Unclassified **NEA/CSNI/R(2000)20**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 19-Feb-2001
Dist. : 21-Feb-2001

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2000)20
Unclassified

ICDE Project Report on Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators

May 2000

English text only

99339

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

* * * * * * * * * * *

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France

ICDE Project Report: Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators

T. E. Wierman
D. M. Rasmuson, USNRC
F. M. Marshall

May 17, 2000

Idaho National Engineering and Environmental Laboratory
Nuclear Operations Support Programs Department
Lockheed Martin Idaho Technologies Company
Idaho Falls, Idaho 83415

Prepared for the Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington D.C. 20555

ABSTRACT

This report documents a study performed on the set of common cause failures (CCF) of emergency diesel generators (EDG). The data studied here were derived from the International CCF Data Exchange (ICDE) database, to which several countries have submitted CCF event data. The data span a period from 1982 through 1997. The purpose of the ICDE is to allow multiple countries to collaborate and exchange CCF data to enhance the quality of risk analyses that include CCF modeling. Because CCF events are typically rare events, most countries do not experience enough CCF events to perform meaningful analyses. Data combined from several countries, however, yields sufficient data for more rigorous analyses. This report is the result of an in-depth review of the EDG events and presents several insights about them. The objective of this document is to look beyond the CCF parameter estimates that can be obtained from the CCF data, to gain further understanding of why CCF events occur and what measures may be taken to prevent, or at least mitigate the effect of, EDG CCF events. The report presents details of the ICDE project, a quantitative presentation of the EDG events, and a discussion of some engineering aspects of the events.

TABLE OF CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

This study examined 106 events in the International CCF Data Exchange (ICDE) database by tabulating the data and observing trends. Once trends were identified, individual events were reviewed for insights.

The database contains information developed during the original entry of the events that was used in this study. The data span a period from 1982 through 1997. The data is not necessarily complete for each country through this period. This information includes root cause, coupling factor, common cause component group (CCCG) size, and corrective action. As part of this study, these events were reviewed again and additional categorizations of the data were included. Those categories included the degree of failure, affected subsystem, and detection method.

This study begins with an overview of the entire data set (Section Five). Charts and tables are provided exhibiting the event count for each of these event parameters. This section forms the baseline for the EDG component.

Section Six contains charts that demonstrate the distribution of the same events further refined by failure mode (fail-to-run and fail-to-start) for each event parameter. Each of these charts is replicated with the further distinction that only those events classified as *complete* are included. Distinctions are drawn as these parameters shift.

Section Seven contains charts that demonstrate the distribution of events even further refined into groups of root causes. Each root cause group is analyzed independently. Events within each root cause group are studied together to identify similarities and differences within the group based on the remaining parameters. These distributions are also compared with the distributions developed in previous sections.

Section Eight is similar to Section Seven except that the events are grouped by subsystem rather than root cause.

This study took place using four different means of combining the same data. Each data combination produced results that were unique to that particular view as well as a degree of commonality between these combinations.

The overall view of the ICDE EDG CCF events provided a baseline set of parameters, which were then compared to the various more detailed groupings. The similarities and differences between these provide insights.

The largest set of *complete* failures (62 percent) occurs in the fail-to-start group. This contradicts the overall distribution, which shows that the set of all EDGs have 45 percent of events as fail-to-start. The data supports the conclusion that CCF events tend to have impairment vector values of less than “C” for those events categorized as fail-to-run and more events with a “C” for the fail-to-start. Fail-to-start also tends to be a stronger failure mode.

The most likely root cause is design, manufacture, or construction inadequacy (43 percent). This is consistent with CCF analysis since the most effective mechanism to fail multiple redundant components is to mechanically introduce a fault into each one. Most of the

complete design faults are in the instrumentation and control subsystem, which contributes a significant portion of its CCFs to the fail-to-start mode. It should be noted that the design category includes events that were faults of the initial design as well as modifications made subsequent to the original installation. These are powerful mechanisms to introduce CCF to a piece of equipment.

The term vibration is used in the event description repeatedly. In the course of this study, it was determined that vibration is not a root cause, but is a manifestation of another more basic failure. Most events that used the term vibration were categorized as design faults. Generally, the design should take into account the large amount of vibration that occurs during EDG operation. The next most common root cause for vibration is environment. The original analyst assumed that the high vibration environment was the cause of the event.

Hardware is the dominant coupling factor (55 percent) and design modification is the most common possible corrective action (26 percent). These are consistent with design being the dominant root cause.

This category is worth mentioning because it is so prevalent. The instrumentation and control subsystem is especially vulnerable to CCF from the human factor, due to the complexity and the function of instrumentation and control. Procedures, maintenance, and operations all contribute to this root cause.

The distribution of CCF events by the CCCG size of the event indicates that the largest contributors are from CCCG sizes two and four. These are consistent with the distribution of the installed CCCGs. The general shape of the distributions of CCF events by CCCG size is similar between the actual distribution of counts of plants with those numbers of EDGs installed. However, a subtle shift occurs where the count of CCFs of two EDGs is slightly higher than the installed count and is slightly lower in the count of three and four EDGs. This becomes exaggerated when the *complete* CCF events are considered. Over 70 percent of *complete* CCF events are in CCCG size two systems. This behavior is consistent with CCF theory, which believes that the observation of 2-out-of-2 components failing due to CCF should be more likely than 3-out-of-3 or 4-out-of-4 components failing due to CCF.

Testing is the primary way to detect CCF failures. It is interesting to note that the inspection method of *complete* detection, represented in the set of all CCF events, is not represented in the set of *complete* CCF events. This is due to the nature of faults detected by inspection. The most common failure detected by inspection is leakage of a minor nature.

Cooling, engine, and fuel oil are most likely to result in fail-to-run. Instrumentation and control, output breaker, and starting are most likely to result in a fail-to-start. This does not shift significantly between all CCFs and *complete* CCFs. Cooling and engine become much less significant and the instrumentation and control and fuel oil become much more significant. The instrumentation and control contribution is consistent with the nature of that system since it controls the shutdown and control of the EDG. The fuel oil subsystem shifts from mostly fail-to-run to all fail-to-start between the all CCF case and the *complete* CCF case. This is primarily due to most of the fuel oil fail-to-run events involving minor leaks.

The instrumentation and control subsystem is a complicated and diverse system that contains the functions of shutdown and control. Therefore, small errors can propagate into *complete* failures of the EDG component. This subsystem has experienced many design modifications.

ACRONYMS

BWR	boiling water reactor
CCCG	common cause component group
CCF	common cause failure
CSNI	Committee for Scientific Nuclear Installations
ECCS	emergency core cooling system
EDG	emergency diesel generator
I&C	instrumentation and control
ICDE	International Common Cause Failure Data Exchange
IRS	Incident Reporting System
LOCA	loss-of-coolant accident
LOSP	loss of offsite power
MCC	motor control centers
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
OECD	Organization for Economic Cooperation and Development
PSA	probabilistic safety assessment
PWG1	Principal Working Group 1
PWR	pressurized water reactor
RPS	reactor protection system

ICDE Project Report
Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators

1. INTRODUCTION

This report presents an overview of the exchange of emergency diesel generator (EDG) common cause failure (CCF) data among several countries. The objectives of this report are the following:

- To describe the data profile in the ICDE database for emergency diesel generators and to develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors, and corrective actions; and

- To develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes, and possibilities for improvement.

The ICDE Project was organized to exchange CCF data among countries. A brief description of the project, its objectives, and the participating countries is contained in Section Two. Section Three presents a definition of common cause failure. Section Four presents a description of the emergency diesel generator and a short description of the subsystems that comprise it. An overview of the data is presented in Section Five. Section Six contains a description of the data by failure mode and also a comparison of *complete* CCF events with all of the events collected in this effort. Section Seven discusses the events by root cause, and Section Eight summarizes the events by subsystem. A summary and conclusions are presented in Section Nine.

2. ICDE PROJECT

This section contains information about the ICDE Project.

2.1 Background

Several member countries of OECD/NEA established the ICDE Project to encourage multilateral co-operation in the collection and analysis of data relating to CCF events.

The project was initiated in August 1994 in Sweden and was discussed at meetings in both Sweden and France in 1995. A coding benchmark exercise was defined which was evaluated at meetings held in Germany and in the US in 1996. Subsequently, the exchange of centrifugal pump data was defined; the first phase of this exchange was evaluated at meetings in Switzerland and in France in 1997.

The pilot activity was financially supported by SKI, Sweden, from its initiation to March 1998, and partly by GRS, Germany, from initiation to December 1995. As of April 1998, the project is formally operated by OECD/NEA.

The ICDE project is operated under the umbrella of the OECD/NEA whose representative for this purpose is the Secretariat for Principal Working Group 1 (PWG1).

The ICDE project member countries and their sponsoring organisations are:

- Canada : AECB
- Finland : STUK
- France : IPSN
- Germany : GRS
- Spain : CSN
- Switzerland : HSK
- United Kingdom: NII
- United States : NRC

Other countries have recently expressed their interest to participate.

2.2 Objectives of the ICDE Project

The objectives of the ICDE project are:

- To collect and analyse CCF events in the long term so as to better understand such events, their causes, and their prevention.

- To generate qualitative insights into the root causes of CCF events, which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.

- To establish a mechanism for the efficient feedback of experience gained on CCF phenomena, including the development of defences against their occurrence, such as indicators for risk based inspections.

2.3 Scope of the ICDE Project

The ICDE Project is envisaged as including all possible events of interest, comprising *complete*, *partial*, and incipient CCF events, called "ICDE events" in this report. The project covers the key components of the main safety systems, including centrifugal pumps, diesel generators, motor operated valves, power operated relief valves, safety relief valves, check valves, reactor protection system (RPS) circuit breakers, batteries and transmitters.

In the long term, a broad basis for quantification of CCF events could be established, if the participating organisations wish to do so.

2.4 Reporting and Documentation

All reports and documents related to the ICDE project can be accessed through the ES-Konsult web site [2].

2.5 Data Collection Status

Data are collected in an MS ACCESS based databank implemented and maintained at ES-Konsult, Sweden, the appointed NEA clearing house. The databank is regularly updated. The clearinghouse and the project group operate it.

2.6 ICDE Coding Format and Coding Guidelines

An ICDE coding format was developed for collecting the ICDE event data for the ICDE database. Definition and guidance are provided in the ICDE coding guidelines [3].

2.7 Protection of Proprietary Rights

Incident Reporting System (IRS) procedures for protecting confidential information have been adopted. The co-ordinators in the participating countries are responsible for maintaining proprietary rights. The data collected in the clearinghouse database are password protected and are only available to ICDE participants who have provided data.

3. DEFINITION OF COMMON-CAUSE EVENTS AND ICDE EVENTS

In the modelling of common-cause failures in systems consisting of several redundant components, two kinds of events are identified:

Unavailability of a specific set of components of the system, due to a common dependency, for example on a support function. If such dependencies are known, they can be explicitly modelled in a PSA.

Unavailability of a specific set of components of the system due to shared causes that are not explicitly represented in the system logic model. Such events are also called "residual" CCFs, and are incorporated in PSA analyses by parametric models.

There is no rigid borderline between the two types of CCF events. There are examples in the PSA literature of CCF events that are explicitly modelled in one PSA and are treated as residual CCF in other PSAs (for example, CCF of auxiliary feed-water pumps due to steam binding, resulting from leaking check valves).

Several definitions of CCF events can be found in the literature, for example, "Common Cause Failure Data Collection and Analysis System, Vol. 1, NUREG/CR-6268": [4]

Common-Cause Event: A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.

Data collection in the ICDE project comprises *complete* as well as potential CCF. To include all events of interest, an "ICDE event" is defined as follows:

ICDE Event: Impairment[1] of two or more components (with respect to performing a specific function) that exists over a relevant time interval[2] and is the direct result of a shared cause.

The ICDE data analysts may add interesting events that fall outside the ICDE event definition but are examples of recurrent - eventually non random - failures.

With growing understanding of CCF events, the relative share of events that can only be modelled as "residual" CCF events will decrease.

---

[1] Possible attributes of impairment are the following:

- Complete failure of the component to perform its function
- Degraded ability of the component to perform its function
- Incipient failure of the component

Default is component is working according to specifications.

[2] Relevant time interval: two pertinent inspection periods (for the particular impairment) or if unknown, a scheduled outage period.

4. COMPONENT DESCRIPTION

4.1 System Description

The EDGs are part of the class safety-related ac electrical power distribution system providing reliable emergency power to electrical buses that supply the emergency core cooling system (ECCS) and various other equipment necessary for safe shutdown of the reactor plant. In general, each EDG configuration ensures that adequate electrical power is available in a postulated loss-of-offsite power (LOSP), with, or without a concurrent large break loss of coolant accident (LOCA). Gas turbine generators and hydroelectric generators (used at some locations for emergency power) are not part of this study. High-pressure core spray diesels are considered (for this study) to be a separate train of the emergency ac power system. Diesel engines used for fire pumps, and other non safety-related backup generators are not included.

The EDGs are normally in standby, whether the plant is at power or shutdown. At least one EDG is required by Technical Specifications to be aligned to provide emergency power to safety related electrical buses in case of a LOSP to the plant. In some cases a "swing" EDG is used to supply power to more than one power plant (but not simultaneously). The result is that two power plants will have a total of only three EDGs: one EDG dedicated to each specific power plant, and the third, a swing EDG, capable of powering either plant. Electrical load shedding (intentional load removal) of the safety bus and subsequent sequencing of required loads after closure of the EDG output breaker, is considered part of the EDG function. The EDG system is automatically actuated by signals that sense either a loss of coolant accident or a loss of, or degraded, electrical power to its safety bus. The control room operator accomplishes manual initiation of the EDG system if necessary.

4.2 Component Boundaries

The super component, EDG, is defined as the combination of the diesel engine(s) with all components in the exhaust path, electrical generator, generator exciter, output breaker, combustion air, lube oil systems, cooling system, fuel oil system, and the starting compressed air system. All pumps, valves and valve operators with their power supply breakers, and associated piping for the above systems are included. The only portions of the EDG cooling systems included were the specific devices that control cooling medium flow to the individual EDG auxiliary heat exchangers, including the control instruments. The service water system outside the control valves was excluded. The EDG room ventilation was included if the licensee reported ventilation failures that affected EDG functional operability. Figure 4-1shows the component boundary as defined for this study.

Included within the EDG system are the circuit breakers that are located at the motor control centers (MCC) and the associated power boards, that supply power specifically to any of the EDG equipment. The MCCs and the power boards are not included except the load shedding and load sequencing circuitry/devices that are, in some cases, physically located within the MCCs. Load shedding of the safety bus and subsequent load sequencing onto the bus of vital electrical loads is considered integral to the EDG function and is therefore considered within

the bounds of this study. All instrumentation, control logic, and the attendant process detectors for system initiations, trips, and operational control are included. Batteries were included if failures impacted EDG functional operability.

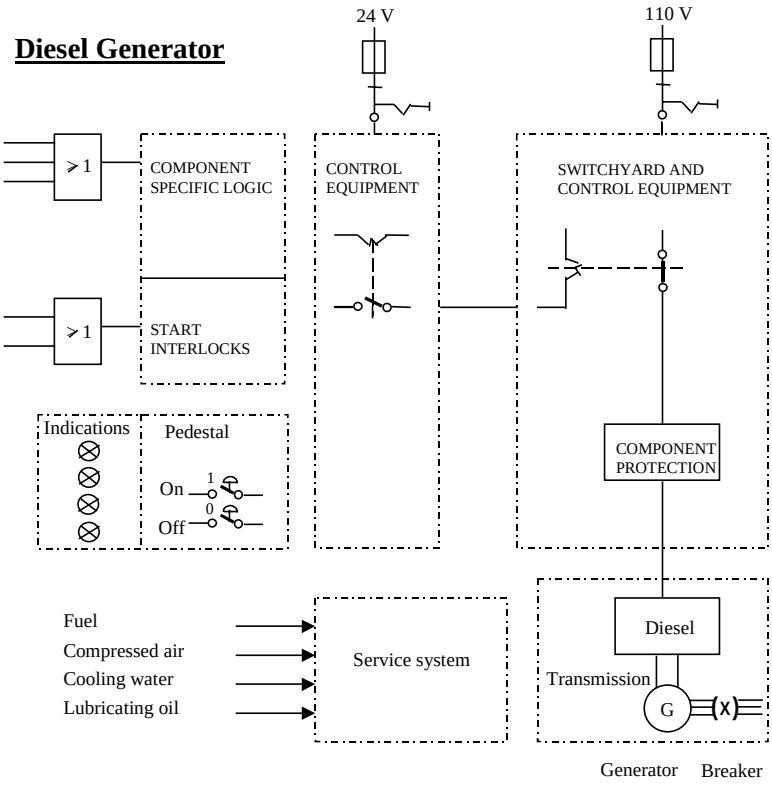


Figure 4-1. Emergency diesel generator and subsystems.

4.3 Subsystem Descriptions

This section contains a brief description of each of the subsystems that comprise the emergency diesel generator. These descriptions are intended only to provide a general overview of the most common EDGs.

4.3.1 Breaker

The breaker subsystem includes the main EDG output breaker as well as the loading and sequencing circuitry. The automatic load shedding and sequencing controls the order and timing of emergency loads that are loaded onto the safety-related bus. The purpose of this equipment is to prevent the instantaneous full loading (ECCS loads during a LOCA event) of the engine when the output breaker is closed.

4.3.2 Combustion Air

The combustion air subsystem receives air from the outside and passes it to the EDG through a filter and a damper.

4.3.3 Cooling

The cooling subsystem is a closed-loop water system that is integral to the engine and generator, and has an external-cooling medium, typically, the plant emergency service water. The pumps, heat exchangers, and valves are part of this system. The cooling water jacket is part of the Engine subsystem.

4.3.4 Engine

The engine subsystem is the physical engine block and piece-parts internal to it. These parts include pistons, crankshafts, turbochargers, cooling water jackets, and the governor. The engine governor maintains correct engine speed by metering the fuel oil to each cylinder injector.

4.3.5 Exhaust

The exhaust subsystem consists of the piping and valves installed to direct the engine exhaust out of the building.

4.3.6 Fuel Oil

The fuel oil subsystem provides fuel oil from large external storage tanks, having a capacity for several days of system operation, to a smaller *day* tank for each engine. The day tank typically has capacity to operate the engine for 4 to 6 hours. Day tank fuel is supplied to the cylinder injectors, which inject the fuel to each individual cylinder for combustion.

4.3.7 Generator

The generator subsystem consists of the generator casing, rotor, windings, and exciter. These components all function to deliver electrical power to the output breaker.

4.3.8 Instrumentation & Control

The instrumentation and control I&C) subsystem components function to start, stop, and provide operational control and protective trips for the EDG. Controls for the EDGs are a mix of pneumatic and electrical devices, depending on the manufacturer. These function to control the voltage and speed of the EDG. Various safety trips for the engine and generator exist to protect the EDG. During the *emergency start* mode of operation, some of these protective trips associated with the EDG engine are bypassed.

4.3.9 Lubrication Oil

The lubrication oil subsystem is closed loop system integral to the engine and generator, consisting of a sump, various pumps, and a heat exchanger.

4.3.10 Starting Air

The starting air subsystem consists of those components required to start the EDG. Typically, this system uses compressed air. The air start system provides compressed air to the engine through a system of valves, relief valves, compressed gas cylinders, air motor, and a distributor.

5. OVERVIEW OF DATABASE CONTENT

CCF data for the EDG component have been collected. Organisations from Finland, France, Germany, Sweden, Switzerland, United Kingdom and the United States contributed data to this data exchange. One hundred fifteen (115) ICDE events were reported from nuclear power plants [pressurized water reactor, boiling water reactor, Magnux, and AGR]. The data span a period from 1982 through 1997. The data is not necessarily complete for each country through this period. Six events were reported and classified as interesting events, but they were not CCF events and are not included in this study. One event was classified as a failure to stop, another did not have enough information to classify, and another was not in the time period of this study. These events are not included in this study. Table 5-1 summarises, by failure mode, the EDG CCF events used in this study. *Complete* CCF events are CCF events in which each component fails completely due to the same cause and within a short time interval. All other events are termed *partial* CCF events. A subclass of *partial* CCF events are those that are *almost-complete* CCF events. Examples of events that would be termed *almost-complete* are those events in which all but one of the components are completely failed and one component is degraded, all components are completely failed but the time between failures is greater than an inspection interval.

Table 5-1. Summary statistics of emergency diesel generator data.

Event reports received	Total	Degree of Failure Observed		
		Partial	Almost-Complete	Complete
ICDE events				
Failure to run	61	46	10	5
Failure to start	45	22	11	12
Total	106	68	21	17

Figure 5-1 shows the distribution of CCF events by root cause. The dominant root cause, design or manufacture, or construction inadequacy, accounts for about 43 percent of the events. The CCF events are about equally distributed among the other causes. Section 7 provides an in-depth analysis of the root cause distribution.

Figure 5-2 shows the coupling factor distribution for the events. Hardware is the largest coupling factor (55 percent). Environmental (17 percent) and operational (28 percent) couplings account for the remaining events.

Figure 5-3 shows the distribution of identified possible corrective actions for CCF events. Design modifications rank highest, accounting for 26 percent of the corrective actions. Administrative/ procedural actions rank next accounting for about 17 percent of the actions. The remaining actions are about equally distributed among the remaining actions.

Figure 5-4 shows the distribution of the events by CCCG size. The CCCG size ranges from two to eight. The majority of the group sizes are two, three, or four. The distribution of installed EDGs is given here for reference.

Table 5-2. Installed EDG distribution.

CCCG Size	Number of CCCG	Percent
1	3	1%
2	116	50%
3	42	18%
4	63	27%
5	6	3%
6	1	<1%
7	0	0%
8	1	<1%
Total	232	100%

Figure 5-5 shows the distribution of how the events were discovered or detected. Testing accounts for 67 percent of the events and inspection 21 percent. Only 13 events were discovered during an actual demand or during maintenance activities.

Figure 5-6 shows the distribution of the CCF events by EDG subsystem. The majority (86 percent of the CCF events) is involved with the cooling, engine, fuel oil and instrumentation and controls subsystems. Section 8 provides an in-depth analysis of the subsystems.

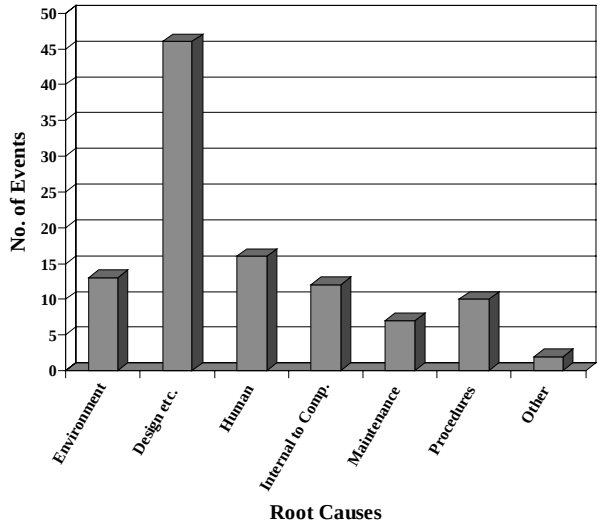


Figure 5-1. Root cause distribution**.**

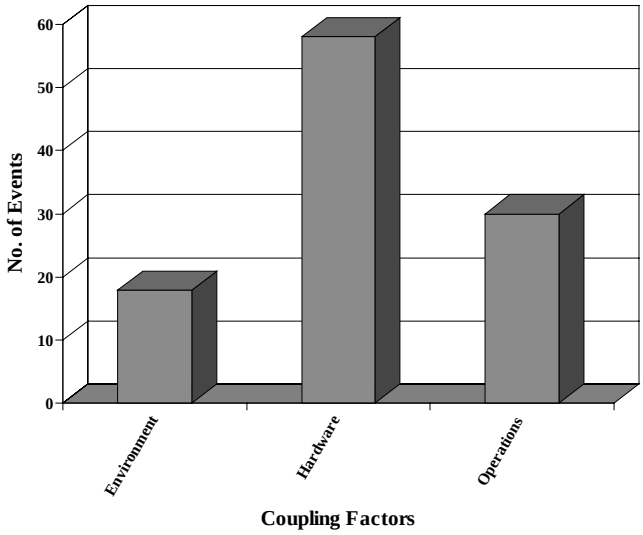


Figure 5-2. Coupling factor distribution.

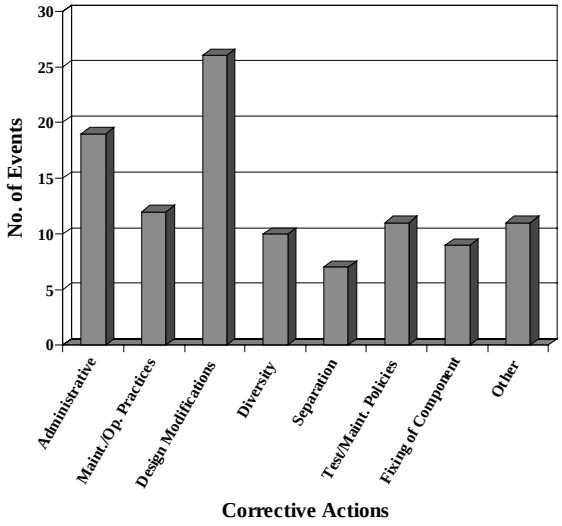
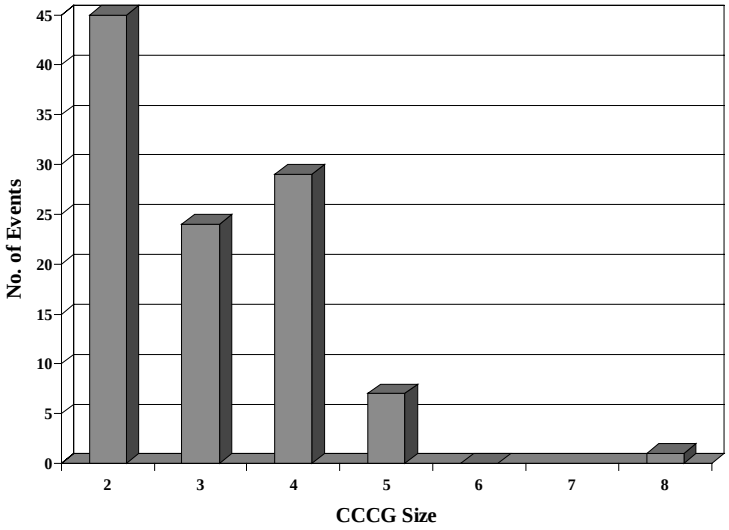


Figure 5-3. Corrective action distribution.



.

Figure 5-4. CCCG size distribution.

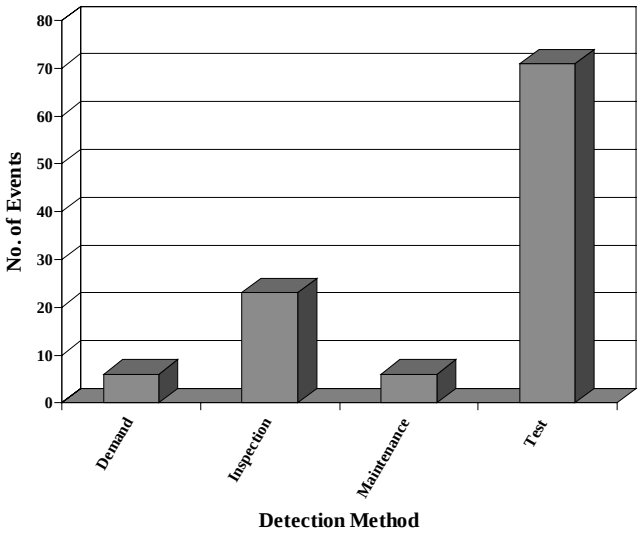


Figure 5-5. Detection method distribution.

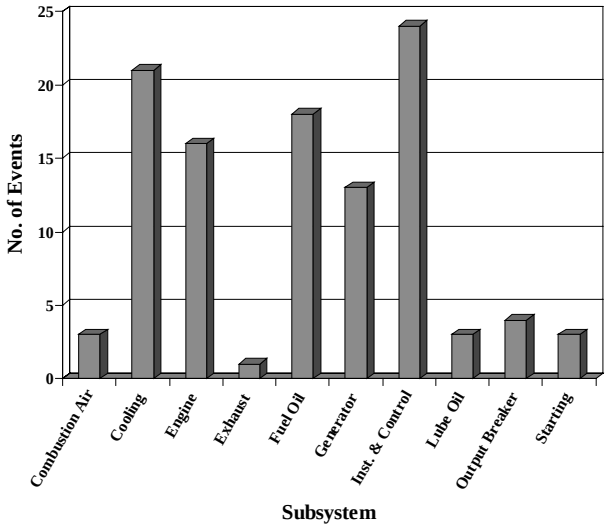


Figure 5-6. Subsystem distribution.

6. SUMMARY OF EVENTS BY FAILURE MODE AND DEGREE OF FAILURE

This section discusses the CCF events by failure mode and contrasts the distributions of complete CCF events with the distributions of the total group. A discussion of degree of failure is included in Section 5.

Figure 6-1 and Figure 6-2 show the distributions of CCF events for root causes for all events and *complete* CCF events by failure mode. The design root cause contribution is the most important and maintains its importance from the total group to the group of *complete* CCF events. However, the composition between fail-to-start and fail-to-run shifts from more fail-to-run events to approximately the same number of fail-to-run and fail-to-start events. Most of the *complete* design faults are in the I&C subsystem, of which most of the CCF events are fail-to-start mode. These faults were spread out evenly over original design errors and design modification errors.

The human error root cause category increases in importance between all events and the set of *complete* CCF events. They also exhibit a shift from an even number of fail-to-start and fail-to-run events to more fail-to-start events. The human errors contributing to this phenomenon include mis-positioned valves, inadvertent switch operation, and a design modification error.

Figure 6-3 and Figure 6-4 show the distributions of CCF events for coupling factors for all events and *complete* CCF events by failure mode. The increase of importance of the operations coupling factor group is also consistent with the dominant root causes. Again, the human element is most likely to participate in the fail-to-start mode.

Figure 6-5 and Figure 6-6 show the distributions of CCF events for corrective actions for all events and *complete* CCF events by failure mode. The most important corrective action identified in this study is design modifications. This is consistent with the observed dominant root cause. Again, the composition between fail-to-start and fail-to-run shifts from mostly fail-to-run for the set of all events to an even number of fail-to-start and fail-to-run for the set of *complete* events for the design modifications corrective action. Improving procedures becomes important as a corrective action for the *complete* CCF events fail-to-start. This is consistent with the human error being a high contributor to the root cause distribution.

Figure 6-7 and Figure 6-8 show the distributions of CCF events for CCCG size for all events and *complete* CCF events by failure mode. The general shape of the distributions of CCF events and the CCCG size is similar between the distributions shown in these figures and the actual distribution of counts of plants with those numbers of EDGs installed. However, a subtle shift

occurs where the count of CCFs of two EDGs is slightly higher than the installed count and is slightly lower in the count of three and four EDGs. This becomes exaggerated when the *complete* CCF events are considered. Over 70 percent of *complete* CCF events are in CCCG size two systems. This behavior is consistent with CCF theory, which believes that the observation of 2-out-of-2 components failing due to CCF should be more likely than 3-out-of-3 or 4-out-of-4 components failing due to CCF. The breakdown between fail-to-start and fail-to-run shifts from mostly fail-to-run to fail-to-start. This is consistent with the overall spectrum of *complete* and *partial* CCF events.

Figure 6-9 and Figure 6-10 show the distributions of CCF events for detection method for all events and *complete* CCF events by failure mode. These two distributions are very similar, with testing being the primary method of detection of CCF events for both failure modes. Inspection is the second most frequently used method of detection for the set of all CCF events, but identified none of the *complete* CCF events. This is due to the nature of faults detected by inspection. The most common failure detected by inspection is leakage of a minor nature.

Figure 6-11 and Figure 6-12 show the distributions of CCF events for subsystems for all events and *complete* CCF events by failure mode. Cooling, engine, and fuel oil are most likely to result in fail-to-run. I&C, output breaker, and starting air are most likely to result in a fail-to-start. This does not shift significantly between the set of all CCF events and the set of *complete* CCF events. Cooling and engine become much less significant and the I&C and fuel oil become much more significant. The I&C contribution is consistent with the nature of that system since it controls the EDG during operation and contains the shutdown controls. The fuel oil subsystem shifts from mostly fail-to-run to all fail-to-start between the all CCF case and the *complete* CCF case. This is primarily due to most of the fuel oil fail-to-run events involving minor leaks.

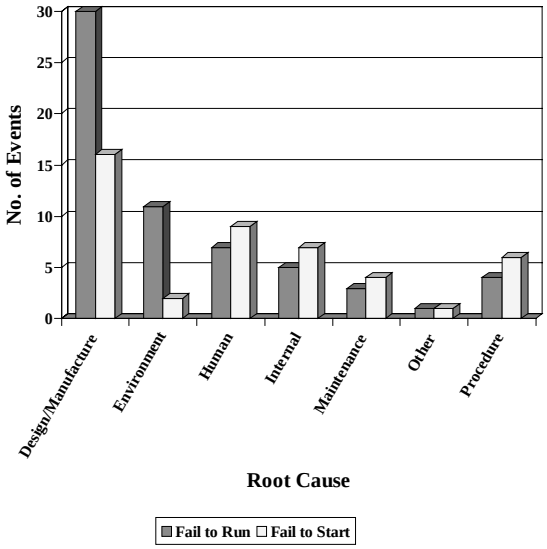


Figure 6-1. Root cause distribution for all CCF events.

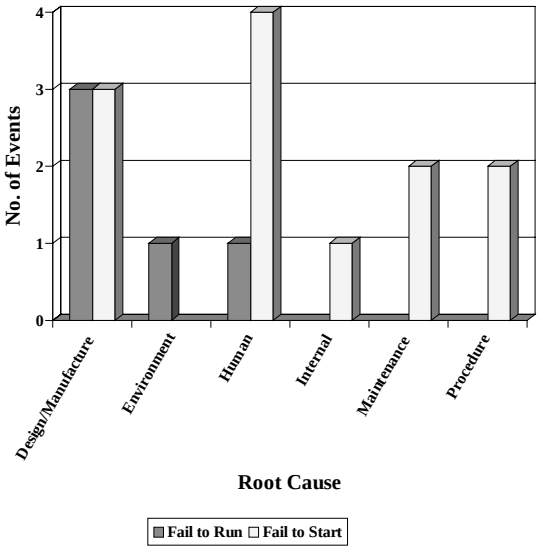


Figure 6-2. Root cause distribution for ***complete*** CCF events.

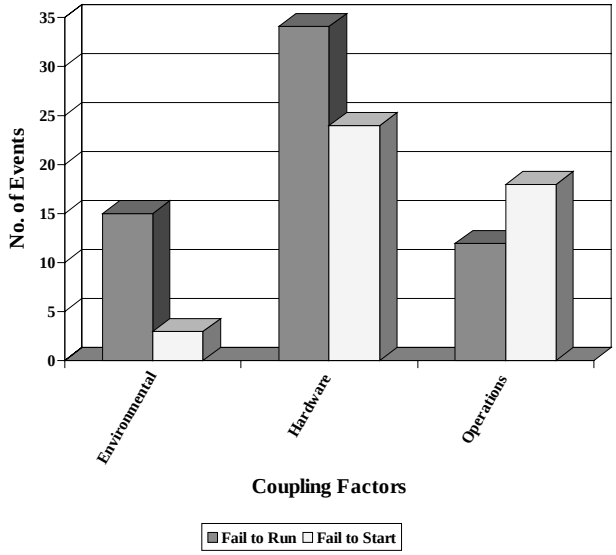


Figure 6-3. Coupling factor distribution for all CCF events.

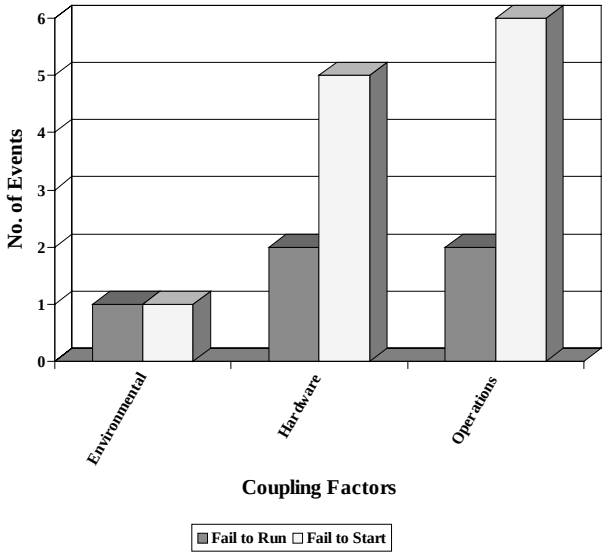


Figure 6-4. Coupling factor distribution for ***complete*** CCF events.

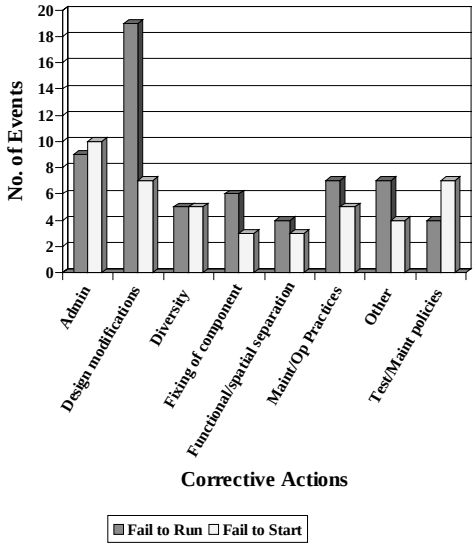


Figure 6-5. Corrective action distribution for all CCF events.

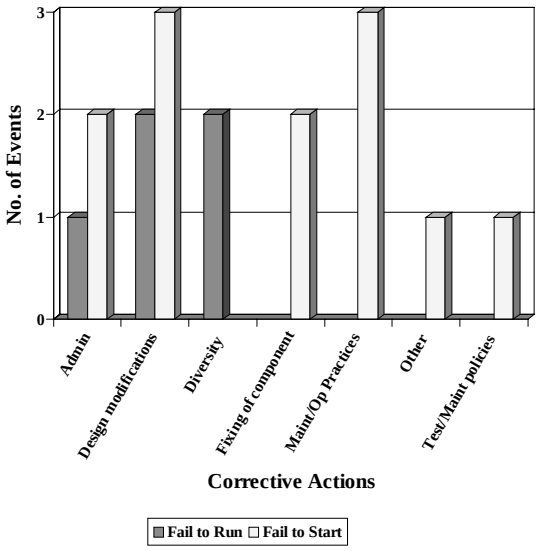


Figure 6-6. Corrective action distribution of ***complete*** CCF events.

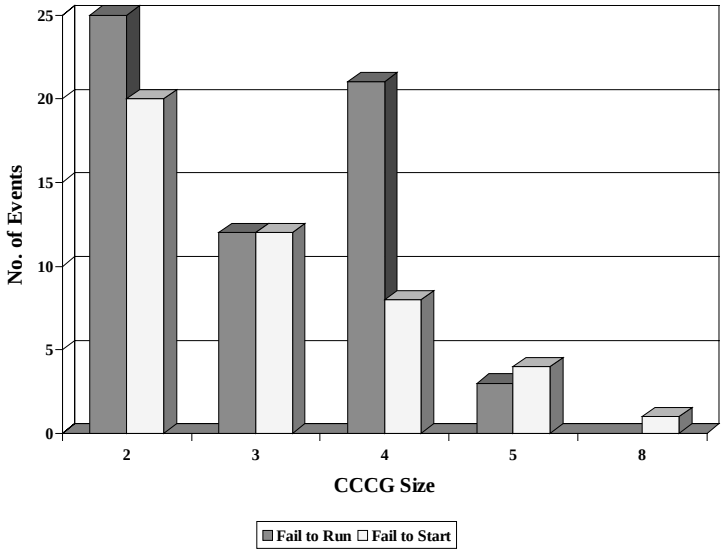


Figure 6-7. CCCG size distribution for all CCF events.

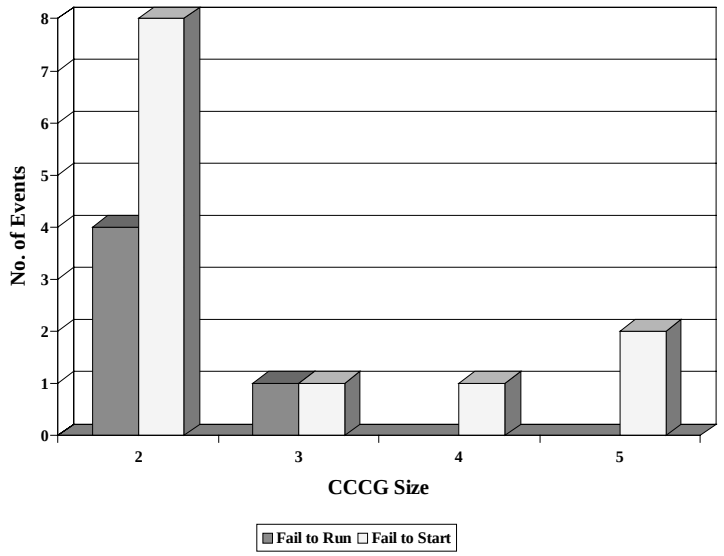


Figure 6-8. CCCG size distribution for ***complete*** CCF events.

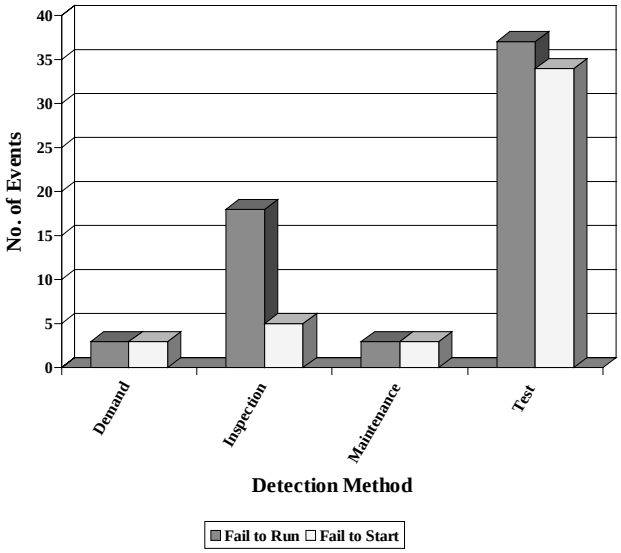


Figure 6-9. Detection method distribution for all CCF events.

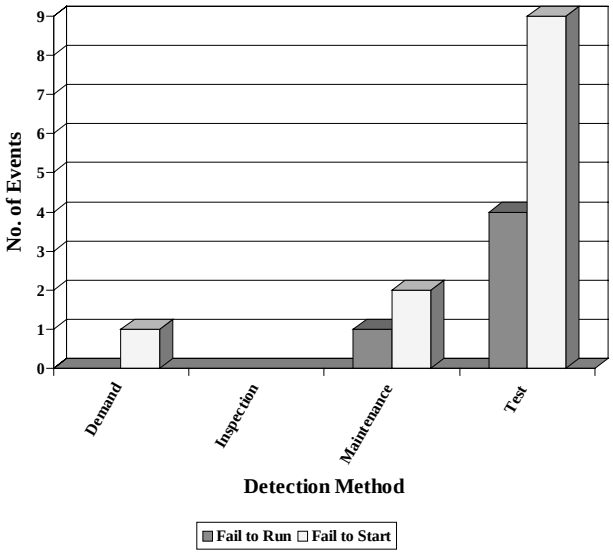


Figure 6-10. Detection method distribution for ***complete*** CCF events.

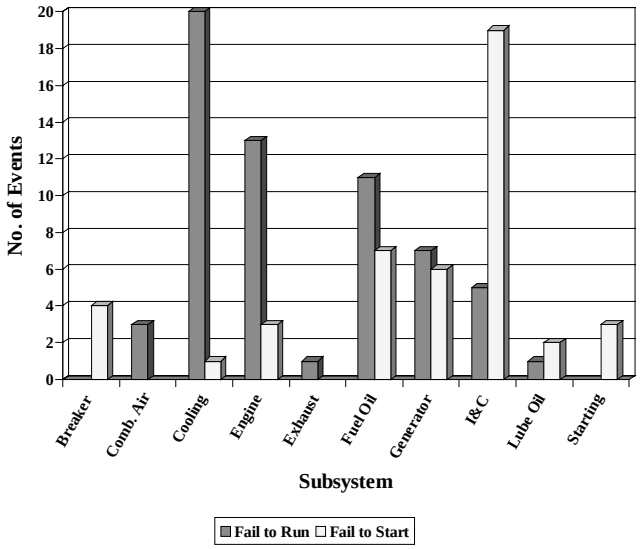


Figure 6-11. Subsystem distribution for all CCF events.

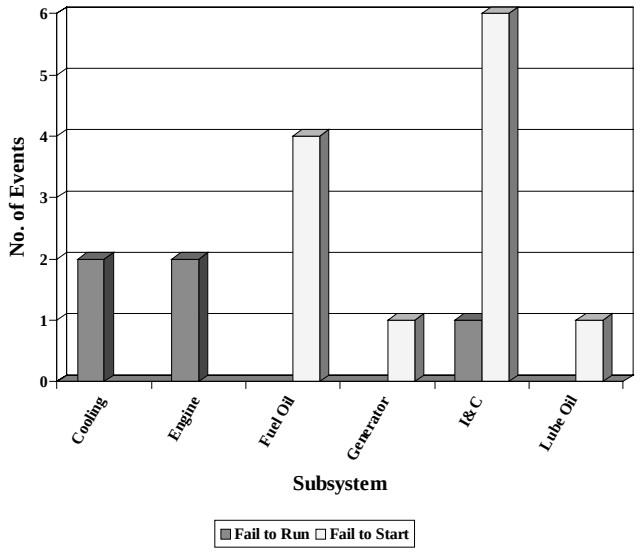


Figure 6-12. Subsystem distribution for ***complete*** CCF events.

7. OVERVIEW OF EVENTS BY ROOT CAUSE

This section contains a discussion of the CCF events by root cause. Table 7-1 contains the number of CCF events for each root cause and the percent of the total number of events. The most likely the root cause is design/manufacture inadequacy majority (46 percent) of the events. The root causes are abnormal environmental stress, human actions procedure inadequacy, and internal to the component, have about the same number of events.

Table 7-1. Summary of root causes.

Root Cause	No. of Events	Percent
Abnormal Environmental Stress	13	12.3
Design, Manufacture, or Construction inadequacy	46	43.4
Human Actions	16	15.1
Internal to Component, piece part	12	11.3
Maintenance	7	6.6
Procedure Inadequacy	10	9.4
Other	2	1.9
Total	**106**	100

7.1 Abnormal Environmental Stress

This root cause category represents causes related to harsh environment that is not within the component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperature, vibration load, and acts of nature (high wind, snow, etc.).

Abnormal environmental stress caused 13 events. Four events resulted from the inability of the cooling water heat exchanger to provide adequate cooling to the EDGs; these were due to both high temperatures in the ultimate heat sink and debris in the heat exchangers. Three events were caused by vibration of the EDG. Two events resulted from snow blockage of the air intake lines. Two events were caused by excessive heating of the sub-component (control relays). Inadequate cooling of the exciter cabinet caused one event and one event was caused by an inadvertent actuation of the fire suppression system that resulted in fire foam present in the environment in the EDG building.

The failure mode for 11 events is fail-to-run and two events have fail-to-start as the failure mode. This distribution of failure modes is not similar to the overall set of data, mostly because the environmental factors are more likely to affect the EDG during running time. For example, high temperature cooling water is not likely to be too hot when the EDG starts, but after some amount of running time, due to the higher than average initial temperature, the cooling water temperature will increase above the acceptable limit. Figure 7-1 displays the

distribution for coupling factors by failure mode for the environmental events. As might be expected for the events caused by environmental factors, a shared environment coupled most of the events. Figure 7-2 contains the distribution by corrective actions by failure mode. Figure 7-3 contains the distribution for CCCG size by failure mode. Figure 7-4 contains the distribution for detection method by failure mode. No environmental events were detected by either the "demand" or "maintenance" detection methods. Figure 7-5 contains the distribution for subsystem by failure mode. More environmental events affected the cooling system than any other subsystem; primarily due to the dependence of the cooling system on the ultimate heat sink temperature and debris level, two factors that are not in direct licensee control.

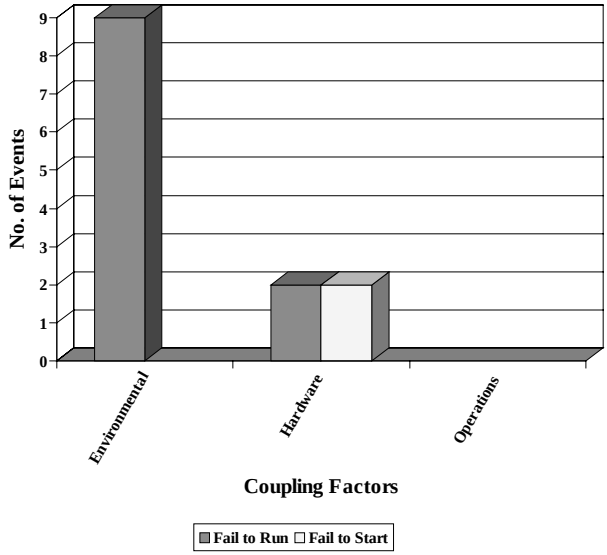


Figure 7-1. Coupling factor distribution for environmental stress root cause.

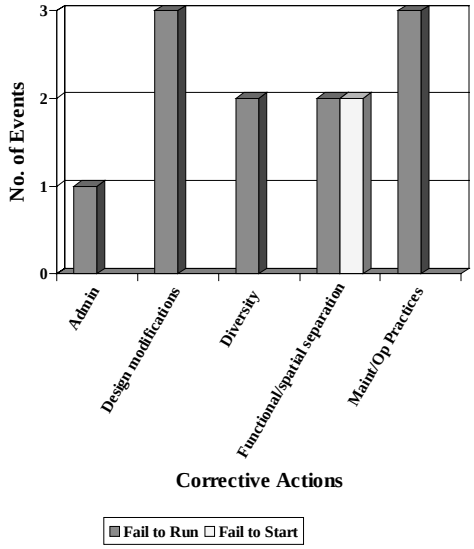


Figure 7-2. Corrective action distribution for environmental stress root cause.

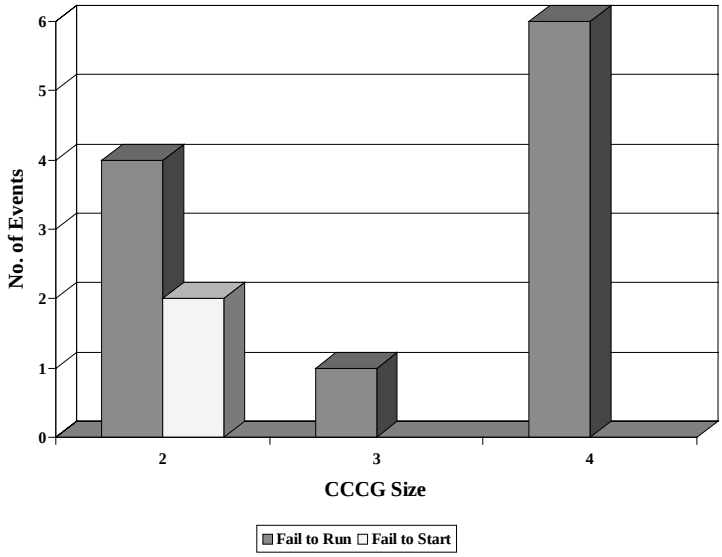


Figure 7-3. CCCG size distribution for environmental stress root cause.

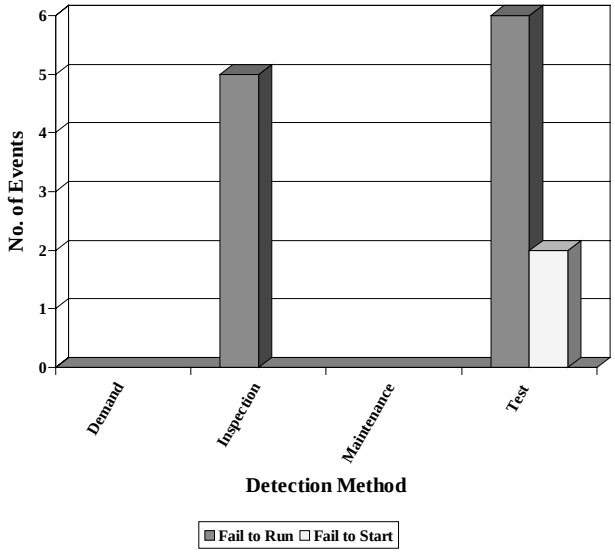


Figure 7-4. Detection method distribution for environmental stress root cause.

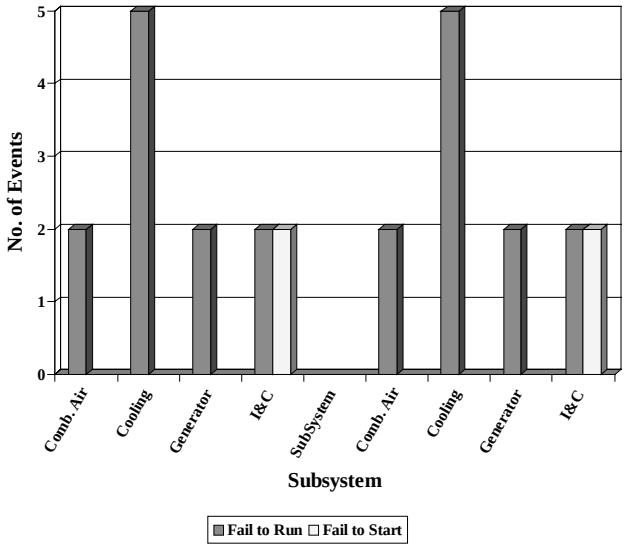


Figure 7-5. Subsystem distribution for environmental stress root cause.

7.2 Design, Manufacture or Construction Inadequacy Root Cause

This category encompasses actions and decisions taken during design, manufacture, or installation of components both before and after the plant is operational. Included in the design process are the equipment and system specification, material specification, and initial construction that would not be considered a maintenance function. This category also includes design modifications.

Design, manufacture, or construction errors resulted in 46 events. The most common type of design error was original design deficiency (accounting for 30 of the 46 design events), affecting both the individual EDG component and the interface between the EDG and other systems. Some of the EDG failures from these design deficiencies occurred on the fuel oil instruments, fuel piping supports, engine piston design, loading sequencer, cooling water piping. These design errors include undersized equipment, incorrect specification of setpoints, and improperly installed components (such as time delay relays and pipe supports). A design fault accounting for seven of the events was incorrect material specification. Some of the equipment affected by the incorrect material specifications includes an air pressure regulator, cooling piping, exhaust dampers, and air start valves. Six events resulted from construction deficiencies such as incorrect wiring and incomplete assembly of cooling water subsystem. Manufacturing defects and design change errors caused the other four events.

The failure mode for 30 events is fail-to-run, and 16 events have fail-to-start as the failure mode. Figure 7-6 contains the distribution for coupling factors by failure mode for this cause. The coupling factor affecting most of the events is the hardware group, accounting for 41 of the 46 design-caused events. This is reasonable, since many plants have more than one EDG of the same design, and it would be expected that a design problem affecting one EDG would also affect EDGs of similar design. Figure 7-7 contains the distribution by corrective actions by failure mode. As might be expected, most of the corrective actions for design related events were to modify the design. Figure 7-8 contains the distribution for CCCG size by failure mode. This is somewhat consistent with the overall distribution of CCCG size shown in Figure 5-4, with a shift to the lower group sizes. Figure 7-9 contains the distribution for detection method by failure mode. Consistent with the set of all EDG events, testing revealed more CCF events than any other detection method. Figure 7-10 contains the distribution for subsystem by failure mode. This figure is comparable to Figure 6-11, which shows the set of all EDG CCF events by subsystem and failure mode.

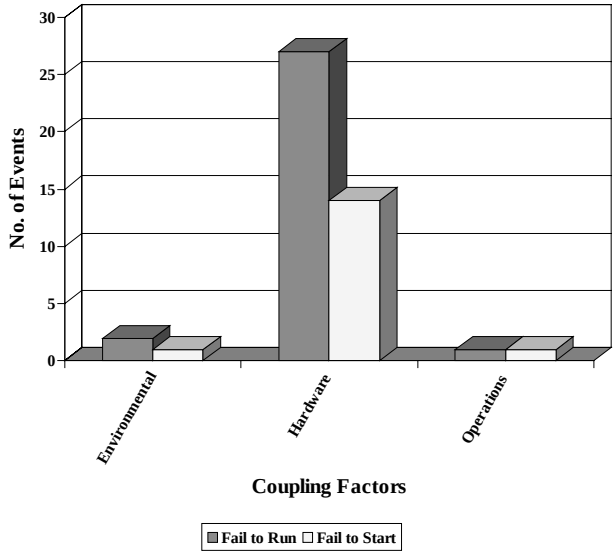


Figure 7-6. Coupling factor distribution for design/manufacture inadequacy root cause.

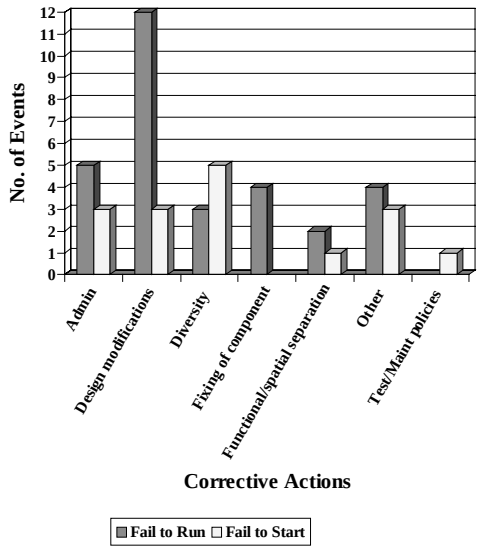


Figure 7-7. Corrective action distribution for design/manufacture inadequacy root cause.

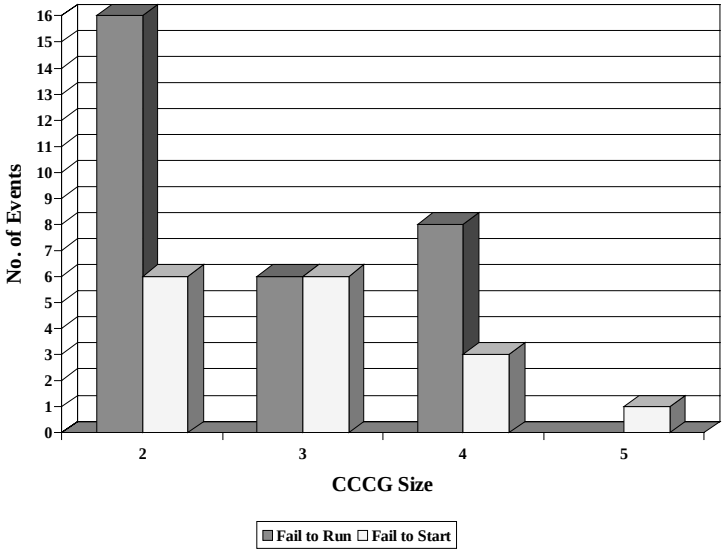


Figure 7-8. CCCG size distribution for design/manufacture inadequacy root cause.

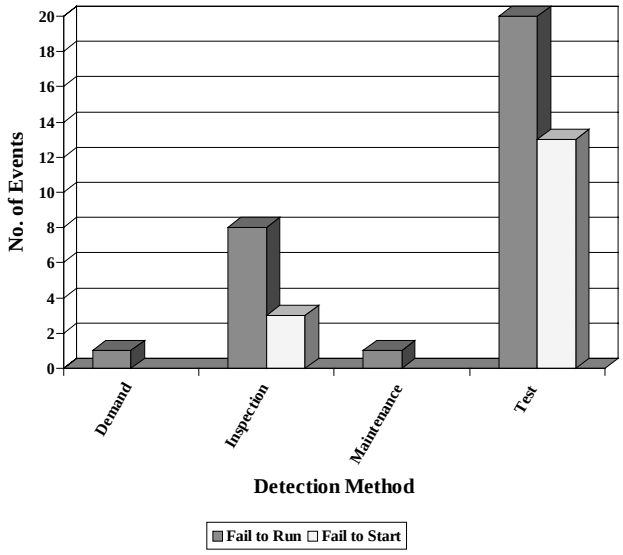


Figure 7-9. Detection method distribution for design/manufacture inadequacy root cause.

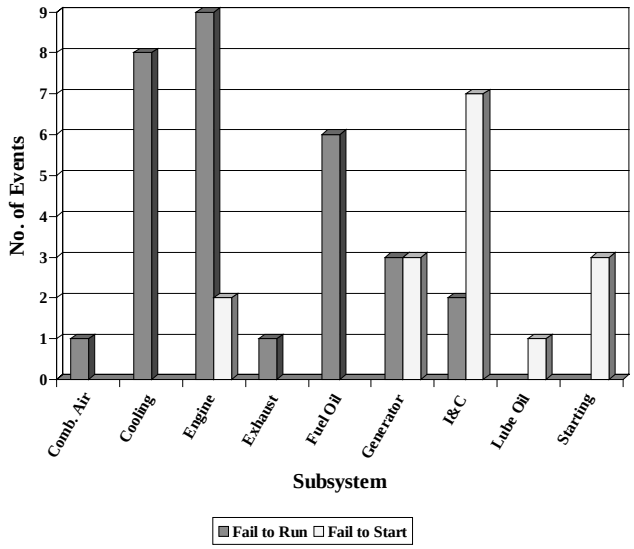


Figure 7-10. Subsystem distribution for design/manufacture inadequacy root cause.

7.3 Human Action Root Cause

Human actions represent cause related to errors of omission or commission on the part of plant staff or contractor staff. An example is failure to follow the correct procedure. This category includes accidental actions and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. This category also includes deficient training.

Human error resulted in 16 EDG CCF events. These events included seven occurrences of failure to follow procedures, during both operation and maintenance activities, and include such actions as installing a solenoid valve backwards and reading the lubrication oil level incorrectly. Three events were caused by poor work practices. Four events resulted from incorrect equipment restoration following maintenance or test activities. These events involved the trip lockout relays, sea water gates, and pressure instrumentation. The remaining two events were caused by inadvertent operation of equipment that resulted in EDG failure or in-operability.

The failure mode for seven events is fail-to-run, and nine events have fail-to-start as the failure mode. Figure 7-11 contains the distribution for coupling factors by failure mode for this cause. It is reasonable to expect that human events are coupled by operations, since there is less human effect on the environment and hardware than on operations activities. Figure 7-12 contains the distribution of corrective actions by failure mode. Many proposed and implemented corrective actions are intended to lessen the need for human decisions; thus the administrative category has a high number of corrective actions for the human error events. Figure 7-13 contains the distribution for CCCG size by failure mode. Figure 7-14 contains the distribution of detection method by failure mode. Figure 7-15 contains the distribution of subsystem by failure mode. As with the set of all EDG events, more human error events occurred in the I&C system than in any other system.

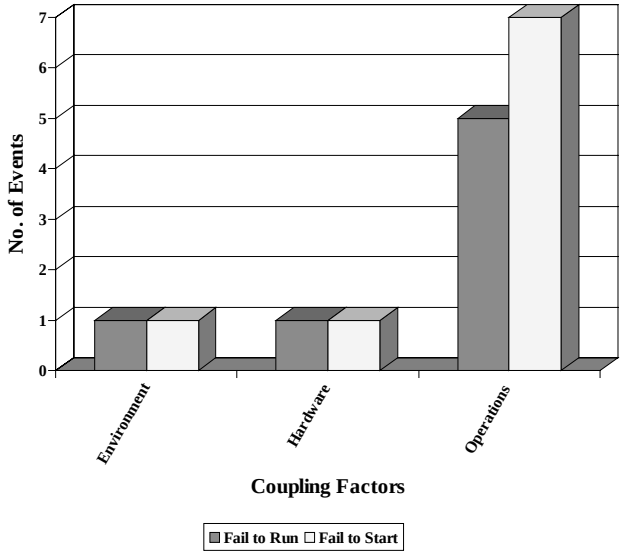


Figure 7-11. Coupling factor distribution for human action root cause.

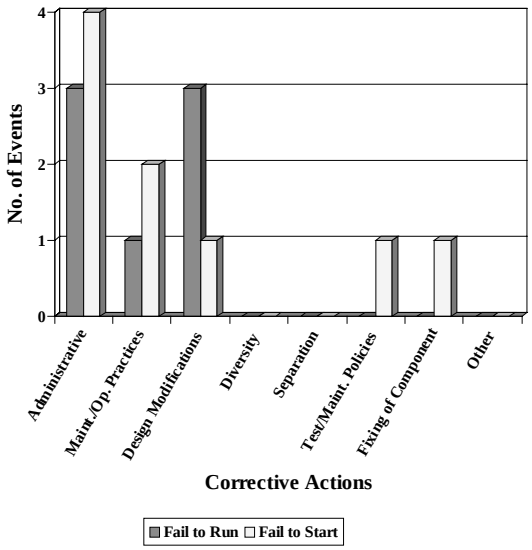


Figure 7-12. Corrective action distribution for human action root cause.

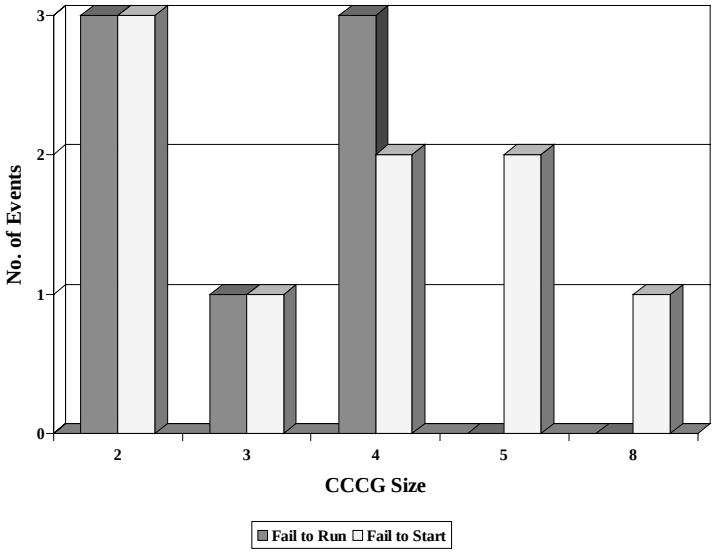


Figure 7-13. CCCG size distribution for human action root cause.

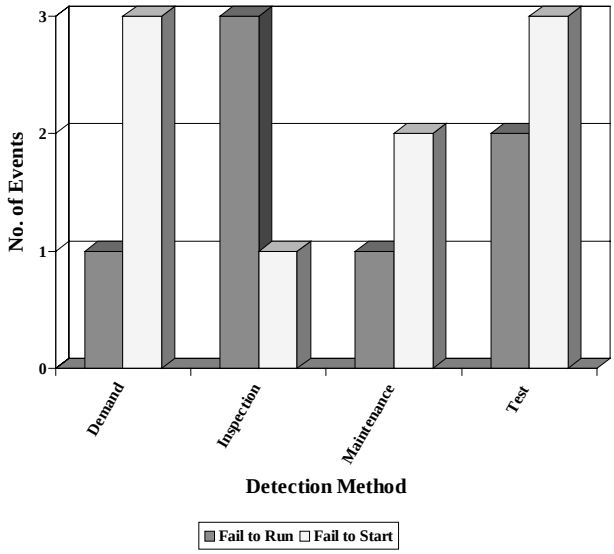


Figure 7-14. Detection method distribution for human action root cause.

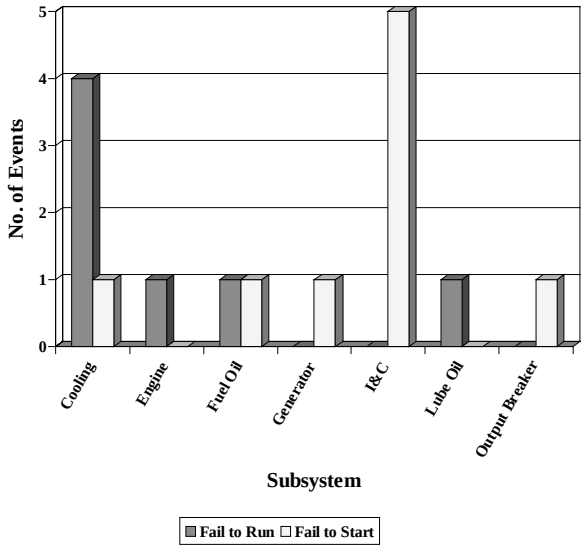


Figure 7-15. Subsystem distribution for human action root cause.

7.4 Internal to Component Root Cause

This category deals with the malfunctioning of something internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the ambient environment of the component. Specific mechanisms include erosion, corrosion, internal contamination, fatigue, wear-out, and end of life. These mechanisms can be divided into internal environmental causes and hardware-related causes.

Reviewers identified 12 events that were caused by failures internal to the component. These failures included fatigue failure of some fuel oil equipment, lagging failure that resulted in clogged air intakes, cracks in air monitors, broken output breaker switch, loose tachometer connector, and foreign material in the combustion air subsystem.

Seven events were classified as fail-to-start and the other five were fail-to-run. Figure 7-16 contains the distribution for coupling factors by failure mode for this cause. More events were coupled by hardware than either of the other two coupling factor groups, which would be expected since most plants have multiple EDGs of the same design and age. Figure 7-17 contains the distribution by corrective actions by failure mode. The events in this set were caused by equipment failures, so it is reasonable that most of the corrective actions were to fix the component and to modify the maintenance plans (e.g., to increase the replacement frequency of components susceptible to repeated failures). Figure 7-18 contains the distribution for CCCG size by failure mode. This distribution is inconsistent with the overall distribution, Figure 5-4. It is unclear as to why that should be except that the data set is small. Figure 7-19 contains the distribution for detection method by failure mode. Figure 7-20 contains the distribution for subsystem by failure mode.

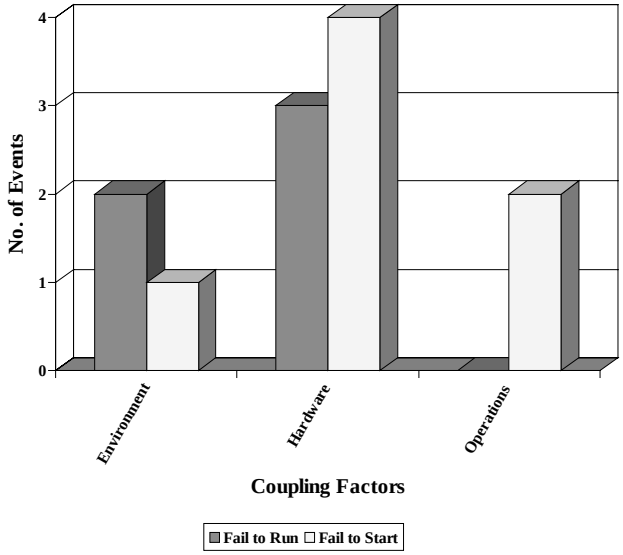


Figure 7-16. Coupling factor distribution for internal to component root cause.

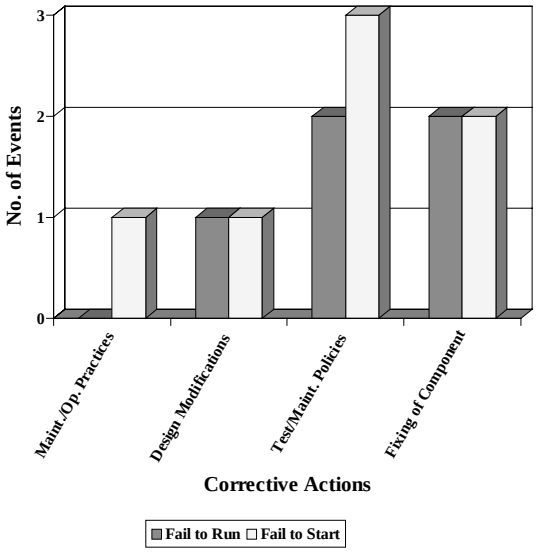


Figure 7-17. Corrective action distribution for internal to component root cause.

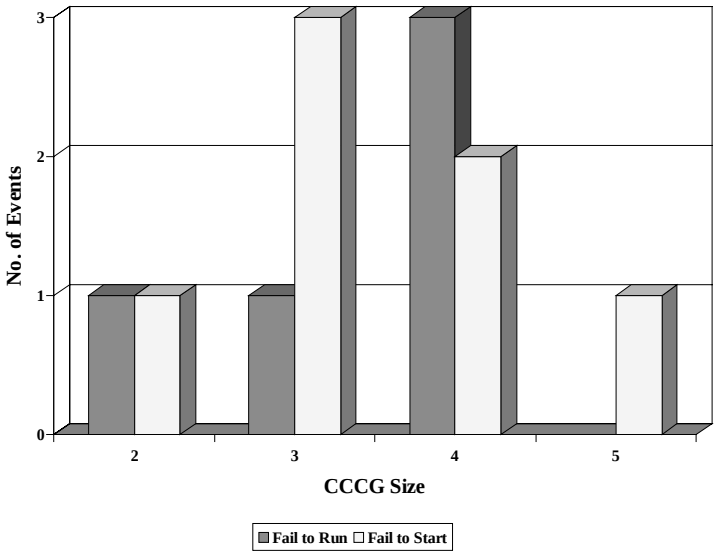


Figure 7-18. CCCG size distribution for internal to component root cause.

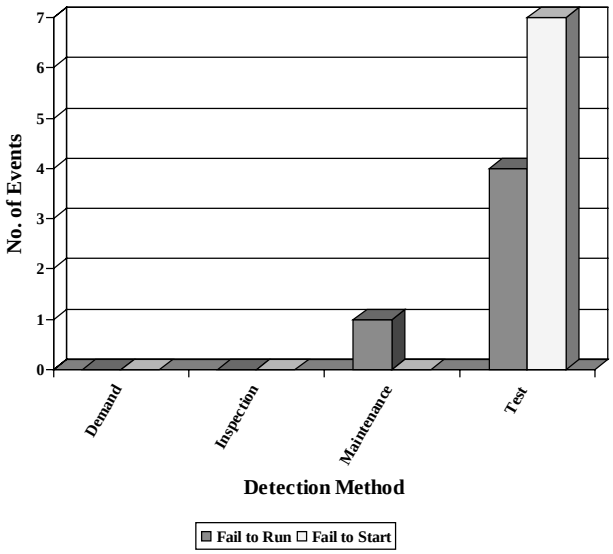


Figure 7-19. Detection method distribution for internal to component root cause.

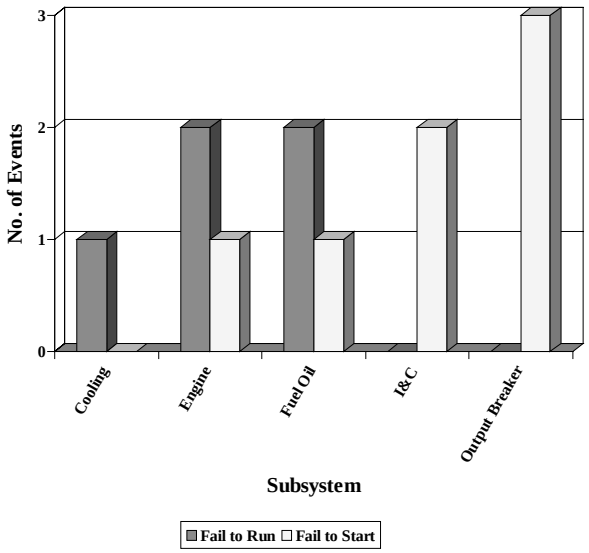


Figure 7-20. Subsystem distribution for internal to component root cause.

7.5 Procedure Inadequacy Root Cause

Procedure inadequacy refers to ambiguity, incompleteness, or errors in procedures for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test, and calibration procedures. This can also include the administrative control procedures such as change control.

Ten EDG CCF events were caused by procedural inadequacies that either caused the EDG to be inoperable, or actually caused an equipment failure. Of these, four were inadequate maintenance procedures, three were test procedures, and three were operational procedures. The failure mode for four events is fail-to-run and six events have fail-to-start as the failure mode. Figure 7-21 contains the distribution for coupling factors by failure mode for this cause. Operations is the dominant coupling factor which is consistent with the procedural inadequacy root cause, since procedures are more linked to the operations of the plant than to the environment and design (hardware group) of the plant. Figure 7-22 contains the distribution by corrective actions by failure mode. As would be expected, procedure modification (operational, test, and maintenance) is the most frequently used corrective action for this cause. Figure 7-23 contains the distribution for CCCG size by failure mode. Figure 7-24 contains the distribution for detection method by failure mode. Figure 7-25 contains the distribution for subsystem by failure mode. The procedure-caused events are fairly evenly distributed among several subsystems; due to the relatively small number of events in this category, there is no clear dominant subsystem.

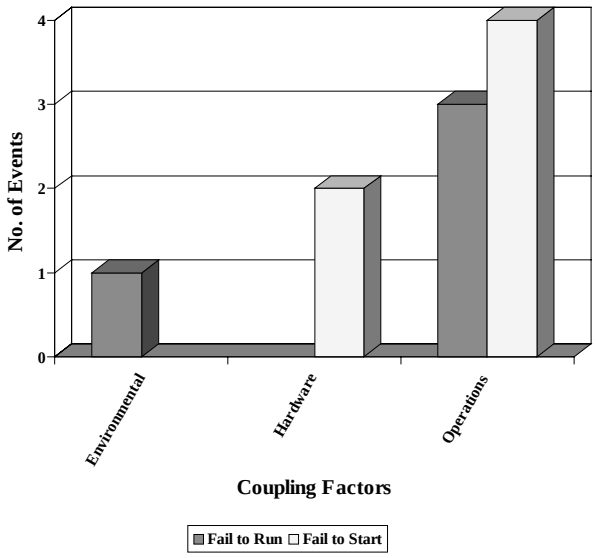


Figure 7-21. Coupling factor distribution for procedure inadequacy root cause.

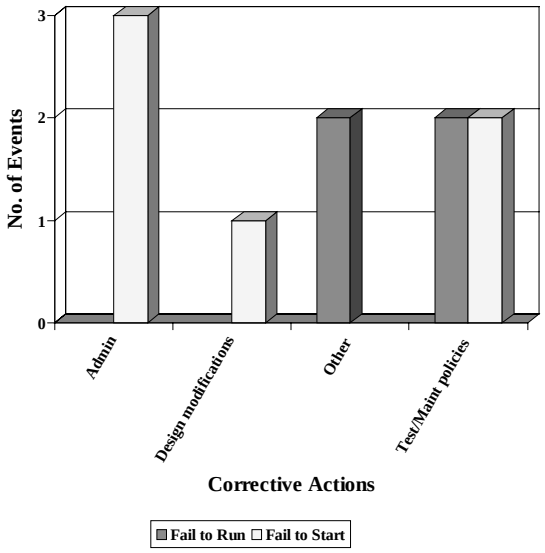


Figure 7-22. Corrective action distribution for procedure inadequacy root cause.

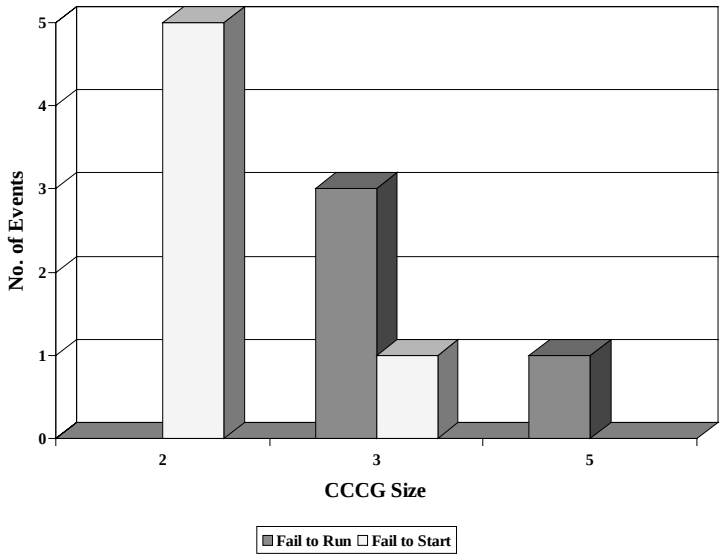


Figure 7-23. CCCG size distribution for procedure inadequacy root cause.

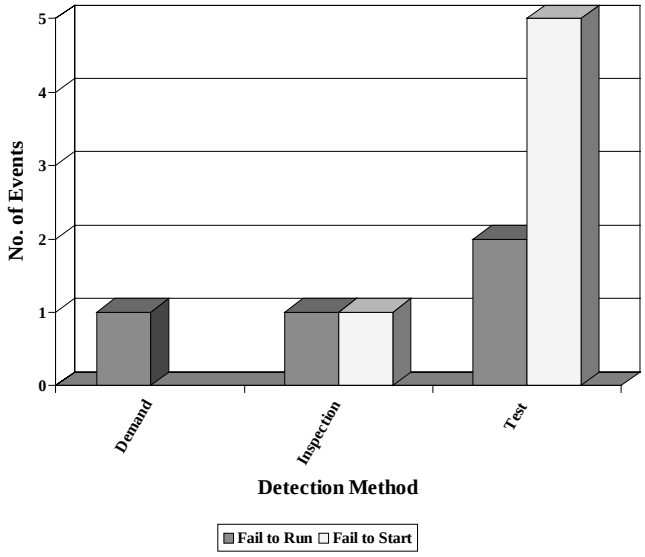


Figure 7-24. Detection method distribution for procedure inadequacy root cause.

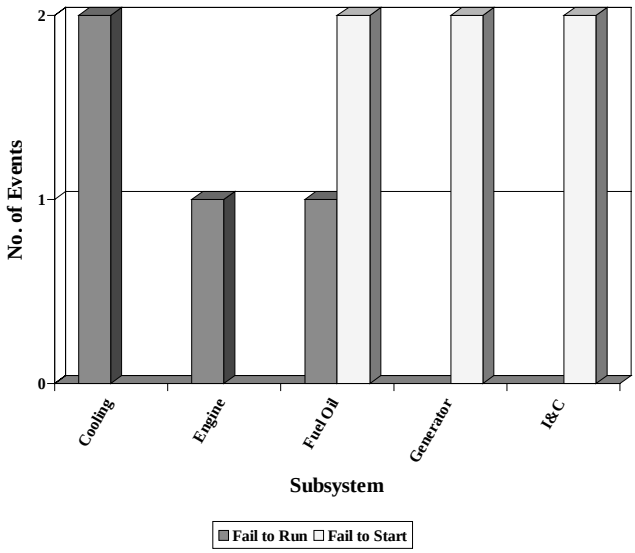


Figure 7-25. Subsystem distribution for procedure inadequacy root cause.

7.6 Maintenance Root Cause

This category includes all maintenance activities not captured by human actions and procedure inadequacy. Seven EDG CCF events included in this study were caused by maintenance activities. These events included such items as: lubrication oil contamination due to work practices, incorrect fuel oil sampling schedule, bearing lubrication frequency too low, and fuel oil filter maintenance schedule not in accordance with manufacturer recommendations.

Due to the smaller number of events in this category compared to other cause categories, no graphs were produced for this set of events. Information similar to the graphical presentation for other causes will be summarized here. Four of the maintenance events were fail-to-start, and three were fail-to-run. The fuel oil subsystem was affected by maintenance problems, with four failures, more than any other subsystem; two events occurred on the generator subsystem, and one event affected the lubrication oil subsystem. The coupling factor for four events was determined to be maintenance practices, and the other three events coupled by shared operational practices. As might be expected for maintenance caused events, the corrective actions for most of the events (five of the seven) were modification to maintenance practices; one event had no corrective action identified, and one event identified design modification as the corrective action.

7.7 Other Root Cause

Two events were identified resulting from causes that did not fit the other categories of root causes. Both of these causes were identified as setpoint drift, with no underlying reason for the setpoint drift. Both events occurred in the I&C subsystem, one on the overspeed protection circuit and the other on the governor control unit. In both events, the multiple EDG failures were coupled by shared hardware design. One event was fail-to-start and the other was fail-to-run.

8. OVERVIEW OF EVENTS BY SUBSYSTEM

This section presents an overview of the EDG CCF events by subsystem. Each discussion of an EDG subsystem summarizes selected attributes of that subsystem. Then the discussion will turn to looking at each root cause. When discussing a subsystem–root cause combination, salient points will be made with regard to failure mode and failure mechanism. Individual events will be discussed as they apply to insights and comparisons. Table 8-1 provides a summary of the CCF events by subsystem. One event did not provide enough information to assign a subsystem.

Table 8-1. Summary of subsystems.

Subsystem	No. of Events	Percent
Combustion Air	3	2.8
Cooling	21	19.8
Engine	16	15.1
Exhaust	1	0.9
Fuel Oil	18	17.0
Generator	13	12.3
Instrumentation & Control	24	22.6
Lube Oil	3	2.8
Output Breaker	4	3.8
Starting Air	3	2.8
Total	106	100.0

8.1 Combustion Air

Reviewers assigned three events to the combustion air subsystem. All of the events were classified as fail-to-run. All three events were detected by testing. None of the events were *complete* CCF events. Two events had abnormal environmental stress assigned as the root cause. These events occurred at "sister" plants simultaneously and were caused by snow plugging of the combustion air intake filters. The coupling factor assigned to these events was external environment.

The root cause assigned to the other event was design/manufacture inadequacy. This event was initiated by a spurious closing of the intake flapper valve. Vibrations from the EDGs

initiated the closure. An indication that the limit switches were inadequate was given in the description. Only one of the EDGs failed, but all were suspect due to the similarity in position switches. The coupling factor for this event was hardware design.

8.2 Cooling

Reviewers assigned 21 events to the cooling air subsystem. All of the events except one were classified as fail-to-run.

8.2.1 Cooling Overview

Figure 8-1 shows the distribution for the root causes. The causes are discussed in more detail below.

Figure 8-2 shows the coupling factor distribution. The hardware category accounts for 48 percent of the events. The environment is the coupling factor for 33 percent of the events. "Operations" was the coupling factor for four events (19 percent).

Figure 8-3 contains the distribution for the corrective actions. As can be seen from the figure, all corrective actions are viable actions for this subsystem. Design modification is the most common, but it accounts for only 29 percent of the events.

Figure 8-4 shows the distribution of the cooling subsystem events by CCCG size. The sizes are almost equally distributed among two, three, and four with four having the most. The fail-to-start event was involved in a group of size eight. This does not correlate with the distribution of installed EDGs at the plants. Essentially, there is an external dependency such as the service water, which is not affected by how many EDGs there are.

Figure 8-5 shows the detection method distribution. Test and inspection account for 18 events (86 percent) which is consistent with the overall distribution shown in Figure 5-5.

8.2.2 Cooling Root Causes

Table 8-2 shows the distribution of failure degree across the root causes.

Table 8-2. Cooling subsystem failure degree.

Description	Complete	Almost-Complete	Partial
Design/Manufacture	1	1	6
Environment		1	4
Human	1		4
Internal			1
Procedure		1	1

The design/manufacture category is the most common root cause (eight events) in the cooling subsystem, which is not inconsistent with the overall root cause distribution shown in Figure 5-1. One of the eight events was a *complete* CCF event. Three events involved leakage due to corrosion, an inadequate design of a pipe coupling, and a supply hose. Another event involved failure of a pump due to excessive vibration. In another event the governor failed

due to inadequate design. The *complete* CCF event consisted of failure of the temperature controller of the water cooling system that cooled the lubricating oil.

The human action root cause has five events. One event was a *complete* common cause failure. One event involved valve problems due to incorrect installation of piece parts. The other three events involved human actions that led to the introduction of sludge into the lines to the heat exchangers.

The abnormal environmental stress root cause was assigned to five events. Four events involved reduced flow to the heat exchangers due to sludge, mussels, or corrosion nodules. Another event involved excessive vibration.

Two events were assigned to the procedure inadequacy root cause. One event involved zebra mussels in the heat exchangers. The other event involved putting valves in the wrong positions due to inadequate procedures.

In summary, 10 events involved reduced flow to the heat exchangers. Seven events involved seawater. These conditions were detected early. Four events involved leakage, two of which were caused by corrosion. These conditions are also amenable to early detection. Three events involved valve problems; one was a *complete* CCF event.

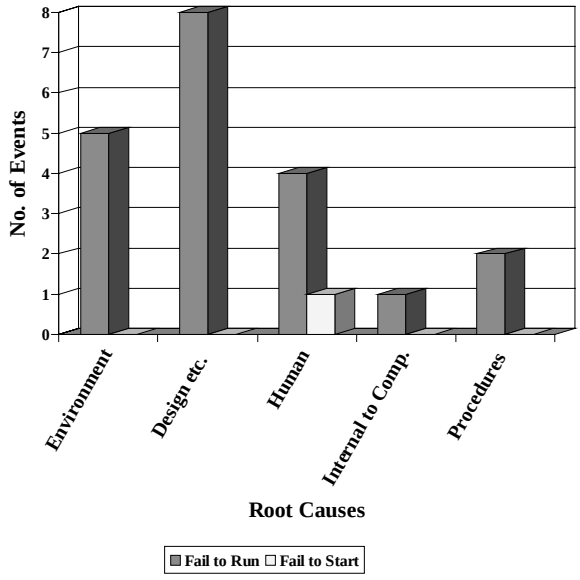


Figure 8-1. Root cause distribution for cooling subsystem.

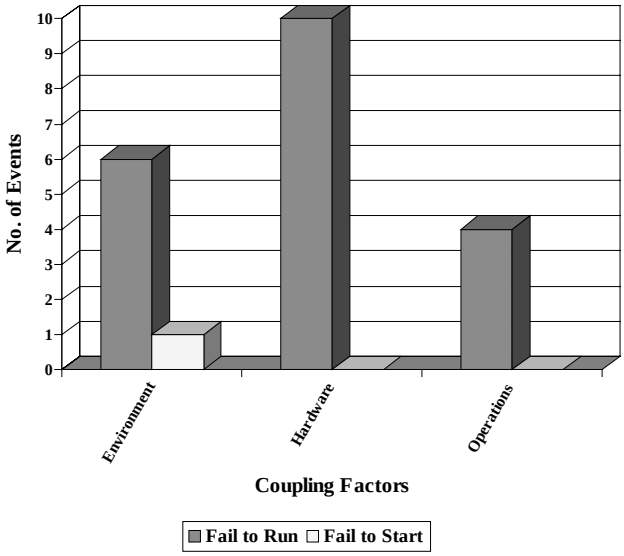


Figure 8-2. Coupling factor distribution for cooling subsystem.

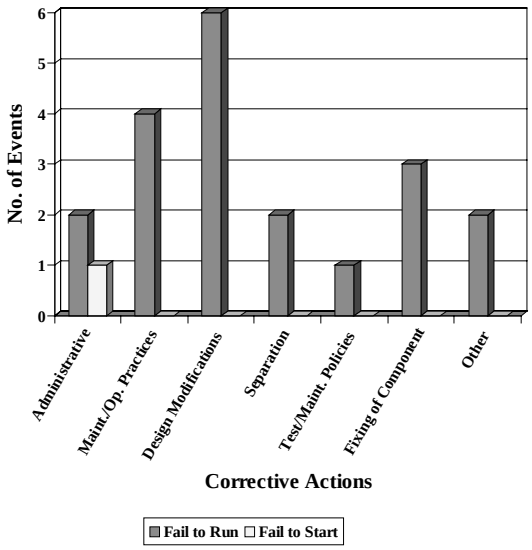


Figure 8-3. Corrective actions distribution for cooling subsystem.

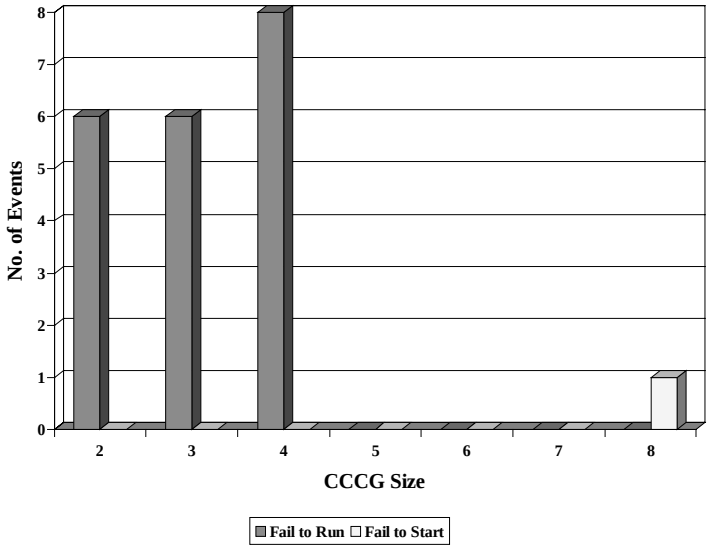


Figure 8-4. CCCG size distribution for cooling subsystem.

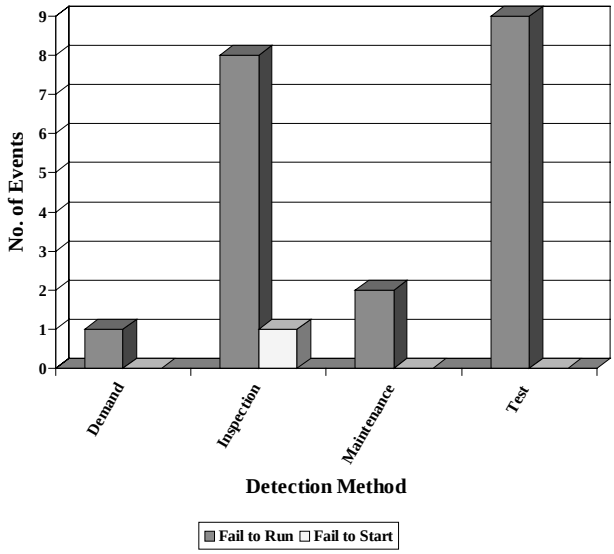


Figure 8-5. Detection method distribution for cooling subsystem.

8.3 Engine

8.3.1 Engine Overview

Reviewers assigned 16 events to the engine subsystem. The failure mode for 13 of those events is fail-to-run and fail-to-start for three events. It seems significant that the large majority of failure modes are fail-to-run. The overall distribution (Table 5-1) is approximately 60/40 fail-to-run.

Figure 8-6 shows the root cause distribution for the CCF events for the engine, which is similar to the overall root cause distribution shown in Figure 5-1.

Figure 8-7 shows the coupling factor distribution. The hardware element is the most significant coupling factor. In view of the root cause discussion above and the overall distribution in Figure 5-2, this is consistent.

Figure 8-8 contains the corrective action distribution. This figure indicates that the most important category is design/manufacture, which is consistent with the root causes and the overall distribution shown in Figure 5-3.

The CCCG size distribution, given in Figure 8-9, shows that CCCG size two is the most common engine failure CCCG. This is not inconsistent with expected results based on group size two being the most common and the overall distribution shown in Figure 5-4.

Throughout this study, testing has been shown to be by far the most common way of detecting CCF events. Figure 8-10 shows that testing is also the most common method for detecting CCF events for the engine and the overall distribution shown in Figure 5-5.

8.3.2 Engine Root Causes

Table 8-3 shows the distribution of failure degree across the root causes.

Table 8-3. Engine subsystem failure degree.

Description	Complete	Almost-Complete	Partial
Design/Manufacture	2	1	8
Human			1
Internal			3
Procedure			1

The dominant root cause is the design/manufacture category. Of the 11 events in this category, two were *complete* CCFs. One was an inadequate piston design aggravated by the testing procedure, which did not allow the lubrication to form before full operation. In the other event, a recent modification to the turbocharger led to a vibration failure of the turbocharger. Inadequate

design oversight was identified as the ultimate cause. One significant event was identified. A connecting sleeve on the turbocharger loosened on all four of EDGs. This led to failure of the turbocharger on one EDG. The corrective action was to solder the sleeve to prevent movement. Of the other root causes, none were identified as either *complete* or *almost-complete*. The human root cause event was caused by the intake of sand particles through the air system. This caused scoring of the cylinder walls. The source of the sand was a sandblasting operation nearby which in retrospect should have taken into account the concurrent operation of the EDGs for testing. A second event attributed to procedure was due to the same cause, sandblasting in the vicinity of the EDGs. These events were coded as *partial* events, but in the reviewers' opinion, had a strong probability of having a *complete* failure if the EDGs were allowed to continue to run.

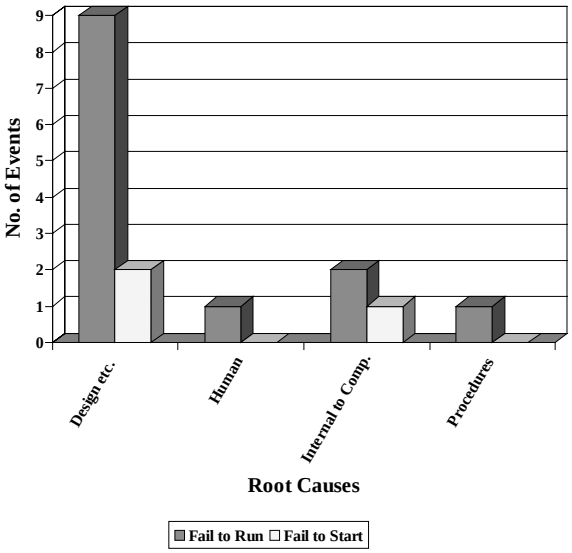


Figure 8-5. Root cause distribution for engine subsystem.

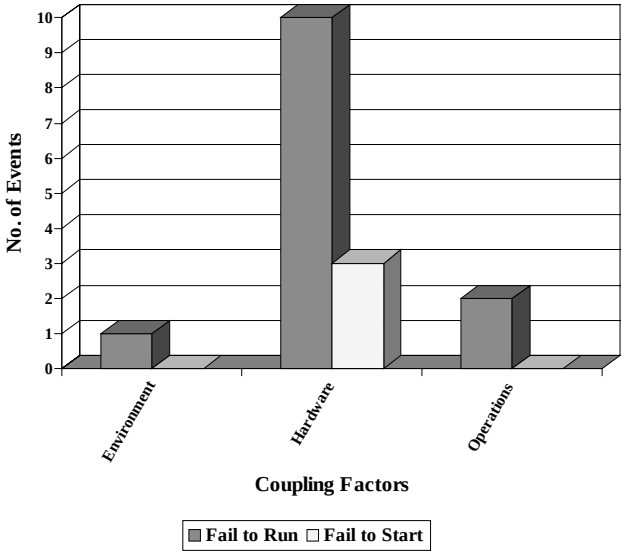


Figure 8-7. Coupling factor distribution for engine subsystem.

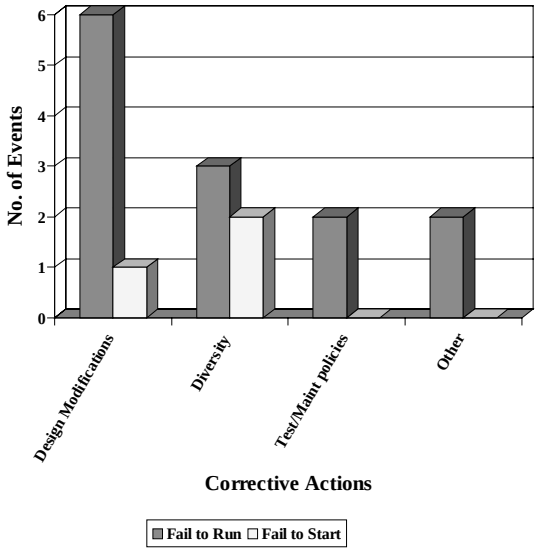


Figure 8-8. Corrective action distribution for engine subsystem.

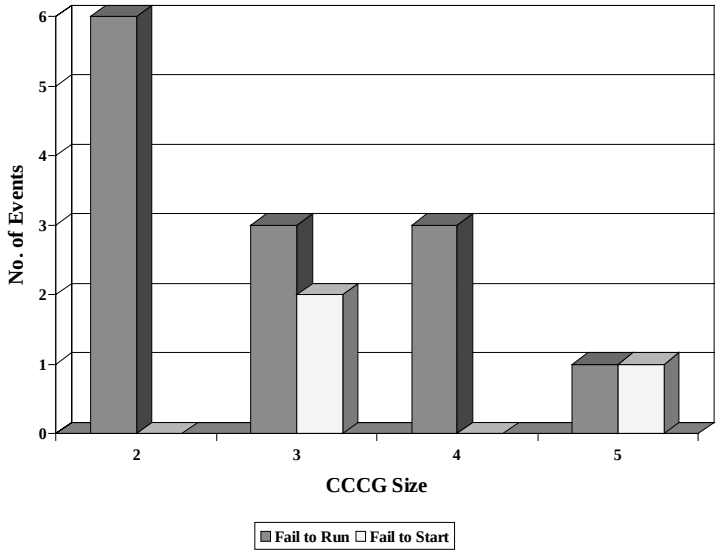


Figure 8-9. CCCG size distribution for engine subsystem.

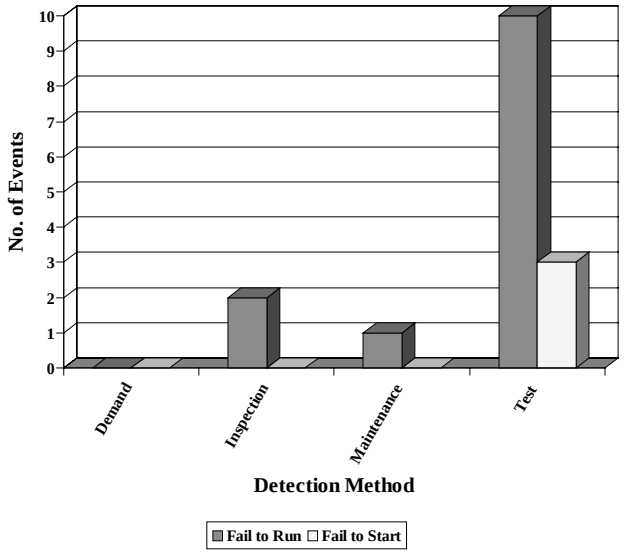


Figure 8-10. Detection method distribution for engine subsystem.

8.4 Exhaust

The exhaust subsystem has only one CCF event. This event is consistent with the overall EDG distribution shown in Section 5 in that it is due to a design error and was detected during a test.

8.5 Fuel Oil

8.5.1 Fuel Oil Subsystem Overview

Reviewers assigned 18 events to the fuel oil subsystem. Eleven events were fail-to-run and seven events were fail-to-start.

Figure 8-11 shows the distribution for the fuel oil subsystem root causes. The causes are discussed in more detail below.

Figure 8-12 shows the coupling factor distribution for the fuel oil subsystem. The hardware category accounts for 44 percent of the events. The environment is the coupling factor for 11 percent of the events. Operations were the coupling factor for 44 percent of the events.

Figure 8-13 contains the distribution for the corrective actions for the fuel oil subsystem. As can be seen from the figure, all corrective actions are viable actions for this subsystem. Design modification is the most common, but it accounts for only 28 percent of the events. Administrative and maintenance accounted for 22 percent each.

Figure 8-14 shows the distribution for the fuel oil subsystem events by CCCG size. The CCCG size distribution does not conform to the installed distribution. There appears to be independence to CCCG size. It is apparent that the fuel oil system acts like an independent external system.

Figure 8-15 shows the detection method distribution for the fuel oil subsystem. Test and inspection account for 16 events (over 89 percent).

8.5.2 Fuel Oil Subsystem Root Causes

Table 8-4 shows the distribution of failure degree across the root causes.

Table 8-4. Fuel oil subsystem failure degree.

Description	Complete	Almost-Complete	Partial
Design/Manufacture			6
Human	1	1	
Internal	1		2
Maintenance	2		2
Procedure			3

The most common root cause is design/manufacturing (33 percent). None of these events were determined to be significant. The design/manufacturing root cause events were made up of two inadequate level detectors, three leaks, and vibration induced wear. Maintenance is the next most common root cause (22 percent). Of these, two are *complete* CCFs. One event was due to the fuel injection pumps seizing due to lubrication problems resulting from inadequate fuel quality. In the second event the two EDGs were unavailable due to erroneous maintenance activities. The next most common root cause is internal component. This category had one *complete* CCF event: The fuel feed pumps coupling pins were broken due to fatigue cracking. The human error category accounts for one *complete* event and one *almost-complete* event. The *complete* event was caused by the operator leaving a fuel oil tank outlet valve closed this isolated the fuel supply to all four EDGs. The *almost-complete* event occurred when the fuel transfer pumps were inoperable due to improper greasing of motor bearings during cold weather operations.

The procedure root cause produced no *complete* failures. However, the events were detected on the first failure and the procedures were modified before further failures could be observed.

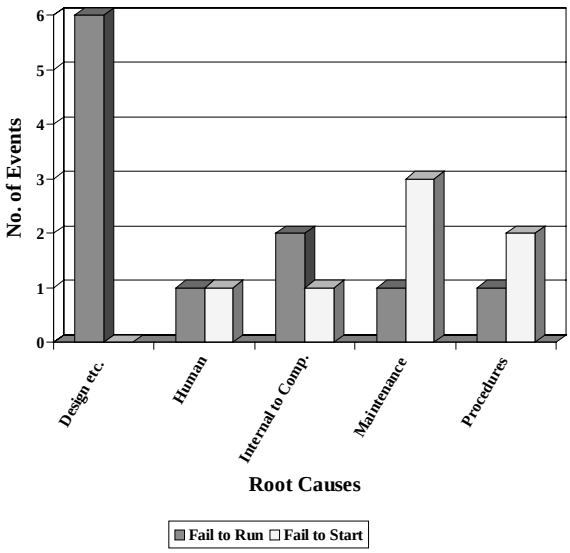


Figure 8-11. Root cause distribution for fuel oil subsystem.

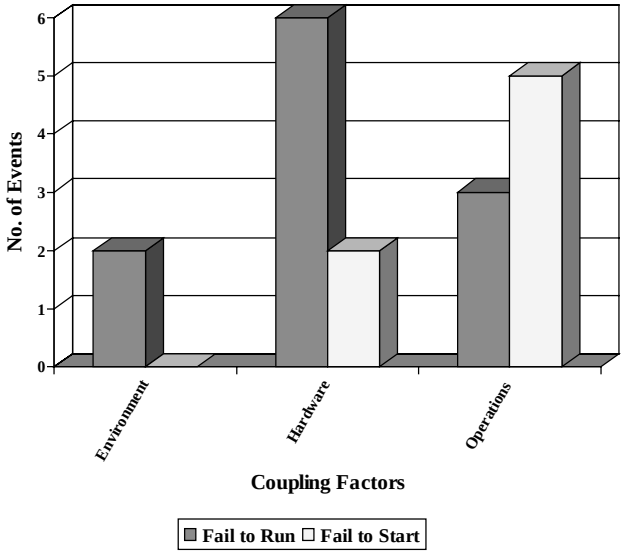


Figure 8-12. Coupling factor distribution for fuel oil subsystem.

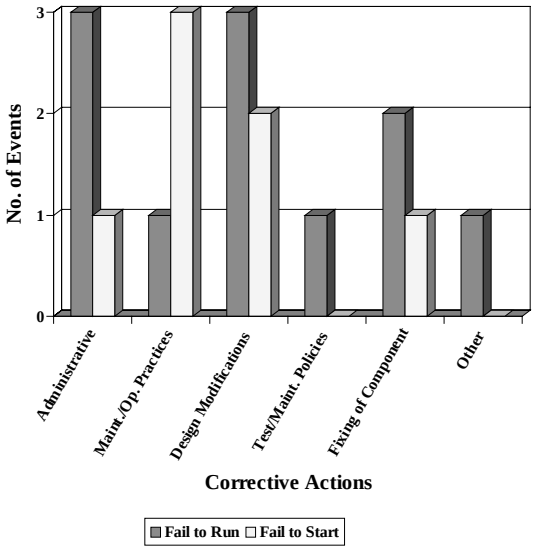


Figure 8-13. Corrective action distribution for fuel oil subsystem.

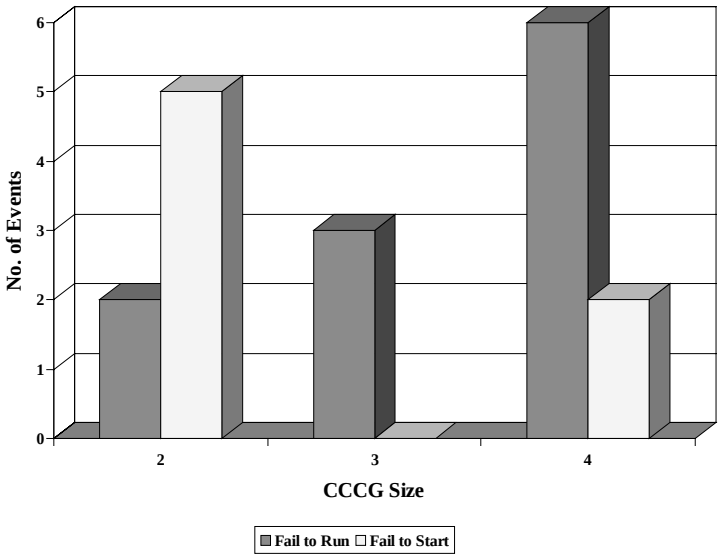


Figure 8-14. CCCG size distribution for fuel oil subsystem.

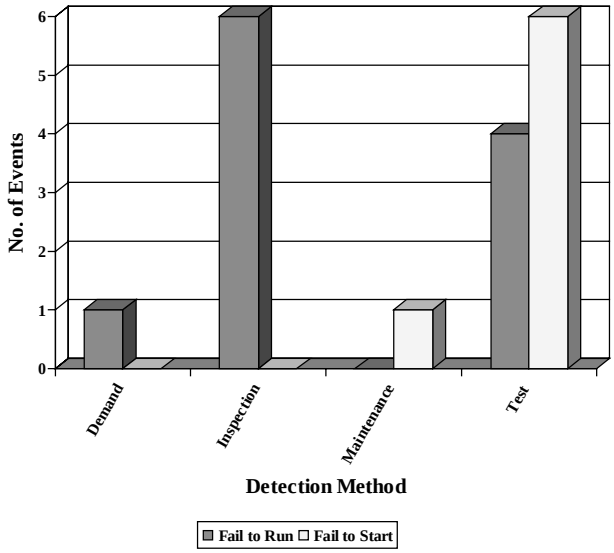


Figure 8-15. Detection method distribution for fuel oil subsystem.

8.6 Generator

8.6.1 Generator Subsystem Overview

Reviewers assigned 13 events to the generator subsystem. Of these 13 events, 7 were fail-to-run and 6 were fail-to-start.

Figure 8-16, the root cause distribution, shows that the design/manufacture category is the most common (46 percent). Environmental, maintenance, and procedure each contributed 15 percent.

Figure 8-17 shows the coupling factor distribution for the generator subsystem. The hardware category accounts for 46 percent of the events. The environment is the coupling factor for 15 percent of the events. Operations were the coupling factor for 39 percent of the events.

Figure 8-18 contains the distribution for the corrective actions for the generator subsystem. As can be seen from the figure, all corrective actions are viable actions for this subsystem. The administrative corrective action accounts for 31 percent of the events. Maintenance, design, separation, and test account for 15 percent each.

Figure 8-19 shows the distribution for the generator subsystem events by CCCG size. This distribution approximately follows the installed distribution. There were fewer than expected events in the CCCG size four group, but it is difficult to say whether the difference is statistically significant.

Figure 8-20 shows the detection method distribution for the generator subsystem. Testing accounts for the detection of 61 percent of events.

8.6.2 Generator Subsystem Root Causes

Table 8-5 shows the distribution of failure degree across the root causes.

Table 8-5. Generator subsystem failure degree.

Description	Complete	Almost-Complete	Partial
Design/Manufacture		3	3
Environment		1	1
Human		1	
Maintenance		1	1
Procedure	1	1	

Three design/manufacture events were classified as *almost-complete*. Relays were improperly wired, which led to one observed failure, the other EDGs in the group were repaired before failure was detected. In another event, improper exciter switches were installed. One observed failure and multiple EDGs repaired before failure was detected. In another event, the voltage regulator failed due to inadequate piece-parts. One observed failure and multiple EDGs repaired before failure was detected. The three *partial* events included inadequate equipment and another instance of the improperly wired relays at a sister plant that were repaired before failures were observed.

Five important events were coded in this grouping. Both procedure events are important. One was coded as a *complete* failure. Paint was applied to the fuel racks, which caused two of two EDGs to fail-to-start due to an inadequate procedure. The other was classified as *almost-complete*. This event was due to a mis-adjusted automatic voltage control.

One important event classified in the environment category: inadequate cooling in the exciter cabinet. One important event classified in the maintenance category: failure of the clutch occurred due to glazing of the shoes/drum. One important event classified in the human error

category: the cause was an insufficiently torqued screw in a connection block in a voltage measuring circuit supplying too low a voltage to the voltage regulator.

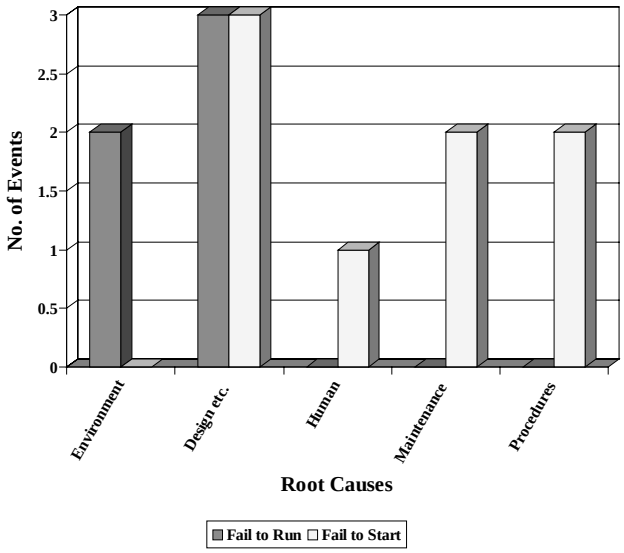


Figure 8-16. Root cause distribution for generator subsystem.

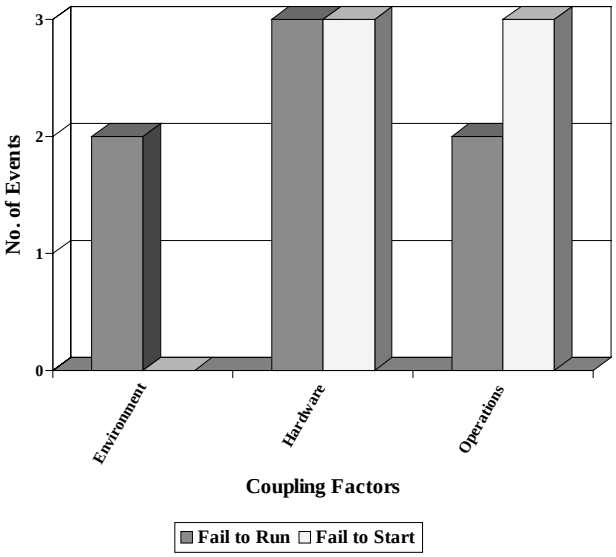


Figure 8-17. Coupling factor distribution for generator subsystem.

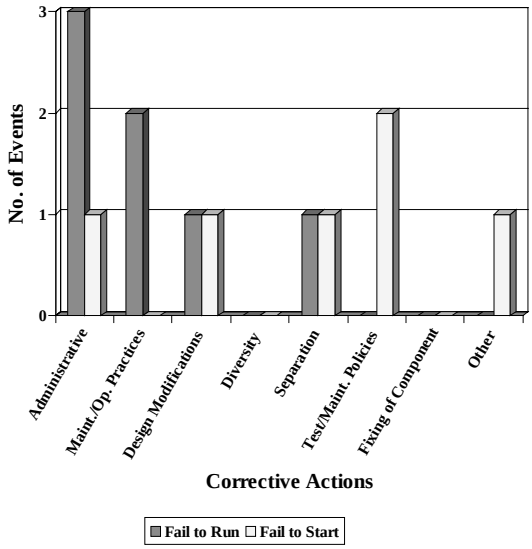


Figure 8-18. Corrective action distribution for generator subsystem.

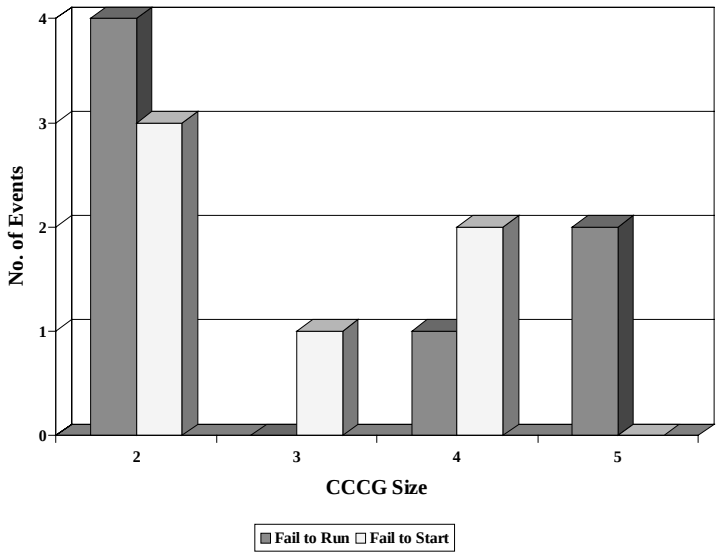


Figure 8-19. CCCG size distribution for generator subsystem.

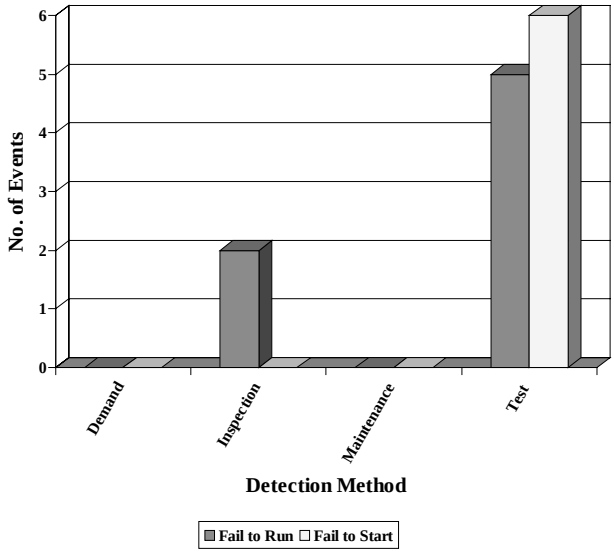


Figure 8-20. Detection method distribution for generator subsystem.

8.7 Instrumentation and Control

8.7.1 Instrumentation and Control Subsystem Overview

Reviewers assigned 24 events to the instrumentation and control subsystem. Of these 24 events, 5 were fail-to-run and 19 were fail-to-start. The distribution of fail-to-run and fail-to-start in this subsystem is inconsistent with the other subsystems. It makes sense, since the instrumentation and control subsystem contains piece-parts that can disable the entire system.

Figure 8-21 shows the distribution for the root causes for the instrumentation and control subsystem. The causes are discussed in more detail below.

Figure 8-22 shows the coupling factor distribution for the instrumentation and control subsystem. The hardware category accounts for 58 percent of the events. The environment is the coupling factor for 13 percent of the events. Operations were the coupling factor for seven events (29 percent).

Figure 8-23 contains the distribution for the corrective actions for the instrumentation and control subsystem. As can be seen from the figure, all corrective actions are viable actions for this subsystem. "Administrative" is the most common, but it accounts for only 25 percent of the events and design accounts for 13 percent of the events.

Figure 8-24 shows the distribution for the instrumentation and control subsystem events by CCCG size. The distribution of CCCG size follows the installed distribution with the exception of CCCG size four, which is much smaller than expected. This may imply that the increased redundancy level is improving the reliability of the EDGs in this subsystem.

Figure 8-25 shows the detection method distribution for the instrumentation and control subsystem. Testing detected 17 events (71 percent).

8.7.2 Instrumentation and Control Subsystem Root Causes

Table 8-6 shows the distribution of failure degree across the root causes.

Table 8-6. Instrumentation and control subsystem failure degree.

Description	Complete	Almost-Complete	Partial
Design/Manufacture	2	2	5
Environment	1	2	1
Human	3	1	1
Internal		1	1
Other			2
Procedure	1		1

The design/manufacture category is the most common root cause in the I&C subsystem. The *complete* CCF events consisted of the following:

- Sequencers did not load. Inadequate design and post-modification testing.
- Design deficiency in the fire protection system created a short in the EDG breaker closing circuit under certain conditions.

The *almost-complete* CCF events consisted of the following:

- Deficient wiring connections (crimps). One EDG failed to start and the others were found to have the same condition, but were repaired before they could fail.
- A wiring error was introduced during a modification in 2 of the 4 EDGs. The drawing was incorrect.

In two of the *partial* events, the parts were replaced prior to the next failure. Three were not fully failed.

The human category is the next most common root cause in the I&C subsystem. Three *complete* CCF events were recorded:

- Master trip relays were not reset after a test. All EDGs were then unavailable.
- Both EDGs were tripped when a cleaning crewmember inadvertently pressed the trip buttons while cleaning the panel.
- Control cable to both EDGs was cut by mistake during EDG modifications.

The environment category is the next most common root cause in the I&C subsystem. One *complete* CCF event was recorded:

- Relay sockets degraded causing high resistance connections. Vibrations induced the degradation.

The *almost-complete* CCF events consisted of the following:

- The two events in this category occurred at sister plants. Failed resistors in the governor units. One EDG failed at each plant. The cause was long-term heat fatigue.

The internal and procedure categories each had one event:

- Foreign material under the seat of an air system check valve allowed air pressure to decay which led to a trip of one EDG. This event is classified as *almost-complete*.

- A testing procedure required the lockout of both EDGs. This event is classified as *complete*.

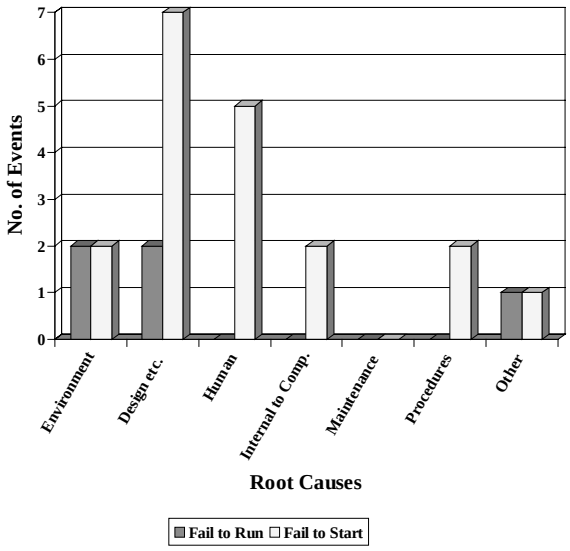


Figure 8-21. Root cause distribution for instrumentation and control subsystem.

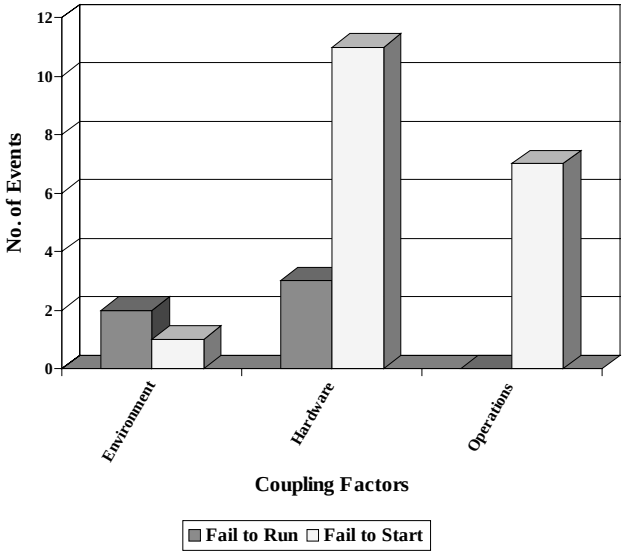


Figure 8-22. Coupling factor distribution for instrumentation and control subsystem.

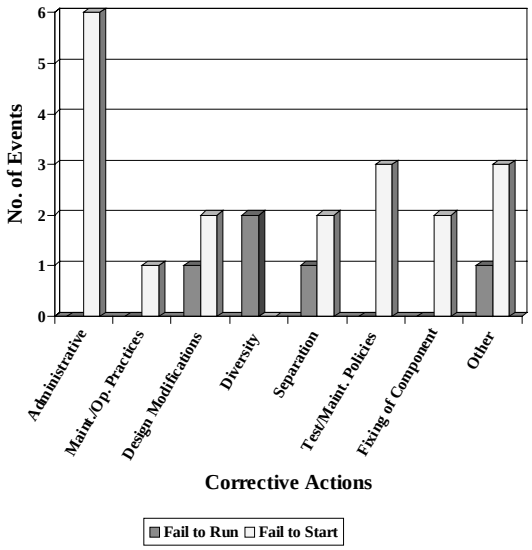


Figure 8-23. Corrective action distribution for instrumentation and control subsystem.

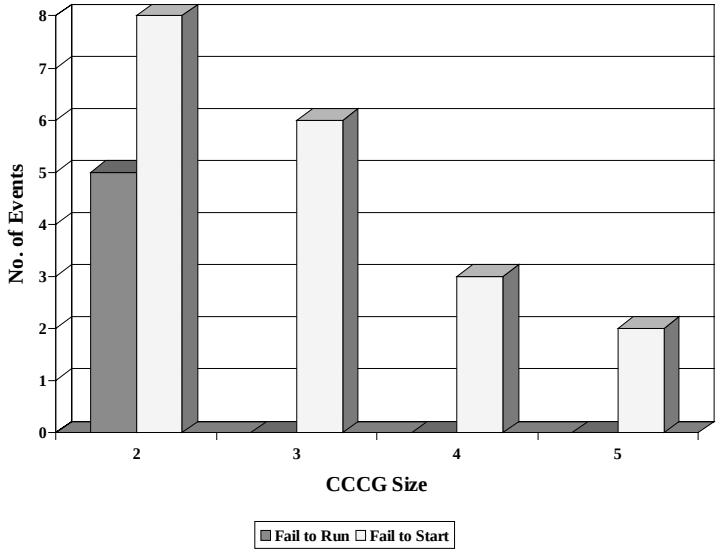


Figure 8-24. CCCG size distribution for instrumentation and control subsystem.

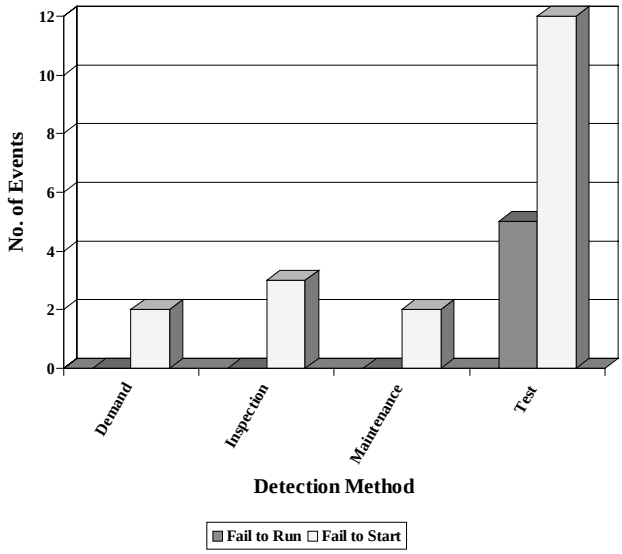


Figure 8-25. Detection method distribution for instrumentation and control subsystem.

8.8 Lubrication Oil

Reviewers assigned three events to the lubrication oil subsystem. Two events were classified as fail-to-run and one was classified as fail-to-start. All events were detected by testing. Table 8-7 shows the distribution of failure degree across the root causes.

Table 8-7. Lubrication oil degree of failure.

Description	Complete	Almost-Complete	Partial
Design/Manufacture	1		
Human			1
Maintenance			1

One of the events was a *complete* CCF event. Five EDGs failed to start due to cold temperatures in the lubricating oil subsystem. The other events are generally due to improper maintenance.

8.9 Output Breaker

Reviewers assigned four events to the output breaker subsystem. All events were classified as fail-to-start. Three of the four events were detected by testing. Table 8-8 shows the distribution of failure degree across the root causes.

Table 8-8. Output breaker degree of failure.

Description	Complete	Almost-Complete	Partial
Human		1	
Internal			3

One of the events was an almost-*complete* CCF event. The operator did not reset relays. The internal events were worn and failed piece-parts.

8.10 Starting Air

Reviewers assigned three events to the starting air subsystem. All events were classified as fail-to-start. Two of the three events were detected by testing.

All events were due to the design root cause. Two events occurred at sister plants, one of which was identified as *almost-complete*. The air valve pistons were sticking due to inadequate manufacturing tolerances.

9. SUMMARY AND CONCLUSIONS

9.1 Summary

This study examined 106 events in the ICDE database by tabulating the data and observing trends. Once trends were identified, individual events were reviewed for insights.

The database contains information developed during the original entry of the events that was used in this study. This information includes root cause, coupling factor, CCCG size, and corrective action. As part of this study, these events were reviewed again and additional categories of the data were included. Those categories included the degree of failure, affected subsystem, and detection method.

This study begins with an overview of the entire data set (Section Five). Charts and tables are provided which show the event count for each of these event parameters. This section forms the baseline for the EDG component.

Section Six contains charts that demonstrate the distribution of the same events further refined by failure mode (fail-to-run and fail-to-start) for each event parameter. Each of these charts is replicated with the further distinction that only those events classified as *complete* or *almost-complete* are included. Distinctions are drawn as these parameters shift.

Section Seven contains charts that demonstrate the distribution of events even further refined into groups of root causes. Each root cause group is analyzed independently. Events within each root cause group are studied together to identify similarities and differences within the group based on the remaining parameters. These distributions are also compared with the distributions developed in previous sections.

Section Eight is similar to Section Seven except that the events are grouped by subsystem rather than root cause.

9.2 Conclusions

This study took place using four different means of combining the same data. Each data combination produced results that were unique to that particular view as well as a degree of commonality between these combinations.

The overall view of the ICDE EDG CCF events provided a baseline set of parameters, which were then compared to the various more detailed groupings. The similarities and differences between these provide insights.

9.2.1 Failure Mode and Completeness

The largest set of *complete* failures (71 percent) occurs in the fail-to-start group. This contradicts the overall distribution, which shows that the set of all EDGs have 43 percent of events as fail-to-start. The data supports the conclusion that CCF events tend to have impairment vector values of less than "C" for those events categorized as fail-to-run and more events with a "C" for the fail-to-start. Fail-to-start also tends to be a stronger failure mode.

9.2.2 Design

The most likely root cause is design, manufacture, or construction inadequacy (43 percent). This makes sense in a CCF analysis since the most effective mechanism to fail multiple redundant components is to mechanically introduce a fault into each one. Most of the *complete* design faults are in the instrumentation and control subsystem, which contributes a significant portion of its CCFs to the fail-to-start mode. It should be noted that the design category includes events that were faults of the initial design as well as modifications made subsequent to the original installation. These are powerful mechanisms to introduce CCF to a piece of equipment.

The term vibration is used in the event description repeatedly. In the course of this study, it was determined that vibration is not a root cause, but is a manifestation of another more basic failure. Most of the events that used the term vibration were categorized as design faults. Generally, the design should have taken into account the large amount of vibration that occurs during EDG operation. The next most common root cause for vibration was environment. The original analyst assumed that the high vibration environment was the cause of the event.

Hardware is the dominant coupling factor (65 percent) and design modification is the most common possible corrective action (26 percent). These are consistent with the dominant root cause being design.

9.2.3 Human Errors

This category is worth mentioning. The instrumentation and control subsystem is especially vulnerable to CCF from the human factor. Again, this is due to the complexity and the function of instrumentation and control. Procedures, maintenance, and operations all contribute to this root cause.

9.2.4 Common Cause Component Group (CCCG Size)

The distribution of CCF events by the CCCG size of the event indicates that the largest contributors are from CCCG sizes two and four. These are consistent with the distribution of the installed CCCGs. The general shape of the distributions of CCF events by CCCG size is similar between the actual distribution of counts of plants with those numbers of EDGs installed. However, a subtle shift occurs where the count of CCFs of two EDGs is slightly higher than the installed count and is slightly lower in the count of three and four EDGs. This becomes exaggerated when the *complete* CCF events are considered. Over 70 percent of *complete* CCF events are in CCCG size two systems. This behavior is consistent with CCF theory, which believes that the observation of 2-out-of-2 components failing due to CCF should be more likely than 3-out-of-3 or 4-out-of-4 components failing due to CCF.

9.2.5 Detection Method

Testing is the primary way CCF failures are detected. It is interesting to note that the inspection method of detection represented in the set of all CCF events is not represented in the set of *complete* CCF events. This is due to the nature of faults detected by inspection. The most common failure detected by inspection is leakage of a minor nature.

9.2.6 Subsystem

Cooling, engine, and fuel oil are most likely to result in fail-to-run. Instrumentation and control, output breaker, and starting are most likely to result in a fail-to-start. This does not shift significantly between all CCFs and *complete* CCFs. Cooling and engine become much less significant and the instrumentation and control and fuel oil become much more significant. The instrumentation and control contribution is consistent with the nature of that system since it controls shutdown and control of the EDG. The fuel oil subsystem shifts from mostly fail-to-run to all fail-to-start between the all CCF case and the *complete* CCF case. This is primarily due to most of the fuel oil fail-to-run events involving minor leaks.

The instrumentation and control subsystem is a complicated and diverse system that contains the functions of shutdown and control. Therefore, small errors can propagate into *complete* failures of the EDG component. This subsystem has experienced many design modifications.

10. REFERENCES

1. International common-cause failure data exchange (ICDE) project, terms and conditions. OECD/NEA, 1998.

2. OECD/NEA's web site: http://www.nea.fr. ICDE project documentation, 1995-1998.

3. ICDE Coding Guidelines (NEA/SEN/SIN/WG1(98)3).

4. Marshall, F. M., D. M. Rasmuson, and A. Mosleh, 1998. *Common Cause Failure Data Collection and Analysis System, Volume 1—Overview*, U.S. Nuclear Regulatory Commission, NUREG/CR-6268, INEEL/EXT-97-00696, June.

APPENDIX A

ROOT CAUSE COMPARISON BY SUBSYSTEM

It can be helpful to compare the root cause of the CCF events by the subsystem affected by the CCF event. Tables A-1 and A-2 correlate the root cause and subsystem and show the counts of events at each intersection. The highlighted rows and columns point out the significant contribution root causes and subsystems. More detail on the events can be found in Sections 7 and 8.

Table A-1. Matrix of root cause and subsystem CCF event counts using all events.

Description	Engine	Cooling	Generator	Fuel Oil	I&C	Lube Oil	Starting Air	Comb. Air	Exhaust	Breaker	Total
Design/ Manufacture	11	8	6	6	9	1	3	1	1		46
Environment		5	2		4			2			13
Human	1	5	1	2	5	1				1	16
Internal	3	1		3	2					3	12
Maintenance			2	4		1					7
Other					2						2
Procedure	1	2	2	3	2						10
Total	16	21	13	18	24	3	3	3	1	4	106

Table A-2. Matrix of root cause and subsystem CCF event counts using only complete events.

Description	Engine	Cooling	Generator	Fuel Oil	I&C	Lube Oil	Starting Air	Comb. Air	Exhaust	Breaker	Total
Design/ Manufacture	2	1			2	1					6
Environment					1						1
Human		1		1	3						5
Internal				1							1
Maintenance				2							2
Other											0
Procedure			1		1						2
Total	2	2	1	4	7	1	0	0	0	0	17