IN-31
198077
7P

NASA Technical Memorandum 106413
AIAA–93–4703–CP

Reducing the Cognitive Workload: Trouble Managing Power Systems

David B. Manner and Eugene M. Liberman
Sverdrup Technology, Inc.
Lewis Research Center Group
Brook Park, Ohio

and

James L. Dolce and Pamela A. Mellor
National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio

Prepared for the
AIAA: Computing in Aerospace 9
sponsored by the American Institute of Aeronautics and Astronautics
San Diego, California, October 19–21, 1993

Reducing the Cognitive Workload: Trouble Managing Power Systems

David B. Manner and Eugene M. Liberman
Sverdrup Technology, Inc.
Lewis Research Center Group
Brook Park, Ohio 44142

and

James L. Dolce and Pamela A. Mellor
National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135

ABSTRACT

The complexity of space-based systems makes monitoring them and diagnosing their faults taxing for human beings. Mission control operators are well-trained experts but they can not afford to have their attention diverted by extraneous information. During normal operating conditions monitoring the status of the components of a complex system alone is a big task. When a problem arises, immediate attention and quick resolution is mandatory. To aid humans in these endeavors we have developed an automated advisory system. Our advisory expert system, Trouble, incorporates the knowledge of the power system designers for Space Station Freedom. Trouble is designed to be a ground-based advisor for the mission controllers in the Control Center Complex at Johnson Space Center (JSC). It has been developed at NASA Lewis Research Center (LeRC) and tested in conjunction with prototype flight hardware contained in the Power Management and Distribution testbed and the Engineering Support Center, ESC, at LeRC. Our work will culminate with the adoption of these techniques by the mission controllers at JSC. This paper elucidates how we have captured power system failure knowledge, how we have built and tested our expert system, and what we believe are its potential uses.

1.0 INTRODUCTION

We have developed an expert system, Trouble, as a ground-based advisory system. Its purpose is to aid the humans whose job it is to monitor and diagnose faults in the Space Station Freedom Electric Power System. Trouble provides a graphical status-at-a-glance screen for ease in monitoring the power system. When an anomaly occurs, the operator is alerted to the location of the problem as well as being presented with the possible causes of the malfunction.

Developed as one of the projects of the Power System Advanced Automation Lab located at LeRC, Trouble is an object-oriented expert system built using LISP and the ART (Automated Reasoning Tool from Inference Corporation) inference engine. By connecting Trouble to the DC Power Management and Distribution Testbed at LeRC, live data can be used to test Trouble for accuracy. Integrated into the Engineering Support Center, Trouble simulates backroom EPS ground operations when Space Station Freedom is operational.

2.0 FAILURE KNOWLEDGE CAPTURE

One of Trouble's unique features is its set-covering approach to storing failure knowledge and system configuration. This approach maintains a readable and easily reconfigurable data dictionary to encode the failures and their component relationships.[1] This data dictionary is populated with the information captured by a failure modes and effect analysis, FMEA, a standard engineering process. Most system development today includes an FMEA describing possible failures for each component and how failures propagate through the system. Trouble uses this failure data to search backwards from the effects to their causes rather than forward from the causes to the effects.

3.0 FAILURE KNOWLEDGE REPRESENTATION

A generic object is made for all similar components. Our current representation includes components for the power distribution as well as power generation and storage. These components are cables, busses, remote bus isolators (RBI), remote power converters (RPC), DC to DC convertor units (DDCU), battery charge discharge units (BCDU), solar arrays and batteries. Each component type has its own attribute list that contains the important characteristics for that type of device. These attributes include such things as input voltage, output voltage, current, setpoint limits, state of the device, interconnections, etc. The individual components are instances of the generic object and inherit its attributes.

The failure knowledge is also stored in the generic object representation.[2] This failure knowledge, obtained from a FMEA, is stored in the failure data dictionary which enumerates all known causes, their subcauses, their sub-subcauses, etc. To simplify the search for possible causes, we do not store a completely connected failure tree. We store each object as a related triple; failure, cause and symptom, and only generate linkages for those failures whose symptoms have been detected.

The linked failure chains form the basis for Trouble's advisory screens, providing an operator with a complete set of reasoning from the detection of an anomaly to all the known causes. This approach provides the operator with the full set of relevant knowledge, much like a reference in an encyclopedia. In critical situations, a list of all known causes is very helpful since operators might overlook unusual or highly unlikely failure causes when they are pressed for time. Mission controllers at the Johnson Space Center expressed interest in this particular feature. They want an automated advisory system to provide relevant information and let the human draw the conclusions.

4.0 DESIGN

Trouble is a multi-process diagnostic expert system made up of the following independent subsystems: data acquisition, symptom detection, diagnosis and graphical user interface. Data acquisition is responsible for reading telemetry data and updating objects. Symptom detection is a set of complex rules that determines whether or not any anomalies are present in the system and, if so, generates symptoms. Diagnosis is responsible for using the generated symptoms to search the failure data dictionary to find causes for the anomaly. The graphical user interface communicates with the operator. Each process is independent, and interactions between processes are limited to simple exchanges of results. To reduce processing time, diagnosis and detection are performed only when needed. The two other modules operate continuously.

4.1 Data Acquisition

To reason about the system and to perform diagnostics, Trouble's data objects must use the most recent data. During each sampling period, measurements are stored in the corresponding component. Trouble then compares this data to the last set of collected data. If the two sets are within tolerance, no new information is present and no further processing is required. If the changes are not within tolerance, the detection process is begun.

4.2 Detection

The essence of detection is the conversion of quantitative measurements into qualitative symptoms that describe the system's performance. The goal of detection is the generation of the symptoms that provide the link between telemetry data and failure modes, since each linkage in the failure chain is accessed by its corresponding symptom. When the detection module executes, it runs a set of rules which look for predefined patterns in the data which indicate an anomaly. If there is a match in the data, symptoms are generated. There can be multiple symptoms for a particular anomaly pattern, as well as multiple patterns for a particular symptom.

The complexity in Trouble resides in the detector rules. Rules are difficult to maintain, hard to read and hard to verify. We intentionally limited application specific rules in Trouble to the detection task alone.

Determining how to detect a particular failure is challenging. Experts can explain how a device might fail, what might be the cause as well as specify how to detect the failure. Unfortunately, many power system hardware components do not have instrumentation that allows the ground system to detect certain problems. To be able to make such a specific judgement, special tests may need to be run or collateral information gathered. An operator on the ground will be able to make those choices because Trouble provides all known possible causes of an anomaly, even if some are highly unlikely.

4.3 Diagnostics

Trouble's set-covering technique is encapsulated in the diagnostic process where the detected symptoms are matched to failure knowledge. The data dictionary representation facilitates modification to the failure knowledge since the knowledge can be read in its stored format, a data table. Tables are easy to change, thus the actual software is easy to maintain as well. The diagnostic process begins with a search of the failure database. The failure database stores its knowledge as failure objects which are related triples; failure mode, cause and symptom. The database search process finds all failure objects containing the detected symptoms. When a symptom match is made, a special data record is created. This is the failure hypothesis record or FHR, which contains information about a single link in the failure mode tree. The FHR contains the failed device's name, the time, the detecting device's name as well as the specific failure mode with its possible cause. The FHRs are connected into linked-lists incorporating the parent-child nature of failures, their causes, and subcauses. Each linked-list represents a path through the failure tree from the top failure down to the root cause.

The diagnostic process generates complete failure paths for every anomaly detected at a particular instant in time. Trouble presents each anomaly and all of its potential root causes. In this fashion, Trouble presents its entire knowledge of the state of the power system for the operator's perusal.

4.4 Human Interface

An advisory system must present its information in a way that is easy for a human to understand and to manipulate. Ground operators are busy people and it is our job to make their lives easier. Trouble knows the current state of the power system whether it is operating within tolerances or not. It has information on the causes of any anomalies both past and present. The interface design emphasizes the location of information, the format of that information and the amount of human manipulation required to access information. We consulted with David Woods, a human factors expert from Ohio State University, before beginning the screen development.[3] With his help, we used functional decomposition to define screen requirements. We began by asking: "What does the power system do and how important are the various functions?" In this fashion we defined a hierarchy of importance for power system functions. We then used a function's importance to select size, color, and brightness for its icons. Those that represented very important functions became brighter than their less important neighbors.

We found that our interface had two separate yet related tasks: monitor the power system at all times and effectively present diagnostic information. In order to monitor a system, an operator needs to know where the system is operating in order to take action to prevent failures from occurring and interrupting power to the station. Our status-at-a-glance screen was created for this purpose. For a further discussion of this screen and its icons, see Liberman, et al.[4]

The second interface task was to present the diagnostic information in an effective manner. Our experiences led us to building a set of text screens to present this information. Operators will have varying levels of experience and we wanted to provide optional levels of detail to support different levels of expertise. As such we have three separate text screens. The first and smallest screen contains the minimum required data; where the problem is, when we found it, which device detected it and what kind of anomaly did we have. For an experienced operator and for a simple problem this information may be all that is desired. However, if the operator chooses to click on any particular anomaly in that window another window will appear which contains further diagnostic information. This window repeats the anomaly description data of the previous window adding all the possible root causes for that problem. These causes may be sufficient for determining what actions might be taken to identify the specific source of the problem and initiating corrective actions. However, if the operators want to question the reasoning that Trouble used to make those root cause associations, they can click on any line in the second window and a third window will open. This window contains all of Trouble's information about that particular anomaly. It details the main problem and all of the associated causes and subcauses that apply. Operators can use this level of detail to rule out potential causes that they deem are too unlikely to have occurred, or perhaps takes steps to acquire corollary information that would substantiate one of these as the true cause of the failure.

4.5 Operating Environment

We developed Trouble by interrogating the power system engineers who test the prototype flight power system component hardware. This information produced our FMEA data and became the focus of our integrated testing of Trouble. Connected directly to the PMAD testbed, Trouble is able to detect and diagnose failures from live hardware. This testing effort served as our method of validation for the knowledge in Trouble. It also presented us with software challenges with respect to networking and data requirements. Another challenge has been the constant reconfiguration of the power system hardware as it has been tracking the changes within the Space Station program. Due to the data dictionary design, accommodating these changes has been relatively easy.

When the Engineering Support Center became operational, we integrated into that environment, simulating a ground operations environment similar to that at the Control Center Complex, CCC, at NASA JSC. We simulate flight operations for the EPS back room using the PMAD testbed as the substitute for the Space Station. It is our goal to utilize the methodologies in Trouble as a cornerstone of an EPS operations console for the CCC.

5.0 AN EXAMPLE

The operator is monitoring the EPS and sees an anomaly message on the screen. The message is "SA22 detected Over Current Trip at 0:31:40". SA22 is an RPC in the secondary power distribution network from whom power flows into three channels through three tertiary RPCs; TA24, TA25 and TA26. Immediately the operator checks the status-at-a-glance screen and determines the breaker is in a tripped state and that power is not flowing through SA22. Searching for possibilities, the operator clicks on the anomaly message and receives a list of all the possible causes. In this case there are nine locations where failures might have occurred. Four of these locations are the lines connecting SA22, TA24, TA25 and TA26 to the tertiary distribution bus. Each line has one possible cause, a low resistance path leaking power from the line to ground. Four of the failure locations are the RPCs themselves. Each tertiary RPCs has one possible cause, an internal hard short before the current sensor. The secondary RPC (which is the tripped breaker) has three possible causes; over current trip level too low, failure of trip electronics or internal hard short after the current sensor. The last possible failure location is the tertiary bus which has four possibilities; load drawing more current than scheduled, too many loads scheduled, closed breaker allowing non scheduled loads to run and the existence of a low resistance path leaking power from the bus to ground. The operator believes that it is unlikely that there is a resistance path to ground in any of the lines, or an internal short in the tertiary RPC. The operator decides to investigate the load history on that tertiary bus, believing load fluctuations to be the most likely cause of the problem. Once the cause of this failure is established, corrective action can be taken to restore power to the affected area.

6.0 CONCLUSION

Operating the EPS for Space Station Freedom will be a difficult and human intensive task. We have built an advisory expert system to aid the human operators in monitoring and diagnosing faults in the power system. Our advisory system, Trouble, demonstrates that our concepts are viable. It is our goal to develop an advisory system based on this work to be incorporated in the JSC Control Center Complex.

REFERENCES

1. J.L. Dolce and K.A. Faymon, " A systems engineering approach to automated failure cause diagnosis in space power systems," in *Proc. 22nd Intersociety Energy Conversion Engineering Conference*, AIAA 1, 590-600 (1987).

2. D.B. Manner, "TROUBLE III: A Fault Diagnostic Expert System for Space Station Freedom's Power System," *NASA Contractor Report 187113*, NASA LeRC (1990).

3. D.D. Woods and S.S. Potter, "Visualization of dynamic processes: Function-based displays for human-intelligent system interaction," *Proceedings of the 1992 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, (1992).

4. E.M. Liberman, D.B. Manner, P.A. Mellor, and J.L. Dolce, "Design and Implementation of a Status at a Glance User Interface for a Power Distribution Expert System," in *Proc. 9th Computing in Aerospace Conference*, AIAA 1, (1993).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1993	Technical Memorandum

4. TITLE AND SUBTITLE
Reducing the Cognitive Workload: Trouble Managing Power Systems

5. FUNDING NUMBERS
WU–476–14–10

6. AUTHOR(S)
David B. Manner, Eugene M. Liberman, James L. Dolce, and Pamlea A. Mellor

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135–3191

8. PERFORMING ORGANIZATION REPORT NUMBER
E–8249

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, D.C. 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
NASA TM–106413
AIAA–93–4703–CP

11. SUPPLEMENTARY NOTES
Prepared for the AIAA: Computing in Aerospace 9, sponsored by the American Institute of Aeronautics and Astronautics, San Diego, California, October 19–21, 1993. David B. Manner and Eugene M. Liberman, Sverdrup Technology, Inc., Lewis Research Center Group, 2001 Aerospace Parkway, Cleveland, Ohio 44142 (work funded by NASA Contract NAS3–25266) and James L. Dolce and Pamela A. Mellor, NASA Lewis Research Center. Responsible person, James L. Dolce, (216) 433–8052.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 31

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The complexity of space-based systems makes monitoring them and diagnosing their faults taxing for human beings. Mission control operators are well-trained experts but they can not afford to have their attention diverted by extraneous information. During normal operating conditions monitoring the status of the components of a complex system alone is a big task. When a problem arises, immediate attention and quick resolution is mandatory. To aid humans in these endeavors we have developed an automated advisory system. Our advisory expert system, Trouble, incorporates the knowledge of the power system designers for Space Station Freedom. Trouble is designed to be a ground-based advisor for the mission controllers in the Control Center Complex at Johnson Space Center (JSC). It has been developed at NASA Lewis Research Center (LeRC) and tested in conjunction with prototype flight hardware contained in the Power Management and Distribution testbed and the Engineering Support Center, ESC, at LeRC. Our work will culminate with the adoption of these techniques by the mission controllers at JSC. This paper elucidates how we have captured power system failure knowledge, how we have built and tested our expert system, and what we believe are its potential uses.

14. SUBJECT TERMS
FDIR; Expert systems; Object oriented programming; Power system diagnosis; Failure diagnosis; Space power system

15. NUMBER OF PAGES
07

16. PRICE CODE
A02

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	