UNCLASSIFIED

AD NUMBER
AD885324
NEW LIMITATION CHANGE
TO Approved for public release, distribution unlimited
FROM Distribution authorized to U.S. Gov't. agencies only; Proprietary Information; MAY 1971. Other requests shall be referred to Army Mobility Equipment Research and Development Center, Fort Belvoir, VA.
AUTHORITY
USAMERDC ltr, 2 Apr 1975

THIS PAGE IS UNCLASSIFIED

UNCLASSIFIED

AD

AD885324

RELIABILITY REVIEW AND ANALYSIS OF THE OPEN-CYCLE FUEL-CELL POWER PLANT

by
John P. McCormick

AD No. ____
DDC FILE COPY

10 MAY 1971

Prepared for
U. S. ARMY MOBILITY EQUIPMENT
RESEARCH AND DEVELOPMENT CENTER
under Contract DAAK01-70-D-4142-C003

UNCLASSIFIED

Unclassified
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) ARINC Research Corporation 2551 Riva Road Annapolis, Maryland 21401	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

Reliability Review and Analysis of Open-Cycle Fuel-Cell Power Plant

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Final Report

5. AUTHOR(S) (First name, middle initial, last name)

John P. McCormick

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
May 1971	49	

8a. CONTRACT OR GRANT NO. DAAK01-70-D-4142-0003 b. PROJECT NO. c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) B03-01-1-1120 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEMENT

Distribution limited to U.S. Government agencies only; proprietary information; May 10, 1971. Other requests for this document must be referred to the Electrotechnology Department, U.S.A. MERDC.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	U.S. Army Mobility Equipment Research and Development Center Electrotechnology Lab-SMEFB-EE, Ft. Belvoir, Va

13. ABSTRACT

This report presents the results of a reliability review and analysis of two competing open-cycle fuel-cell designs. A mathematical model is presented which allows for evaluating the reliability of the designs. A failure modes and effects analysis is presented for each of the proposed designs. A prediction of the reliability and availability of each of the competing designs is presented.

DD FORM 1 NOV 65 1473 REPLACES DD FORM 1473, 1 JAN 64, WHICH IS OBSOLETE FOR ARMY USE.

Unclassified
Security Classification

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Fuel Cell, Open Cycle						
Reliability						
Failure Modes and Effects Analysis						
Maintainability						

Security Classification

UNCLASSIFIED

RELIABILITY REVIEW AND ANALYSIS OF THE OPEN-CYCLE FUEL-CELL POWER PLANT

by
John P. McCormick

10 May 1971

Prepared for
U.S. Army Mobility Equipment
Research and Development Center
under Contract DAAK01-70-D-4142-0003

Distribution limited to U.S. Government agencies only; proprietary information; May 10, 1971. Other requests for this document must be referred to the Electrotechnology Department, U.S.A. MERDC.

ARINC Research Corporation
a Subsidiary of Aeronautical Radio, Inc.
2551 Riva Road
Annapolis, Maryland 21401
Publication B03-01-1-1120

UNCLASSIFIED

ABSTRACT

ARINC Research Corporation conducted a reliability review and analysis program to provide the U.S. Army Mobility Equipment Research and Development Center with an evaluation of the failure modes and effects and a quantitative reliability prediction for two manufacturers' proposed Open-Cycle Fuel-Cell Power Plant systems. The failure modes and effects analyses produced recommendations concerning the design adequacy and ultimate maintainability of the proposed systems. Historical failure-rate data were compiled, and a reliability-prediction mathematical model was developed for each manufacturer's system. A computer program was developed to exercise this model, and reliability predictions were made for the two systems for different environmental conditions.

FOREWORD

This report was prepared by ARINC Research Corporation for the U.S. Army Mobility Equipment Center, Fort Belvoir, Virginia, under Contract DAAK01-70-D-4142. Its purpose is to provide a quantitative reliability prediction of the Open-Cycle Fuel-Cell Power Plants being developed by Engelhard Industries and Pratt and Whitney Aircraft Corporation.

ARINC Research Corporation wishes to express its thanks to Mr. M. Collins of Engelhard Industries and Mr. T. Schiller of Pratt and Whitney Aircraft Corporation for their excellent cooperation during the conduct of this program.

SUMMARY

RELIABILITY PREDICTIONS

The results of the reliability predictions made for the Engelhard Industries and Pratt and Whitney Aircraft Open-Cycle Fuel-Cell designs are summarized as follows:

Environment	Predicted Reliability*	
	Engelhard	Pratt & Whitney
Laboratory	.9540	.9130
Portable Ground	.9185	.8189
Tracked Vehicle	.7870	.6828

*Probability of completing 24-hour operation without failure.

The analyses conducted in this study indicate that only the Engelhard design meets the reliability goal of 95 percent. If Pratt and Whitney substituted a nickel-cadmium secondary battery for a silver-zinc battery, their proposed design would also meet the goal. This study, however, was based on the contractor's tentative design midway through Phase I. Certain component changes could result in higher reliability.

ARINC Research believes that currently the design is not final enough and there is not enough experience on the system or its components to determine an absolute value for reliability. For the purpose of comparing the two manufacturers' designs, the reliability predictions made in this study are adequate. They are, however, inadequate for comparison against another power-plant technology. In addition, because the open-cycle fuel cell is in an early stage of development, it was not possible to obtain data that would permit determining the confidence levels on the computed reliability values.

CONCLUSIONS AND RECOMMENDATIONS

The conclusions and recommendations resulting from this study are summarized as follows:

- The Engelhard Industries design shows a higher reliability than the Pratt and Whitney Aircraft design. If P&WA followed the recommendation to use a nickel-cadmium secondary battery in place of a silver-zinc battery, the P&WA design would show the slightly higher reliability. ARINC Research believes that the weight penalty involved in using the nickel-cadmium battery rather than the silver-zinc battery is compensated for by the increased reliability and is also mitigated by the USAMERDC decision to eliminate the fuel tank from the design.

- The most prevalent failure mode identified in the Failure Mode and Effects Analysis was leakage, which varied in its effects from critical to minor. Because this mode can occur at a great number of points in the system, a comprehensive leakage specification should be prepared and imposed on every new power plant and on every power plant that is rebuilt.
- Some provisions should be made for identifying the components or subsystems of the power plant that have failed. There are no monitoring devices for either system design that would allow maintenance personnel to pinpoint the cause of cell-output failure. There are many components in the subsystems whose failure could result in cell-output failure. Isolating the cause is currently a trial-and-error task.
- The fuel solenoid valve in the Engelhard design appears to serve no essential purpose. Since its failure to open would preclude fuel-cell operation, it should be eliminated. A manually operated valve could be substituted to provide for servicing and safety. Consideration should also be given to redesigning the Engelhard system to use only a single fuel pump; this would reduce the pump failure rate by one-half.
- It is recommended that another reliability and availability prediction of the Open-Cycle Fuel-Cell Power Plant be performed before the Advanced Development Model (ADM) is completed. This would update the prediction made in this study and permit the use of operational and test data accumulated on the system and its components. In addition, the design of the electronic systems should be completed by that time, which would permit a more precise prediction than was made in this study.

CONTENTS

CONTENTS (continued)

CHAPTER ONE

INTRODUCTION

Under Contract DAAK01-70-D-4142 to the U.S. Army Mobility Equipment Command, ARINC Research evaluated the reliability of two Open-Cycle Fuel-Cell Power Plants under development for the Electrotechnology Department at the U.S. Army Mobility Equipment Research and Development Center (USAMERDC).

The purpose of these evaluations was to make quantitative reliability predictions for the two candidate configurations and to provide USAMERDC with the basic tools for performing future reliability analyses. The following tasks were performed for each configuration:

- Review available information on the open-cycle fuel-cell power plant to establish baseline data
- Identify a representative mission and define failure
- Perform a failure modes and effects analysis
- Develop a reliability-prediction model at the major-component level that is flexible enough to permit configuration changes and the use of various types of failure distributions, and to determine sensitivity to input data
- Perform a reliability prediction for the two candidate systems in the anticipated operating environments and for a hypothetical system with idealized characteristics
- Develop an estimate of the mean active-repair times and availabilities for the candidate systems
- Identify the functional level of maintenance

This report presents a background discussion and description of the candidate systems, a failure modes and effects analysis for each system, the reliability-prediction model used and the predictions resulting from its use, and the conclusions and recommendations resulting from the study.

CHAPTER TWO

BACKGROUND

2.1 GENERAL

The U.S. Army is currently conducting a technical evaluation of silent ground-power systems. The Open-Cycle Fuel-Cell Power Plant, designed by USAMERDC, is one of the candidate systems. Two contracts to develop an Open-Cycle Fuel-Cell Power Plant were awarded by USAMERDC. One was awarded to Engelhard Industries of Newark, New Jersey, and the other to Pratt and Whitney Aircraft of East Hartford, Connecticut. The contracts called for the development of a system in accordance with "Purchase Description for Open-Cycle Fuel-Cell Power Plant, Direct Current, 1.5 Kilowatt," dated 23 January 1970.

The Purchase Description outlined the specifications for the development of an Advanced Development Model (ADM) Open-Cycle Fuel-Cell Power Plant set. The set is to consist of a phosphoric-acid fuel-cell subsystem and fuel-conditioner subsystem with as many of the following items as required: voltage regulator, controls, fuel tank, batteries, battery-charging system, winterization equipment, weather-resistant housing, rigid skid base, and other devices as required to achieve a complete Open-Cycle Fuel-Cell Power Plant. (The requirement for a fuel tank was subsequently deleted by USAMERDC.)

Engelhard Industries and Pratt and Whitney Aircraft have been developing a 1.5-kW breadboard power plant and will submit a design for a 1.5-kW ADM power plant as part of the Phase I requirements. USAMERDC will evaluate the proposed ADM design in order to determine which contractor is to be awarded the Phase II contract for the development of the family of fuel-cell power plants. Phase II requires deliveries of 1.5-kW ADM power plants.

2.2 SYSTEM REQUIREMENTS

The salient features of the ADM Purchase Description are the noise, weight, volume, and starting requirements. During operation, the generator set shall be inaudible in any direction at a distance of 100 meters. Its weight, exclusive of fuels, shall be 150 pounds or less, and its volume shall be less than eight cubic feet. Without a winterization system, the set shall be capable of starting within 15 minutes; and with winterization equipment, it must be capable of starting within 30 minutes. A minimum operating time of 1500 hours (5000 hours desired) without servicing, maintenance, overhaul, or replacement of parts other than routine servicing and periodic adjustment is required. The set shall have a reliability of 95 percent with a confidence level of 90 percent for a mission duration of 24 hours, with an inherent availability of 98 percent. The set must also be capable of operating with combat fuels.

2.3 SYSTEM DESCRIPTION

The open-cycle fuel cell is an indirect hydrocarbon-air fuel-cell system tailored specifically for low-power tactical uses. The process schematic, Figure 1, shows this system. A regenerative thermo-catalytic cracker converts the fuel (gasoline, kerosene, etc.) to a hydrogen-rich gas, which in turn is electrochemically oxidized in a fuel cell to produce electrical power. The hydrogen-generation and fuel-cell subsystems are described below.

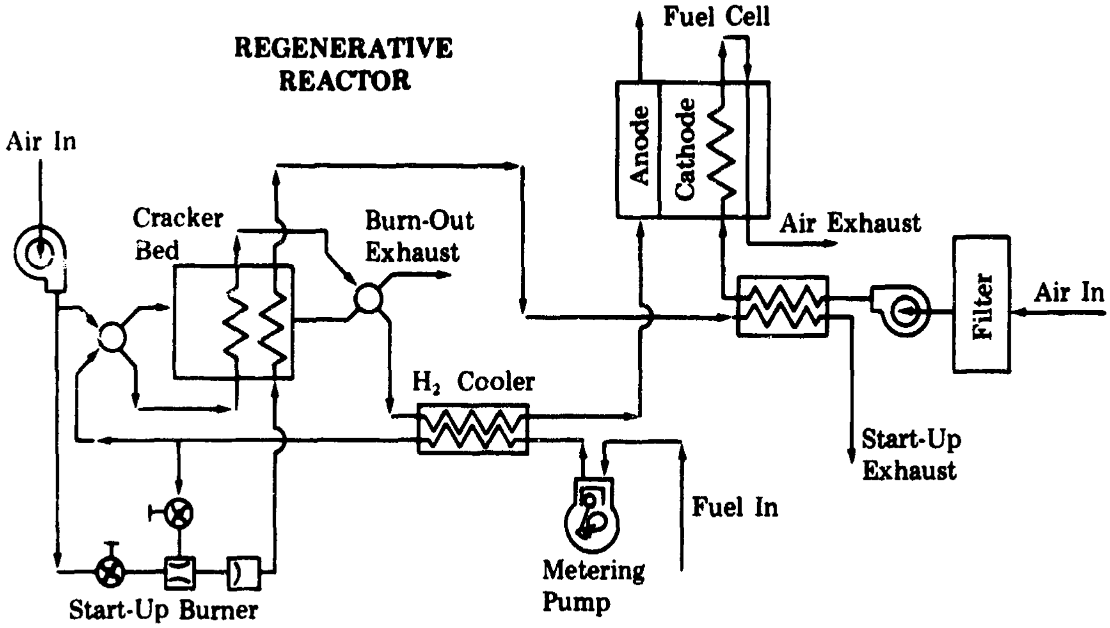


Figure 1. SCHEMATIC, OPEN-CYCLE FUEL-CELL POWER PLANT

The open-cycle system has no closed process loops, which gives this system its name. As shown in Figure 1, the fuel passes through the cracker to the cell, where most of the hydrogen is consumed and the excess and diluents are exhausted. The primary control fluid for each subsystem is air. Each subsystem has its own air supply and control operating in total independence of each other. One feedback control is desirable, however, to throttle the power plant by matching fuel flow rate to hydrogen demand. Unlike earlier closed-loop systems, no special control logic is required to stabilize the system during transient-load conditions.

2.3.1 Hydrogen-Generation Subsystem

In regenerative thermo-catalytic cracking, the hydrocarbon fuel passes through a hot catalyst bed, cracking to hydrogen and carbon. The carbon is retained by the catalyst, and the endothermic cracking energy is supplied by the sensed heat change of the bed. Before the bed plugs with carbon or its temperature drops below an efficient cracking level, the fuel flow is switched to a second bed so that hydrogen production is not interrupted. The first bed is regenerated by burning the stored carbon, which reheats the catalyst bed. The process streams are switched at approximately three-minute intervals, depending on bed size and fuel flow rates. Bed-temperature variations during a complete cracking-regeneration cycle are usually maintained between limits of 1500° and 1900° F.

The product gas compositions and flow rates for a complete cycle are shown in Figure 2. The hydrogen produced represents approximately 88 percent of that contained in the combat gasoline. The remaining hydrogen is formed into methane plus small amounts of ethane, benzene, and water, and is not usable. The product composition and yield for kerosene-type fuels is similar.

The burn-out-cycle gas composition shown in Figure 2 represents the minimum air flow found necessary for carbon removal, equal to an average combustion product of equal volumes of CO and CO_2. The heat of combustion for this product exceeds the cracking-energy requirement. With ambient air used for combustion and exhausted at bed temperature, the heat of combustion is more than twice that required for cracking. At high fuel-flow rates, burning the carbon to less than stoichiometric CO_2 minimizes the bed's cooling requirement. Conversely, at low fuel-input rates representative of part-load power-plant operation, a proportionally higher air flow completes the combustion to CO_2, releasing additional heat to offset thermal losses.

The most important aspect of the regenerative cracking process for military use is its performance using low-grade, impure fuels, such as combat gasoline. In the regenerative cracker, lead is removed from the bed during the burn-out in much the same way as in an engine. Sulfur in the fuel is retained on the catalyst during the hydrogen-generation portion of the cycle and is then burned off by the air. The nickel catalyst favors reduction of hydrogen sulfide in the reducing atmosphere of the cracking cycle, while the formation of sulfur dioxide is favored thermodynamically when oxygen is present.

2.3.2 Fuel-Cell Subsystem

The fuel-cell subsystem is based on phosphoric-acid-electrolyte fuel-cell technology. A phosphoric-acid fuel cell has two characteristics that make it desirable in this application:

1. It is thermally stable and nonreactive with any component in air or in a hydrogen-product stream derived from logistic fuels.
2. It is usable at moderate temperatures — 250° to 300° F — temperatures at which carbon monoxide is not strongly absorbed on the anode catalyst and at which the fuel-cell waste heat can be removed by the process air stream.

These two characteristics benefit the power plant because they minimize subsystem interface with the fuel conditioner and permit singularly simple fuel-cell-subsystem control.

The hydrogen-generator product stream, dilute in hydrogen and containing carbon monoxide, can be used by this fuel cell without purification. Similarly, the reactant air needs no pretreatment.

The process-control requirements for the phosphoric-acid-electrolyte fuel cell (reactant oxygen supply, product water removal, thermal control) are simple. The water produced in any air-breathing fuel cell is removed by evaporation into the reactant air stream. With other aqueous electrolytes, the air stream must be carefully proportioned to electrical-current drain to prevent either electrolyte dilution or concentration beyond narrow limits. Anhydrous phosphoric acid at 250° to 300° F. retains an adequate ionic conductivity; therefore, there is no constraint on maximum air flow over the cathode to prevent excessive

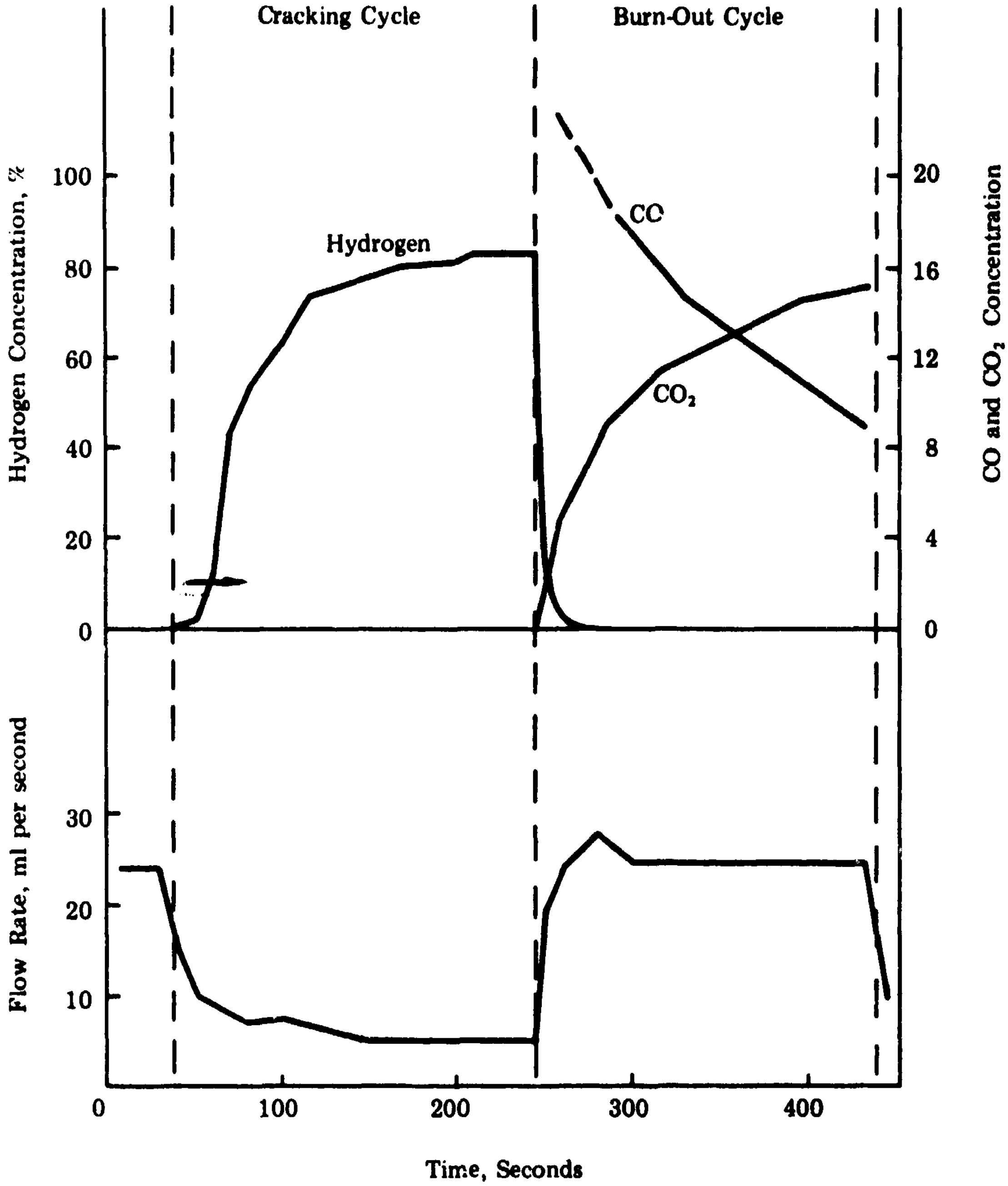


Figure 2. **REGENERATIVE-CRACKER PRODUCT**

electrolyte concentration. An air-flow rate high enough to remove all the cells' waste heat will automatically provide the oxygen for the electrochemical reaction and remove all product water without disabling the cell.

Phosphoric acid has two major electrochemical deficiencies in comparison with other fuel-cell electrolytes: first, it has by far the poorest conductivity, which limits the power capability of a unit of cell area because of internal resistance losses; second, its corrosiveness limits the electro-catalyst, with present technology, to platinum-group metals.

CHAPTER THREE

RELIABILITY-PREDICTION MODEL

3.1 SYSTEM DEFINITIONS

Each of the contractors, Engelhard Industries and Pratt and Whitney Aircraft, is developing a 1.5-kW breadboard power plant and will submit a design for a 1.5-kW Advanced Development Model. Each of the contractor's proposed models consists of hydrogen-generation, fuel-cell, and electronic-control subsystems. The hydrogen-generation and fuel-cell subsystems of each are designed to accomplish the functions described in Chapter Two. The electronic-control subsystems provide power regulation as well as control of the electrically actuated components of the system.

The following subsections provide a brief description of the proposed designs of each of the contractors.

3.1.1 Engelhard Industries System

Figure 3 is a schematic of the proposed ADM design from Engelhard. This design incorporates dual fuel pumps that are alternately cycled-on electronically to provide fuel to the reactors (cracker beds) during the thermal-cracking or hydrogen-generation phase. They are alternately cycled-off during the burn-off phase. A check-relief valve is inserted in each fuel-supply line to guard against back pressure to the pump. Air is cycled alternately to the reactors by means of spring-loaded, cam-actuated valves. A cam drive train, actuated by a slow-speed motor, actuates the air-inlet valves, the burn-off exhaust valves, and the hydrogen-supply valves. The cams are designed to provide the proper sequencing of: (1) fuel and air into each of the reactors, (2) burn-off effluent to the three-way valve, and (3) generated hydrogen to the fuel-cell stack. The three-way valve is used either to exhaust the burn-off effluent to the atmosphere or to divert it through a heat exchanger in the fuel-cell stack to bring it to the proper operating temperature.

A gas trap is placed in the hydrogen stream between the hydrogen-generation and fuel-cell subsystems to cleanse the hydrogen of any methane, lead, or sulfur impurities.

The fuel-cell stack consists of approximately 60 phosphoric-acid cells that are cooled by an air-manifold device. The temperature of the stack is controlled by allowing exhaust gas to be diverted through the heat exchanger as described above.

Control of the fuel cell is provided by the power conditioner, central sequence timer, fuel-cell demand detector, and other circuits as shown in Figure 3.

The cell is started up initially by burning fuel in both reactors and venting the exhaust through the fuel-cell-stack heat exchanger. Fuel is ignited by the use of a platinum-wire

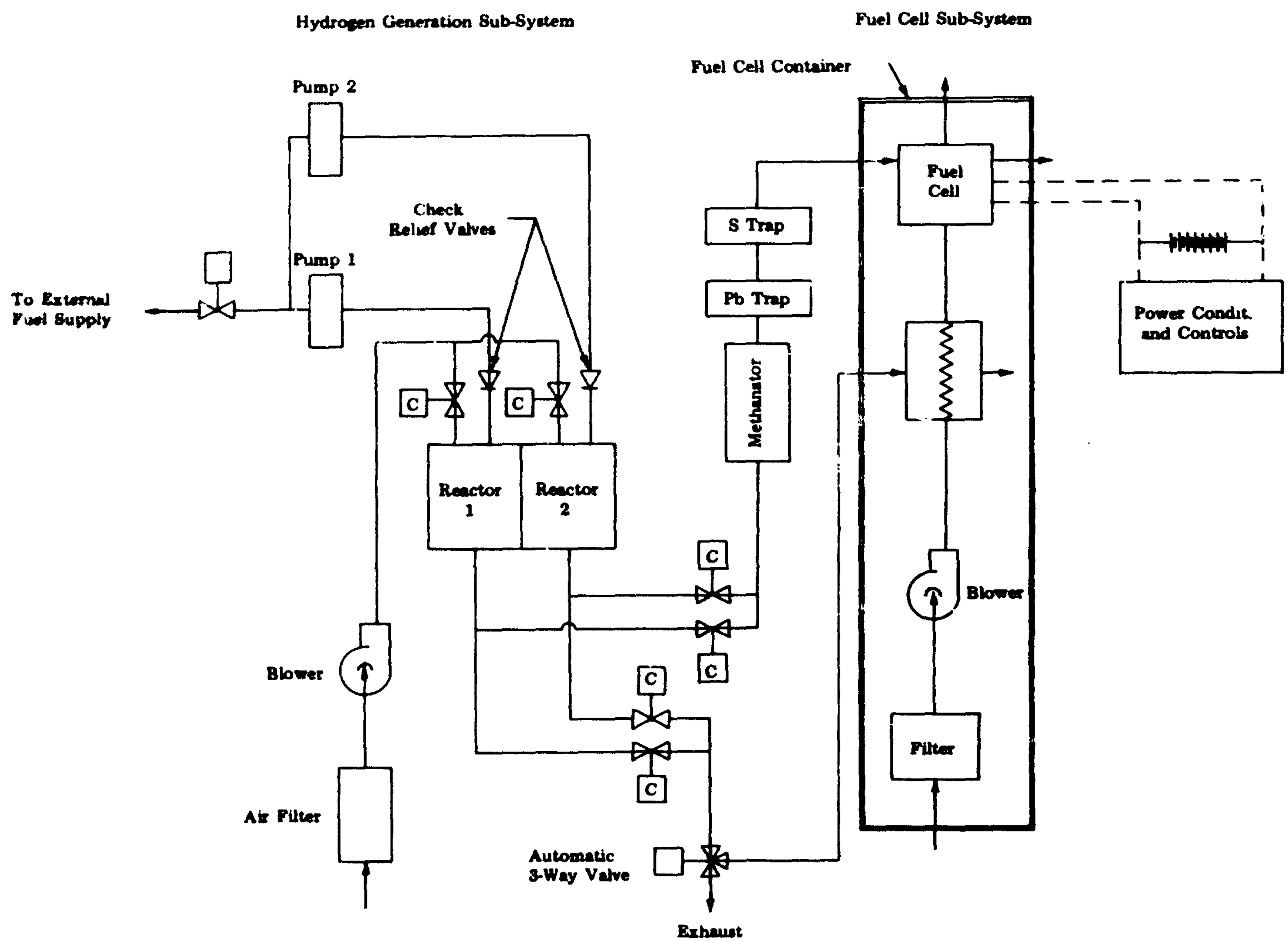


Figure 3. **ENGLEHARD INDUSTRIES OPEN-CYCLE FUEL-CELL POWER PLANT**

igniter in the reactor. This ignition continues until the cell stack reaches its operating temperature. The number 2 fuel pump is then shut off and the thermal cracking process is started in the number 1 reactor. The cell is then operated by cycling between reactor number 1 and reactor number 2. The optimum cycle time has not yet been determined. Start-up power for the igniters and pumps is provided by a nickel-cadmium secondary battery.

3.1.2 Pratt and Whitney Aircraft System

Figure 4 is a schematic of the proposed Pratt and Whitney ADM design. This design incorporates a single fuel pump that is continuously energized during system operation. Cycling between crackers is accomplished by means of fuel solenoid valves actuated by an electronic control unit. Similarly, air is cycled into the crackers during the purge cycle by means of solenoid valves that are actuated by an electronic control unit. A diverter valve is positioned downstream to divert hydrogen gas into the fuel-cell stack and the burn-off effluent into the fuel-cell-stack heat exchanger. Fuel-cell process air is suppiied by an air blower. The fuel-cell stack is equipped with a recycle control system, which allows the air not used in the electrolytic process to be recycled, thus retaining some of its heat. A recycle control valve is provided to open the exit-air plenum to the atmosphere in the event that the recycle air is too hot.

A hydrogen vent is supplied in the stack to exhaust any impurities in the hydrogen gas stream that will not react electrochemically in the cell. This vent will be some type of orifice or valve.

Electrical control is supplied by a voltage regulator (buck regulator) and an electronic control unit. The buck regulator regulates the dc power output from the cell to a constant voltage and supplies parasitic power to the electrically controlled devices in the system. The electronic control unit, not yet designed, provides approximately 15 regulating or control functions.

The Pratt and Whitney system is started up by opening up both fuel-cell solenoid valves and burning fuel in the cracker beds. The fuel is ignited by use of a conventional spark plug actuated by an exciter. Battery power from a silver-zinc secondary battery supplies the start-up power to energize the exciter and the blowers.

3.2 SYSTEM MISSION

The mission for which the reliability of the open-cycle fuel-cell system is predicted is a 24-hour system-operating time, including start-up. The system is externally connected to a fuel supply, which is not part of the reliability prediction.

3.3 ENVIRONMENTS

There is little operational information on mechanical or electromechanical equipment that relates environmental effects to equipment failure rate. Various handbooks provide data from which environmental effects can be grossly estimated by the use of a weighting factor. The three environments for which some weighting factors are available are described below.

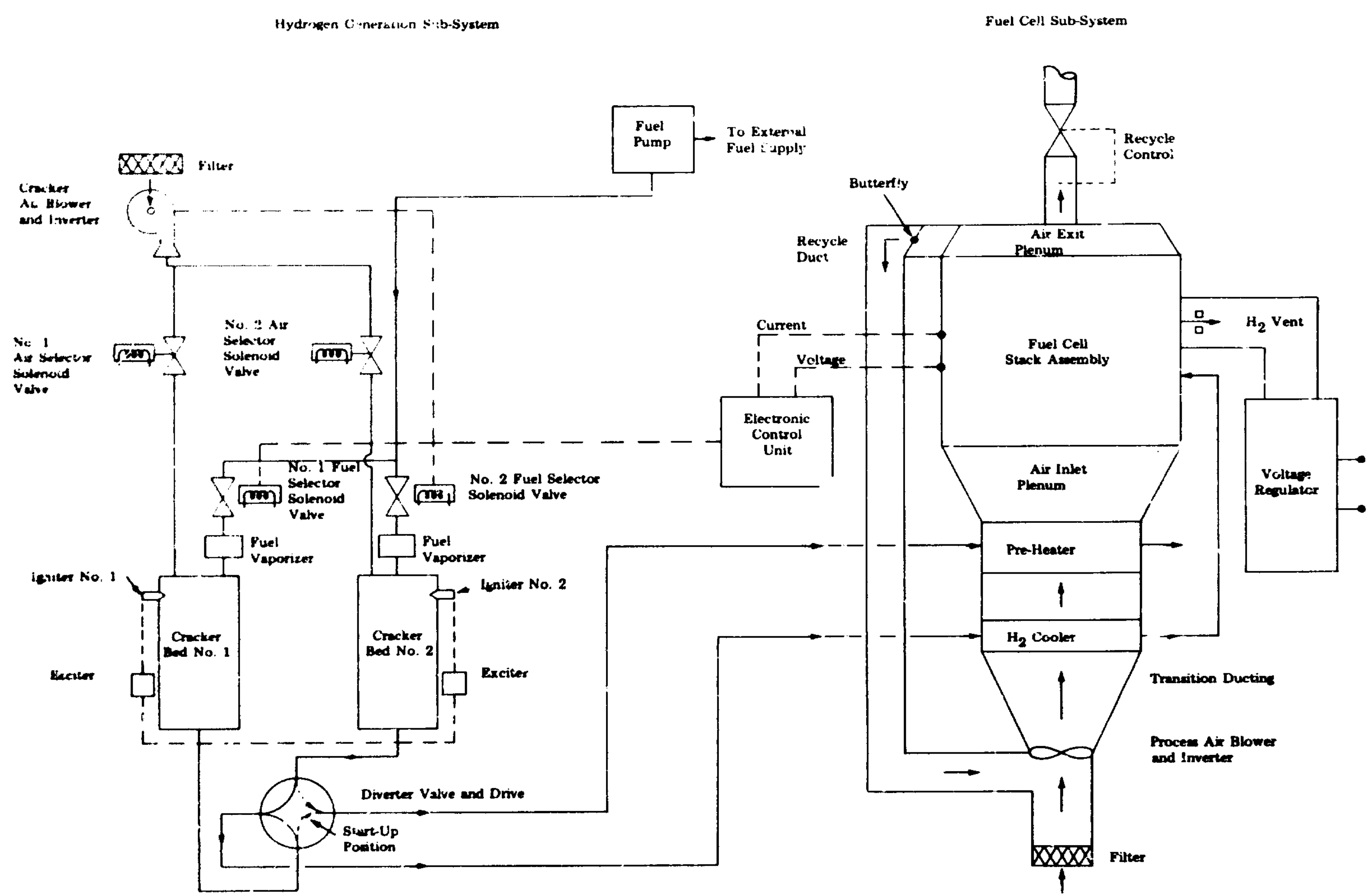


Figure 4. **PRATT & WHITNEY AIRCRAFT OPEN-CYCLE FUEL-CELL POWER PLANT**

3.3.1 Portable Ground Environment

The set is in a portable condition, not rigidly mounted in a fixed installation; it can be moved from place to place in vehicles traveling over unimproved roads and can be loaded and unloaded manually.

3.3.2 Tracked-Vehicle Environment

The set is mounted on a tracked vehicle capable of traveling over open terrain. The set is subject to severe shock and vibration in transport. It will normally be operated while the vehicle is not moving, although operation is not restricted to times when the vehicle is stationary.

3.3.3 Laboratory Environment (Hypothetical System with Idealized Characteristics)

The laboratory environment was used to meet the contract requirement to develop a prediction for a hypothetical system with idealized characteristics. It is assumed that the sets are functioning in a laboratory, with skilled personnel operating and maintaining the power plants.

3.4 FAILURE DEFINITION

The failure of any critical component that prevents the Open-Cycle Fuel-Cell Power Plant from meeting 100-percent power-output capability constitutes system failure. A critical component is any item or part whose failure would preclude successful operation of the system or create a safety hazard. This category includes the components required for starting the system.

3.5 RELIABILITY ASSUMPTIONS

In predicting the reliability of the two power-plant system designs, it was necessary to make certain asusmptions that provided the basis for the predictions. These assumptions, applied to both contractor's systems, are as follows:

- Once the system has exceeded the infant-mortality period, the failure rate does not change during the life of the system. This assumption permits using the exponential distribution to evaluate system reliability. It is imprecise to make this assumption in the case of mechanical components because such components generally experience wear-out and fail more frequently as they get older. Their reliability is more aptly characterized by the normal distribution. In using the exponential distribution, we assume an average failure rate, which might be higher than the failure rate for the time period for which the reliability is computed. An assumption is necessary here, however, because we do not have enough data or experience with the equipment's performance to characterize the failure distributions precisely. For purposes of comparing the two designs, this assumption is adequate.
- For complete mission success, all components must function in accordance with their specified requirements, without degradation or failure, for the prescribed time in the mission. This assumption does not consider the effects of any scheduled maintenance. Maintenance plans have not yet been developed.

3.6 RELIABILITY BLOCK DIAGRAMS

A reliability block diagram can be considered a logic chart that depicts, by means of an arrangement of blocks and lines, the effect of failure of equipment items on the system's functional capability. Items whose failure causes system failure are shown in series with other items. Items whose failure causes system failure only when some other item has also failed are shown in parallel with the other items.

Neither the Engelhard nor the Pratt and Whitney system incorporates component redundancy. Piece-part redundancy may exist in some of the electronic components, but reliability values were developed only at the component level. Therefore, the reliability diagram for each proposed system is a simple series arrangement of components. If we considered a degraded mode in which maximum output power was not required, the cracker beds could be considered somewhat redundant. This would be the case only if the secondary battery were so configured into the system as to provide power during the burn-out cycle. Such a configuration is most easily made in the Pratt and Whitney system since sequencing is accomplished electrically rather than mechanically, as it is in the Engelhard system.

The basic reliability block diagram for an open-cycle fuel-cell power plant is shown in Figure 5.

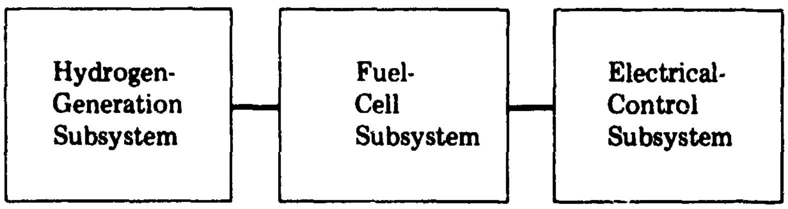


Figure 5. **RELIABILITY BLOCK DIAGRAM, OPEN-CYCLE FUEL-CELL POWER PLANT**

Basically, the open-cycle fuel-cell power plant is composed of three primary subsystems:

- **Hydrogen-Generation Subsystem.** This subsystem is made up of all the components that are required for hydrogen generation or fuel cracking. It includes all tubing to the fuel-cell stack, which carries generated hydrogen or hot gases, and the components required for start-up.
- **Fuel-Cell Subsystem.** This subsystem includes all those components involved in the process of electrochemically combining H_2 and O_2 and producing electrical power.
- **Electronic Control Subsystem.** This subsystem includes all electronic components used either to regulate fuel-cell output and provide parasitic power to the electrically actuated components or to provide electrical control of these components. It also includes the battery used for start-up.

Figures 6 and 7 are the reliability block diagrams for the Engelhard and Pratt and Whitney systems, respectively. A five-digit code is assigned to each block in the diagrams to uniquely identify each component in each subsystem. This facilitates computer processing of the data and makes it easier to add or eliminate components as the design changes.

3.7 RELIABILITY-PREDICTION EQUATION

The reliability-prediction equation expresses the mathematical relationships between the system components in the reliability block diagram, showing how they are related to overall system reliability.

The system components of the open-cycle fuel-cell power plant have essentially a direct series relationship. The computer model calculates the reliabilities of all the components individually. The elements required for these calculations are the failure distribution of each component or circuit, the component operating time or cycles, and whether or not the component is a redundant element in the overall model. These data are inputted into the model with the component's five-digit identification number (see Chapter Seven).

The series model for either system composed of n components can be simply expressed as

$$R_s = \prod_{i=1}^{n} R_i(t) = R_1 \cdot R_2 \cdot R_3 \cdots R_n$$

where

R_s = system reliability

$R_i(t)$ = reliability of the i^{th} component as a function of time (t)

t = mission time

The equations for calculating the reliabilities of three distributions for any single component are as follows:

Exponential

$$R_i(t) = e^{-\lambda_i t}$$

Normal

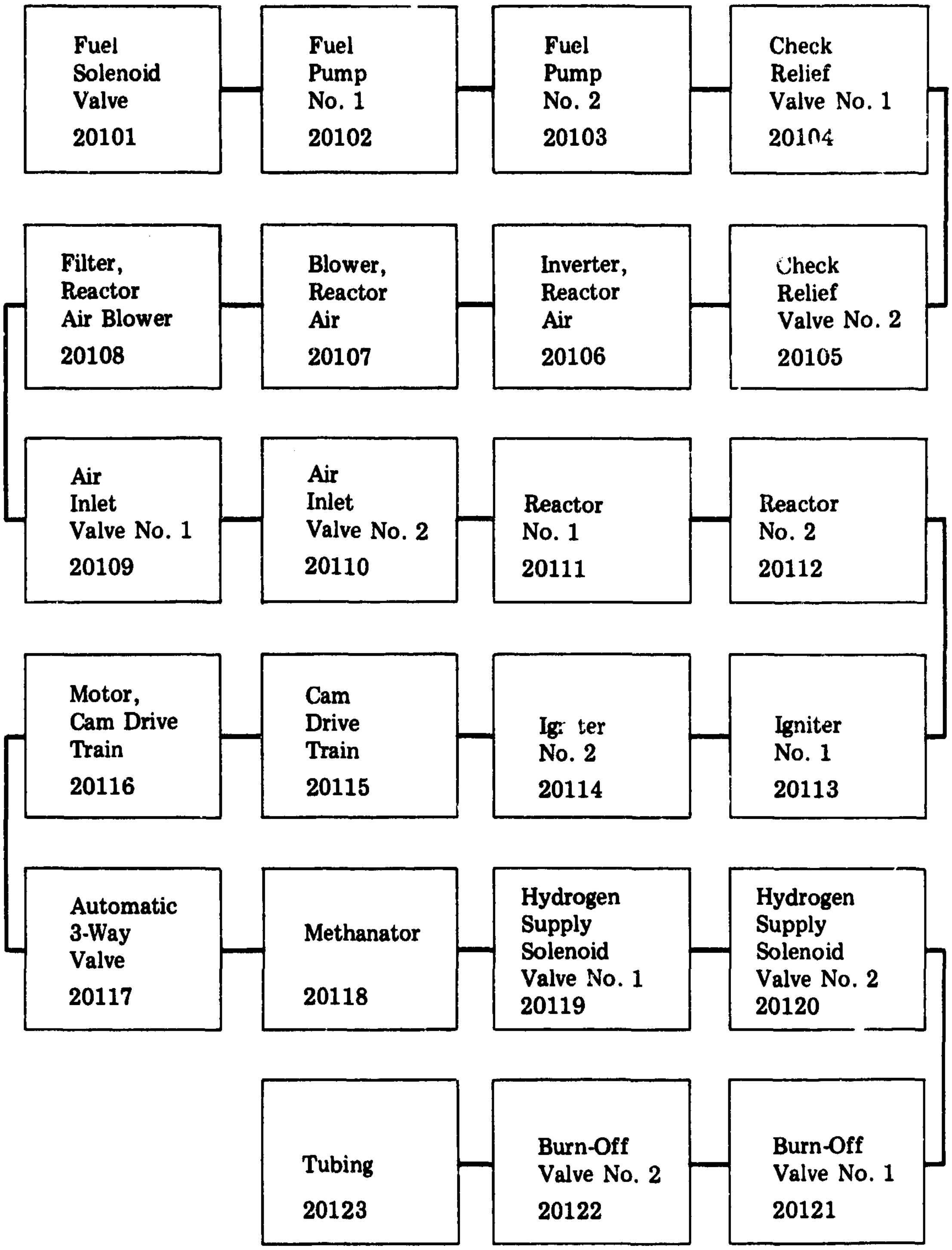
$$R_i(t) = \int_t^{\infty} \frac{1}{\sigma\sqrt{2\pi}} \, e^{-\frac{(t-\theta_i)^2}{2\sigma^2}} \, dt$$

Log Normal

$$R_i(t) = \int_t^{\infty} \frac{1}{\sigma\sqrt{2\pi}} \frac{1}{t} e^{-\frac{(\ln \theta_i t)^2}{2\sigma^2}} dt$$

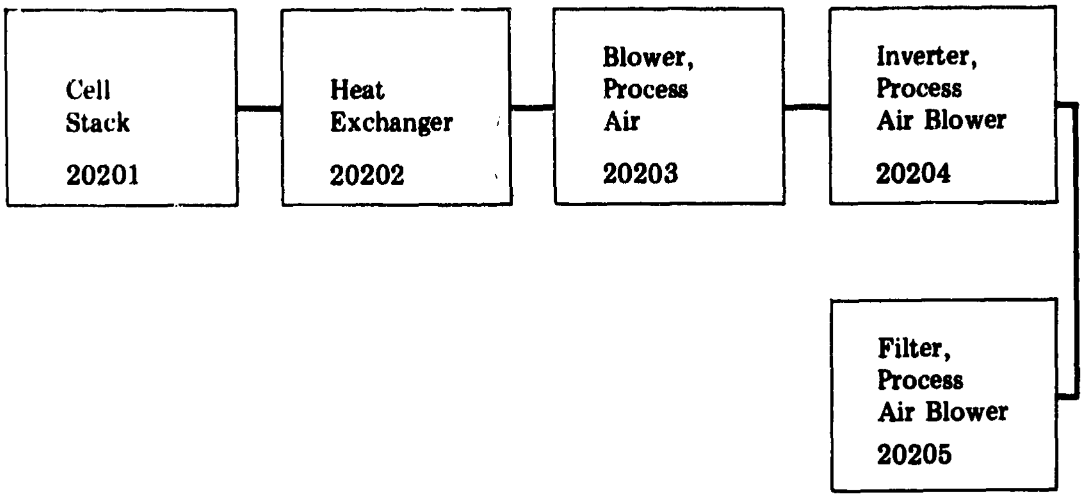
The computer program has an additional option for including a value of reliability for a component without regard to its failure distribution.

It was necessary to assume an exponential distribution of failures for the predictions in this study. However, during prototype testing and development testing, with the proper data-collection techniques and sufficient test time, it will be possible to determine the true failure distributions for each component.

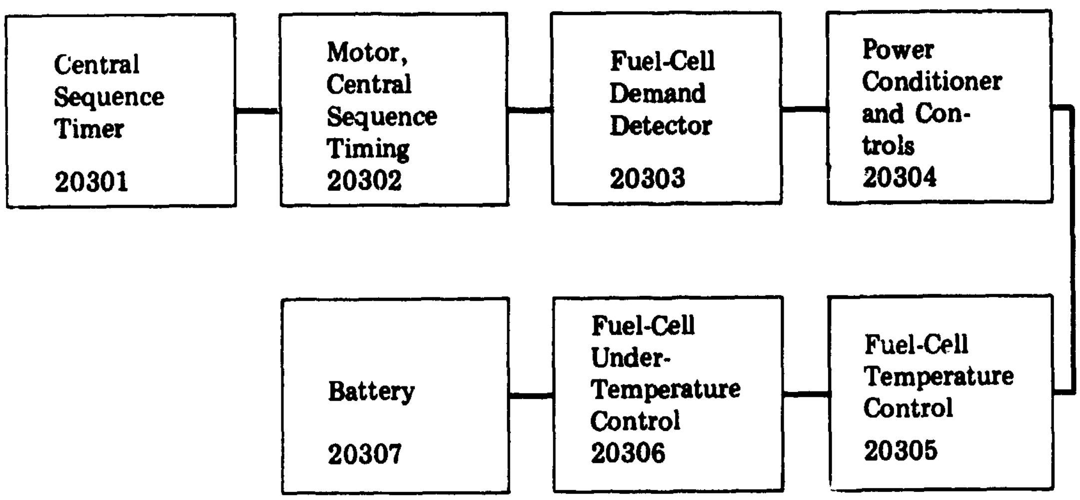


Hydrogen-Generation Subsystem

Figure 6. **RELIABILITY DIAGRAM, ENGELHARD INDUSTRIES OPEN-CYCLE FUEL-CELL POWER PLANT**



Fuel-Cell Subsystem



Electrical Subsystem

Figure 6. **(continued)**

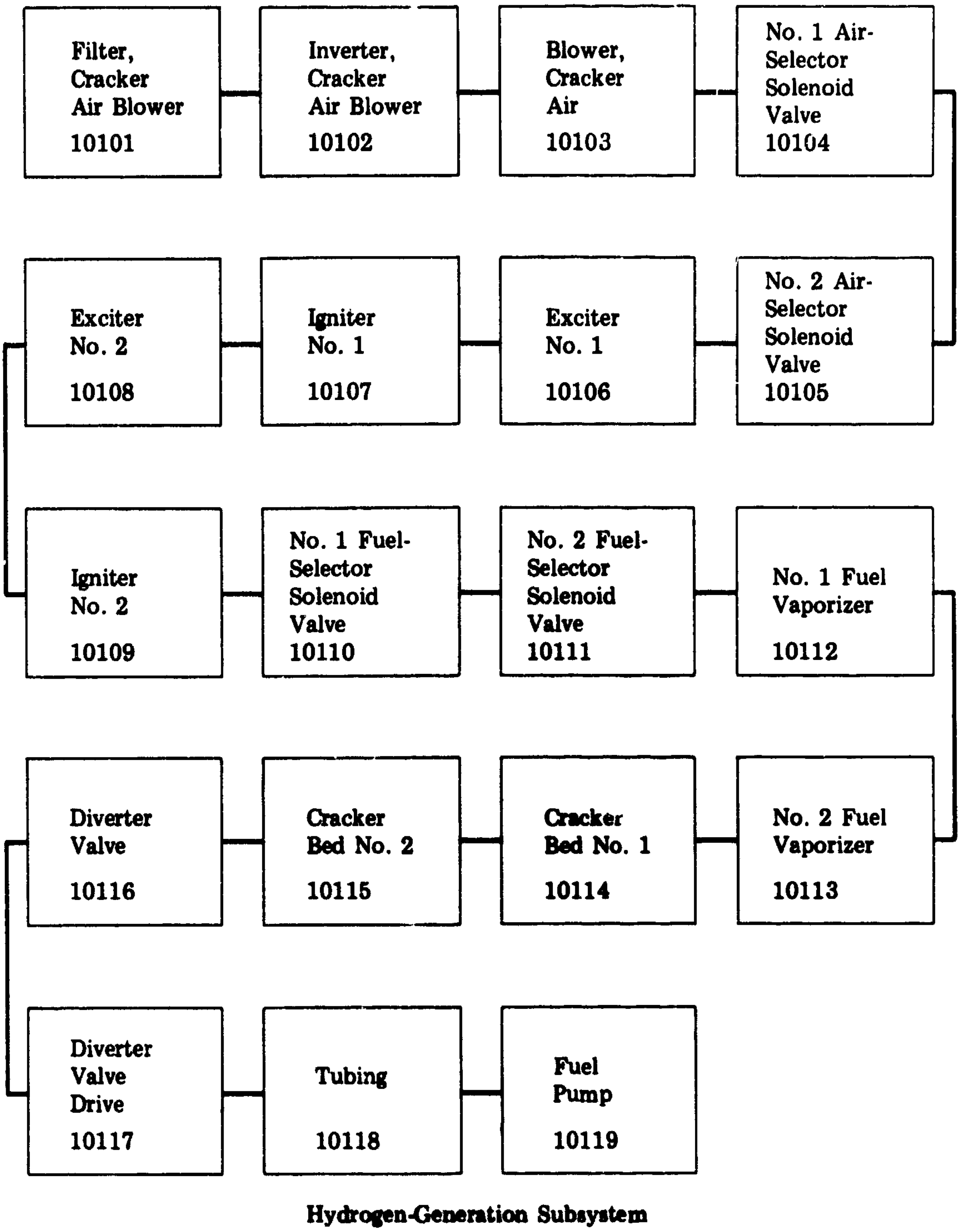
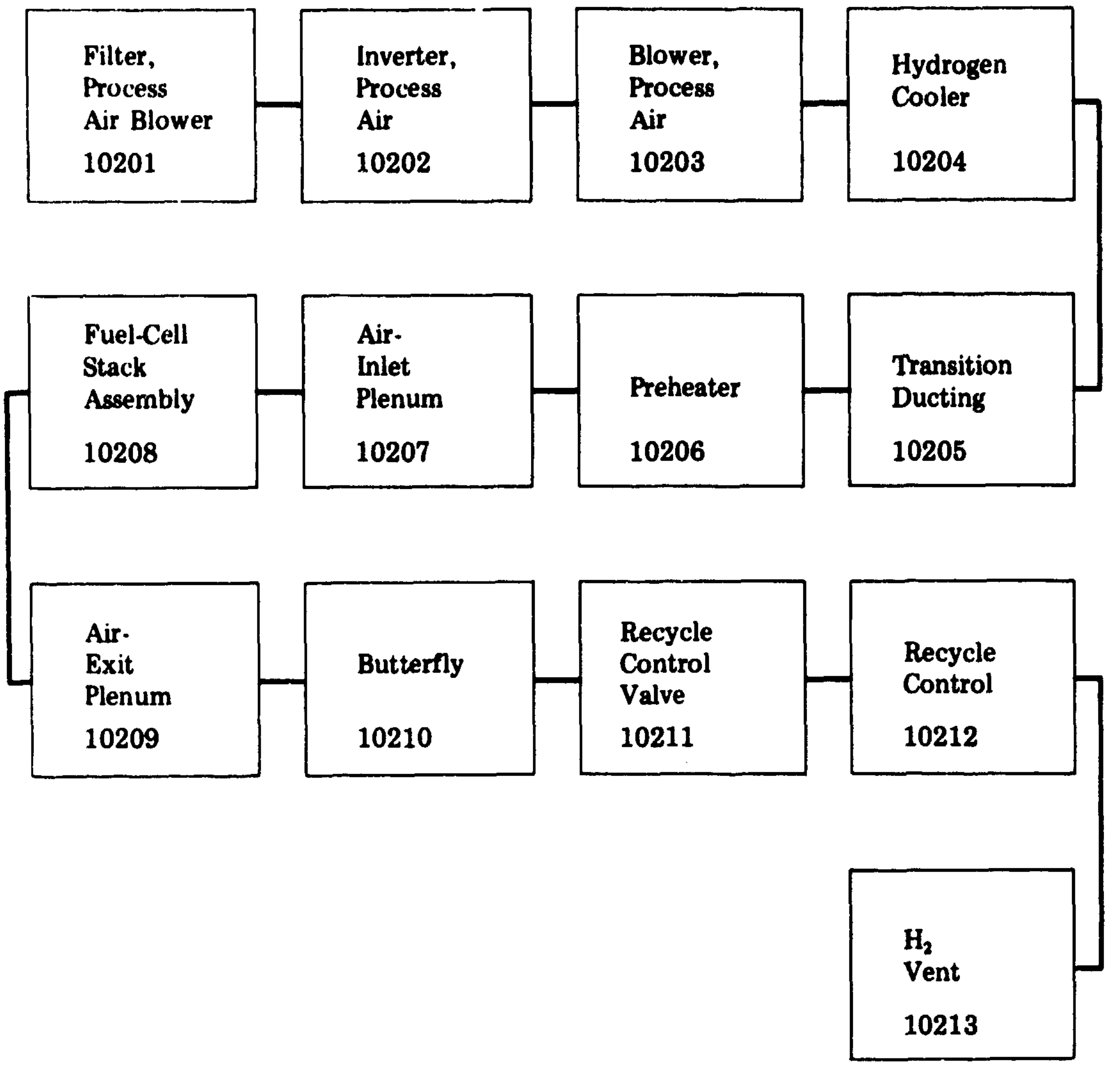
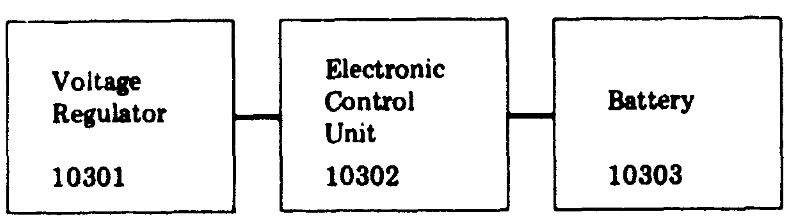


Figure 7. **RELIABILITY DIAGRAM, PRATT & WHITNEY AIRCRAFT OPEN-CYCLE FUEL-CELL POWER PLANT**



Fuel-Cell Subsystem



Electrical-Control Subsystem

Figure 7. **(continued)**

CHAPTER FOUR

DATA COLLECTION

4.1 DEVELOPMENT OF EQUIPMENT FAILURE RATES

Operational data for the fuel-cell systems being developed by each of the contractors were not available for this study. It was therefore necessary to research a number of failure-rate data sources to obtain data on components similar to those of the fuel-cell systems. The primary sources used were Government and contractor data banks, which list failure rates for a variety of mechanical, electrical, and electronic components. The sources used in this study are listed in Appendix A.

The failure rate of the generic component from each source that was found to describe best the nature and use of the components of the proposed fuel-cell systems was recorded. When failure rates for a component were available in more than one source, the sources were compared and a decision was made concerning which was most representative.

Failure-rate estimates were also obtained from manufacturers of all of the commercially available components of the two systems. In some instances, this was the only source of data.

Where the components of the two proposed systems were similar (e.g., fuel-cell stack, blowers, etc.), the same failure rate was used for both.

The failure rates tabulated in Tables 1 and 2 were assumed to have been derived under laboratory or zero-environmental-stress conditions. To project the rate of failure at other than laboratory conditions, modifying or K-factors were developed. The environmental-adjusting factors were derived by using the information given in the various failure-rate-data sources. These K-factors adjust the failure rates to the anticipated environment.

In Tables 1 and 2, three K-factors are listed. They correspond to the environmental categories listed in Chapter Three:

K_1 — Fixed Ground

K_2 — Tracked Vehicle

K_3 — Laboratory (Hypothetical System)

The same set of adjusting factors was used for all mechanical and electromechanical components. A different set of adjusting factors was used for the electronic and electrical components. The data sources used showed that these two classes of components were affected differently by environment.

Table 1. **COMPONENT FAILURE DATA, ENGELHARD FUEL-CELL SYSTEM**

Group Code No.	Component Name	Failures Per Million Hours or Cycles (cy)	K_1	K_2	K_3	Duty Cycle	Source (see Appendix A)
20101	Fuel Solenoid Valve	11.0	1.4	6	1	1	R-11
20102	Fuel Pump No. 1	8.70	1.4	6	1	0.5	R-11
20103	Fuel Pump No. 2	8.70	1.4	6	1	0.5	R-11
20104	Check Relief Valve No. 1	0.08 cy	1.4	6	1	240 cy/day	R-11
20105	Check Relief Valve No. 2	0.08 cy	1.4	6	1	240 cy/day	R-11
20106	Inverter, Reactor Air	21.00	2.5	3.5	1	1	R-11
20107	Blower, Reactor Air	55.55	1.4	6	1	1	Manufacturer
20108	Filter, Reactor Air	0.55	1.4	6	1	1	FARADA
20109	Air-Inlet Valve No. 1	16.00	1.4	6	1	1	R-11
20110	Air-Inlet Valve No. 2	16.00	1.4	6	1	1	R-11
20111	Reactor No. 1	0.2	1.4	6	1	0.5	P&WA
20112	Reactor No. 2	0.2	1.4	6	1	0.5	P&WA
20113	Igniter No. 1	0.02	1.4	6	1	10 sec.	R-11
20114	Igniter No. 2	0.02	1.4	6	1	10 sec.	R-11
20115	Cam Drive Train	0.40	1.4	6	1	1	R-11
20116	Motor, Cam Drive	9.36	1.4	6	1	1	R-11
20117	Automatic 3-Way Valve	47.3	1.4	6	1	1	FARADA
20118	Methanator	0.2	1.4	6	1	1	P&WA
20119	H_2 Supply Solenoid No. 1	50.0 cy	1.4	6	1	240 cy/day	Manufacturer
20120	H_2 Supply Solenoid No. 2	50.0 cy	1.4	6	1	240 cy/day	Manufacturer
20121	Burn-Off Valve No. 1	16.00	1.4	6	1	0.5	R-11
20122	Burn-Off Valve No. 2	16.00	1.4	6	1	0.5	R-11
20123	Tubing	0.20	1.4	6	1	1	FARADA
20201	Cell Stack	6.00	1.4	6	1	1	P&WA
20202	Heat Exchanger	5.00	1.4	6	1	1	R-11
20203	Blower, Process Air	19.00	1.4	6	1	1	Manufacturer
20204	Inverter, Process Air Blower	21.00	1.4	6	1	1	R-11
20205	Filter, Process Air	0.55	1.4	6	1	1	FARADA
20301	Central Sequence Timer	*	2.5	3.5	1	1	
20302	Motor, Central Sequence Timing	9.36	1.4	6	1	1	R-11
20303	Fuel-Cell Demand Detector	*	2.5	3.5	1	1	
20304	Power Conditioner and Controls	228.31	2.5	3.5	1.0	1	ARINC Research (AEG)
20305	Fuel-Cell Temperature Control	*	2.5	3.5	1.0	1	
20306	Fuel Cell Under Temperature	*	2.5	3.5	1.0	1	
20307	Battery	500 cy**	2.5	3.5	1.0	1 cy	ARINC Research

*Data not available, see Section 6.1 for reliability treatment.

**Assumes a complete discharge and a corresponding recharge.

Table 2. COMPONENT FAILURE DATA, PRATT & WHITNEY AIRCRAFT FUEL-CELL SYSTEM							
Group Code No.	Component Name	Failures Per Million Hours or Cycles (cy)	K_1	K_2	K_3	Duty Cycle	Source (see Appendix A)
10101	Filter, Cracker Air	0.55	1.4	6	1	1	FARADA
10102	Inverter, Cracker Air Blower	21.00	1.4	6	1	1	R-11
10103	Blower, Cracker Air	19.00	1.4	6	1	1	Manufacturer
10104	No. 1 Air-Selector Solenoid Valve	10.00	1.4	6	1	0.5	Manufacturer
10105	No. 2 Air-Selector Solenoid Valve	10.00	1.4	6	1	0.5	Manufacturer
10106	Exciter No. 1	16.70	2.5	3.5	1	10 sec.	Mfg. (MIL-STD-756)
10107	Igniter No. 1	275.00	1.4	6	1	10 sec.	FARADA
10108	Exciter No. 2	16.70	2.5	3.5	1	10 sec.	Mfg. (MIL-STD-756)
10109	Igniter No. 2	275.00	1.4	6	1	10 sec.	FARADA
10110	No. 1 Fuel-Selector Solenoid Valve	11.00	1.4	6	1	0.5	R-11
10111	No. 2 Fuel-Selector Solenoid Valve	11.00	1.4	6	1	0.5	R-11
10112	No. 1 Fuel Vaporizer	0.02	1.4	6	1	15 min.	R-11
10113	No. 2 Fuel Vaporizer	0.02	1.4	6	1	15 min.	R-11
10114	Cracker Bed No. 1	0.20	1.4	6	1	0.5	P&WA
10115	Cracker Bed No. 2	0.20	1.4	6	1	0.5	P&WA
10116	Diverter Valve	47.3	1.4	6	1	1	FARADA
10117	Diverter Valve Drive	40.0 cy	1.4	6	1	240 cy/day	Manufacturer
10118	Tubing	0.20	1.4	6	1	1	FARADA
10119	Fuel Pump	8.70	1.4	6	1	1	
10201	Process Air Filter	0.55	1.4	6	1	1	FARADA
10202	Inverter, Process Air	21.00	2.5	3.5	1	1	R-11
10203	Blower, Process Air	88.88	1.4	6	1	1	Manufacturer
10204	Hydrogen Cooler	5.00	1.4	6	1	1	R-11
10205	Transition Ducting	0.51	1.4	6	1	1	R-11
10206	Preheater	5.00	1.4	6	1	1	R-11
10207	Air-Inlet Plenum	0.51	1.4	6	1	1	R-11
10208	Fuel-Cell Stack Assembly	6.00	1.4	6	1	1	P&WA
10209	Air-Exit Plenum	0.51	1.4	6	1	1	R-11
10210	Butterfly	3.40	1.4	6	1	1	R-11
10211	Recycle Control Valve	10.00	1.4	6	1	1	Manufacturer
10212	Recycle Control Duct	0.51	1.4	6	1	1	R-11
10213	H_2 Vent	12.2	1.4	6	1	1	FARADA
10301	Voltage Regulator	186.212	2.5	3.5	1.0	1	Mfg. 217A
10302	Electronic Control Unit	450.00	2.5	3.5	1.0	1	AEG Estimate
10303	Battery	50,000 cy*	2.5	3.5	1.0	1	ARINC Research

*Assumes a complete discharge and a corresponding recharge.

There are very few failure data on mechanical equipment that show the effects of temperature extremes on operating life. Temperature effects were therefore not considered in the environmental conditions.

Tables 1 and 2 also show the mission duty cycle considered for each component. Numerical values represent the ratio of component operating time to the 24-hour mission time. Times or cycles indicate the amount of time or number of cycles the component is expected to operate during a 24-hour mission.

4.2 DEVELOPMENT OF EQUIPMENT MAINTENANCE DATA

Because development of the open-cycle fuel-cell power plant is in an early stage, there are no available data for estimating system maintainability. For the purpose of this study, it was thus assumed that the contractors can at least meet the goal established in the Purchase Description. The Purchase Description requires that the system have a mean corrective-maintenance time of three man-hours. It is assumed that corrective maintenance can always be accomplished by a single maintenance man and that the mean time to repair (MTTR) for the open-cycle fuel-cell power plant is three hours.

The maintenance policy for the system is outlined generally in the Purchase Description, which requires that the system be designed to facilitate servicing and maintenance. All components that require periodic servicing as a matter of normal routine maintenance must be readily accessible without removal of any other parts. Routine-maintenance components include filters, methanators or gas traps, igniters (spark plugs or ignition wires), gauges, etc. The location of high-failure-rate parts and parts that require frequent preventive maintenance must be such as to minimize the time and effort required to perform the necessary maintenance action.

Both Engelhard and Pratt and Whitney are designing their systems to these requirements, with a goal of easy replacement of all components. Our review of the proposed designs of both contractors indicates that this goal can be met.

With regard to maintainability, it is strongly recommended that a monitoring system be incorporated that will permit diagnoses of the cause of system failure. In the failure modes and effects analysis, it was found that several failure modes that can occur in any of the three subsystems would result in system shutdown or loss of power output. Without some form of monitoring device, the cause cannot always be determined from a visual examination of the set. Therefore, diagnostic time (and hence total repair time) will be excessive. This tends to decrease system availability and increase the spare-system requirements.

The recommended monitoring subsystem should be developed during the development of the ADM. Its design should be based on the monitoring of those failure modes that have the highest probability of causing mission failure. For example, it should be able to monitor the power conditioner and controls of the Engelhard system or the electronic control system of the Pratt and Whitney system in order to determine readily which circuits have failed.

CHAPTER FIVE

FAILURE MODES AND EFFECTS ANALYSIS

5.1 ANALYSIS METHOD

The Failure Modes and Effects Analysis (FMEA) is a systematic examination of all components of the system to identify their functions, the manner in which they might fail, and the effects of failure on the overall system in relation to mission performance and personnel safety.

The identification of problem areas can lead to design changes that will improve reliability and maintainability and produce savings for the entire program. With the results of an FMEA, program management can adjust the design test and evaluation programs to provide maximum assurance that the possibility of occurrence of critical failures has been either eliminated or reduced to an insignificant level.

In this study, a Failure Modes and Effects Analysis was conducted on the fuel-cell design proposed by each contractor — Engelhard and Pratt and Whitney. These analyses are presented in Tables 3 and 4.

The following elements comprise the FMEA format used:

- Group Code Number — the numbers assigned to each component or circuit in the reliability block diagrams in Section 3.6
- Description of Component/Assembly — the nomenclature of the components or circuits as specified by each manufacturer
- Function — the general description of each FMEA component's functioning in the system
- Failure Mode — the type of failure judged to have a significant probability of occurring during a mission
- Failure Cause — the most probable cause of the failure
- Failure Effect — the effect of the failure on the system and the mission
- Criticality — the severity of each failure mode and its related failure effect on a discrete phase of the mission:
  - Critical (C) — a failure that is judged hazardous to personnel
  - Major (M) — a failure that significantly degrades the performance of the component or delays its function such that it may not complete a mission or a discrete phase thereof

- Minor (m) — a failure that does not have a significant effect on the ability of the component to complete the discrete phase of the mission, but should be repaired eventually

- Action Taken/Avoidance Technique — the action to be taken by the user to return the set to operational condition; or the technique that can be used during manufacture to eliminate, or minimize the effect of, the failure mode or to make the set easier to repair in the field

5.2 GENERAL CONCLUSIONS AND RECOMMENDATIONS FROM FMEA

The failure mode that can occur most frequently for both the Engelhard and Pratt and Whitney designs is leakage. The failure effect varies according to the location and severity of the leakage. In some cases, the effect would be minor. In any event, this mode can occur on most of the components. It is recommended, therefore, that specifications be developed for leakage and that leak tests be designed accordingly. As a minimum, each newly built system or rebuilt system should be thoroughly leak-tested prior to use. The cause of any detected leakage above the specification limits should be determined and eliminated.

In the design of the ADM, and ultimately the production-model fuel cell, serious consideration should be given to the logistics implications of cost, schedule, availability, maintainability, spares, and training requirements. For example, the manufacturer of the blowers for both the fuel-cell air and the reactor air recommends that the blower-motor bearings not be stored for more than six months in humid climates and one year in dry climates. This will have an important impact on spares-provisioning and replacement policies. It may be necessary, for example, to develop some sort of storage container for the blowers or bearings, or both, that would minimize the effects of long-term storage. This, in turn, would add to the total system cost. Alternatively, an investigation could be made to determine the possibility of incorporating a blower with longer bearing shelf life.

In the design of the production model, provisions should also be made for monitoring the various functional elements of the system to determine their operability. There is little provision for such monitoring in either the Engelhard or Pratt and Whitney proposed designs. Monitoring is necessary for efficient troubleshooting of the system and for repair without excessive downtime. The monitoring system developed should be compatible with the maintenance philosophy. Monitoring of field-replaceable units, for example, should be a prime consideration.

5.3 ENGELHARD DESIGN CONCLUSIONS AND RECOMMENDATIONS

The following conclusions and recommendations resulted from the FMEA of the Engelhard design:

- The fuel solenoid valve appears to serve no real purpose except as a backup check valve to the fuel pumps and the check-relief valves. Failure of this solenoid to open would preclude fuel-cell operation. (This is the predominant and most probable mode since the valve is normally closed.) Failure to close would have little or no effect since the head pressure of the fuel on the nonoperating pump would be too slight to be of any consequence. Therefore, the solenoid should be eliminated. A manually operated valve could be substituted to provide for servicing and safety.

Table 3. FAILURE MODES AND EFFECTS ANALYSIS, ENGELHARD INDUSTRIES DESIGN

Group Code No.	Description of Component/ Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/ Avoidance Technique
20101	Valve, Fuel Solenoid	Normally closed; solenoid-actuated open to allow fuel flow to fuel pump	Closed	Open circuit due to wire breakage or contact deterioration. Short circuit due to vibration or contamination.	Fuel cannot be delivered to pump and hence not into reactor. Fuel-cell operation will cease or not be started.	M	
			Open	Damaged valve spring, contamination	No effect; fuel pump spring closes cup valve, preventing fuel flow.	m	
			Leak	Vibration, poor seal, shock	Fuel will be spilled, causing fire hazard.	C	Visually check for leakage prior to operation.
20102	Pump 1, Fuel	Pumps fuel into reactor bed 1	Short, open	Vibration and/or shock	Pump will not operate, and fuel will not be delivered to reactor 1.	M	
			Leak	Damaged cover gasket, improper securing of cover, diaphragm rupture	Fuel will be spilled, causing fire hazard. May result in insufficient delivery of fuel to pump.	C	Check for leakage during operation. If leakage is detected, shut down and determine and rectify cause.
20103	Pump 2, Fuel	Pumps fuel into reactor bed 2	Short, open	Vibration and/or shock	Pump will not operate, and fuel will not be delivered to reactor 2.	M	
			Leak	Damaged cover gasket, improper securing of cover, diaphragm rupture	Fuel will be spilled, causing fire hazard. May result in insufficient delivery of fuel to pump.	C	Check for leakage during operation. If leakage is detected, shut down and determine and rectify cause.
20104	Check Relief Valve No. 1	Provides protection against reverse flow of fuel or exhaust to fuel pump 1	Open	Vibration or contamination preventing valve from seating	None, without simultaneous failure of H_2 supply solenoid 1 (closed).	m	
			Closed	Contamination or damaged spring, preventing valve from opening	Fuel cannot be delivered to reactor 1 (could be catastrophic if pressure builds up high enough.	M	
20105	Check Relief Valve No. 2	Provides protection against reverse flow of fuel or exhaust to fuel pump 2	Open	Vibration or contamination preventing valve from seating	None, without simultaneous failure of H_2 supply solenoid 2 (closed).	m	
			Closed	Contamination or damaged spring, preventing valve from opening	Fuel cannot be delivered to reactor 2 (could be catastrophic if pressure builds up high enough).	M	
20106	Inverter, Cracker Air Blower	Converts dc output from battery or fuel cell to ac input to air blower	Open, short	Vibration and/or shock, causing breaking or shorting of wiring	Cracker air blower will not operate and start-up will not be accomplished; or cracker cannot be purged.	M	
			Dielectric breakdown	Contamination by moisture, poor power regulation	Cracker air blower will not operate and start-up will not be accomplished; or cracker cannot be purged.	M	Replace inverter.
20107	Blower, Reactor Air	Provides purge air to reactors	Motor failure	Vibration, shock, etc., causing open or short circuit	Reactors cannot be purged.	M	Operation should be shut down and motor replaced.
			Bearing failure	Contamination, wear, storage deterioration	Will result in either poor blower operation or blower shutdown; resulting in subsequent system shutdown.	m	Replace blower when bearings become noisy. Bearings cannot be replaced or greased. Manufacturer recommends no more than 6 months' storage of bearings.
20108	Filter, Reactor Air	Filters purge air	Clogged	Ambient dust and dirt particles	Air blower operates inefficiently.	m	Periodically replace filter. Replace frequently in dusty environments.
			Leaking	Structural failure, seal failure	Purge air is contaminated.	m	Periodically replace filter.
20109	Air Inlet Valve 1	Normally closed; mechanically actuated to allow purge air to flow into reactor 1	Open, leak	Spring binding, spring fatigue, contamination, broken shaft due to vibration or shock	Fuel-cell output failure occurs due to loss of H_2 flow to stack. Open valve will preclude pressure build-up required to allow H_2 to flow to stack.	M	Visually check spring integrity.
			Closed	Spring binding	Reactor 1 cannot be purged. Drive train could be damaged if binding precludes valve opening.	M	Visually check spring integrity.
20110	Air Inlet Valve 2	Normally closed; mechanically actuated to allow purge air to flow into reactor 2	Open, leak	Spring binding, spring fatigue, contamination, shaft break	Fuel-cell output failure occurs due to loss of H_2 flow to stack. Open valve will preclude pressure build-up required to allow H_2 to flow to stack.	M	Visually check spring integrity.
			Closed	Spring binding	Reactor 2 cannot be purged. Drive train could be damaged if binding precludes valve opening.	M	Visually check spring integrity.

*C = Critical, M = Major, m = minor.

(continued)

Table 3 (continued)

Group Code No.	Description of Component/Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/Avoidance Technique
20111	Reactor 1	Contains catalyst and provides environment for fuel cracking	Structural failure, crack, weld failure	Excessive shock and/or vibration	Pressure will drop, and H_2 flow may be degraded. All output may drop.	m	Conduct a thorough leak test on reactor prior to assembling system. Periodically inspect for cracks or weld anomalies.
			Breakdown of catalyst	Inadequate purging of reactor, thermal cycling	Catalytic action is degraded, possibly allowing impure H_2 to enter stack, thus limiting stack life.	m	
20112	Reactor 2	Contains catalyst and provides environment for fuel cracking	Structural failure, crack, weld failure	Excessive shock and/or vibration	Pressure will drop and H_2 flow may be degraded. All output may drop.	m	Conduct a thorough leak test on reactor prior to assembling system. Periodically inspect for cracks or weld anomalies.
			Breakdown of catalyst	Inadequate purging of reactor, thermal cycling	Catalytic action is degraded, possibly allowing impure H_2 to enter stack, thus limiting stack life.	m	
20113	Igniter 1 (Platinum Wire)	Provides energy source for start-up ignition in reactor 1	Open, break	Vibration, shock, degradation	Fuel cannot be ignited in reactor 1, thus precluding start-up.	M	
20114	Igniter 2 (Platinum Wire)	Provides energy source for start-up ignition in reactor 2	Open, break	Vibration, shock, degradation	Fuel cannot be ignited in reactor 2, thus precluding start-up.	M	
20115	Cam Drive Train	Actuates air-inlet valves and burn-off outlet valves	Broken or bent shaft	Vibration or shock	If broken, valve actuation cannot occur. If bent, valve actuation may not occur and will not be properly sequenced if actuation does occur.	M	Periodically inspect drive.
20116	Motor, Cam Drive Train	Actuated by central sequence timer to drive cam drive train	Open, short	Vibration, shock, contamination	Motor will not operate and valves will not be actuated. System will not function properly.	M	System should be shut down.
			Bearing failure, seizure	Contamination, corrosion	Motor may not operate and valves will not be actuated.	M	Periodically inspect motor for free-moving shaft. Replace whenever bearings are noisy.
			Shaft failure or seizure, bent	Misalignment, shock	Motor may not operate properly. Drive train may not be actuated properly.	M	
20117	Valve, Automatic 3-Way	Motor-driven to allow for diverting burn-off effluent to exhaust or to fuel-cell heat exchanger. Thermo switch on fuel cell actuates motor.	Open, leak	Spring binding, spring fatigue, contamination, shaft break	Valve must be open during run cycle; therefore, there would be no effect. During the start-up cycle, valve should be closed to allow heated gases to flow through stack heat exchanger. If it is not, stack will not reach adequate temperature.	m	During start-up, cell temperature should be monitored to determine if it is increasing to the desired level. If not, shut down and replace or repair valve.
			Closed	Shaft or spring binding	Regardless of whether it is in the start-up or run cycle, gas pressure will be built up.	C	Meter gas pressure.
20118	Methanator	Gas trap for cleansing H_2 gas supply of any methane, lead, or sulphur prior to entering cell	Clogged	Improper servicing	May inhibit flow of H_2 gas to stack.	m	With periodic replacement, this failure mode should not occur.
			Leak	Poor weld, damaged gasket or sealant	May result in pressure drop, and H_2 flow will be degraded. Cell output may drop.	m	Conduct leak test after installing new methanator.
20119	H_2 Supply Solenoid Valve 1	Normally closed, actuated open to allow H_2 gas generated from reactor 1 to flow to fuel cell	Closed	Open circuit due to wire breakage or contact deterioration. Short circuit due to vibration or contamination.	H_2 gas pressure will be built up and may cause catastrophic rupture and possible explosion.	C	Monitor pressure and tie monitor to shut-down circuit.
			Open	Damaged valve spring, contamination	Burn-off effluent will be vented to fuel cell. Cell may be poisoned and electrical output will drop. H_2 pressure will be higher than burn-off exhaust, therefore, H_2 will be exhausted out 3-way valve. Methanator may be burned out due to mixture of hot exhaust and H_2.	M	
			Leak	Improper seal caused by vibration or improper installation	H_2 gas will be leaked to surrounding environment.	C	Conduct leak test on all new system builds or rebuilds.

(continued)

Table 3. (continued)

Group Code No.	Description of Component/ Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/ Avoidance Technique
20120	H_2 Supply Solenoid Valve 2	Normally closed; actuated open to allow H_2 gas generated from reactor 2 to flow to fuel cell	Closed	Open circuit due to wire breakage or contact deterioration. Short circuit due to vibration or contamination.	H_2 gas pressure will be built up and may cause catastrophic rupture and possible explosion.	C	Monitor pressure and tie monitor to shut-down circuit.
			Open	Damaged valve spring, contamination	Burn-off effluent will be vented to fuel cell. Cell may be poisoned, and electrical output will drop. H_2 pressure will be higher than burn-off exhaust; therefore, H_2 will be exhausted out 3-way valve. Methanator may be burned out due to mixture of hot exhaust and H_2.	M	
			Leak	Improper seal caused by vibration or improper installation	H_2 gas will be leaked to surrounding environment.	C	Conduct leak test on all new system builds or rebuilds.
20121	Burn-Off Valve 1	Normally closed; cam-actuated to allow burn-off gas to exhaust from reactor 1 into the atmosphere	Open, leak	Spring binding, spring fatigue, contamination, broken shaft due to vibration and/or shock	H_2 gas pressure decreases and cell output will be lowered.	M	Visually check valve spring and shaft for structural integrity.
			Closed	Spring binding, broken shaft	Burnoff exhaust cannot be vented properly.	m	Visually check valve spring and shaft for structural integrity.
20122	Burn-Off Valve 2	Normally closed; cam-actuated to allow burn-off gas to exhaust from reactor 2 into atmosphere	Open, leak	Spring binding, spring fatigue, contamination, broken shaft due to vibration and/or shock	H_2 gas pressure decreases and cell output will be lowered.	M	Visually check valve spring and shaft for structural integrity.
			Closed	Spring binding, broken shaft	Burn-off exhaust cannot be vented properly.	m	Visually check valve spring and shaft for structural integrity.
20123	Tubing	Allows gas flow through system	Leak, rupture, crack	Vibration, shock	H_2, fuel, or air pressure will drop.	M	Conduct leak test on entire system after fabrication and after rebuild.
20201	Cell Stack	Phosphoric-acid fuel cell which provides dc electrical power through electrochemical reaction of H_2 and 0_2	Structural damage, cracked cell, broken electrode	Excessive vibration and/or shock	Stack will be unable to produce electrical power.	M	
			Clogged manifold	Impure cooling air	Cells will not be cooled properly, and output will be degraded.	m	
20202	Heat Exchanger	Provides for stack heating during start-up	Leak, crack	Excessive vibration and/or shock	Process air will become contaminated with hot exhaust effluent from reactor. Cell will be poisoned.	m	
20203	Blower, Process Air	Provides air source for fuel-cell operation	Motor failure	Vibration, shock, etc., causing open or short circuit	Fuel cell will be deprived of its oxygen source and will be shut down.	M	
			Bearing failure	Contamination, wear, storage contamination	Blower will not operate properly, with the ultimate possibility of seizure and motor shutdown. This will result in depriving fuel cell of its oxygen source.	M	Replace blower when bearings become noisy. Bearings cannot be replaced or greased. Manufacturer recommends no more than 6 months' storage of bearings.
20204	Inverter, Process Air Blower	Converts dc output from battery or fuel cell to ac input to air blower	Open, short	Vibration and/or shock, causing breaking or shorting of wire	Process air blower will not start or run, and cell output will drop to zero.	M	
			Dielectric breakdown	Contamination by moisture, poor power regulation	Process air blower will not start or run, and cell output will drop to zero.	M	Replace inverter
20205	Filter, Process Air	Filters incoming process air	Clogged	Ambient dust and dirt particles	Blower operates inefficiently.	m	Provide for periodic replacement
			Leaking	Structural failure, seal failure due to shock and/or vibration	There is a possibility of contamination of process air and subsequent contamination of cell stack	m	Provide for periodic replacement
20301 20302	Central Sequence Timer and Motor	Contains 6 microswitches which, in concert with timing motor, sequence operation of solenoid valves	Closed, shorted contacts	Contacts welded, contamination	Corresponding solenoid will not close or pump will not cut off, resulting in potentially hazardous situation	C	Circuit should be monitored to allow for automatic shutdown in event of switch failure closed
			Open, high-resistance contact	Mechanical failure caused by shock and or vibration, contamination, or worn contacts	Corresponding pump or solenoid valve will not be actuated when required, resulting in potential hazard	C	

(continued)

Table 3. (continued)

Group Code No.	Description of Component/Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/Avoidance Technique
20303	Fuel-Cell Demand Detector	Monitors cell voltage at last cell and causes fuel pump to increase or decrease depending on voltage output from cell	Electrical failure	Open or short caused by vibration, and/or shock, contamination	Fuel pump will cease operating, and cell will not function.	M	
20304	Power Conditioner and Controls	Regulates fuel-cell output power and provides parasitic power for fuel-cell components	Output failure	Open, short caused by vibration and/or shock, contamination	All control functions are lost, thus negating fuel-cell operations.		
20305	Fuel-Cell Temperature Control	Thermo-switch which controls two-speed blower to control cell-stack temperature	Open, short	Vibration and/or shock	Blower will not operate; cell will not function.	M	
20306	Fuel-Cell Under-Temperature Control	Actuates automatic 3-way valve to divert burn-off exhaust to stack heat exchanger when temperatrue drops below prescribed level	Open, short	Vibration and/or shock	Fuel-cell output will be degraded.	m	
20307	Battery	Nickel-cadmium secondary battery used to supply start-up	No output	Broken electrodes, cracks, leaks due to vibration and/or shock	System cannot be started.	M	Check battery output prior to start-up. Replace battery if output is zero.
			Thermal runaway	Inadequate recharging control	Catastrophic breakup or explosion of battery occurs.	C	Provide for control of charging current.

- Consideration should be given to a redesign in which only a single fuel pump is used, with a two-way solenoid valve for directing fuel to the proper reactor. In addition to eliminating a pump (which is susceptible to failure), this will eliminate the two check-relief valves. In the current design, if either pump fails, the system will fail, and if either check-relief valve fails to open, the system will fail. Thus there are four chances for failure. If only one pump and one two-way solenoid valve were used, there would be two less chances for failure. Additionally, the requirement for the check-relief valves is questionable because the fuel pump has a check valve that can guard against any back pressure.

5.4 PRATT AND WHITNEY AIRCRAFT DESIGN CONCLUSIONS AND RECOMMENDATIONS

The use of a silver-zinc secondary battery in the Pratt and Whitney design should be reconsidered. While a silver-zinc battery is smaller and lighter than a nickel-cadmium battery, it has two serious drawbacks for the application intended. First, it is much more susceptible to thermal runaway than a nickel-cadmium battery. Thermal runaway results from uncontrolled charging and manifests itself ultimately in a catastrophic breakup of the battery, causing a hazardous environment for personnel. Secondly, a silver-zinc battery is much less reliable than a nickel-cadmium battery.

It is recommended, therefore, that Pratt and Whitney Aircraft consider using a nickel-cadmium secondary battery in place of the planned silver-zinc secondary battery.

Table 4. **FAILURE MODES AND EFFECTS ANALYSIS, PRATT & WHITNEY AIRCRAFT DESIGN**

Group Code No.	Description of Component/ Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/ Avoidance Technique
10101	Filter, Cracker Air	Filters purge air	Clogged	Ambient dust and dirt particles	Air blower operates inefficiently.	m	Periodically replace filter. Replace frequently in dusty environments.
			Leaking	Structural failure, seal failure	Purge air is contaminated.	m	Periodically replace filter.
10102	Inverter, Cracker Air Blower	Converts dc output from battery or fuel cell to ac input to air blower	Open, short	Vibration and/or shock, causing breaking or shorting of wiring	Cracker air blower will not operate and start-up will not be accomplished; or cracker cannot be purged.	M	Replace inverter.
			Dielectric breakdown	Contamination by moisture, poor power regulation	Cracker air blower will not operate and start-up will not be accomplished; or cracker cannot be purged.	M	
10103	Blower, Cracker Air	Provides purge air to cracker	Motor failure	Vibration and/or shock, causing open or short circuit	Cracker beds cannot be purged.	M	A sensing circuit should be incorporated to provide shutdown of system when motor fails.
			Bearing failure	Contamination, wear, storage deterioration	Will result in either poor blower operation or blower shutdown, resulting in ultimate system shutdown.	m	Replace blower when bearings become noisy. Bearings cannot be replaced or greased. Manufacturer recommends no more than 6 months' storage of bearings.
10104	Air Selector Solenoid Valve No. 1	Normally closed; energized open to allow purge air to enter cracker bed 1	Open	Damaged valve spring caused by excessive vibration and/or shock	Air will be mixed with fuel in cracker bed 1 during cracking cycle, resulting in burning, which would not yield H_2 gas. Fuel back-mixing into inlet air. System will be shut down.	M	
			Closed	Electrical-connection failure due to shock and/or vibration or deterioration; spring binding	Cracker bed 1 cannot be purged, resulting in ultimate breakdown of catalyst.	M	
			Leak	Vibration and/or shock, causing seal or connection damage	May degrade flow of process air to cracker during purge cycle. May also allow H_2 gas generated in cracker to leak into atmosphere.	m	Conduct leak test on all new units or newly rebuilt units.
10105	Air Selector Solenoid Valve No. 2	Normally closed; energized open to allow purge air to enter cracker bed 2	Open	Damaged valve spring caused by excessive vibration and/or shock	Air will be mixed with fuel in cracker bed 2 during cracking cycle, resulting in burning, which would not yield H_2 gas.	M	
			Closed	Electrical connection failure due to shock and/or vibration or deterioration; spring binding	Cracker bed 2 cannot be purged, resulting in ultimate breakdown of catalyst.	M	
			Leak	Vibration and/or shock, causing seal or connection damage	May degrade flow of process air to cracker during purge cycle. May also allow H_2 gas generated in cracker to leak into atmosphere.	m	
10106	Exciter No. 1	Provides high-voltage excitation current to energize igniter	Open	Wire or connection break caused by improper assembly and/or excessive shock or vibration	Igniter will not be energized, and system cannot be started.	M	
			Short	Contamination due to bad seal or cracked case	Igniter cannot be energized, and system cannot be started.	M	
10107	Igniter No. 1	Spark plug, used during start-up to provide initial energy for fuel ignition in cracker 1	Cracked insulator	Excessive vibration and/or shock	Igniter will not function, and system cannot be started.	M	Replace plug.
			Eroded electrodes	Improper gap, inadequate replacement cycle	Igniter will not function, and system cannot be started.	M	Periodically replace spark plug
10108	Exciter No. 2	Provides high-voltage excitation current to energize igniter 2 at start-up	Open	Wire or connection break caused by improper assembly and/or excessive shock or vibration	Igniter will not be energized, and system cannot be started	M	
			Short	Contamination due to bad seal or cracked case	Igniter cannot be energized, and system cannot function	M	
10109	Igniter No. 2	Spark plug, used during start-up to provide initial energy for fuel ignition in cracker 2	Cracked insulator	Excessive vibration and/or shock	Igniter will not function, and system cannot be started	M	Replace plug
			Eroded electrodes	Improper gap, inadequate replacement cycle	Igniter will not function, and system cannot be started	M	Periodically replace spark plug

*C - Critical, M - Major, m - minor

(continued)

Table 4. (continued)

Group Code No.	Description of Component/ Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/ Avoidance Technique
10110	Fuel Selector Solenoid Valve No. 1	Normally closed; actuated open to allow fuel to be pumped into cracker bed 1	Open	Damaged valve spring caused by excessive vibration and/or shock	Possible damage to fuel pump due to chance of burn-off exhaust backing up to pump.	m	
			Closed	Electrical failure due to open or short circuit, precluding solenoid operation	Cracker bed number 1 cannot generate hydrogen gas.	M	There should be some provision made for monitoring this valve and shutting down the system.
			Leak	Vibration and/or shock, improper seal	Fuel could be spilled in surrounding environment, causing fire hazard.	C	System should be completely leak-tested when new and after every rebuild.
10111	Fuel Selector Solenoid Valve No. 2	Normally closed, actuated open to allow fuel to be pumped into cracker bed 2	Open	Damaged valve spring caused by excessive vibration and/or shock	There is a possibility of damage to fuel pump due to chance of burn-off exhaust backing up to pump.	m	
			Closed	Electrical failure due to open or short circuit, precluding solenoid operation	Cracker bed number 2 cannot generate hydrogen gas.	M	Some provision should be made for monitoring this valve and shutting down the system.
			Leak	Vibration and/or shock, improper seal	Fuel could be spilled in surrounding environment, causing fire hazard.	C	System should be completely leak-tested when new and after every rebuild.
10112	Fuel Vaporizer No. 1	Electrical heating coil used to vaporize fuel as it enters cracker bed 1	Open, broken	Vibration and/or shock	Fuel will not be vaporized. Effect not determined.	Unknown	
10113	Fuel Vaporizer No. 2	Electrical heating coil used to vaporize fuel as it enters cracker bed 2	Open, broken	Vibration and/or shock	Fuel will not be vaporized. Effect not determined.	Unknown	
10114	Cracker Bed No. 1	Contains catalyst and provides environment for fuel cracking	Structural failure, crack, weld failure	Excessive shock and/or vibration	Pressure will drop, and H_2 flow may be degraded.	m	Conduct a thorough leak test on reactor prior to assembling system. Periodically inspect for cracks or weld anomalies.
			Breakdown of catalyst	Inadequate purging of reactor	Catalytic action is degraded, possibly allowing impure H_2 to enter stack, thus limiting stack life.	m	
10115	Cracker Bed No. 2	Contains catalyst and provides environment for fuel cracking	Structural failure, crack, weld failure	Excessive shock and/or vibration	Pressure will drop, and H_2 flow may be degraded.	m	Conduct a thorough leak test on reactor prior to assembling system. Periodically inspect for cracks or weld anomalies.
			Breakdown of catalyst	Inadequate purging of reactor	Catalytic action is degraded, possibly allowing impure H_2 to enter stack, thus limiting stack life.	m	
10116	Diverter Valve	Three-way valve for diverting burn-off exhaust to exhaust, fuel-cell stack or fuel-cell preheater. Electric-actuator-driven	Leak	Particles between boron-nitrate rotor and valve surface	There is a possibility of a reduction in the flow of heating air to the cell stack.	m	
			Seizure	Corrosion, bending, spring failure	Valve will be stuck in one position, negating ability to control fuel-cell temperature.	M	Replace valve.
10117	Diverter Valve Drive	Electrical actuator, energized by the electronic control unit to actuate diverter valve	Electrical failure	Open or short circuit caused by excessive shock and/or vibration, poor electrical connection	Ability to actuate diverter valve will be precluded, with possible reduction in cell output due to either too much or not enough heat. Stack will not get fuel when required.	M	
			Mechanical failure	Contamination in gears, overheating, causing lubrication breakdown	Ability to actuate diverter valve will be precluded, with possible reduction in cell output due to either too much or not enough heat. Stack will not get fuel when required	M	
10118	Tubing	Allows gas flow through system	Leak, rupture, crack	Vibration, shock, poor weld	H_2, fuel, or air pressure will drop	M	Conduct leak test on entire system after fabrication or rebuild
10119	Fuel Pump	Pumps fuel into cracker beds	Short, open	Vibration and/or shock	Pump will not operate, and system will be shut down	M	Conduct periodic electrical checks. Replace pump if open or shorted
			Leak	Damaged cover gasket, faulty welds, diaphragm failure	Fuel will be spilled, causing fire hazard. May result in insufficient delivery of fuel to pump	C	Check for leakage during operation. If leakage is detected, shut down and determine and rectify cause
10201	Process Air Filter	Filters incoming process air	Clogged	Ambient dust and dirt particles	Blower operates inefficiently	m	Provide for periodic replacement of filter
			Leaking	Structural failure, seal failure due to shock and/or vibration	There is a possibility of contamination of process air and subsequent contamination of the cell stack	m	Provide for periodic replacement of filter

(continued)

Table 4. (continued)

Group Code No.	Description of Component/ Assembly	Function	Failure Mode	Failure Cause	Failure Effect	Criticality*	Action Taken/ Avoidance Technique
10202	Inverter, Process Air Blower	Converts dc output from battery or fuel cell	Open, short	Vibration and/or shock, causing breaking or shorting of wire	Process air blower will not start or run, and cell output will drop to zero.	M	Replace inverter.
			Dielectric breakdown	Contamination by moisture, poor power regulation	Same as above.	M	Replace inverter.
10203	Blower, Process Air	Provides air source for fuel-cell operation	Motor failure	Vibration, shock, etc., causing open or short circuit	Fuel cell will be deprived of its oxygen source and will be shut down.	M	
			Bearing failure	Contamination, wear, storage deterioration	Blower will not operate properly, with the ultimate possibility of seizure and motor shutdown. This would result in depriving fuel cell of its oxygen source.	M	Remove and replace bearing when it becomes noisy. Manufacturer recommends that storage not exceed 6 months.
10204	H_2 Cooler	Heat exchanger; cools processed H_2 from cracker	Leak, crack	Excessive vibration and/or shock, poor weld	Stack could become overheated. System would be shut down.	M	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10205	Transition Ducting	Sheet-metal formed ducting to provide medium for process air flow	Leak	Puncture, weld failure, crack	Flow and amount of process air might be hampered.	m	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10206	Preheater	Heat exchanger; uses burn-out exhaust gases to heat incoming process air when necessary	Leak, crack	Excessive vibration and/or shock, poor weld	Burn-off exhaust may be allowed to become mixed with process air and poison cell.	m	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10207	Air Inlet Plenum	Sheet-metal formed ducting to provide medium for process air to flow into cell stack	Leak	Puncture, weld failure, crack	Flow and amount of process air might be hampered.	m	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10208	Fuel Cell Stack Assembly	Phosphoric-acid fuel cell which produces dc electrical power through electrochemical reaction of O_2 and H_2	Structural damage, cracked cell, broken electrode	Excessive vibration and/or shock	The stack is unable to produce electrical power.	M	
10209	Air Exit Plenum	Sheet-metal formed ducting to provide medium for flow of process air exiting from stack assembly	Leak	Puncture, weld failure, crack	No effect, unless crack or puncture is extreme, in which case recycling function will be aborted.	m	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10210	Butterfly	Flapper-type valve used to allow recycle air to flow to recycle duct	Frozen, stuck	Rust, corrosion, foreign particles	Exit air cannot be recycled when recycle control valve is closed. Will cause cell cooling and subsequent cell-output degradation.	m	
10211	Recycle Control Valve	Remote temperature-sensing and control valve opens to exhaust recycle air when it is too hot; normally closed	Open	Spring binding	Recycle air is continuously exhausted. Cell-stack temperature may drop below proper operating level.	m	
			Closed	Failure of temperature-sensing mechanism	Recycle air will not be vented. Stack temperature may rise above proper operating level.	m	
10212	Recycle Duct	Sheet-metal formed ducting to provide flow medium for recycle air	Leak	Puncture, weld failure, crack	Recycle air will be vented to atmosphere. Effect is negligible unless leak is extreme.	m	Leak-test after initial assembly and periodically thereafter. Repair when leak is detected.
10213	H_2 Vent	Vents unreacted gases from fuel cell					
10301	Voltage Regulator	Regulates fuel-cell output power and provides parasitic power for fuel-cell components	No output	Open, short caused by vibration and/or shock, contamination	All control functions and output power are lost, thus negating fuel-cell operation.	M	
10302	Electronic Control Unit	Contains logic circuits for control of valve sequencing and other power-sequencing requirements	No output	Open, short caused by vibration and/or shock, contamination	Control functions are lost. Cell should be shut down.	M	
10303	Battery	Silver-zinc secondary battery used to supply start-up power	No output	Broken electrodes, cracks, leaks due to vibration and/or shock	System cannot be started.	M	Check battery output prior to start-up. Replace battery if output is low.
			Thermal runaway	Inadequate recharging control	Catastrophic breakup or explosion of battery will occur.	C	Provide for control of charging current.

CHAPTER SIX

RELIABILITY AND AVAILABILITY PREDICTIONS

6.1 RELIABILITY PREDICTIONS

Predictions were made of the reliabilities of the Engelhard and Pratt and Whitney proposed open-cycle fuel-cell system design. These predictions used the reliability model and procedure described in Chapter Three and the data presented in Chapter Four. The computer program used for the calculations is described in Chapter Seven.

The predictions are based on the information currently available on both the design of the systems and the failure rates of their components. They provide a fair basis for comparison between the two contractors' systems. Because of the incompleteness of the data as outlined in Chapter Four and because of the relatively early design stage of the open-cycle fuel-cell power plant, the reliability figures should be used only to compare the two competing designs and not to compare the fuel-cell technology with another power-plant technology without careful consideration of the state of development of each.

Table 5 presents the results of the reliability prediction conducted for each manufacturer's design under the environmental conditions discussed in Section 3.3. Methods are not available for establishing confidence levels on predicted reliability values. Therefore, confidence levels are not presented in this report.

Table 5. PREDICTED RELIABILITY* OF OPEN-CYCLE FUEL-CELL SYSTEMS

Environment	Engelhard Design	Pratt & Whitney Design
Laboratory	.9540	.9130
Portable Ground	.9185	.8189
Tracked Vehicle	.7870	.6828

*Probability of completing 24-hour operation without failure.

As expected, the more severe the environmental conditions, the lower the reliability. In both manufacturers' designs, the limiting factors in the reliability computations were the electronic components, for which very little information was available on design, stress

PRECEDING PAGE BLANK

levels, functions, etc. The estimates of their failure rates, therefore, were extremely gross. For example, the Electronic Control Unit in the Pratt and Whitney system is not yet designed, and its failure rate was estimated on the basis of the projected number of active element groups to be incorporated in its design. Several of the electronic devices in the Engelhard system have not yet been designed, and a description of their functions is not available. Therefore, it was assumed that the failure rate for these devices was equivalent to that estimated for the P&WA Electronic Control Unit.

As discussed in Section 5.4, the use of a silver-zinc battery by Pratt and Whitney results in a reduced reliability. To quantify the reduction in reliability, computations were made for the P&WA system with a nickel-cadmium battery substituted for a silver-zinc battery. The results were as follows:

$$R_{Laboratory} = .9593$$

$$R_{Portable\ Ground} = .9268$$

$$R_{Tracked} = .8120$$

Comparing these values with the values shown in Table 5 provides an indication of the reliability penalty being paid by P&WA with the silver-zinc battery.

6.2 AVAILABILITY PREDICTIONS

Inherent availability, a function of active operating and repair time, is the probability that the system will operate satisfactorily when called upon. Mathematically, it can be defined as follows:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

where

A_i = Inherent Availability

MTBF = Mean Time Between Failures (Hours)

MTTR = Mean Time To Repair (Hours)

Estimates of Mean Time To Repair for the proposed open-cycle fuel-cell system designs were not available for this study. The Purchase Description establishes a Mean Corrective Maintenance Time goal of three man-hours. If it is assumed that corrective maintenance can be accomplished in all cases by a single maintenance man and that Mean Corrective Maintenance Time is equivalent to Mean Time To Repair, then the inherent availabilities of the two designs can be estimated as follows (laboratory environment only and assuming that the maintenance goal of three hours can be met):

Contractor	A_i	MTBF	MTTR
Engelhard	.9941	509.55	3
Pratt & Whitney	.9837	263.73	3

CHAPTER SEVEN

COMPUTER PROGRAM

The computer program was developed on a time-sharing system with basic FORTRAN used as the language. This made the program suitable for use on USAMERDC's COMSHARE time-sharing system with their preferred XTRAN language.

The program, described and illustrated in Appendix B, is designed to assess the reliability of a simple series system. It can assess individual component redundancy when the appropriate inputs are provided for the redundant elements. Four reliability or failure distributions can be manipulated in the program: the exponential, normal, and lognormal distributions, and probability. It is not necessary for all components to have the same distribution, but one component cannot have two failure distributions at one time. The three individual K-factors can be applied to the single component failure rate to account for different system environments.

Appendix B also presents detailed instructions for exercising the program on a time-sharing computer terminal.

APPENDIX A

SOURCES OF FAILURE-RATE DATA

APOLLO Reliability Prediction, Estimation, and Evaluation Guidelines, National Aeronautics and Space Administration, December 1963. (R-11)

RADC-TR-114, Volumes I, II, and III, *Data Collection for Nonelectronic Reliability Handbook,* Rome Air Development Center, Air Force Systems Command, Griffiss Air Force Base, New York, June 1968.

Failure Information Notebook, Special Technical Report No. 32, ARINC Research Corporation, December 31, 1965.

Mechanical Design and System Handbook, Harold A. Rothbart, McGraw-Hill Book Company, New York, 1964.

MIL-HDBK-217A, *Reliability Stress and Failure Rate Data for Electronic Equipment,* Department of Defense, 1 December 1965.

Army, Navy, Air Force and NASA FARADA Failure Rate Data Program, Volumes 1, 2, 3, and 4, Naval Fleet Missile Systems Analysis and Evaluations Group, Corona, California.

APPENDIX B

COMPUTER-PROGRAM FLOW CHART AND INSTRUCTIONS FOR USE

FLOW CHART

The flow chart for the computer program is presented in Figure B—1.

INSTRUCTIONS FOR USE ON TIME-SHARING COMPUTER TERMINAL

The steps described herein must be strictly adhered to for the program to function properly.

When a link with the time-sharing system is established, the first symbol seen after "Run" is typed as an equal (=) sign. After the equal sign, type the number of components (N1) in the Pratt and Whitney system and the sum of the components in the Pratt and Whitney system and the Engelhard system (N2). Each of these variables is allocated two places, and the data must be right-justified.

A second equal sign will then appear, and the operate time must be typed. The time is allocated five places; it must be typed with a decimal place and in such a way that none of the five-digit fields overlap.

The third and last equal sign will appear, and the K-factor codes (1 to 3) must then be punched, followed by a "1" or "2", indicating that the calculations are to be made for the Pratt and Whitney system or the Engelhard system, respectively. These K factors are used to adjust the failure rate and mean values. There must be a K factor for each run; the K factor and the system code are each allocated two places, and the data must be right-justified. This ends the data entry at the keyboard at the time of execution.

The failure rates, means, accrued operating time, and K-factors and duty cycles are stored as a file and called "YRDATA."

When the data are prepunched, the following format is used, where one line represents one component:

- Columns 1-5 contain a line number code. This is not used by the model program but is used to edit and update data entries.
- Column 8 contains a "1" if the component is in series and a "2" if it is in parallel.
- Column 11 contains a "1" if the component failure rate is in failures per 10^6 hours, and a "2" if the component failure rate is in failures per 10^6 cycles.
- Column 14 contains the distribution codes:

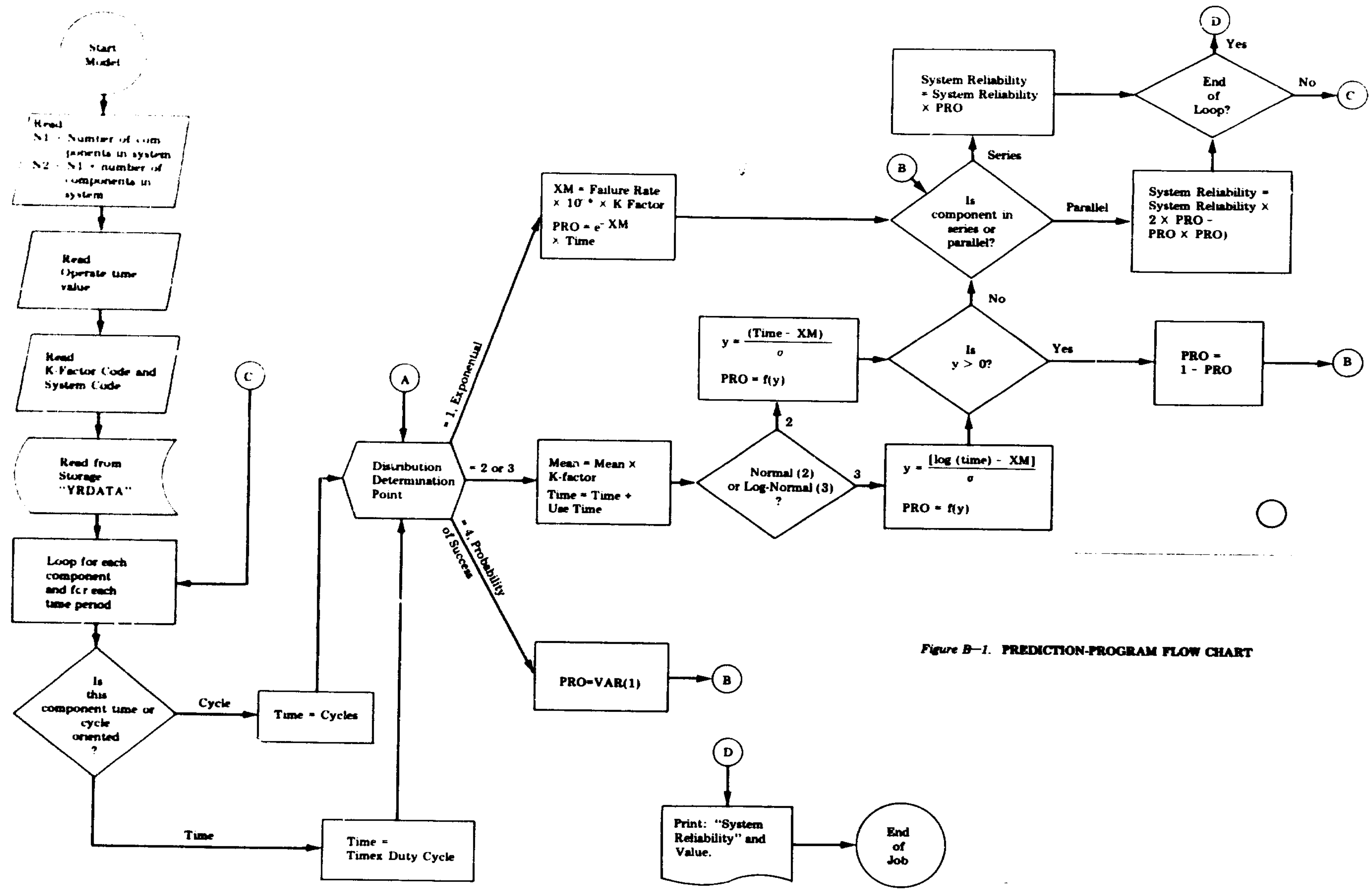


Figure B—1. **PREDICTION-PROGRAM FLOW CHART**

1 = exponential

2 = normal

3 = lognormal

4 = probability of success

- Columns 15-21 contain the exponential failure rate $\times 10^6$, or the mean time to failure (normal or lognormal), or the probability of the component's success.
- Columns 22-28 contain the standard deviation (normal or lognormal) or are set to 0.
- Columns 29-35 contain the time the component has already operated if normal or lognormal is used; otherwise, they are set to 0.
- Columns 36-42 contain K factor number 1.
- Columns 43-49 contain K factor number 2.
- Columns 50-56 contain K factor number 3.
- Columns 57-63 contain the duty cycle if Column 11 is "1" and the number of cycles of operation in 24 hours if Column 11 is a "2".

Note 1: The last seven fields must be punched with a decimal point, and no fields may overlap.

Note 2: The values associated with lognormally distributed variables must be in terms of natural logarithms.

The prediction program is shown in Figure B—2.

```
10    DIMENSIØN ISP(75,2),IDST(75),VAR(75,7),T(1),IN(75.
18    FILENAME YRDATA
20   35 READ 1,N1,N2
30   1 FØRMAT(2I2)
40    IF(N1) 36,36,37
50   36 STØP
60   37 READ 2,T(1)
70   2 FØRMAT(F5.0)
80    BEGIN FILE "YRDATA"
90 READ("YRDATA",4) (IN(I),ISP(I,1),ISP(I,2),IDST(I),
91& (VAR(I,J),J=1,7),I=1,N2)
100   4 FØRMAT(I5,3I3,7F7.2)
104   READ 1,K,M
110    PRINT:"SYSTEM RELIABILITY AND ØPERATE TIME"
120    P=1.0
130    J=1
150    IF(M-1) 17,17,18
160   17 IB=1
170   IE=N1
180   GØ TØ 19
190   18 IB=N1+1
200    IE=N2
210   19  DØ 200 I=IB,IE
212   IF(ISP(I,2)-1) 31,31,32
214   31   TIME=T(J)*VAR(I,7)
216    GØ TØ 33
218   32 TIME=VAR(I,7)
220   33 IJ=K+3
230       II=IDST(I)
240       GØ TØ (21,22,22,24),II
250    21 XM=VAR(I,1)/1000000.0*VAR(I,IJ)
260   PRØ=(EXP(-XM*TIME))
270       GØ TØ 20
280    22 XM=VAR(I,1)*VAR(I,IJ)
290   TIME=TIME+VAR(I,3)
300       IF(II-2) 25,25,23
310   25 Y=(TIME-XM)/VAR(I,2)
320       GØ TØ 26
330   23 Y=(ALØG(TIME)-XM)/VAR(I,2)
340   26 PRØ=0.5*(1.0+(1.0-EXP(-0.63662*Y*Y))**0.5)
350    IF(Y) 20,20,28
360   28 PRØ=1.0-PRØ
380     GØ TØ 20
390   24 PRØ=VAR(I,1)
395    20 IF(ISP(I,1)-1) 27,27,29
397    27 P=P*PRØ
400     GØ TØ 200
403    29 P=P*(2.0*PRØ-PRØ*PRØ)
405   200 CØNTINUE
410     PRINT 9,P,T(J)
420    9 FØRMAT(2E15.8)
470    GØ TØ 35
480    END
```

Figure B–2. **PREDICTION PROGRAM**