability has not been somehow degraded during installation of the modification. The criteria for determining the adequacy of corrective actions are expected to be unique to the problems encountered. For example, if a lube oil pressure transmitter were to fail, the verification would include items (after the repair) such as pressure transmitter calibration and a check for normal operation in the system. Another example might be actions taken as a result of mollusk clogging of service water system heat exchangers (a recent problem discovered at IP3). In this case, long term corrective actions could include installation of a finer mesh screen on the service water intake area, and increasing system flow periodically (daily) to minimize stagnation in the lines, as well as an inspection in the next quarter. If these measures do not prove effective, an increased inspection/cleaning requirement will be added to the detailed maintenance schedule.

The re-test/closeout requirements will be determined by the DG system engineer, in cooperation with members of the OERG, and the maintenance department. The re-test/closeout requirements must be approved by the PORC. These requirements will procedurally become part of the maintenance work package, and must be completed before the work package can be considered closed. The final decision as to when a problem can be closed out is the responsibility of the PORC.

Failure Review Board

Task 105

The purpose of task 105 is to require the establishment of a failure review board to review failure trends, significant failures, corrective action status, and to assure that adequate corrective actions are taken in a timely manner and recorded during the development and production phases of the program. [17]

Due to the criticality of the diesel system to overall plant operation, a failure review board (FRB) will control the failure report, analysis, and corrective action system. When instituting a failure review board, care should be taken to minimize overlap with the total quality control effort for the project. Duplication of quality tasks may not be cost effective.

The FRB will review all performance and failure data. This data will come from inspection and testing reports, including subcontractor reliability and acceptance test data. All failure occurrence information will be available to the FRB. The FRB will maintain a follow-up item list to ensure all required corrective actions are performed.

The utility representative on the FRB will be the Diesel Generator System Engineer. The vendor and subcontractor members of the FRB shall represent the following activities: design, reliability and

maintainability, safety, manufacturing, and quality assurance. Once the diesels go into operation, the FRB members will all be utility personnel, with vendor representatives acting as consultants when required.

CHAPTER 3

DESIGN AND EVALUATION

Task section 200 of MIL-STD-785B assures that, as early as possible, the system and component numerical reliability requirements are examined, to ensure that design compliance can be shown, or shortcomings identified. The numerical requirements should also be evaluated, and if minor changes to them can improve program cost effectiveness, this information should be presented to program management for their consideration. [18] Both quantitative and qualitative analyses can be used to determine where to apply reliability resources. Modeling, allocation, predictions, and the FMECA are all used to ensure compliance with the reliability design requirements. The cost of analyses used is a function of the level and breadth requested of the analysis. An FMECA at the individual part level for the whole diesel system would be very time consuming, and actions taken to increase reliability as a result of the FMECA would probably not be cost effective. However, an FMECA conducted to the major component level of each DG subsystem can identify required design corrections or the need for further analysis. It should be noted that MIL-STD-785B assumes that the FMECA will be performed in the preliminary design phase. The FMECA should be performed as early as possible in the conceptual design phase, so that the wealth of information it provides can be used effectively; this will allow the results of the FMECA to be applied before the design is too mature to be changed.

Reliability Modeling

Task 201

The purpose of task 201 is to develop a reliability model for making numerical apportionments and estimates to evaluate system reliability. [19]

As the diesel system design evolves, a reliability block diagram is developed for the system with associated predictions for each reliability block. The major system requirements are identified from the top-level functional flow diagram. Each block in the functional flow diagram is examined for input and output requirements. The reliability block diagram (or model) is developed from the functional flow diagram, and shows the series-parallel relationships of the subsystems.

To illustrate reliability modeling, reliability block diagrams have been developed for the IP3 diesel generator system from the descriptions of the subsystems which follow. The reliability block diagrams also contain reliability prediction information which will be discussed in task 203. For the diesel generator instrumentation and control system, a block diagram is provided that illustrates the major functions of the system. It should be noted that each of the other systems also contain some elements that are part of the instrumentation and control system.

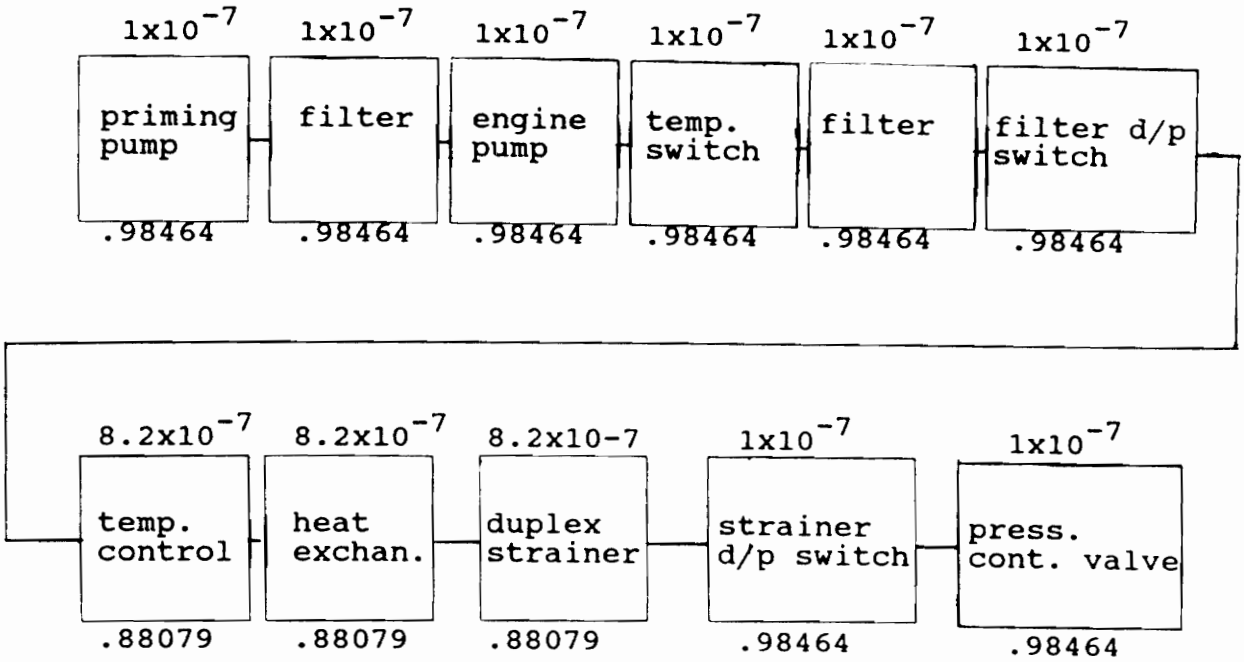
Lube oil system

A motor-driven priming pump operates when the engine is shutdown, to assure positive lube oil flow the moment the diesel is started. The main lube oil pump takes a suction on the oil reservoir and discharges to the header. A temperature switch monitors temperature and activates an alarm at 185°F. The header discharges to a filter with a differential pressure switch (at 15 psid, an alarm is activated: at 20 psid, a relief valve internal to the filter actuates). From the filter, oil goes to the temperature control valve, which maintains temperature by directing some of the flow to the lube oil cooler. The oil then goes through a duplex strainer and back to the engine. A pressure control valve maintains proper inlet pressure to the engine. Figure 9 is a first level reliability block diagram of the lube oil system.

Fuel oil system

The fuel oil inlet header supplies fuel to the injection pumps. Fuel is drawn from the supply tank by a booster pump, filtered through a duplex strainer with a differential pressure switch, and discharged under pressure through a duplex strainer (with a differential pressure switch), into the header. The header supplies fuel to the individual injection pumps. Figure 10 shows a first level reliability block diagram of the fuel oil system.

Lube Oil System

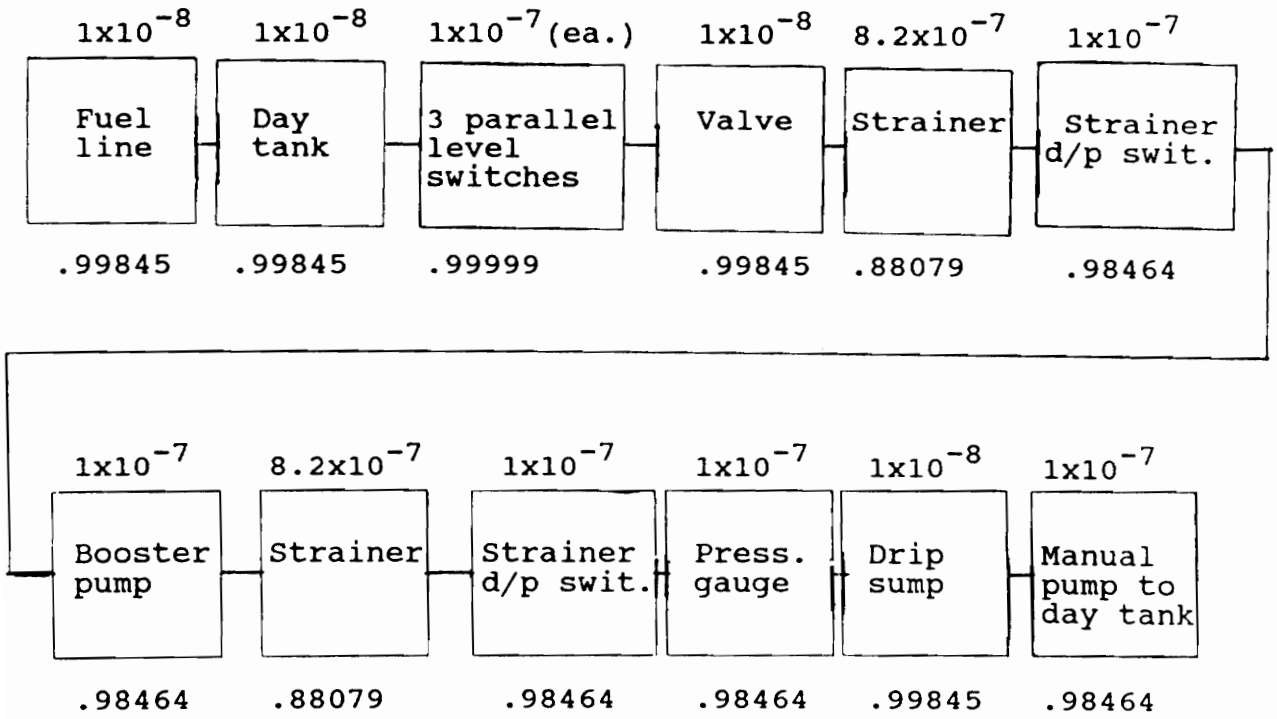


$$R_{system} = (.98464)^8(.88079)^3 = 0.6037$$

Note: The numbers on top of the blocks are the component failure rates (failures/hour). The numbers underneath the blocks are the component reliabilities for 154,800 hours.

Figure 9. Lube Oil System Reliability Block Diagram

Fuel Oil System



$$R_{\text{level switches}} = 1 - (1 - .98464)^3 = 0.99999$$

$$R_{\text{system}} = (.99845)^4(.99999)(.88079)^2(.98464)^5 = 0.7136$$

Figure 10. Fuel Oil System Reliability Block Diagram

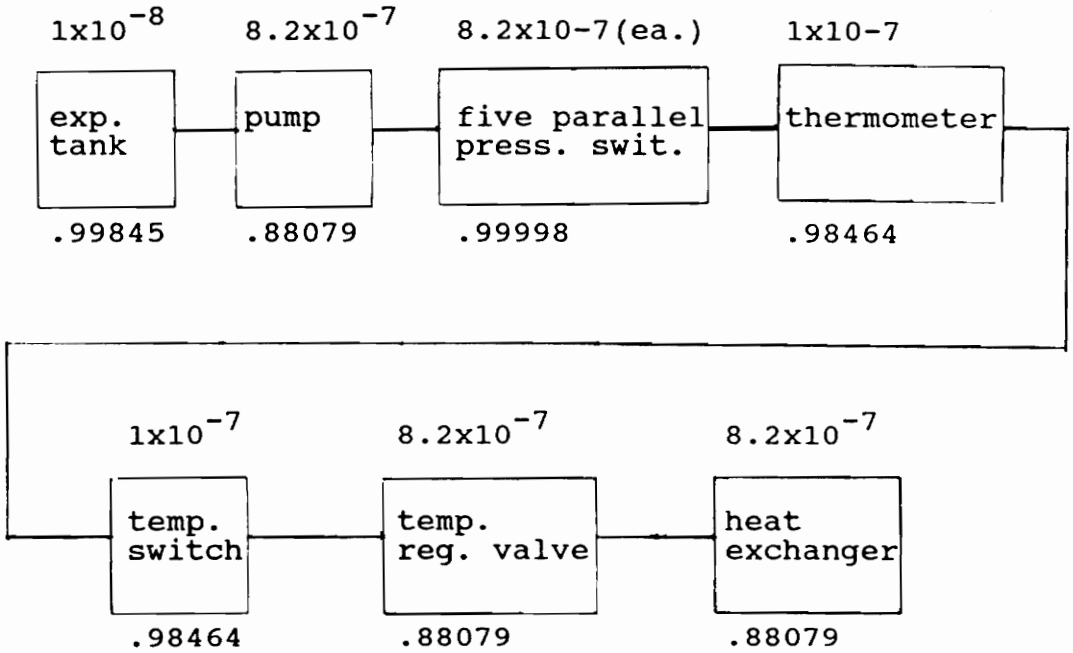
Jacket water system

The engine driven pump discharges the cooling water into the engine. There are five pressure switches and a local gauge. The pressure switches are used in the start circuitry for overcrank protection, control of generator excitation, and starting the lube oil priming pump. The coolant passes through the engine, to the outlet header that is vented to the expansion tank. In this section of the system, there are two temperature switches for high temperature alarms, and a local thermometer. From the outlet header, the coolant goes to a three way temperature controlling valve, with one outlet path to the heat exchanger, and the other to the suction of the pump. Jacket water heaters are also provided, controlled by a thermostat. Figure 11 shows the first level reliability block diagram for the jacket water system.

Starting air system

The main components of the starting air system are the compressor, receiver (with enough air for three or four starts), two control start solenoids, and two start motors. The compressor turns on and off by way of the receiver air pressure switch. The line from the compressor to the air receiver is protected by a relief valve. The air receiver has its' own relief valve. There are two pressure switches on the air receiver; one controls an alarm, while the other

Jacket Cooling Water System



$$R_{\text{pressure switches}} = 1 - (1 - .88079)^5 = 0.99998$$

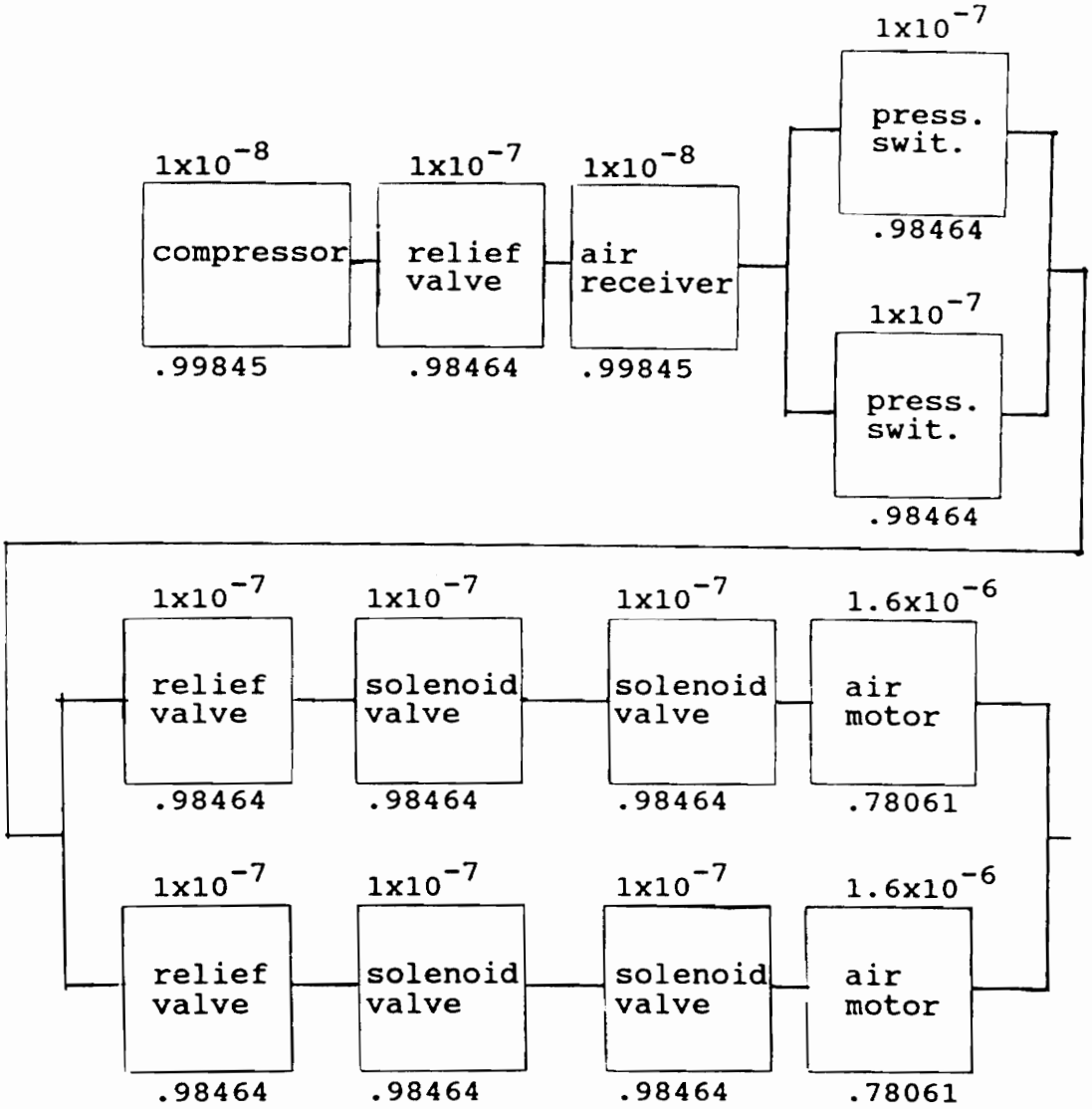
$$R_{\text{system}} = (.99845)(.88079)^3(.99998)(.98464)^2 = 0.6614$$

Figure 11. Cooling Water System Reliability Block Diagram

controls the compressor. An equalizing line can connect all three air receivers if necessary. From the receiver, air goes through two identical lines containing: a pressure reducing valve, a relief valve, a pressure switch (for alarm purposes), a control start valve, and the air start motor. Figure 12 shows the first level reliability block diagram for the starting air system.

Figure 13 shows the major relationships of the different portions of the instrumentation and control (I&C) system. A component level block diagram was not developed for this system, due to the large variation in different plants' EDG I&C systems. This does not mean the I&C system is of lesser importance than the other systems. In fact, in the design of an actual diesel system, this system would be the most important due to the I&C system complexity. The I&C system will be discussed in greater detail in Task 203.

Starting Air System



$$R_{\text{pressure switches}} = .98464 + .98464 - (.98464)^2 = 0.99976$$

$$R_{\text{relief valves}} = .98464 + .98464 - (.98464)^2 = 0.99976$$

$$R_{\text{sol. + sol. + motor}} = (.98464)^2(.78061) = 0.75681$$

$$R_{\text{final six comps.}} = .75681 + .75681 - (.75681)^2 = 0.94086$$

$$R_{\text{system}} = (.99845)^2(.98464)(.99976)^2(.94086) = 0.9231$$

Figure 12. Starting Air System Reliability Block Diagram

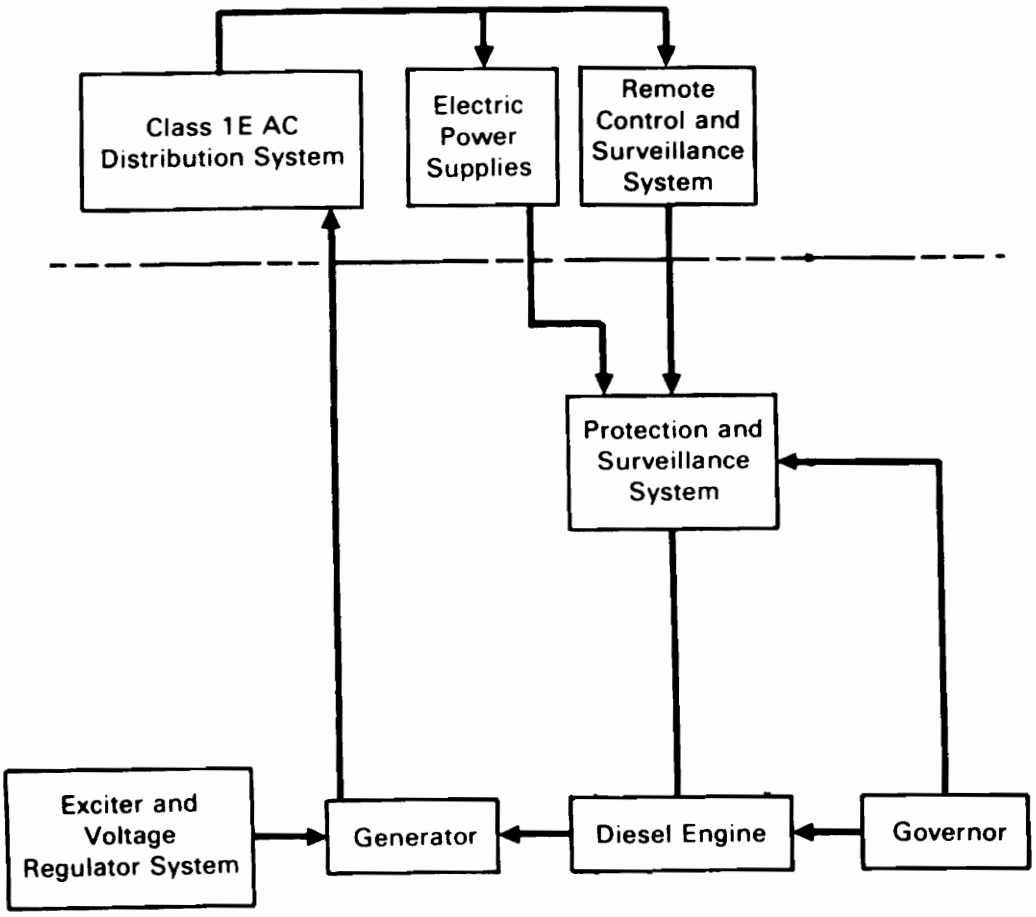


Figure 13. Instrumentation and Control System Functions

Source: NUREG/CR-4590, Vol. 1, "Aging of Nuclear Station Diesel Generators: Evaluation of Operating and Expert Experience," U.S. Nuclear Regulatory Commission, Washington, D.C., August 1987, p. 2.2.

Reliability Allocation

Task 202

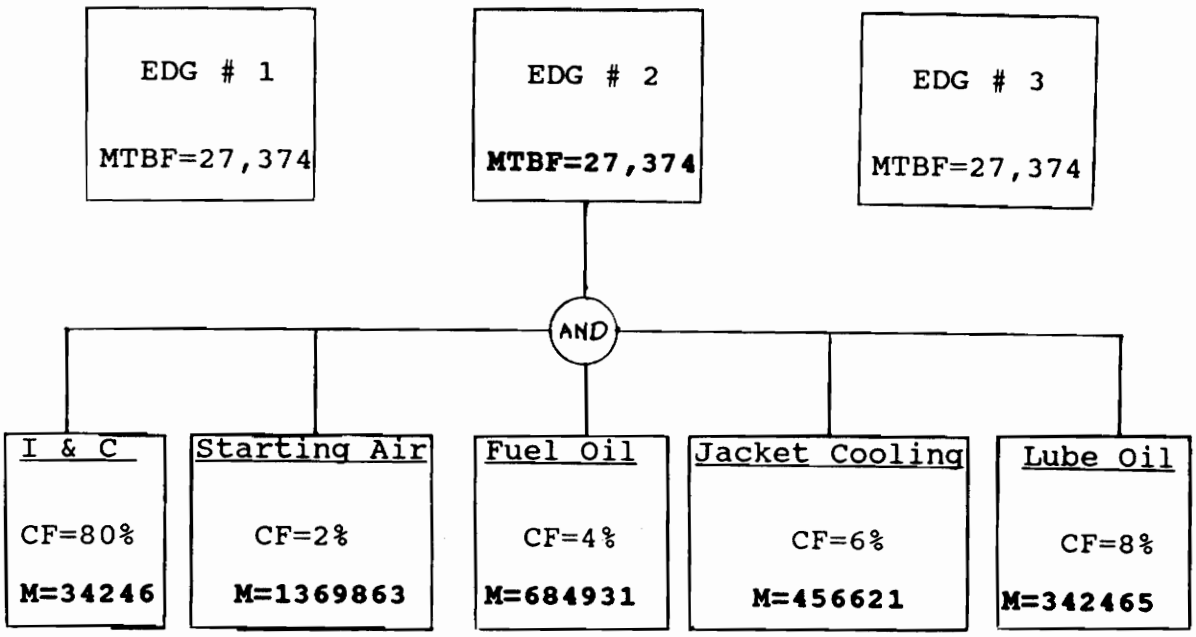
The purpose of task 202 is to assure that once quantitative system requirements have been determined, they are allocated to lower levels. [20]

Once quantitative requirements are determined, they are allocated to the subsystems. The objective is to transform the system requirement into manageable lower level requirements. The initial allocations are gross, but indicate the resources required for the reliability program. The development of the reliability block diagrams facilitate the reliability allocation process.

To accomplish reliability allocation, the following steps are followed: (1) the functional flow diagrams are evaluated and areas identified for which the design is known and failure rate information is available; and (2) areas which are new (with no design information available) are identified and assigned complexity weighting factors, based on the number and relationship of parts, duty cycle, environmental stresses, and other similar factors. [21]

Figure 14 shows a reliability allocation for each diesel generator based on the 27,374 hour MTBF requirement. Allocation is performed using the equation $R = e^{-t/MTBF}$ and the complexity of the subsystem.

Diesel System
Three EDGs in parallel



MTBF = M = mean time between failures (in hours)

CF = complexity factor

Note: The required MTBF is determined using the equation $R = e^{-t/MTBF}$, and allocated using the subsystem complexity.

Figure 14. Diesel System Reliability Allocation

Reliability Predictions

Task 203

The purpose of task 203 is to estimate the basic reliability and mission reliability of the system and to make a determination of whether these reliability requirements can be achieved with the proposed design. [22]

As design work progresses, predictions, based on previously generated data, are used to indicate whether or not the allocated requirements can be met. However, predictions are not the basis for determining attainment of reliability requirements. This can only be done using test results. As engineering data become available, reliability predictions are made for level of the system, from subassemblies up to the system level. Predictions are compared against requirements; any areas where reliability is predicted to fall short signal the need for management and technical attention, to see if design improvement is possible. Possible improvements include simplifying the design, use of higher quality parts, trade-offs between part tolerances, or use of redundancy or different modes of system operation.

Predictions should be made as early as possible, and updated whenever changes occur. Early predictions are really only educated guesses due to lack of design detail, but they provide useful feedback regarding the feasibility

of meeting basic reliability requirements. The basic reliability prediction techniques are: (1) predictions based on analysis of similar equipment; (2) predictions based on an estimate of active element groups; (3) predictions based on an equipment parts count; and (4) predictions based on a stress analysis and environmental factors. [23] These methods are listed approximately from the least sophisticated to the most sophisticated, and also from the earliest point in system design to the latest point in system design.

A reliability prediction for an individual IP3 diesel generator was performed to illustrate reliability prediction based on analysis of similar equipment. The failure rates for the IP3 diesel subsystems have been predicted based on composite data obtained from the NRC publication NUREG/CR-2989. This data (summarized in Table 5) is taken from the operational history of plants with Alco diesel generators, the Power Authority's other nuclear plant (Fitzpatrick), and some plants of the same vintage as Indian Point 3, including: Browns Ferry, Fitzpatrick, Ginna, Indian Points 2 and 3, Palisades, Rancho Seco, Salem, and Trojan. Operating hours for these plants for the years 1976 to 1980 were totaled, as were individual component failures reported. This allowed calculation of individual component failure rates for these components. For components in the first level block diagrams that had no failures recorded,

Table 5

Data Used for Failure Rate Predictions

Plant	Operating Hours	I&C Fail.	Other Comp. Fail.
Browns Ferry	329664	10	heat exchan. foul
Ginna	87696	5	
IP2	131544	1	air start motor
IP3	124632	4	
JAF	175392	9	lube oil heater
Palisades	87696	1	cool. press. switch
Rancho Seco	87696	4	air start motor cool. water pump fuel oil strainer
Salem	106704	0	cooling water valve
Trojan	87696	3	

Failure Rate Predictions (Failures per hour)

I&C failures $37/1218720 = 3 \times 10^{-5}$

air start motor failures $2/1218720 = 1.6 \times 10^{-6}$

failures of cooling water press. switch, pump, and valve; fuel oil strainer; heat exchanger fouling; lube oil heater

$1/218720 = 8.2 \times 10^{-7}$

other components for which no failures were reported; most were assumed at 1×10^{-7}, a few were assumed at 1×10^{-8}

Source of data: NUREG/CR-2989, "Reliability of Emergency AC Power Sources at Nuclear Power Plants," U. S. Nuclear Regulatory Commission, Washington, D. C., July 1983, section 9.4, table 9.5.13.

failure rates were estimated. Once the individual component failure rates were estimated, the individual component reliabilities were calculated assuming an exponential distribution of the reliability function. Time was factored into the reliability equation assuming a 30 year period, 215 day per year, 24 hour a day service. The limitations of this reliability prediction must be recognized. The failure rate predictions are being made using 10 to 14 year old data. The assumptions made for items with no failures recorded may be optimistic in terms of component performance; failures may have occurred that were not recorded. Limitations aside, these data do allow a starting point to make a prediction regarding the reliability of the diesel system.

Figure 9 is a first level reliability block diagram for the lube oil system that shows a predicted reliability of 0.6037. Figure 10 is a first level reliability block diagram for the fuel oil system that shows a predicted reliability of 0.7136. Figure 11 is a first level reliability block diagram for the jacket water system that shows a predicted reliability of 0.6614. Figure 12 is a first level reliability block diagram for the starting air system that shows a predicted reliability of 0.9321.

Figure 13 shows the functions of a typical instrumentation and control system. For the diesel I&C system, the data from NUREG/CR-2989 are used to predict an

overall subsystem reliability. Based on a total reported operating time of 1,218,720 hours (of the plants mentioned previously), and 37 reported failures, a failure rate of 3 x 10^{-5} failures/hour is calculated. This results in a reliability prediction for the instrumentation and control systems of 0.009619. Using all of the predicted subsystem reliabilities in a series relationship, the reliability equation ($R = e^{-\lambda t}$), and the fact that MTBF = $1/\lambda$, an overall predicted MTBF of 27,374 hours for an IP3 diesel can be predicted for a 30 year period.

A component level block diagram was not developed for the I&C system. In actual applications, the complexity of the I&C system, estimated in Figure 14 as 80%, should drive the decision to expend about 80% of the available time and resources on the I&C area. Based on the failure rates predicted for this system, it would be the high cost contributor to system operation and maintenance costs. This prediction should lead to a detailed examination of the I&C area of the diesel, and reliability block diagrams would definitely be prepared.

A review of past diesel experience indicates that the following problem areas are the most frequently encountered I&C problems areas, starting with the most frequent: governors, breakers, relays, and linkages. Governors have had many problems at all power plants, including:

o oil overheating due to proximity to the turbocharger,

- o air in the oil,
- o dirt in the oil,
- o low oil level,
- o vibration-induced failures (loose connections),
- o and defective float valves.

The main problems with circuit breakers have been dirt in the mechanism and loose connections. Relays have failed due to dirt and moisture accumulation. Linkages have failed due to binding (due to improper lubrication), and due to joint wear that caused excessive play.

These are all instrumentation and control problems that should be known already in the conceptual design phase. This is the area where a major portion of the design effort should be focused. With the early design efforts focused on the known problem areas, the predictions for this system should show a substantial improvement in the MTBF over the 34,246 hours shown in the Figure 14 allocation.

Failure Modes, Effects, and Criticality Analysis (FMECA) Task 204

The purpose of task 204 is to identify potential design weaknesses through systematic, documented consideration of the following: all likely ways in which a component can fail; causes for each mode; and the effects of each failure. [24]

The FMECA shall be performed in the conceptual design phase. The FMECA shall include: item identification, description of failure modes, cause of failure, possible effects of failure, probability of occurrence, criticality of failure, and possible corrective action or preventive measures. [25] The FMECA will be used as inputs to design trade-offs, safety engineering, maintenance engineering, maintainability, logistic support analysis, and test engineering. The FMECA shall be conducted in accordance with the Military Standard for a Failure Modes, Effects, and Criticality Analysis (MIL-STD-1629), or an alternative approved by the utility.

To illustrate the process of performing an FMECA, a top level FMECA was performed for the IP3 diesel generator subsystems. The subsystem descriptions that were used earlier in the development of the top level reliability block diagrams (Figures 9 through 12) were used to develop a top level FMECA, which is shown in Table 6. The FMECA

of Table 6 covers each component of the subsystems that are part of the subsystem reliability block diagrams.

The following are the definitions are used in the Table 6 FMECA to describe how critical each failure is to the being able to perform its function. "Catastrophic" failures are those failures that can cause significant system damage and jeopardize the mission success of the diesels, failures that preclude the diesel from starting or from carrying electrical loads. "Critical" failures are those that degrade the system beyond acceptable limits, and may result in failure of the diesels mission. Failures classified as "major" failures by the FMECA are failures that degrade the system beyond acceptable limits, but can be controlled. An example of a diesel failure in this category would air or water in the fuel system. Failures in the "minor" category result in unscheduled maintenance or repair, but do not degrade the overall system performance beyond acceptable limits. An example of a failure in this category is excessive diesel engine valve guide clearances.

There are a few points to note regarding the development of the FMECA. The reliability block diagrams used actually combine the top level functional flow path along with the predicted reliabilities. A more detailed FMECA would most probably use separate reliability block diagrams and functional flow diagrams. The FMECA performed for this report has been qualitative in nature, while a more

Table 6

Failure Modes, Effects, and Criticality Analysis

Jacket Water Cooling System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Expansion tank - keep system full & provide suct. head to pump	Failure: Empty due to leakage	Pump lose suct./ Engine overheat	$1x10^{-8}$	Critical	Record tank level;check for leaks
	Degradation: Restrict flow due to rust	Pump lose suct./ Engine overheat		Critical	Use rust inhibitor; check level
Pump - circ coolant to remove eng. heat	Failure: Pump seize due to wear	No press. to swit./DG trip	$8.2x10^{-7}$	Catastr.	Record sys. press. & temp. hourly when run
	Degradation: Insuff. press due to excess clearance	Low press./ Engine overheat		Critical	
Press.swit. - protect sys.,start L.O. prim. pump	Fail open	Sense no press./ DG trip	$8.2x10^{-7}$	Catastr.	Record press. hourly when run, calibrate switches
	Fail shut	Sense press. continuously/ engine overheat		Critical	
Thermometer - measure sys. temp.	Fail open	Ind. hi temp./ more flow to HX	$1x10^{-7}$	Minor	Record temps. hourly
	Fail closed	Ind. low temp./ sys. temp. rise		Major	

Table 6 (Continued)

Jacket Water Cooling System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Temp. swit. - activate high temp. alarms	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record temps. hourly
	Fail closed	Prevent alarm/ high temps. unnoticed		Minor	
Temp. req. valve - adj. flow to HX	Port to HX or inlet port blocked	No flow to HX/ Engine overheat	$8.2x10^{-7}$	Critical	Record temps. hourly; recondit. valve
	Port to pump suct. blocked	All flow through HX/Sys. cooldown		Minor	
Heat exchan. - transfer eng. heat to serv. water system	Rupture	Lose sys. fluid/ Engine overheat	$8.2x10^{-7}$	Critical	Record temps. & exp. tank level hrly.
	Foul	Lose heat transfer/ Engine overheat		Critical	

Table 6 (Continued)

Lube Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Priming pump - circ. oil while engine shutdown	Failure: Pump seize due to wear	Low pressure/ Hard start of DG	$1x10^{-7}$	Critical	Check pump operation, press. & temp. ea. shift; renew pump
	Degradation: Low press. due to excess clearance	Low pressure/ Hard start of DG		Critical	
Filter - keep oil lines clear of particles	Clog	Block flow in line/Engine overheat	$1x10^{-7}$	Critical	Record press. & temp., inspect & clean filter
	Tear	Pass particles/ clog other strainers		Minor	
Engine pump - circ. oil for engine lubrication	Failure: Pump seize due to wear	Low pressure/ Engine overheat	$1x10^{-7}$	Critical	Record press. & temp., overhaul engine
	Degradation: Low press. due to excess clearance	Low pressure/ Temp. increase		Major	
Temp. swit. - activate high temp. alarms	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record temps. hourly
	Fail closed	Prevent alarm/ high temps. unnoticed		Minor	

Table 6 (Continued)

Lube Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Filter - keep oil, & temp. cont. valve, clean	Tear	Pass particles to cont. valve/ Engine overheat	$1x10^{-7}$	Critical	Record press. & temp., inspect and clean filter
	Clog	Restrict oil flow/Engine overheat			
Filter d/p switch - activate alarm	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record press., calibrate switch
	Fail closed	Prevent alarm/ Lose oil due to relief lift		Major	
Temp. cont. valve - control flow to HX	Port to HX or inlet port blocked	Flow restricted, oil not cooled/ Engine overheat	$8.2x10^{-7}$	Critical	Record temp. & press., recondit. valve
	Outlet blocked	All flow through HX/ Sys. cooldown		Minor	
Heat exchan. - transfer oil heat to serv. water system	Rupture	Lose oil/ Engine overheat	$8.2x10^{-7}$	Critical	Record temp. & oil level
	Foul	Lose heat transfer/ Engine overheat		Critical	

Table 6 (Continued)

Lube Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Strainer - keep oil lines clear of particles	Clog	Block flow in line/Engine overheat	$1x10^{-7}$	Critical	Record press. & temp., inspect & clean strainer
	Tear	Pass particles/ clog engine & other strainers		Minor	
Strainer d/p switch - activate alarm	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record d/p & press.
	Fail closed	Prevent alarm/ High d/p unnoticed		Major	
Press. cont. valve - control sys. press	Port to engine blocked	Flow diverted to sump/ Engine overheat	$1x10^{-7}$	Critical	Record press. & temp., recondit. valve
	Outlet or inlet to sump blocked	Loss of press. control/Sys. overpressurized		Critical	

Table 6 (Continued)

Fuel Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Fuel line - supply fuel to day tank	Rupture or block	No fuel to day tank/ limited supply of fuel	$1x10^{-8}$	Major	Record tank levels & check sys. for leaks
Day tank - supply fuel to engine	Rupture	No fuel to engine/Fail to start	$1x10^{-8}$	Catastr.	Record tank levels
	Allow inleakage	Water in tank/ hard to start		Critical	& check sys. for leaks
Level switches - activate low level alarm	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record levels; switch redundancy
	Fail closed	Prevent alarm/ low level unnoticed		Critical	
Strainer - filter fuel entering pump	Tear	Pass particles/ clog pump	$8.2x10^{-7}$	Critical	Record press. & level;clean strainer
	Clog	Pass no fuel/ engine stall		Catastr.	

Table 6 (Continued)

Fuel Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Strainer d/p switch - activate alarm	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record d/p & press.
	Fail closed	Prevent alarm/ High d/p unnoticed		Major	
Strainer - filter fuel entering engine	Tear	Pass particles/ clog engine	$8.2x10^{-7}$	Critical	Record press. & level;clean strainer
	Clog	Pass no fuel/ engine stall		Catastr.	
Booster pump - supply fuel to engine	Failure: Seize due to wear	Lack of fuel pressure/ Engine stall	$1x10^{-7}$	Catastr.	Record press.; recondit. pump
	Degradation: Insuff. press.due excess clearance	Low press./ Engine runs rough		Critical	
Strainer d/p switch - activate alarm	Fail open	Alarm/none	$1x10^{-7}$	Minor	Record d/p & press.
	Fail closed	Prevent alarm/ High d/p unnoticed		Major	

Table 6 (Continued)

Fuel Oil System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Press. gage - indicate fuel press.	Leak	Lose fuel/ Engine stall	$1x10^{-7}$	Critical	Record press. & d/p; calibrate gage
	Indicate wrong pressure	Not show pressure/ press. problem unnoticed			
Drip sump - collect any excess fuel	Clog	Excess fuel accumulate/ Engine stall	$1x10^{-8}$	Critical	Record press. & check for leaks
	Rupture	Fuel spill/ possible fire		Critical	
Manual pump - pump drip sump to day tank	Seize due to wear	Fuel spill/ possible fire	$1x10^{-7}$	Critical	Record press. & check for leaks

Table 6 (Continued)

Starting Air System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Compressor - charge air receiv.	Fail to run	No air to receiver/ limited air supply	$1x10^{-8}$	Critical	Record air press, check for leaks
Relief Valve - protect line to receiver	Fail open	No air to receiver/ limited air supply	$1x10^{-7}$	Critical	Check sys. for leaks, lift check valve, cross-connect air receivers
	Fail to lift	System rupture/ limited air supply		Critical	
Air Receiver - provide starting air for diesel	Rupture	No starting air/DG fail to start	$1x10^{-8}$	Catastr.	Record press. & maintain redundant relief valves
Pressure switches - control alarm and compressor	Fail open	Alarm & start compressor/charge air receiver	$1x10^{-7}$	Minor	Record press. & calibrate switches
	Fail closed	No alarm or compressor start/limited air supply		Critical	

Table 6 (Continued)

Starting Air System					
Component & function	Failure mode	Effect on next item/end product	Predicted failure rate	Criticality	Preventive action
Relief valves - protect air start motors	Fail open	No air to motor/DG fail to start	$1x10^{-7}$	Catastr.	Record press., lift check relief valves
	Fail to lift	Sys. press. increase/DG fail to start		Catastr.	
Solenoid control valves - control air to start DG	Fail to open	No air to DG/ DG fail to start	$1x10^{-7}$	Catastr.	Use redundancy, recondition valves
	Inadvertently open	False start/ needless component wear		Minor	
Air start motors - start the EDG	Fail to operate	No air to DG/ DG fail to start	$1.6x10^{-6}$	Catastr.	Use redundancy, inspect & clean motor, & recondit. motor

structured FMECA would be of a quantitative nature. The FMECA that was performed actually combines a Failure Mode and Effects Analysis (FMEA) with a Criticality Analysis. In the development of a FMECA, these two elements of the overall analysis would be performed as separate pieces, and be presented as separate tables. The FMECA presented here is a first level effort; for this reason, the failure causes are not fully developed. For example, the root cause of a solenoid valve problem might actually be the solenoid power supply. As a first level analysis, the output is more directed towards major component preventive measures, not preventive measures directed towards the root causes. The fact that the emphasis is on prevention also differs somewhat from a typical FMECA; in general, a typical FMECA would stress the corrective actions more than the preventive actions. This FMECA did not consider personnel injuries at all; for a fully developed FMECA, serious personnel injuries would rank as catastrophic failures. The criticality aspect of the FMECA here is just a first level approach, used to illustrate the process. The purpose of the criticality analysis is to rank each failure mode identified in the FMEA, using the criticality multiplied by the probability of occurrence. The resulting numerical rank would then be used to set priorities for corrective and preventive actions, as well as provide input to other areas such as spare parts inventory.

One final point to note is the usefulness of the FMECA data. The FMECA should be performed in the conceptual design phase of the system, so that catastrophic and critical failures can be designed around or compensated for. One way to compensate for these failures is to use the output of the FMECA in the development of a reliability-centered maintenance (RCM) program. The aim of the RCM program is to design a preventive maintenance program by evaluating item maintenance in accordance with the possible failure modes identified in the FMECA. The FMECA of Table 6 lists preventive measures for the failure modes identified. These preventive measures would be incorporated into the diesel preventive maintenance program. The output of the FMECA/RCM analysis would also be an input to the logistic support analysis, as support required for the preventive maintenance program was identified.

Sneak Circuit Analysis

Task 205

The purpose of task 205 is to identify latent paths which cause occurrence of unwanted functions or inhibit desired functions, assuming all components are functioning properly. [26]

A sneak path could result from an inadvertent cross-connection of two circuits. An example of this could be inadvertent air compressor starting when the low air pressure alarm is tested. Sneak circuit analysis is a useful engineering tool that can identify sneak circuit paths and drawing and design errors. Sneak paths are generally not considered that result from failures, malfunctions, and environmental effects. The identification of a sneak path does not necessarily indicate an undesirable condition; it does point out the need for further investigation.

Sneak circuit analysis is usually performed late in the design cycle after design documentation is complete; therefore any changes needed at that point would be time consuming and costly. Because sneak circuit analyses are generally costly, they should be considered only for circuitry that is critical to mission success and safety.

For the EDG system, sneak circuit analysis may be desirable for the electronic circuitry that sends the

"Start" signal to the EDG's, since this is a mission critical function.

Electronic Parts/Circuits Tolerance Analysis
Task 206

The purpose of task 206 is to examine the effects of parts/circuits electrical tolerances and parasitic parameters over the range of specified operating temperatures. [27]

This analysis will verify that, given reasonable combinations of parts and components that are within their respective specified tolerances, the overall circuitry that they are part of will perform within specification. This analysis will consider such factors as the manufacturing variances, temperature effects, and instrument drift characteristics. Characteristics examined shall include relay actuation times, resistance, inductance, capacitance, maximum voltage current, frequency and phase. The timing of sequential events and power dissipation shall be considered under worst case conditions.

This analysis is generally performed as a matrix-type analysis, with use of a computer to analyze the matrix recommended. For this reason, the analysis is generally expensive due to the time required to prepare the computer input and the skill level of personnel required. For the diesel generator system, this analysis will be limited to the diesel generator "Start" circuitry, because this circuitry is the most crucial. The range of equipment

operating temperatures used for this analysis shall be specified as 60°F to 100°F. This temperature range shall be considered for continuous service, in other words, long-term operation at either extreme of the range. The data and results of this analysis shall be available for the utility to examine at the detail design review.

Parts Program

Task 207

The purpose of task 207 is to control the selection and use of standard and nonstandard parts. [28]

The following paragraph from Appendix A of MIL-STD-785B describes the philosophy behind the parts control program:

> Conducting an aggressive parts control and application program increases the probability of achieving and maintaining inherent equipment reliability, minimizes parts proliferation, logistics support costs, and system life cycle costs. The added investment required for a vigorous program which controls parts selection and application can be offset by reduced system life cycle costs for reparable systems and by overall system effectiveness for nonreparable systems. In some cases the use of higher quality parts can even lower item acquisition cost through reduction in the amount of assembly line rework as well as eliminate additional costs for drawings and test data required when using nonstandard parts. [29]

The parts policy must include consideration of frequency of repair (e.g., mean time between replacement), criticality, and ease of obtaining the part, under both normal and abnormal (e.g., weekends) conditions. This should serve to prevent unusually large logistics downtimes. At Indian Point 3, a DG repair was once delayed for 74 hours while waiting for governor parts. The following is a partial list of spare and repair parts necessary for the

diesel generator system:

- o alarm modules
- o meters
- o gauges
- o seals and gaskets
- o lubricating fluids
- o corrosion inhibitor
- o control circuitry modules
- o air and oil filters
- o breaker repair parts (such as springs and latches)
- o diesel engine rings
- o heat exchanger zinc anodes

The EDG system is a nuclear power plant safety-related system; a safety-related system is one that is required to safely shutdown the reactor, remove decay heat, or prevent a release of radioactivity in excess of federal limits. As a safety-related system, the EDG parts program is required to be governed by the utility's Quality Assurance (QA) program mandated by federal regulations.

The parts control program will require objective evidence of quality for all parts received. This will include part identification and all codes, standards, and specifications met by the parts. The specifications met will include such items as safety margins and derating criteria. Derating refers to use of a component part under stress conditions below rated values in order to achieve a "reliability margin"; for example, using a 200-V capacitor in a 100-V application will in all probability lead to a longer capacitor life than if it was used in a 200-V application. [30]

Parts will be receipt inspected by utility QA personnel when they arrive at the site, and will be certified as ready for use prior to placement in the site inventory system. Receipt inspection will include verification that the part has been properly identified, including the required documentation, vendor acceptance records will be inspected, conformance with the purchase documentation will be established, and all quality records will be available at the plant.

The utility will maintain a list of qualified vendors for all procured parts, including an order of preference ranking for the vendors. One final part of the parts program will be a listing of vendors that have been identified, by utilities or the NRC, as having supplied substandard or fraudulent parts. Use of these vendors will be prohibited.

Reliability Critical Items

Task 208

The purpose of task 208 is to identify and control those items which require "special attention" because of complexity, application of advanced state-of-the-art techniques, and the impact of potential failure on safety, readiness, mission success, and demand for maintenance/logistics support. [31]

Reliability critical items, as defined by task 208, are not limited to items categorized as "catastrophic" or "critical" by the FMECA, although these items are certainly included. Reliability critical items include those whose failure can have a significant negative effect on system safety, availability, or mission success. High value items are considered to be reliability critical for life cycle cost. Other items deemed reliability critical for this task include: items stressed in excess of derating criteria, items that require special handling or precautions, items used in large quantities, or critical-useful-life items. A critical-useful-life item is one which, because of its short life, is incapable of satisfying the functional requirements imposed by its application unless corrective or preventive maintenance is performed. [32] To properly design for system supportability, all critical-useful-life items should be eliminated. Reliability critical items are prime candidates for detailed analysis, growth testing,

reliability qualification testing, stress analysis, and other techniques to point out areas for reliability improvement.

Items identified as catastrophic by the FMECA include: the cooling system pump and pressure switches, the fuel oil system day tank, strainer, and booster pump, and the starting air system starting motors, control valves, and relief valves. Another critical item for task 208 will be the governor, due to its critical system function, cost, and possible extensive time to repair.

Life Criteria

Task 209

The purpose of task 209 is to determine the effects of storage, handling, packaging, transportation, maintenance, and repeated exposure to functional testing on hardware reliability. [33]

The requirements for diesel system transportation will be identified in the preliminary logistic support analysis plan. Shipment will be in a limited quantity (no more than six expected for a two-reactor-plant site), so an ongoing transportation service is not necessary. The diesels will be shipped by truck or rail, using a bonded carrier. Transportation to the site will be fully insured, insurance being the vendor's responsibility. Once at the site, installation into the diesel structure will also be the responsibility of the vendor. Actual subsystem connections to interfacing subsystems will be performed by the utility. Shipping of the diesels to the site is expected to have no detrimental effects on the diesel system components.

Task 209 requires determination of a functional testing profile for the system under consideration. The diesel system testing is governed by existing NRC regulations. The diesels will be operated monthly, for at least one hour at a time. The diesels should reach stable voltage and frequency and be loaded at full load within five minutes during

monthly testing. No pre-planned starts will be made of the diesels with the pre-lubrication or heating systems inoperable. Once every two years, a loss of all ac power will be simulated, and the EDG's should start and assume load within 60 seconds. Following each diesel generator run, the DG loading should be gradually reduced over five to ten minutes, to allow the diesel to cool down. During all diesel operations, important diesel parameters will be recorded and subsequently reviewed. This will help to spot any abnormal trends in performance. Plant operating conditions will allow one diesel to be out of service, as long as the operable unit(s) are tested to ensure operability. This operability test will be required every three days, as opposed to the every day requirement that many plants currently have. This requirement will help to ensure that testing-induced wear of the diesels is minimized.

The primary emphasis of the diesel generator maintenance program will be preventive, determined through the RCM analysis. The RCM analysis takes the preventive maintenance recommendations of the FMECA, and designs the maintenance program for the system according to the possible failure consequences. Maintenance is one of the main areas that affects the operational reliability of the system. The preventive maintenance actions will also take into account the recommendations of the vendor's diesel generator

technical manual, and actions recommended by experts after studying past diesel operating history. Table 7 lists some expert recommended diesel surveillance needs.

Table 7
Expert Recommended Diesel Surveillance

Governor

Little can be done operationally to monitor the hydraulic governors on diesel engines. Two recommended static checks are: check the governor oil level, and check the linkage from the governor to the fuel racks, to ensure it operates smoothly and will prevent overspeed.

Cooling System Piping

The cooling system water level should be checked, along with the concentration of rust inhibitor (potassium chromate). The load and temperature change across the heat exchanger should be monitored for evidence of fouling.

Turbocharger

Turbocharger's critical failure modes are bearing failure, which can be caused by inadequate lubrication or rotor imbalance. Bearing temperatures should be monitored, as well as load versus rpm, and discharge pressure and temperature versus load.

Lubricating Oil Pump

The oil viscosity, engine load, and discharge pressure and temperature should be monitored.

Source: NUREG/CR-5078, Volume I, "A Reliability Program for Emergency Diesel Generators at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1988, p. 4-1.

Necessary corrective maintenance will be determined by the appropriate maintenance supervisor, after consulting with the Diesel Generator System Engineer. The adequacy of any corrective maintenance will be verified by appropriate re-testing. Any non-routine re-test, or re-test requiring special plant conditions to be established, will be performed only in accordance with a procedure prepared by the DG system engineer, with the approval of the plant maintenance department and the Plant Operating Review Committee. One important area of preventive maintenance is the cleaning of all areas housing diesel systems. Many failures recorded industry wide can be traced to a root cause of an unclean operating environment. All areas housing diesel system components will be thoroughly cleaned at least once a week.

Maintenance can be triggered by either time (following the detailed maintenance plan), or by conditions noted while performing other maintenance or surveillance. Maintenance actions will be prioritized for performance. In general, corrective maintenance needs will receive priority over preventive maintenance needs. Inputs to the prioritization process will include any special conditions required to perform the maintenance, anticipated maintenance durations, and the criticality of the problem from both a plant safety and personnel safety viewpoint. Any abnormal conditions, as well as any diesel failures, noted during testing or

maintenance will be evaluated for further surveillance requirements (e.g., increased lube oil consumption may call for checking the oil level more often).

The RCM analysis and the vendor's manual will require the diesels to undergo various degrees of preventive maintenance, including checks performed each shift (such as checking the starting air pressure), daily checks (e.g., system leak checks), weekly checks (such as oil level checks), monthly checks (such as lube oil sampling and analysis), and the more involved, less frequent maintenance such as complete diesel overhauls. The diesel system detailed maintenance plan will be developed based on primarily on the RCM analysis and the vendor's recommendations. Table 8 shows an example of a detailed diesel maintenance plan; this plan is for the IP3 EDG's. Table 8 was developed based on the "Engine Maintenance Schedules for Standby Engines in Use at Nuclear Power Plants" section of the Alco diesel generator technical manual (revised 2-24-89).

Table 8

Detailed Maintenance Plan for IP3 Diesel Generators

Maintenance to be performed with the engine in the standby condition:

Compressed Air System

Record starting air pressure (ES)
Record control air pressure (ES)
Check air compressor oil level (W)
Check oil level in the air start motor lubricator (W)

Cooling Water System

Record jacket water temperature (ES)
Record jacket water expansion tank level (ES)
Check system for leaks; check "telltale" piping (D)
Check coolant for rust inhibitor (BM)

Lube Oil System

Record lube oil temperature (ES)
Check lube oil heater power indicator light (ES)
Ensure pre-lube pump is operating (ES)
Record engine lube oil header pressure (ES)
Record engine crankcase oil level (ES)
Sample lube oil, check for water and sludge (M)

Fuel Oil System

Record day tank level (ES)
Check system for leaks (D)
Sample fuel, check for water and sludge (M)
Operate fuel oil priming system for five minutes (M)

Engine

Check governor oil level (ES)
Test all protection and alarm indicator lights (ES)

Note: Frequency abbreviations are on page 107

Table 8 (Continued)

Piping

Visually inspect all piping and components for deficiencies (leaks, not properly supported, etc.) (M)

Maintenance to be performed with the engine operating:

Compressed Air System

Record starting air pressure (H)
Record control air pressure (H)

Cooling Water System

Record jacket water temperatures (H)
Record jacket water expansion tank level (H)
Record jacket water pressure (H)
Check "telltale" drain pipes (ES)
Check system for leaks (ES)

Lube Oil System

Record lube oil temperature (H)
Record lube oil header pressure (H)
Record lube oil filter differential pressure (H)
Check system for leaks (ES)

Fuel Oil System

Record day tank level (H)
Record fuel oil header pressure (H)
Check system for leaks (ES)

Engine

Record engine room air inlet temperature (H)
Record cylinder exhaust temperature (H)
Record air manifold pressure (H)
Record engine crankcase vacuum (H)
Record engine loading (H)
Record engine RPM (H)

Table 8 (Continued)

Record fuel pump rack indication (H)
Note: Requires cover removal; read only one each hour, but different one each hour if more than one diesel is running
Check governor oil level (ES)
Record all cylinders fuel pump rack indication (S)
Record cylinder compression pressures (S)
Record crankshaft deflection and thrust (A)

Maintenance to be performed when the systems are not required to be operable:

Heat Exchangers

Inspect/clean raw water side (S)
Inspect/replace zinc anodes (S)

Compressed Air

Clean and lubricate air start motor (S)
Remove air start assembly and clean air start motor; use new seals and gaskets (3)
Remove/recondition air system relief valves, air start valves, and air pressure reducer (12)

Lube Oil

Clean lube oil strainer (A)
Check operation of engine low oil pressure circuit (2)
Drain/clean/refill lube oil system; inspect/clean cooler, sump, filter, and strainer (3)
Renew system hoses and couplings (12)
Clean lube oil cooler (12)
Remove/recondition regulating valves (12)
Remove/recondition lube oil priming pump (12)
Renew upper header check valves (12)
Remove/clean/test lube oil heaters (12)

Alarms, Instruments, and Gauges

Test engine alarms and controls (2)

Table 8 (Continued)

Recalibrate the following gauges: (A)
- Starting air pressure
- Jacket water pressure
- Air manifold pressure
- Fuel oil pressure
- Lube oil pressure
- Jacket water inlet pressure
- Raw water inlet temperature
- Jacket water outlet temperature
- Raw water outlet temperature
- Lube oil temperature
- Lube oil cooler inlet temperature
- Lube oil cooler outlet temperature
- Portable pyrometer

Cooling Water System

Check operation of high jacket water temperature circuit (2)
Drain/flush/refill system (6)
Remove/recondition temperature regulating valves (12)
Renew hoses and couplings (12)

Diesel Engine

Check uniformity of rack setting (A)
Check tightness of engine and generator hold down bolts (A)
Check fuel pump timing (A)
Inspect/clean air side of aftercooler (A)
Inspect/clean crankcase exhauster (A)
Drain/flush/refill governor oil (A)
Inspect turbocharger air intake (A)
Remove/recondition fuel injection nozzles (6)
Recondition governor; inspect governor drive and gear backlash (6)
Inspect/clean turbocharger (6)
Recondition fuel pumps (6)
Inspect cylinder heads and liners with boroscope (6)
Inspect camshaft (6)
Remove/inspect cylinder heads, piston liners; replace rod bearings and piston rings; replace all seals and gaskets (12)

Table 8 (Continued)

Fuel Oil System

Renew hoses and couplings (12)
Remove/recondition regulating valves (12)

Frequency abbreviation legend:

H - hourly
ES - once each shift
D - daily
W - weekly
BM - bimonthly
M - monthly
S - semiannually
A - annually
2 - every 2 years
3 - every 3 years
6 - every 6 years
12 - every 12 years

CHAPTER FOUR

DEVELOPMENT AND PRODUCTION TESTING

Task section 300 of MIL-STD-785B covers the reliability test program. The reliability test program must serve three objectives in the following priority: (1) disclose deficiencies in item design, materiel, and workmanship; (2) provide measured reliability data as input for estimates of operational readiness, mission success, maintenance manpower cost, and logistic support cost; and (3) determine compliance with quantitative reliability requirements. [34] Task section 300 contains four types of reliability testing; environmental stress screening and reliability development/growth tests, and reliability qualification and production reliability acceptance tests. The majority of the testing described in the MIL-STD-785B tasks takes place in the detail design phase, using a prototype unit. The ultimate objective of reliability testing is to determine that the system meets the specified MTBF requirement; to this end, the system is operated in a prescribed manner for a designated period and failures are recorded and evaluated as the test progresses. [35] This is the acceptance test performed on each unit manufactured and installed. According to MIL-STD-785B, a properly balanced reliability program will emphasize both environmental stress screening and reliability development/growth tests, and limit reliability qualification and production reliability acceptance tests.

One thing MIL-STD-785B does not consider is that planning for testing should begin in the conceptual design phase, because the system must be able to be evaluated against any and all specified requirements. A test and evaluation plan should be prepared early in the system life cycle that should include: Scheduling of tests, test requirements and conditions, test activity organization, test support requirements, and test procedures and required data.

Testing of the design should begin as soon as possible in the life cycle. Analytical evaluations of system design are performed in all three phases of system design identified in Table 1. As the design becomes more defined, individual components can also be tested. In the detail design phase, testing of mock-ups and engineering models should be performed. These tests are not formal demonstrations, but can yield useful information about logistic support of the system. Near the end of the design phases, testing of prototype units begins, as a check on the design process before production begins. Once units are produced, they undergo acceptance testing. During actual system use, testing is conducted to obtain knowledge about the true system capabilities while deployed in the operational environment.

Environmental Stress Screening

Task 301

The purpose of task 301 is to establish and implement environmental stress screening procedures so that early failures due to weak parts, workmanship defects, and other nonconformance anomalies can be identified and removed from the equipment. [36]

Environmental stress screening (ESS) testing shall be designed to stimulate relevant failures by stressing the item. [37] The system or items should be cycled through required operational modes while simulated environmental stresses are applied. The test conditions for ESS (also known as preconditioning) should concentrate on identifying early life cycle type failures, rather than simulating the precise operational environment the system or item will see. Environmental stresses (such as vibration and thermal cycling) may be applied in series rather than in combination.

Environmental stress screening should not be confused with reliability acceptance testing. ESS is recommended for 100% sampling; acceptance testing is not, due to the fact that it requires realistic simulation of the life cycle profile of the system. ESS is a prerequisite for reliability qualification and acceptance testing, because those test plans assume that "burn-in" type failures have

already been eliminated. The ESS will be conducted entirely by the diesel vendor, with all test results forwarded to the utility within five working days of test completion.

The diesel generator vendor will perform the ESS testing prior to shipment to the power plant site. The diesels will be tested on a test platform in a controlled environment. The test platform will have the diesel engine and generator mounted on it, along with the diesel control cabinets. This mounting arrangement will allow substantial vibration to be experienced by the diesel system components. Vibration effects on the diesel components would be of concern during normal operation, and even more so during a seismic event.

The diesel subsystems will undergo ESS testing through the representative subsystem configuration connected to the test platform. Each diesel engine and generator unit (including the prototype unit) will be tested on the platform for 100 hours of operation. The first 20 hours of operation will be at high humidities (70% or greater), with the ambient air quality similar to that found near the ocean or large salt water rivers. The next 30 hours of diesel operation will be at an ambient air temperature of 120°F. The next 20 hours of diesel operation will be conducted at an ambient air temperature 40°F. The preceding conditions are extremes of temperature and humidity. The operational profile for the diesels will be operation in a

climate-controlled structure, with the temperature between 55°F and 95°F, and relative humidity of less than or equal to 35%. The final 30 hours of operation for each diesel will be at normal temperature and humidity conditions, but a high level of dust, dirt, and grit in the diesel room ambient air. This condition will simulate the atmosphere expected at the new nuclear power plant construction site while the construction is in progress.

While the ESS testing is being conducted, the following parameters will be monitored and recorded hourly: air system pressure, cooling system temperature, pressure, and level, lube oil system temperature and pressure, fuel oil system pressure, engine air inlet and exhaust temperatures, air manifold pressure, crankcase vacuum, engine load and revolutions per minute, and vibration monitored at discrete points on the engine. Any abnormal trends or system failures during ESS testing will immediately be made known to the utility (and subcontractor if applicable). The failure review board will perform the required failure analysis and institute the required corrective actions before continuing with the reliability test program.

Reliability Development/Growth Test (RDGT) Program
Task 302

The purpose of task 302 is to conduct pre-qualification testing to provide a basis for resolving the majority of reliability problems early in the development phase, and incorporating corrective action to preclude recurrence, prior to the start of production. [38]

RDGT is a test, analyze, and fix process intended to disclose design deficiencies and defects, so they can be corrected prior to the beginning of full scale production. Reliability growth is expected in two distinct manners: (1) the screening of weak or substandard parts, and (2) the growth achieved by design corrections or modifications. The emphasis of this task is engineering corrective actions properly implemented. As stressed by MIL-STD-785B, reliability is not improved by testing itself, only by corrective actions that prevent the recurrence of failures.

An appropriate sequence for RDGT would be: (1) ESS to remove defects in test items, (2) environmental testing, and (3) combined-stress, life profile, test, analyze, and fix. [39] RDGT is conducted by the vendor, and it is intended to disclose failures.

The intent of RDGT is to test one of the first, full scale prototype units available, before production is entered into. For the diesel system, the main components

are the subsystems and the diesel generator itself. For the subsystems, the "prototype" will be the subsystem configuration connected to the test platform. The diesel generator prototype will be purchased by the utility for training purposes. The prototype unit will undergo 150 hours of RDGT testing; the 100 hours required for ESS plus an additional 50 hours. All diesel problems noted during this test sequence will corrected and retested prior to production beginning on the first diesel generator and associated subsystems. The incorporation of ESS and RDGT programs into the diesel reliability program are not meant to dissuade modifications from being performed once production or installation has begun; rather, these programs are intended to identify all design deficiencies and perform corrective actions prior to entering production, ensuring the highest reliability achieved at a lower cost than is possible if all modifications were performed after the units were produced.

Reliability Qualification Test (RQT) Program

Task 303

The purpose of task 303 is to determine that the specified reliability requirements have been achieved. [40]

For the reliability qualification test (RQT) program, utility personnel will test the prototype diesel generator and subsystems, at the vendor's facility, using the test platform. The RQT provides the utility with an evaluation of diesel system development progress, and assurance that the specified requirements have been met prior to proceeding to production of the units. Figure 15 illustrates a typical approach to an RQT program. The system is operated under specified operating conditions over an extended period of time, while being monitored for the occurrence of failures. Failures are noted (events), the root cause is determined and corrected, and testing is continued. The approach to testing used will be testing of the prototype unit. The specified MTBF of each diesel was 27,374 hours.

For the diesels, the complete diesel generator and associated subsystems will be tested, and failures recorded, to determine whether or not the MTBF requirement of approximately 28,000 hours for each individual diesel is met. The prototype diesel will be operated on the test platform. The environment will be maintained between 55°F and 95°F, with relative humidity less than or equal to 35%.

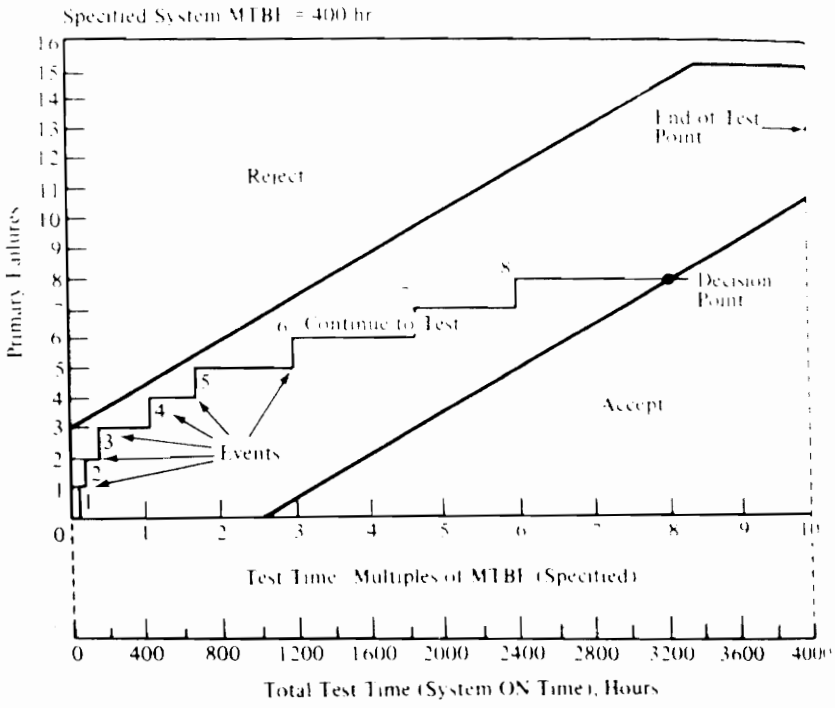


Figure 15. Reliability Qualification Testing

Source: Blanchard, Benjamin S., and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981, p. 364.

The diesel will be started, loaded, and run for one hour at a time, 24 hours per day, seven days a week until 3000 hours of run time are accumulated (this should take about five months). Ten of every 11 starts will be manual starts, and the eleventh will be "automatic", in response to a simulated loss of bus voltage. Assuming 25 demands per diesel per year in operation (and 24 hours of run time) gives a total lifetime run time of 750 hours over 30 years. The RQT time will be four times that amount. At 215 days per year, 24 hours per day, 28,000 hours (MTBF) would be accumulated after about five and one-half years. Therefore, the test simulates about 120 years of operation, or about 20 times the required MTBF. This seems to be a lot of testing, but the limitations of the test assumptions must be examined. The 750 lifetime run hours for the diesels is only a good approximation for the diesel generator itself, and the fuel oil, instrumentation and control, and starting air systems. The jacket water cooling and lube oil systems are really in operation 5160 hours per year (215 days per year, 24 hours per day), keeping the diesel in a standby condition. This limitation is acceptable; most of the FMECA identified "catastrophic" failures do not come from the lube oil or air systems.

Production Reliability Acceptance Test (PRAT) Program
Task 304

The purpose of task 304 is to assure that the reliability of the hardware is not degraded as the result of changes in tooling, processes, work flow, design, parts quality, or any other characteristics. [41]

Production reliability acceptance tests (PRAT) are intended to be realistic simulations of operational equipment conditions. PRAT's are usually based on a statistical quality control sampling plan method. A certain percentage of each production lot would be sampled to assess the MTBF, with statistical assurance that the sample's conditions represent the condition of the whole lot.

For the diesel generator system, required testing has been specified by the NRC in Reg. Guide 1.9. The NRC has determined that 100% sampling be performed. This is partly due to the limited production quantities, and partly due to the safety importance of the EDG's. The NRC required testing is 69 diesel starts per plant, a minimum of 23 or 69/n tests per diesel (n = number of diesels at site), without a failure to start. Also required by the NRC is testing (once) to ensure the diesels can start and achieve proper voltage and frequency after shutdown from a two hour run at full load.

Once the diesel system is operational, the number of diesel starts, load-runs, and failures will be tabulated, for the last 20, 50, and 100 starts, as the NRC desires. To get a true picture of diesel operation, total operational time will be recorded, along with any diesel failures, and maintenance times, so that an actual MTBF, and diesel availability, can be determined.

CHAPTER 5

SUMMARY AND CONCLUSIONS

The purpose of this report is to describe a proposed nuclear power plant diesel generator reliability program based on the requirements of MIL-STD-785B. The descriptions used to illustrate various portions of the report are based on the diesel system configuration of the Indian Point 3 Nuclear Power Plant. The calculations used for illustration are based on a composite of data reported to the NRC by various utilities. The NRC is requiring a reliability program for equipment for which a true reliability program was not formally considered during any part of the design and construction; therefore what the NRC wants is really a strong maintenance and logistic support program coupled with an ongoing assessment of some measure of reliability.

The reliability program described herein follows the tasks in MIL-STD-785B, although it does not cover each task in to the same degree. In actual applications, not all tasks described by MIL-STD-785B would be applicable. An effective reliability program based on the military standard would be tailored to fit the programs needs and constraints, including the systems life cycle cost. Life cycle cost was not the focus of this report, so it was mentioned only briefly. In real applications, the importance of life cycle cost can not be overemphasized. Each decision made in the development of a system should be examined from a life cycle

cost standpoint. Decisions made early in the system life cycle can have tremendous cost impact further on in the system life cycle. Throughout the development of the system, design for supportability (including reliability) has a large impact on the resources required down the road for system support. Logistics, cost, and performance factors are the factors which systems engineering attempts to balance, while transforming a need into a preferred system design, always looking at the total life cycle. System reliability and maintainability have a large impact on consumption of resources during operation, such as repair parts and test equipment, and therefore on logistic support cost.

As stated, the focus of this report is system reliability. Another aspect of system development that needs to be mentioned is the interface of various disciplines during system development. While designing for system reliability, care must be taken not to overlap other tasks, such as quality assurance and logistic support analysis, so that the system's cost effectiveness is not reduced.

Before attempting to institute a "reliability" program in response to the NRC's desires, utilities must make sure they have a good understanding of what reliability actually is (an inherent design characteristic) and what it is not. The nuclear industry as a whole has much to gain by

understanding and utilizing knowledge of systems engineering principles, both in terms of operational costs and system performance.

One conclusion to be drawn from this report is that the Emergency Diesel Generator I&C system, and diesel governors in particular, really need to be reviewed for reliability improvement. The I&C area should be seriously looked at for both operational systems and systems being designed. The second area that should be reviewed is maintenance. An FMECA/RCM analysis should be performed, and the preventive maintenance program should be tailored based on the failure consequences identified in the FMECA/RCM analysis.

WORKS CITED

[1] Regulatory Guide 1.155, "Station Blackout," U. S. Nuclear Regulatory Commission, Washington, D. C., August 1988, p. 1.155-3.

[2] "Market Study," Nuclear News, American Nuclear Society, La Grange Park, Illinois, December 1989, p. 72.

[3] Indian Point Station, Unit No. 3, System Description No. 27.3, "Emergency Diesels," August 1985, p. 3.

[4] Ibid, p. 3.

[5] Indian Point Station, Unit No. 3, System Description No. 27.1, "Electrical Systems," October 1988, p. 134.

[6] Blanchard, Benjamin S., Logistics Engineering and Management, Prentice Hall, Inc., Englewood Cliffs, New Jersey, Third Edition, 1986, p. 9.

[7] MIL-STD-785B, Military Standard, "Reliability Program, Systems and Equipment Development and Production," Department of Defense, Washington, D.C., September 15, 1980, p. 4.

[8] Ibid, p. A-2.

[9] Blanchard, Benjamin S., and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981, p. 493.

[10] Proposed Revision 3 to Regulatory Guide 1.9, "Selection, Design, Qualification, Testing, and Reliability of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., November 1988, p. 3.

[11] MIL-STD-785B, p. A-4.

[12] Ibid, p. 101-1.

[13] Ibid, p. 102-1.

[14] Ibid, p. 103-1.

[15] Blanchard and Fabrycky, p. 293.

[16] MIL-STD-785B, p. 104-1.

Works Cited (Continued)

[17] Ibid, p. 105-1.

[18] Ibid, p. A-11.

[19] Ibid, p. 201-1.

[20] Ibid, p. 202-1.

[21] Blanchard and Fabrycky, pp. 341 and 342.

[22] MIL-STD-785B, p. 203-1.

[23] Blanchard and Fabrycky, pp. 355 and 356.

[24] MIL-STD-785B, p. 204-1.

[25] Blanchard and Fabrycky, pp. 353 and 354.

[26] MIL-STD-785B, p. 205-1.

[27] Ibid, p. 206-1.

[28] Ibid, p. 207-1.

[29] Ibid, p. A-19.

[30] Blanchard and Fabrycky, pp. 345 and 346.

[31] MIL-STD-785B, p. 208-1.

[32] Blanchard and Fabrycky, p. 353.

[33] MIL-STD-785B, p. 209-1.

[34] Ibid, p. A-23.

[35] Blanchard and Fabrycky, p. 358.

[36] MIL-STD-785B, p. 301-1.

[37] Ibid.

[38] Ibid, p. 302-1.

[39] Ibid, p. A-29.

[40] Ibid, p. 303-1.

[41] Ibid, p. 304-1.

APPENDIX

List of Abbreviations

AC	Alternating current
Con Ed	Consolidated Edison Company, Incorporated
DG	Diesel Generator
EDG	Emergency Diesel Generator
ESS	Environmental stress screening
FMECA	Failure mode, effect, and criticality analysis
FRB	Failure review board
HX	Heat exchanger
I & C	Instrumentation and control
IP2	Indian Point 2 Nuclear Power Plant
IP3	Indian Point 3 Nuclear Power Plant
JAF	James A. FitzPatrick Nuclear Power Plant
KW	Kilowatt
λ (lambda)	Failure rate
LCC	Life cycle cost
MIL-STD	Military standard
MTBF	Mean time between failure
NRC	U. S. Nuclear Regulatory Commission
NYPA	New York Power Authority
OERG	IP3 Operational experience review group
PORC	IP3 Plant operating review committee
PRAT	Production reliability acceptance test
R	Reliability
RCM	Reliability-centered maintenance
RDGT	Reliability development/growth test
Reg. Guide	U.S. NRC Regulatory guide
RPM	Revolutions per minute
RQT	Reliability qualification test
SBO	Station Blackout
TSS	IP3 Technical Services Superintendent

VITA

Kenneth John Peters was born in Paterson, New Jersey on October 1, 1959. He graduated from high school in June, 1977, and pursued an engineering education at the New Jersey Institute of Technology (NJIT). He received a Bachelor of Science in Electrical Engineering from NJIT in May, 1982. He began graduate study in Systems Engineering at Virginia Polytechnic Institute and State University in September, 1985.

Mr. Peters began his career at Newport News Shipbuilding as an Electrical Test Engineer in June, 1982. In 1985, he became a qualified Shift Test Engineer, responsible for the direction of 688-Class submarine reactor plant testing and operation.

Mr. Peters joined the New York Power Authority as a Licensing Engineer in June, 1989. His responsibilities include ensuring compliance with the Indian Point 3 Nuclear Power Plant operating license, developing modifications and submitting schedules to meet commitment dates, and negotiating licensing requirements.

Mr. Peters is a member of the Institute of Electrical and Electronics Engineers.

Kenneth J. Peters

Kenneth J. Peters