

1N-61  
21406  
815

# An Autonomous Fault Detection, Isolation, and Recovery System for a 20-kHz Electric Power Distribution Test Bed

Todd M. Quinn  
*Sverdrup Technology Inc.*  
*Lewis Research Center Group*  
*Brook Park, Ohio*

and

Jerry L. Walters  
*National Aeronautics and Space Administration*  
*Lewis Research Center*  
*Cleveland, Ohio*

June 1991

(NASA-TM-104344) AN AUTONOMOUS FAULT  
DETECTION, ISOLATION, AND RECOVERY SYSTEM  
FOR A 20-KHZ ELECTRIC POWER DISTRIBUTION  
TEST BED (NASA) 10 p

91-25600

CSCI 098

Unclass

63/51

0021405





AN AUTONOMOUS FAULT DETECTION, ISOLATION, AND RECOVERY SYSTEM FOR A 20-kHz

ELECTRICAL POWER DISTRIBUTION TEST BED

Todd M. Quinn  
Sverdrup Technology  
Lewis Research Center Group  
Brook Park, Ohio 44142

and

Jerry L. Walters  
National Aeronautics and Space Administration  
Lewis Research Center  
Cleveland, Ohio 44135

SUMMARY

Future space explorations will require long term human presence in space. Planned space environments that provide working and living quarters for manned missions are becoming increasingly larger and more sophisticated. With limited crew size, the expertise needed to maintain reliable operation of the various integrated subsystems may not always be available. Even if there were an expert for each subsystem, the routine monitoring and control of the space environment would consume a large portion of the crew's time.

Monitor and control of the space environment subsystems by expert system software, which emulate human reasoning processes, could efficiently maintain the health of the subsystems and help reduce the human workload. The expert systems can supply the needed technical knowledge and expertise for the various subsystems, thus allowing nonexperienced personnel to solve difficult problems requiring expertise in the particular subsystem domain. The expert systems can also take over routine tasks such as monitoring and analyzing sensor data values.

Among the various subsystems is the power distribution system that supplies electrical energy throughout the space-based facility. The autonomous power expert (APEX) system has been developed to emulate a human expert's reasoning processes used to diagnose fault conditions in the domain of space power distribution. APEX is a fault detection, isolation, and recovery (FDIR) system capable of autonomous monitoring and control of the power distribution subsystem.

APEX consists of a knowledge base, a data base, an inference engine, and various support and interface software. APEX provides the user with an easy-to-use interactive interface. When a fault is detected, APEX will inform the user of the detection. The user can direct APEX to isolate the probable cause of the fault. Once a fault has been isolated, the user can ask APEX to justify its fault isolation conclusion and to recommend actions to correct the fault. This paper discusses APEX implementation and capabilities.

INTRODUCTION

Our future presence in space will require larger and more sophisticated working and living environments. Such environments will consist of numerous integrated subsystems that will have to be maintained with a high degree of reliability. Primary among the various subsystems is the power distribution system that supplies

electrical energy throughout the space-based facility. The availability of space power will be finite; therefore, optimal utilization of the limited power resources is required. If a fault occurs within the power distribution system, disruption of power availability will result in a costly loss of mission time and could threaten the operation of vital subsystems such as life support.

Quick and automatic reconfiguration of the power distribution system by power management controllers and the switching devices themselves provide the necessary capability to maintain power when a system threatening fault occurs (Ringer et al. 1991). However, to preserve the health of the power distribution system, the fault must be isolated and appropriate recovery procedures must be performed to repair the problem. Potential power disruptions can also be avoided by detecting incipient fault conditions that are, at present, nonthreatening to the power distribution system but that, over a period of time, will become a fault. Isolation of and recovery from a fault condition depend on the technical knowledge and experience of power systems personnel.

In a real space environment, with a limited crew size, space power expertise may be unavailable when needed, and with a large number of switching devices, routine maintenance checks and power system data analyses would require a significant amount of crew time. Therefore, autonomous control of space power distribution by expert systems will greatly reduce errors due to the burden of mundane data monitoring tasks and will also reduce the human workload. In addition, recovery and repair time will be shortened because the needed expertise will automatically be available at the time the fault occurs.

The autonomous power expert (APEX) system (Quinn Walters 1990) (Walters et al. 1990) has been developed to emulate a human expert's reasoning processes used to diagnose fault conditions in the domain of space power distribution. Currently, APEX is implemented as a fault detection, isolation, and recovery advisor. It autonomously monitors the operational status of a given power distribution system. Upon detection of a fault condition, APEX accesses a set of isolation rules to determine the most probable cause. After the probable cause has been established, APEX uses a set of recommended action rules to provide appropriate recovery procedures needed to restore the power distribution system to the correct operational status.

Development and testing for the present APEX design were based on a power distribution unit (PDU) subsystem of an early 20-kHz Space Station Freedom power system design (Ringer et al. 1991). APEX is currently interfaced to a power management controller (PMC), which communicates with an existing 20-kHz test bed. APEX sends a request for data to the PMC. The PMC acquires the requested data from sensors on the power distribution switching devices and passes the data to APEX. (See Ringer for a complete description of the test bed hardware and for more information on the lower level power controllers.) When APEX has collected the power distribution parameter data, a fault detection phase is initiated.

APEX detects faults by comparing expected values to the measured operating values (parametric values) obtained from the controller. The expected values are calculated by APEX from the scheduled profile data of the loads connected to the PDU. If no deviations from the expected operating state of the PDU are found, APEX will again request data from the PMC and re-initiate the fault detection activity with the new data. If an anomaly is found within the data acquired from the PMC, APEX will inform the user that a fault has been detected.

The user can direct APEX to isolate the probable cause of the fault. APEX accesses information and rules contained in its knowledge base, reaches a conclusion, and displays the probable cause for the detected fault to the user. The user can then ask APEX to justify its fault isolation conclusion and to recommend actions to correct the fault.

## IMPLEMENTATION OVERVIEW

APEX is currently implemented on a Texas Instruments Explorer II workstation in Lisp and employs the knowledge engineering environment (KEE) expert system shell (KEE User's Guide 1989). As shown in figure 1, APEX consists of a knowledge base, a database, an inference engine, various support and interface software, and a data simulator module. The knowledge base comprises facts and rules that correspond to knowledge acquired from the human expert during problem solving. The data base is the basic working area where storage and calculations of sensory data for incipient fault detection occur. The inference engine is the reasoning mechanism that, during fault isolation, draws conclusions from information stored within the knowledge base. In choosing the appropriate recovery procedures for the isolated fault, APEX also relies on the reasoning capabilities of the inference engine. Software implemented in Lisp provides the user with an interactive interface and also allows APEX to obtain data from various sources such as the power distribution test bed and the scheduler software. The data simulator module allows testing APEX even if the test bed is unavailable. The data simulator module also allows the human experts to display actual test bed data and send commands to control the test bed.

## USER INTERFACE

The goal of the user interface is to provide access to APEX, which is intuitive, and requires only a small amount of training. Communication between APEX and the user is accomplished with easy to use mouse-selectable menus, color graphics, and text displays. The user interface presents a color display that is divided into three areas as shown in figure 2. The top portion of the screen is the control menu that allows the user to select the desired APEX function. When a function is selected, mouse-selectable options for that function appear in the options menu located in the lower portion of the screen. Located on the left side of the control menu is the APEX mode/interface menu. Fault detection and fault isolation results are shown within the main display area by means of color diagrams and text explanations.

The control menu contains six mouse-selectable functions. The MONITOR selection causes APEX to acquire and check parametric values from the power distribution system. When either an active or incipient fault is detected, APEX displays a "fault detected" message in the upper left corner of the user interface screen. Once alerted, the user can display the fault detection analysis by selecting DETECTION in the control menu. When ISOLATE CAUSE is selected from the menu, APEX will access the fault isolation rules to determine the probable cause of the detected fault. The RESET SYSTEM function clears the working space of the APEX system to prepare APEX for monitoring the power distribution system. If the user wants to record the session with APEX, a file can be opened/closed and printed with the LOG FILE function. The EXIT function allows the user to either terminate APEX, switch over to the power system data simulator, or to communicate with a remote scheduler.

The mode/interface menu provides controls for selecting the operational mode of APEX as well as changing the online/offline status of the data acquisition and scheduler interfaces. APEX currently operates in manual mode where the user selects appropriate commands from the control menu. An autonomous mode option is available which will allow the user to place APEX in full autonomous mode. APEX will be able to monitor the power distribution system, detect faults, isolate the probable cause, and provide appropriate fault recovery automatically without input from the user.

APEX acquires load scheduling data from a scheduler and actual power system data from sensors located on the switching device hardware. The mode/interface menu allows the user to select whether APEX is to acquire data from a real or simulated source. Clicking the mouse on the test bed status line toggles the status between online and offline. If the status is online, then the data acquisition interface reads data directly from the hardware. If, however, the test bed status is selected offline, then data are acquired from a test bed data simulator. When the scheduler status line indicates online, APEX can request and receive scheduling information from the scheduler. When the scheduler interface is offline, APEX does not issue scheduling requests and reads pre-saved scheduling information.

The graphical displays in the main display area consist of a set of hierarchical diagrams that represent three different levels of the power distribution system. The diagram in the main display area shown in figure 2 represents the overall power distribution system. When an active fault is detected in the diagram, the area of detection is outlined in red and a red flashing cursor appears next to the area. For an incipient fault condition, the area is outlined in yellow and has a yellow flashing cursor. The yellow indicates that a parametric value is probably going to go out of tolerance if preventive action is not taken. The user can get a more detailed diagram of an area by choosing the particular area of interest and clicking the mouse. Figure 3 shows the user interface screen after the user clicks the mouse on PDUA of the top level diagram. In this PDUA subsystem diagram, the user can easily see the location of the detected parametric abnormality at the switching device level. Figure 4 shows the switch level diagram after the user clicks the mouse on one of the switching devices, such as RBI 3/3. Each switch level diagram displays the actual measured data values enabling the user to see which parametric attribute is out of tolerance.

#### TEST BED SIMULATION, DISPLAY, AND CONTROL

Part of the user interface, the data simulator/display/control interface screen, is displayed in figure 5. The three main functions contained in the control menu are SIMULATE, DISPLAY, and CONTROL. In the SIMULATE mode, the user can set sensory data to any values to simulate various fault scenarios. In the DISPLAY mode, actual sensor data from the test bed can be displayed and recorded for the user's observation. In the CONTROL mode, the user has the capability of issuing commands to the test bed in order to turn switching devices on/off and set trip limits.

In the simulation mode, as shown in figure 5, the main display area contains a diagram of the test bed. Each switch device (RBI's and RPC's) in the diagram is mouse selectable. As each device is selected, the switch related data are displayed on the left side of the screen. Along with simulated switching device data, the simulated data for each load on the test bed are also displayed. The options menu contains various selections allowing the user to quickly change values within the data simulator.

The main display area shown in figure 6 shows the format of the DISPLAY selection in the control menu. The line voltage (V-A), load voltage (V-B), A current (I-A), B current (I-B), power, and trip limit are displayed for each switching device on the test bed. Using the options menu for DISPLAY, the user can monitor, record, and print the data obtained from the test bed sensors.

#### TEST BED DATA ACQUISITION

APEX acquires power distribution data from a power management controller (PMC) over a RS-232 serial connection. The PMC communicates with the power distribution system via a 1553 bus. The PMC queries the switching devices for the following sensor data (see fig. 4): (1) A current, (2) B current, (3) line voltage, (4) load voltage, (5) power, (6) phase angle, and (7) overcurrent trip set point. Sensor data also include 12 bits of status indicating the operational state of the switching device. After the data have been received from the PMC, APEX checks for any abnormal values. If no abnormalities are found, APEX stores the information in a historical data base and then acquires a new set of data values. In the event that the test bed or the PMC is unavailable, APEX can obtain realistic sensor data values from a PDU data simulator. By using Remote Procedure Calls over ethernet, APEX has the ability to obtain sensor information remotely, either from the test bed or the data simulator.

The PMC 1553 bus communication with the test bed is implemented in Ada programming language. APEX sends a request for data to the PMC over the RS-232 link. The PMC then acquires the data from the test bed and returns the requested information back to APEX. Originally, the Ada code would only accept requests from APEX limited to one data sensor on one switch per request. The time required for APEX to monitor all the necessary sensor data on the test bed added up to over 2 min.

Modifications were made to the Ada code allowing APEX to request a block of sensor data from a specified switch. The returned block would contain the previous seven sensor values plus a 16-bit status register built from available status indicators. The amount of time APEX needed to acquire data from the test bed was reduced down to approximately 15 sec. Using a table of power devices already maintained within the Ada code permitted adding another modification which allowed APEX to make a single request for blocks of data for all known switching devices. This further reduced the data acquisition time to its present value of approximately 4.5 sec.

#### FAULT DETECTION

A fault can be classified as being either hard or soft. A hard fault generally is a catastrophic event that affects the flow of power. An example of a hard fault would be a short across the power transmission lines causing a high surge in current. The overcurrent condition would then cause the switching devices in the affected area to trip. A soft fault does not cause the switching devices to trip because the currents remain under the trip limit threshold. However, the various loads attached to the power distribution system may not receive the required power because of the soft fault. Soft faults can be caused by such things as current leakage from the transmission lines to ground, faulty components in the switching devices, or a degradation of the power components over a period of time. The main focus of APEX development has been in the area of soft fault detection and isolation.

Faults are also classified by APEX as either active or incipient. An active fault is a fault condition that is presently disrupting the power distribution system. An incipient fault condition, however, has little or no effect the power distribution, but, if not corrected, it could develop over a period of time into an active fault. Active faults are detected by comparing the parametric values (measured operating values) of the power distribution system to the expected values and identifying any abnormal operating parameters. When the detection rules have been exhausted, APEX reports to the user whether or not any faults were detected. If a fault was detected, the user can then instruct the expert system to isolate the probable cause of the fault. If no abnormal conditions were detected, the previously recorded (historical) data are analyzed for incipient fault conditions.

Incipient detection is based on statistical linear regression and correlation analysis of the historical data. As new data are received, the parametric values of the power distribution system are stored as historical data under the appropriate parametric attributes for each switching device. Along with each measured value, the expected value that is calculated by the expert system is also saved. The expert system analyzes the historical data looking for any indication of a parametric attribute that has exhibited either an upward or downward trend in the data values over a period of time. The following parametric attributes are stored for each device: switch A current, switch B current, line voltage, load voltage, and power.

Since the power system is dynamic and the measured value fluctuates over a period of time during normal operation, a ratio of the measured-to-expected value is used to identify any increasing or a decreasing trends in the parametric data. Thus, if the measured and the expected values are equal, the ratio will be one. If the measured value is higher than the expected value, the ratio will be greater than one; if the measured value is less than the expected value, the ratio will be less than one.

Once the data have been stored in the data base, correlation coefficients are calculated for each parametric attribute ratio of each switching device. The correlation coefficients are calculated in the following manner (Trivedi 1982):

The mean value  $\bar{a}$  is found from

$$\bar{a} = \frac{1}{N} \sum_{1}^N a_n$$

the time variance  $\sigma_x^2$  from

$$\sigma_x^2 = \overline{X^2} - (\bar{X})^2$$

the parametric variance  $\sigma_y^2$  from

$$\sigma_y^2 = \overline{Y^2} - (\bar{Y})^2$$

and the covariance of X and Y from

$$\overline{XY} - \bar{X}\bar{Y}$$

where X is the relative time of the data acquisition and Y the parametric values.

The correlation coefficient r, then, is

$$r = \frac{\overline{XY} - \bar{X}\bar{Y}}{\sigma_x \sigma_y}$$

where the standard error is

$$S_y = \sigma_y \sqrt{1 - r^2}$$

the slope is

$$m = \frac{\overline{XY} - \bar{X}\bar{Y}}{\sigma_x^2}$$

and the Y-intercept is

$$b = \bar{Y} - m\bar{X}$$

A high correlation coefficient, caused by a parametric ratio trend, indicates that a temporal relationship exists. The value of the correlation coefficient lies between zero and one. A zero indicates that there is no correlation between the time and historical parametric data; however, the closer the correlation coefficient is to one, the stronger the time and parametric value correlation. APEX currently will consider an incipient fault condition to exist if the correlation coefficient of a parametric attribute is higher than 0.75.

Once an incipient fault condition has been detected, the user can view the results of the statistical analysis and also have APEX isolate the probable cause of the incipient condition. Figure 7 shows a typical display indicating a definite increasing trend in the ratio between measured values and expected values. The trend was detected within the switch A current parameter of switching device RBI.3/3. Along with the plot of the linear regression results, the correlation coefficient, slope, standard error, and y-intercept are displayed for the user. A set of isolation rules for detected incipient fault conditions can access the data base and examine correlation coefficients of the various parametric attributes of each switching device.

#### FAULT ISOLATION

The primary function of fault isolation is probable cause determination for a given fault condition. APEX uses the knowledge contained within the fault isolation rules and the backward chaining capabilities of the KEE inference engine to determine the most probable cause. Backward chaining (also known as goal driven) works from a particular goal and tries to either confirm or refute its truth. Figure 8 shows a display of fault isolation analysis for a particular fault condition. In this case, there are three possibilities listed as the probable cause. Based on the present knowledge in the knowledge base and the sensor data obtained from the power distribution system, the probable cause cannot be determined any further.

Figure 9 shows a typical display of probable cause justification. At the top of the main display area, the probable cause, which is the backward chaining goal, is displayed. Below the stated probable cause are the premises which support the truth of the probable cause statement. The unhighlighted numbers (1 to 4) are primitive statements of fact contained within the knowledge base. Numbers that are highlighted represent statements of facts that were inferred as subgoals. By clicking the mouse on a highlighted number, the user can see the premises used to prove the truth of the subgoals. The CONTINUE option displayed in the options menu allows the user to exit justification and return the options menu for fault isolation.

#### FAULT RECOVERY

After APEX has isolated the probable cause of either a detected fault or an incipient fault condition, the user can ask for fault recovery recommendations. APEX will analyze available information about the current operating conditions with respect to the fault and display appropriate actions to be taken. Recommended actions pertain to both short- and long-term recovery. Short-term recovery determines if the fault can be tolerated for a period of time, if the power distribution can be reconfigured, or if load shedding is necessary. For long-term recovery, the repair procedures needed to correct the fault are determined after short-term actions have been implemented.

Short-term recovery analysis is based on a set of "recommended action" rules for the particular fault condition. Information about available power sources, present configuration of the power distribution system, the scheduled run times of the loads, and the effects of the fault on the system are all considered during the analysis. If enough power is available and the effects of the fault are minimal with respect to remaining scheduled run time of the affected loads, then the fault can be tolerated and the loads are allowed to run to completion of their scheduled times. If the fault is seriously affecting the amount of power supplied to a particular load and an alternate path for power distribution exists, then the system can be reconfigured automatically, or with user confirmation, to allow the load to run to completion. When the fault cannot be tolerated and alternate power distribution paths are unavailable, then the schedule for the loads is replanned by the scheduler; resulting in load shedding and a new schedule.

After the short-term recovery phase, the fault in the power distribution system needs to be repaired. The appropriate procedures needed to repair the power distribution system are determined by the long-term recovery phase, which is also based on a set of recommended action rules. In some cases, the cause of the fault is localized to a group of probable causes, such as in figure 8, and additional troubleshooting procedures are displayed to intelligently guide the user to further isolate the exact probable cause and to make repairs.

#### SCHEDULER INTERFACE

The scheduler interface is responsible for source/load power profile and scheduling data exchange between APEX and the scheduler. Source profile data represent the amount of available power resources over a period of time. The load profiles indicate how much of power will be used by the load over a period of time. The scheduler determines the best use of power resources and returns a schedule containing a start time for each load. Profile data for available power sources and load power usage are entered by the user. APEX initiates a request for a load

schedule by transmitting the profile data to the scheduler software over an ethernet connection. The scheduler determines a schedule of starting times for each load and returns the information to APEX. APEX uses the received schedule along with the load profiles as the basis for its expected value calculations.

Figure 10 shows an example of a scheduler interface screen. The control menu contains six function buttons: GENERATE, DISPLAY, EDIT, EXIT, SAVE, and LOAD. Profile data for the sources and loads can be saved and retrieved to/from the disk via the respective SAVE and LOAD commands. Once profile data have been entered, the GENERATE function can be used to request a schedule from the scheduler. Once generated, the DISPLAY function then can be used to display the new schedule. The EDIT function in the control menu allows the user to enter new profile data or select and modify profile data already entered. To exit the scheduler interface, the user can select the EXIT function.

The EDIT function is shown being used in figure 10. There are two options displayed in the options menu: SELECT PROFILE and CLEAR PROFILE. The CLEAR PROFILE option resets all profile data for sources and loads to zero. The SELECT PROFILE options allows the user to select a source or load profile object to edit.

In figure 10, the data object for the load 1 profile has been selected for edit. The profile for the data object is displayed in a profile grid located in the middle of the main display area. In the top portion of the main display area the user has the capability to change the PLANNING HORIZON and the PERIOD LENGTH. These two values globally affect the display of all profile data since they specify the length and interval division of the scheduling time. The MAXIMUM POWER value is specific to the load profile object and indicates the maximum power that can be entered for the particular source or load.

Profile data for the source or load are entered by clicking the mouse on the appropriate interval of the profile grid and entering a new value. For example, the time interval 0:10 - 0:15 has a profile value of 6000 W. The time interval indicates that for the third period after the schedule start of load 1, 6000 W of power will be used by load 1. Attached to each load object is information concerning LOAD DURATION, EARLIEST START time, LATEST END time, the power SOURCE, and PRIORITY.

#### FUTURE DEVELOPMENT AND ENHANCEMENTS

APEX currently is operating on the 20-kHz test bed with the ability to monitor data sensors, detect faults, isolate the probable cause, and perform short-term recommended actions. Besides the ever ongoing addition and modification of rules, there are still some unfinished software areas which could be enhanced or implemented. Enhancements include areas such as updating the log file operations, updating the user interface, completing full autonomous mode operation, and allowing time variant load operations. Additional software implementation of long-term recommended actions is also needed. Future development of APEX will also require a change in knowledge representation in order to obtain a wider set of fault coverage.

When the LOG FILE function in the APEX control menu was developed, recommended actions for fault recovery did not exist. Therefore, the LOG FILE function does not have the ability to record the recommended actions performed by APEX. Also, other aspects of recording a log file should be fully tested and brought up to date because of the many changes in software during the last year.

Currently APEX runs at the command of a user (manual mode), although there are software hooks for autonomous mode. Completion of the autonomous mode operation for APEX is a matter of completing the software to take advantage of the hooks and allow APEX to run without user input.

So far the code written for APEX can only handle constant loads, i.e., loads that do not have changing power requirements over a period of time. Simple enhancements in the area of scheduler interface and expected value calculations could easily allow APEX to handle time variant loads; however, implementation of a mission timer will also be needed.

Long-term recommended action implementation will require developing a set of rules to further troubleshooting and/or repair a given probable cause. Also, software will have to be developed to display, store, and retrieve long-term recommended actions when needed by the user.

Rule-based knowledge representation has allowed the capture and implementation of expert thought processes in some areas of FDIR for power distribution. However, rule generation is time consuming and the rules tend to be limited. Depending on the size and complexity of the power distribution system, there can be an almost infinite amount of fault conditions which can occur. This would require the same order of rules to cover the possible fault conditions. This suggests that, in order to cover a reasonable set of fault conditions, a large rule set will be necessary. Generation and maintenance of such a rule set will be time and cost prohibitive. Alternative methods for knowledge representation and reasoning must be considered. Currently, one area of investigation for APEX is modeled-based approaches to fault diagnostics.

#### CONCLUDING REMARKS

The APEX system provides fault detection, isolation, and recovery for a 20-kHz electrical power distribution test bed. In order to store the information and knowledge of human experts, APEX utilizes the rule-based reasoning facility of the KEE expert system shell. APEX monitors sensors on the 20 kHz-test bed and analyzes the parametric data. If an anomaly is found within the data, APEX will inform the user that a fault has been detected. The user can use APEX to isolate the probable cause and recommend appropriate recovery actions to correct the fault.

APEX consists of various support and interface software which communicates with the user, the 20-kHz test bed, and a scheduler. Communications between APEX and the user are accomplished with easy-to-use mouse-selectable menus, color graphics, and text displays. APEX acquires power distribution data from the test bed via a RS-232 serial connection to a power management controller. The controller communicates with the power distribution system via a 1553 bus. The scheduler interface is responsible for power profile data exchange between APEX and the scheduler. APEX uses a schedule generated by the scheduler along with the load profile information as the basis for fault detection.

APEX is also capable of incipient fault analysis which adds a unique health monitoring feature to prevent faults from occurring. APEX can warn the user of potentially threatening fault conditions before power interruptions are experienced. Moreover, the type of continuous monitoring that APEX provides eliminates problems that can occur with mundane monitoring, such as errors caused by fatigue.

Once the probable cause of a fault condition or incipient condition has been isolated, APEX can recommend the most appropriate procedures for recovering from and preventing power distribution faults. Recommended actions consist of both short- and long-term recovery procedures necessary for maintaining the health of the power system. Execution of short-term recovery procedures restores power to scheduled loads, and execution of long-term actions effectively repairs isolated areas of the power distribution system.

In future space applications, APEX can be applied to help maintain the operational health of power distribution systems. APEX will be able to diagnose fault conditions and recommend appropriate recovery procedures when experienced power system personnel are unavailable. If APEX is allowed to autonomously monitor and analyze power distribution data, faults can be detected before serious problems develop and costly power interruptions occur. Increased reliability of space power distribution and substantial reduction in human labor required for routine monitoring of system operations is the goal of the APEX project.

#### ACKNOWLEDGMENTS

We would like to acknowledge the following employees of Sverdrup Technology Inc., Lewis Research Center Group: Walter Krawczonek, our domain expert, for providing the knowledge used in developing APEX; Anthony Merolla for technical hardware support; Mark Ringer for his scheduler work; and Gene Liberman for his modifications to Ada code which runs on the power management controller. We are also grateful to James Kish and Edward Petrik of NASA Lewis for project leadership.

#### REFERENCES

- KEE User's Guide, Version 3.1, Intellicorp., Mountain View, CA, May 1989.
- Quinn, T.M.; and Walters, J.L.: Autonomous Power Expert System - Advanced Development. Fourth Annual Space Operations, Applications, and Research Symposium (SOAR 1990), Albuquerque, NM, June 26-28, 1990.
- Ringer, M.J., et al.: Autonomous Power System Intelligent Diagnosis and Control. 1991 Goddard Conference on Space Applications of Artificial Intelligence, NASA Goddard Space Flight Center, Greenbelt, MD, May 14-15, 1991.
- Trivedi, K.S.: Regression, Correlation and Analysis of Variance. Probability and Statistics With Reliability, Queuing and Computer Science Applications, Prentice-Hall, 1982.
- Walters, J.L., et al.: Autonomous Power Expert System. *TELEMATICS and INFORMATICS*, vol. 7, nos. 3/4, 1990, pp. 291-300.

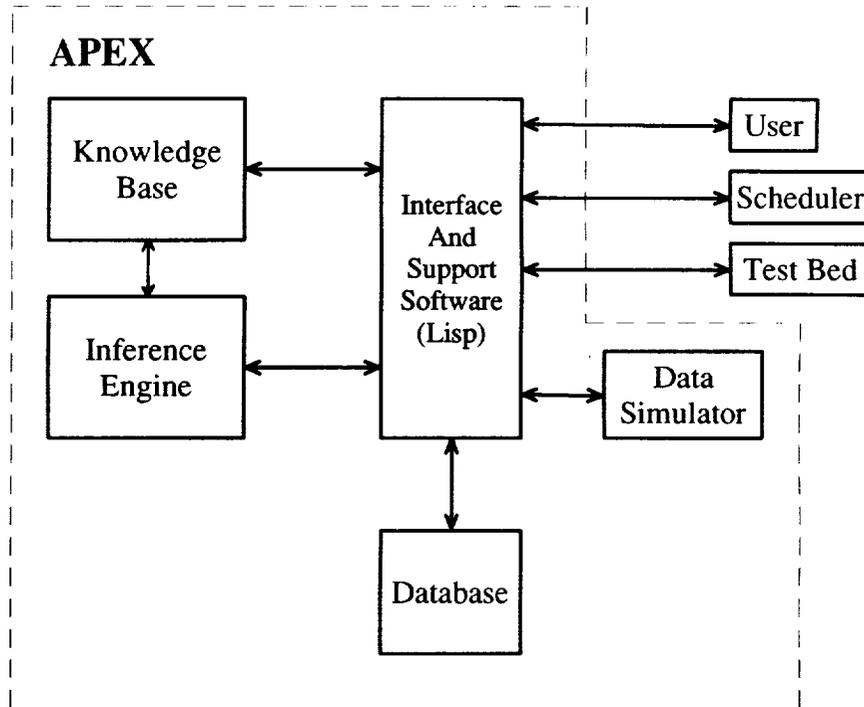


Figure 1.—APEX block diagram.

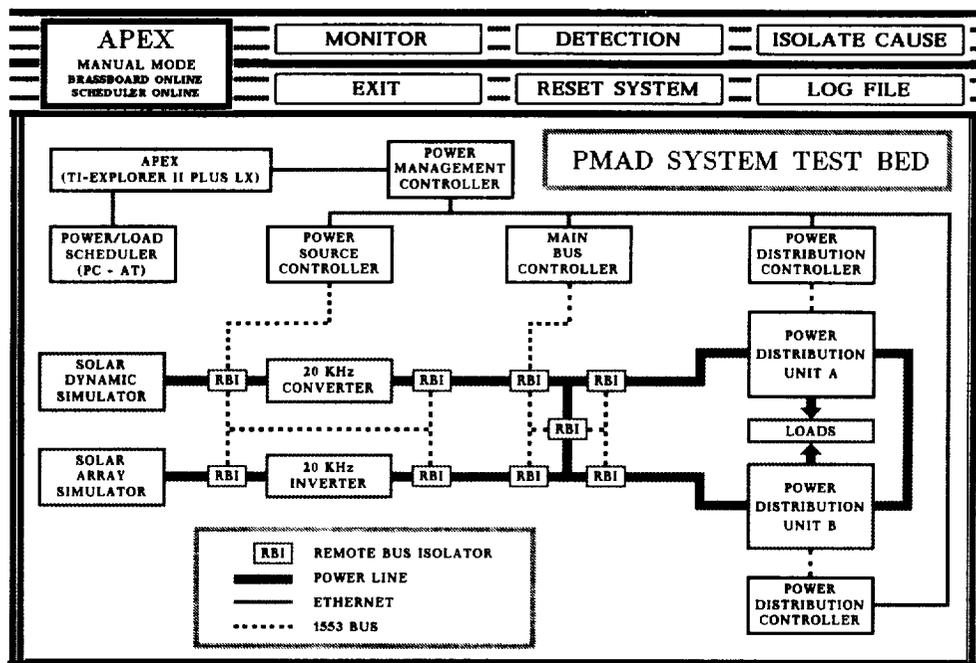


Figure 2.—Main user interface (three main areas).

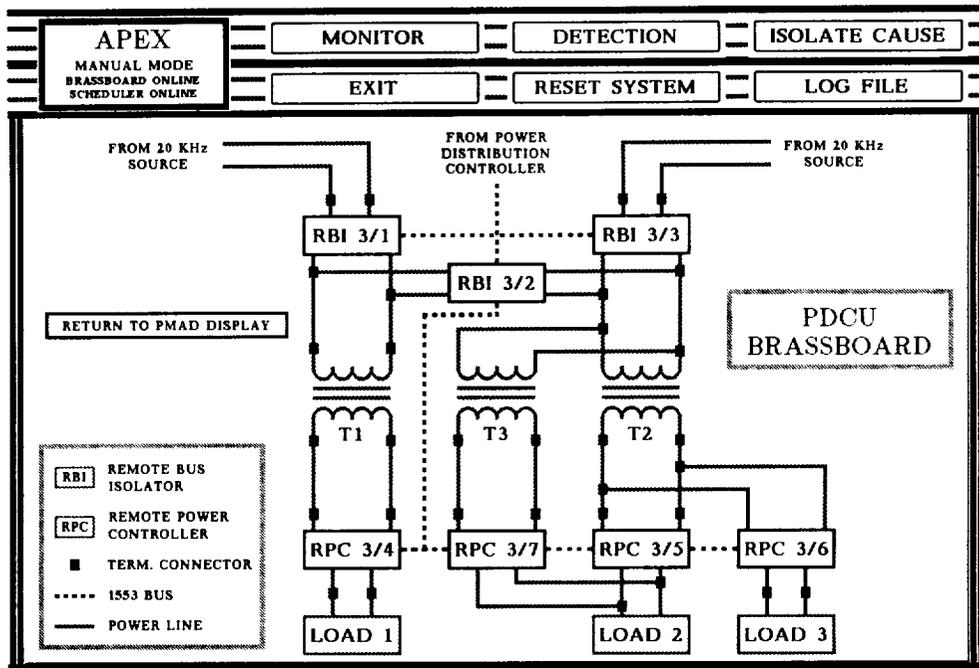


Figure 3.—PDU-A, second level diagram.

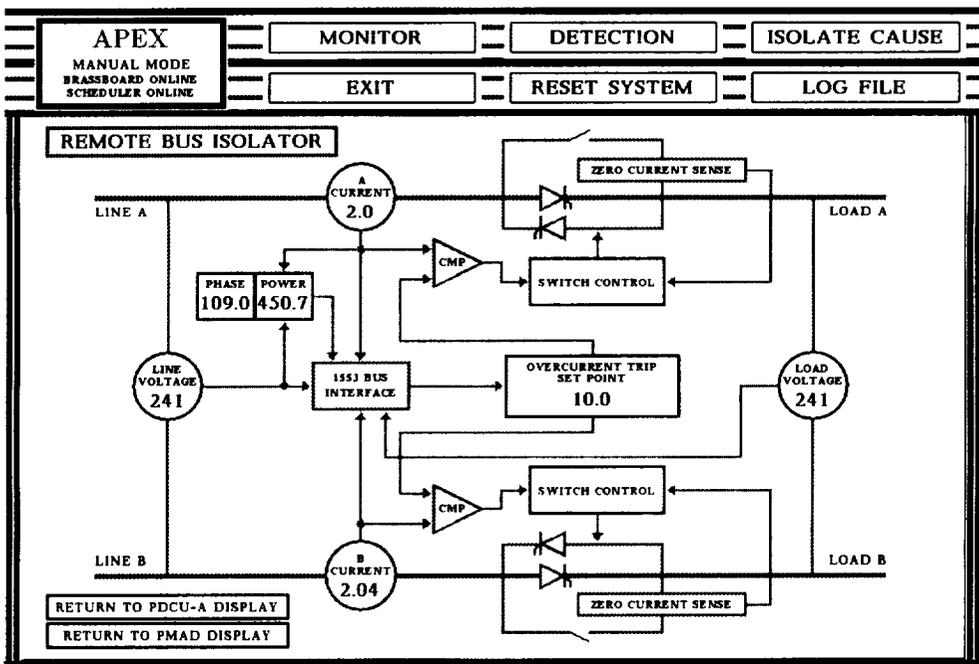


Figure 4.—Switch level diagram.

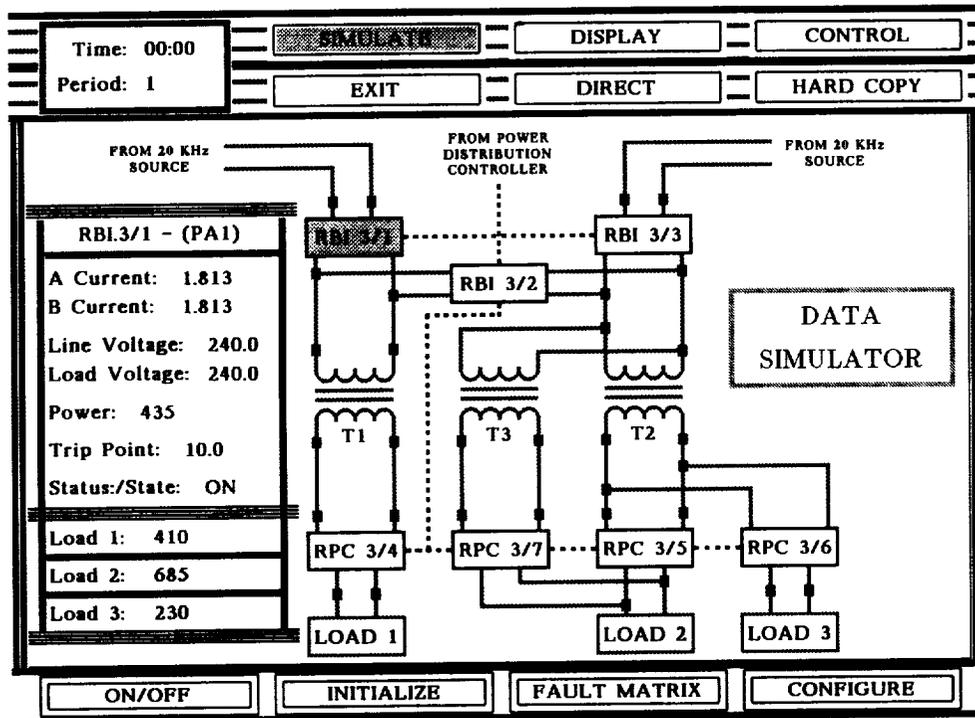


Figure 5.—Brassboard simulator/display/control interface.

	V-A	V-B	I-A	I-B	Power	Trip
RBI.3/1	240.0	240.0	1813	1813	435.0	10.0
RBI.3/3	240.0	240.0	4021	4021	965.0	10.0
RPC.3/4	120.0	120.0	3417	3417	410.0	10.0
RPC.3/5	120.0	120.0	5708	5708	685.0	10.0
RPC.3/6	120.0	120.0	1917	1917	230.0	10.0

MONITOR INTERVAL RECORD EXTRACT

Figure 6.—Display mode screen.

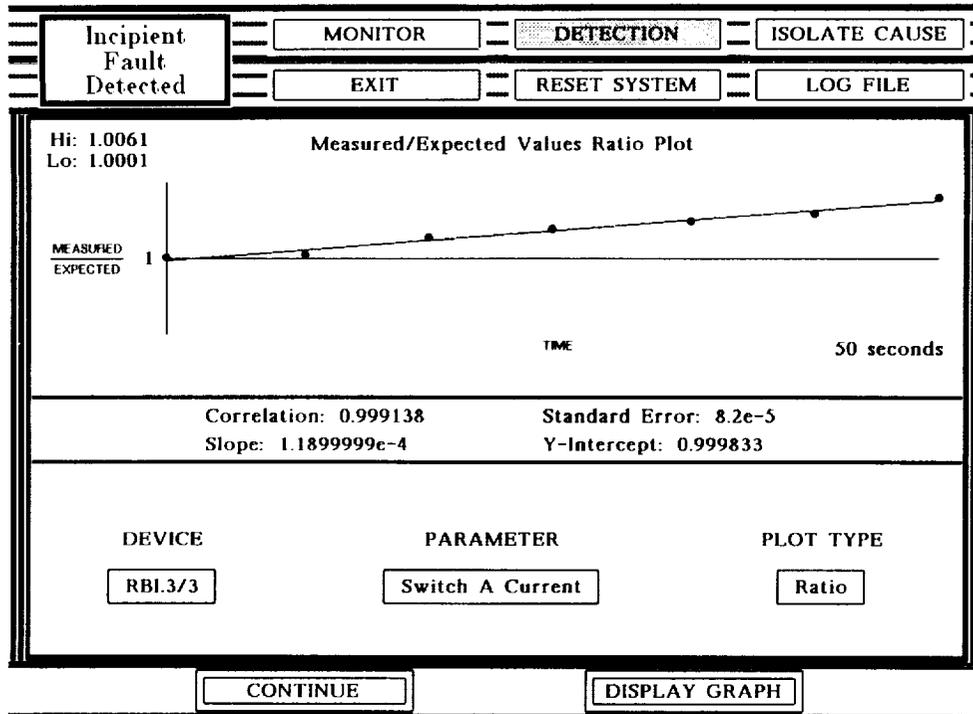


Figure 7.—Incipient detection plot.

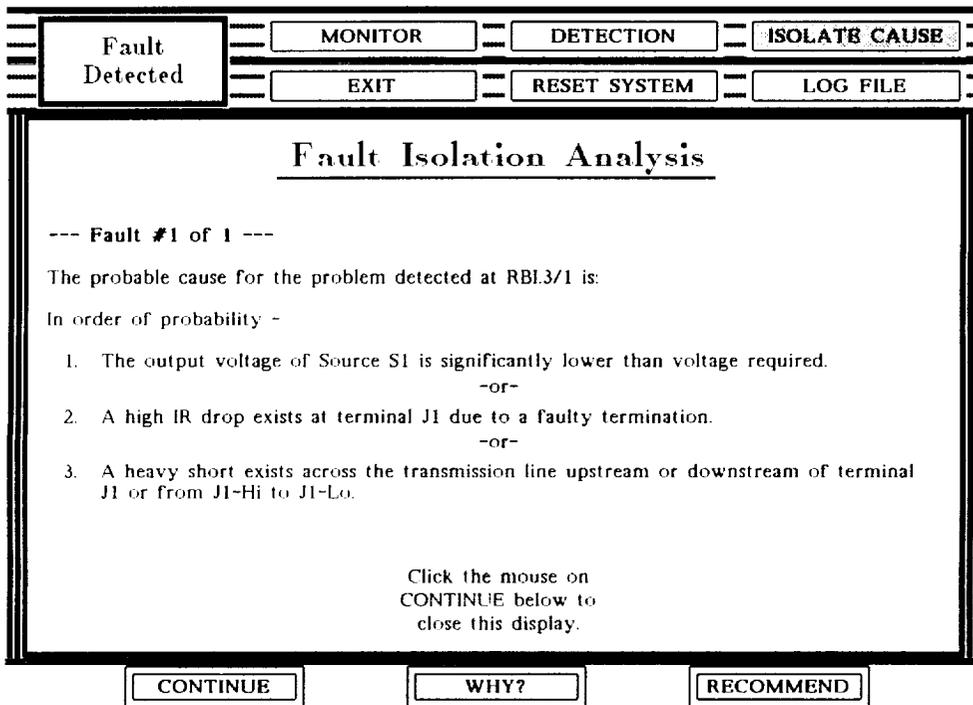


Figure 8.—Fault isolation analysis.

<b>Fault Detected</b>	MONITOR	DETECTION	<b>ISOLATE CAUSE</b>
	EXIT	RESET SYSTEM	LOG FILE

The output voltage of Source S1 is significantly lower than voltage required.  
 A high IR drop exists at terminal J1 due to a faulty termination.  
 A heavy short exists across the transmission line upstream or downstream of terminal J1 or from J1-Hi to J1-Lo.

JUSTIFICATION

1. RBI.3/1 is a Remote Bus Isolator.
2. RBI.3/1 is connected to S1.
3. S1 is a power source.
4. The input terminal connection of RBI.3/1 is j1.
5. A and B currents for RBI.3/1 are equal.
6. The A current is lower than the normal expected current for RBI.3/1.
7. The B current is lower than the normal expected current for RBI.3/1.
8. Line and load voltages for RBI.3/1 are equal.
9. The load voltage of RBI.3/1 is lower than the expected operating voltage.
10. The line voltage of RBI.3/1 is lower than the expected operating voltage.
11. The power of RBI.3/1 is lower than the normal expected power.

**CONTINUE**

Figure 9.—Probable cause justification.

<b>SCHEDULER INTERFACE</b>	GENERATE	DISPLAY	<b>EDIT</b>
	EXIT	SAVE	LOAD

PLANNING HORIZON	PERIOD LENGTH	MAXIMUM POWER
<input type="text" value="4:00"/>	<input type="text" value="0:05"/>	<input type="text" value="10000"/>

Time Interval  
0:10 - 0:15

↑  
Power  
6000

LOAD DURATION	EARLIEST START	LATEST END	SOURCE	PRIORITY
<input type="text" value="0:30"/>	<input type="text" value="0:30"/>	<input type="text" value="1:30"/>	<input type="text" value="SOURCE-1"/>	<input type="text" value="NORMAL"/>

Figure 10.—Scheduler interface.



National Aeronautics and  
Space Administration

## Report Documentation Page

1. Report No. NASA TM - 104344		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle An Autonomous Fault Detection, Isolation, and Recovery System for a 20-kHz Electrical Power Distribution Test Bed				5. Report Date June 1991	
				6. Performing Organization Code	
7. Author(s) Todd M. Quinn and Jerry L. Walters				8. Performing Organization Report No. E-6118	
				10. Work Unit No. 505-12-33	
9. Performing Organization Name and Address National Aeronautics and Space Administration Lewis Research Center Cleveland, Ohio 44135 - 3191				11. Contract or Grant No.	
				13. Type of Report and Period Covered Technical Memorandum	
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Washington, D.C. 20546 - 0001				14. Sponsoring Agency Code	
15. Supplementary Notes Todd M. Quinn, Sverdrup Technology, Inc., Lewis Research Center Group, 2001 Aerospace Parkway, Brook Park, Ohio 44142 (work funded by NASA Contract NAS3-25266). Jerry L. Walters, NASA Lewis Research Center. Responsible person, Todd M. Quinn, (216) 433-3428.					
16. Abstract Future space explorations will require long term human presence in space. Planned space environments that provide working and living quarters for manned missions are becoming increasingly larger and more sophisticated. With limited crew size, the expertise needed to maintain reliable operation of the various integrated subsystems may not always be available. Even if there were an expert for each subsystem, the routine monitoring and control of the space environment would consume a large portion of the crew's time. Monitor and control of the space environment subsystems by expert system software, which emulate human reasoning processes, could efficiently maintain the health of the subsystems and help reduce the human workload. The expert systems can supply the needed technical knowledge and expertise for the various subsystems, thus allowing nonexperienced personnel to solve difficult problems requiring expertise in the particular subsystem domain. The expert systems can also take over routine tasks such as monitoring and analyzing sensor data values. Among the various subsystems is the power distribution system that supplies electrical energy throughout the space-based facility. The autonomous power expert (APEX) system has been developed to emulate a human expert's reasoning processes used to diagnose fault conditions in the domain of space power distribution. APEX is a fault detection, isolation, and recovery (FDIR) system capable of autonomous monitoring and control of the power distribution subsystem. APEX consists of a knowledge base, a data base, an inference engine, and various support and interface software. APEX provides the user with an easy-to-use interactive interface. When a fault is detected, APEX will inform the user of the detection. The user can direct APEX to isolate the probable cause of the fault. Once a fault has been isolated, the user can ask APEX to justify its fault isolation conclusion and to recommend actions to correct the fault. This paper discusses APEX implementation and capabilities.					
17. Key Words (Suggested by Author(s)) Expert systems			18. Distribution Statement Unclassified - Unlimited Subject Category 61		
19. Security Classif. (of the report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of pages 18	22. Price* A03

