373

N90-20673

SPACE STATION FREEDOM INTEGRATED FAULT MODEL

by Fred J. Becker
Lockheed Engineering and Sciences Company
2400 NASA Road 1, C87, Houston, TX 77058-3711

ABSTRACT

This paper describes a demonstration of an integrated fault propagation model for Space Station Freedom. The demonstration uses a HyperCard graphical interface to show how failures can propagate from one component to another, both within a system and between systems. It also shows how hardware failures can impact certain defined functions like reboost, atmosphere maintenance or collision avoidance. The demonstration enables the user to view block diagrams for the various space station systems using an overview screen, and interactively choose a component and see what single or dual failure combinations can cause it to fail. It also allows the user to directly view the fault model, which is a collection of drawings and text listings accessible from a guide screen.

Fault modeling provides a useful technique for analyzing individual systems and also interactions between systems in the presence of multiple failures so that a complete picture of failure tolerance and component criticality can be achieved.

1.0 INTRODUCTION

This paper illustrates a HyperCard user interface for a failure propagation model of the Space Station Freedom integrated systems. It uses as an example a typical session of investigating the failure tolerance of the integrated Space Station Freedom systems. It also provides some background on how the failure model and HyperCard interface was developed.

The failure propagation model was coded and solved using Digraph Matrix Analysis, a proprietary software toolset. The results were transferred from a VAX to a Macintosh and there provided the required data to the HyperCard graphical environment.

This project was performed for the Guidance, Navigation, and Control Systems Branch of the Avionics Systems Division of the Johnson Space Center as a prototype for failure modeling tools which can be used for Space Station Freedom.

2.0 ABOUT FAILURE MODELING

The failure model which is behind the HyperCard user interface contains information about failure propagation in Space Station Freedom systems. This information is accessed by the HyperCard stack on command from cues provided by the user.

The failure model is in the form of a directed graph (digraph), which is a network model of a system pictorially representing failure propagation throughout the system. The digraph consists of nodes representing system components, and arrows representing failure propagation from one component to the next. Inputs to a node represent all things that component depends on for proper functioning. Conversely, outputs from a node represent failure propagation from that component to other components.

AND gates are used to indicate functional redundancy. For example, a computer might be supplied with electrical power from two busses. This would be drawn as two node inputs to an AND gate feeding the computer. Both nodes must fail before the computer fails.

Digraphs can be used to model anything from electrical diagrams to logic diagrams, fluid diagrams,

mechanical systems, procedures or end-to-end functions. Failure tolerance can be studied, when the system digraph is completed, by looking at the failure propagation results to see either what failures a given component failure can cause or what other failures can fail a given component. The latter method (the more difficult problem) is how this demonstration presents the information. Single failures or double failures which can result in the failure of the target component are displayed on the screen.

3.0 SPACE STATION FREEDOM FAULT MODEL

The overall fault model used in this demonstration contains about 600 nodes representing orbital replacement units, data lines, piping, tankage and other components of the Space Station Freedom systems. The purpose of this demonstration is to provide a relatively small model which nevertheless illustrates the highly integrated nature of the Space Station Freedom systems. Therefore, the models have been kept fairly high-level. Several high level functions, felt to be the most critical, are also modeled by showing their dependence on the systems. Systems and functions included in this model are:

Data Management System (DMS)
Guidance, Navigation and Control (GN&C)
Communications and Tracking (C&T)
Thermal Control System (TCS)
Environmental Control and Life Support System (ECLSS)
Propulsion
Electrical Power System (EPS)
Extravehicular Activity System (EVAS)
Reboost
Attitude Control
Docking
Collision Avoidance
Fire Suppression
Atmosphere Maintenance

The initial fault modeling was done by drawing the digraphs on paper, based on the system block diagrams. The failure propagation modeled was based on judgements about whether a particular functional connectivity implied any failure propagation. The resulting drawings were then translated into text listings for use with the Digraph Matrix Analysis software, which computed the failure "reachability". Next the block diagrams were created on HyperCard stacks, using button names which corresponded to the digraphs. Of the total model, 545 buttons were chosen for display. The following section shows how the result works.

4.0 HYPERCARD DEMONSTRATION TUTORIAL

4.1 Navigating Through the Stack

Figure 1 illustrates the opening card. This card is the first card the user sees. It contains an illustration of Freedom Station as a visual cue that the user is at the top level, plus a title bar across the top, a home button, and credits across the bottom. This card gives the user four options--INTRODUCTION, RUN MODEL, VIEW MODEL and FINISH. Clicking on INTRODUCTION will take the user to a section containing tutorial text. The RUN MODEL button starts the demonstration. The VIEW MODEL button allows the user to view the fault model drawings and listings. Clicking on FINISH will exit HyperCard.

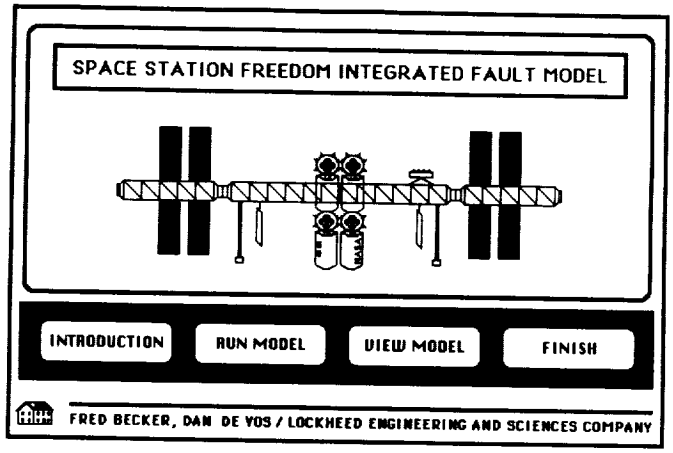

Figure 1
OPENING CARD

Figure 2 shows the introduction card. Instructions printed across the top tell the user what to do. This card guides the user to four areas of tutorial information:

PART 1
HOW TO USE THIS DEMONSTRATION

PART 2
ABOUT DIRECTED GRAPH FAULT MODELING

PART 3
WHAT HAS BEEN MODELED?

PART 4
SYSTEM FAULT MODELING IN THE
SPACE STATION FREEDOM PROGRAM

Part 1 helps the user learn to use the actual demonstration. Part 2 explains in general how directed graphs are used to model failure propagation. Part 3 details how the space station systems were modeled, and what source materials were used. Part 4 then gives a perspective on how fault modeling may be used in designing and

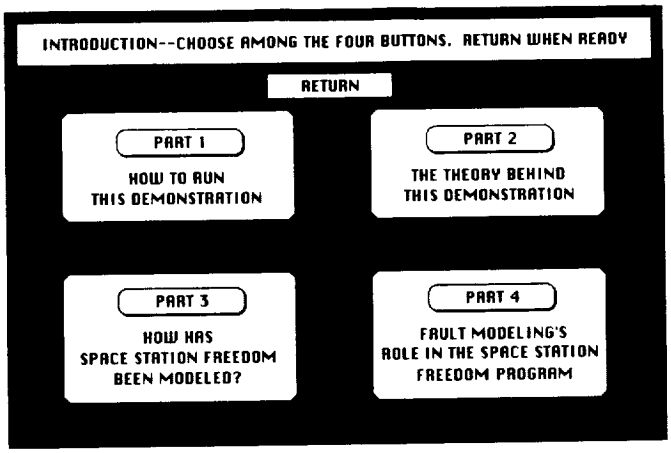

Figure 2
INTRODUCTION CARD

operating Space Station Freedom. These cards all contain text in a scrolling field. The RETURN button on these four cards will return the user to the introduction card. The RETURN button on the introduction card will then allow the user to return to the opening card. The introduction portion of the demonstration is optional. The user can go directly to the demonstration if desired by clicking on RUN MODEL on the opening card.

Figure 3 shows the result of clicking on RUN MODEL from the opening card. It has two buttons to allow the user to chose between two types of demonstration. The HARDWARE button goes into a demonstration in which individual hardware items are chosen as the ultimate targets of other hardware failures. The FUNCTION button takes the user into a demonstration which shows how Freedom Station's functions can be affected by various hardware failures. It was felt that an entire card dedicated to this choice would emphasize to the user the distinction between the two types. The RETURN button on this card allows the user to return to the opening card if desired. This card will be referred to as the "hardware or functions?" card.

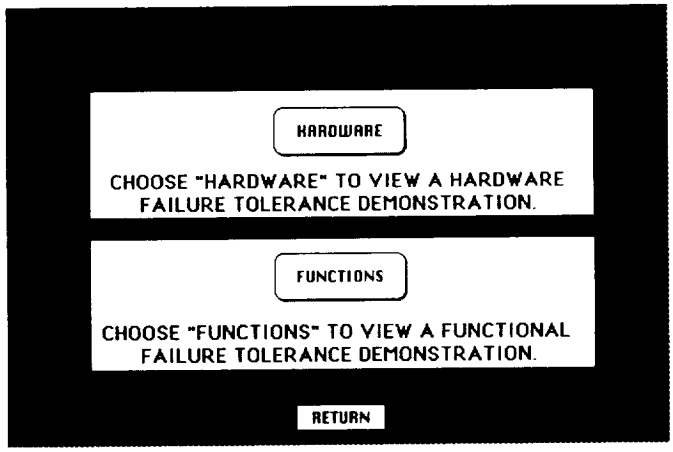

Figure 3
"HARDWARE OR FUNCTIONS?" CARD

Figure 4 shows the systems hardware card, identified by its title bar across the top of the screen. The user will see this card when the HARDWARE button is chosen from the "hardware or functions?" card. This card has a selection of Space Station Freedom systems from which the user will go into the demonstration. The user can view the block diagrams for these systems by clicking on the desired system. The SHOW DATA button allows viewing of singleton and doubleton data from the previous target chosen (an advanced feature). The VIEW DIGRAPHS button allows the user to view the entire digraph listing, taking the user to the same card as does the SHOW MODEL button on the opening card (a short cut from this card to the digraph). A message box across the bottom informs the user to click on one of the system boxes. MENU BAR will turn off the Macintosh menu bar, which is useful on

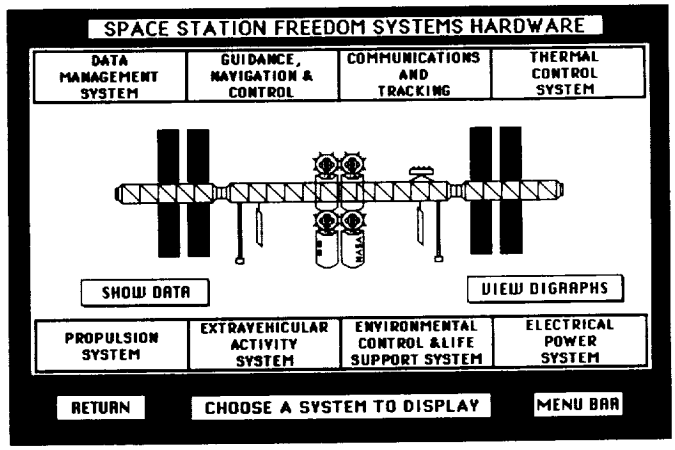

Figure 4
SYSTEMS HARDWARE CARD

Macintosh SE's or when making a presentation. RETURN will take the user back to the opening card.

Figure 5 shows the functions card. This card will allow the user to see how selected functions can be affected by various hardware failures. It is reached by clicking on the FUNCTIONS button from the "hardware or functions" card. When one of the six

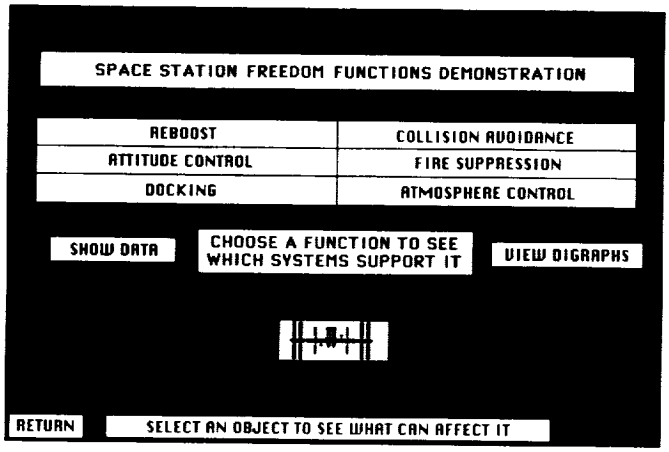

Figure 5
FUNCTIONS CARD

function buttons is clicked on, the associated systems which have hardware supporting that function will be highlighted across the bottom of the card. The user can then jump over to those system drawings to view the particular hardware combinations which can cause the loss of the chosen function. The remaining buttons have the same function as on the systems hardware card.

4.2 Starting the Demonstration

Figure 6 shows a typical system block diagram card, reached by clicking on one of the systems listed on the systems hardware card. This particular card shows the Guidance, Navigation and Control System block diagram. Each object in this card represents a node in the integrated Space Station Freedom fault model. By clicking on one of the objects, the user will be able to view all single and double hardware failures anywhere in the station which can propagate and eventually cause the failure of that object. These objects are the lowest level of detail contained in this demonstration, and when the user clicks on one of them the demonstration becomes active.

Other buttons on this card include an ACRONYMS button for displaying and removing a scrolling field

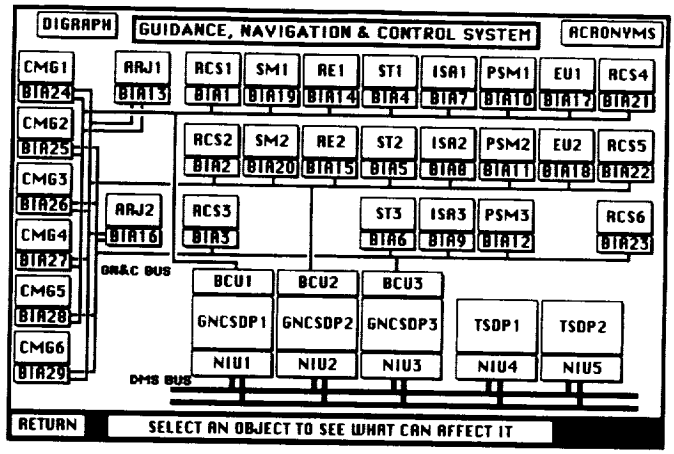

Figure 6
GN&C SYSTEM BLOCK DIAGRAM

containing the full names of the objects on the screen, a DIGRAPH button for viewing the associated digraph drawing or listing directly, and a RETURN button for returning to the systems hardware card.

When the user has clicked on a target object, in this case the Star Tracker #1 (ST1), buttons for the various systems will appear across the bottom of the screen (DMS, GN&C, C&T, etc.) with instructions on what to do. See **Figure 7**. Certain system buttons will be highlighted. These are the systems containing failures which can propagate to the target object, and are therefore a guide to viewing the

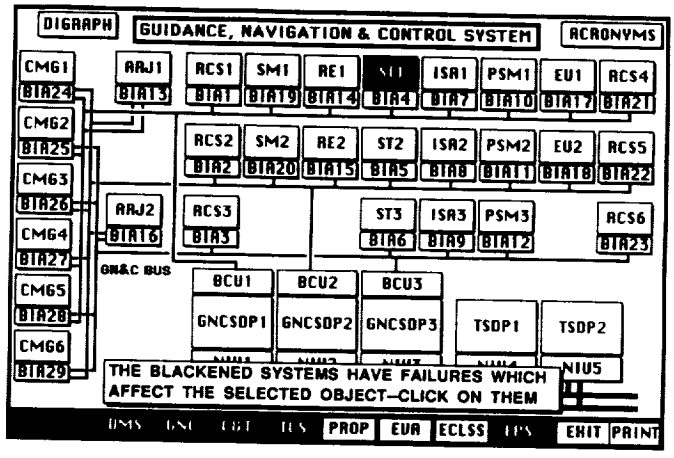

Figure 7
SYSTEMS WHICH REACH ST1

failure sources. When the user clicks on one of these highlighted systems buttons, the card for that system will be displayed.

As shown in **Figure 8**, the user has gone ahead and clicked on the GNC system button, which is the same card from which the target was already selected. Clicking on another system would have taken the user to that card. The GNC card remains, but two buttons, SINGLETONS and DOUBLETONS will appear at the bottom of the card. Clicking on one of these buttons will highlight one of the singletons or doubletons on (or partially on) this card which can reach the original target, ST1.

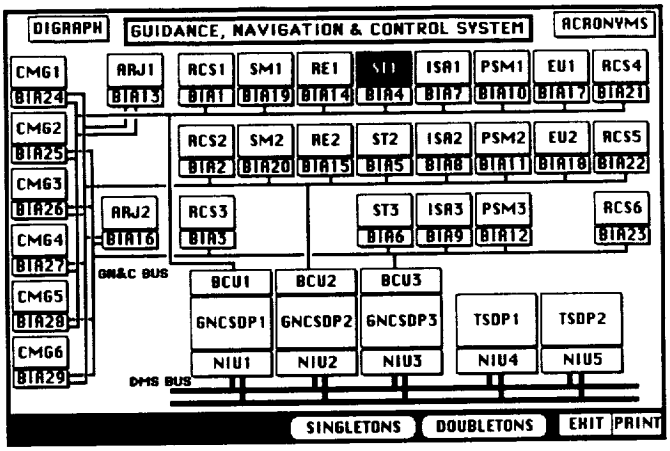

Figure 8
GN&C CARD, READY TO DISPLAY
SINGLETONS AND DOUBLETONS TO ST1

In **Figure 9**, the user has clicked on SINGLETONS, and the first singleton, Bus Interface Adapter #4 (BIA4), has been highlighted. A SHOW NEXT SINGLETON button will appear at this time. This button allows the user to cycle through all the single point failures. The components which can fail the original target will be independently highlighted. The original target remains highlighted as a reference.

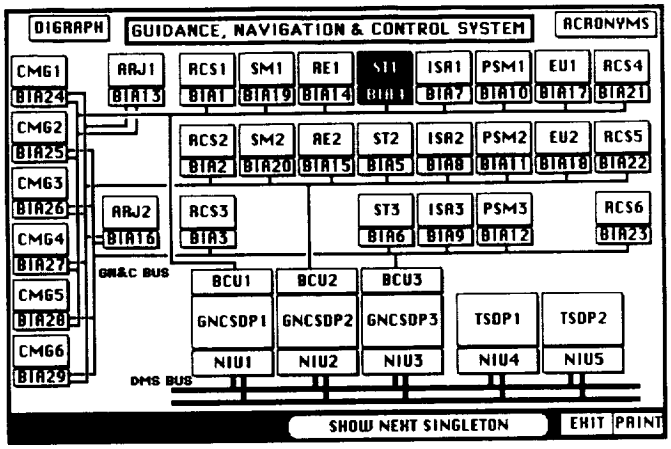

Figure 9
BIA4 IS A SINGLETON TO ST1

Doubletons are viewed in a similar way. **Figure 10** shows how two components, BIA13 and BIA16, are highlighted as a double-point failure which causes loss of the target, ST1.

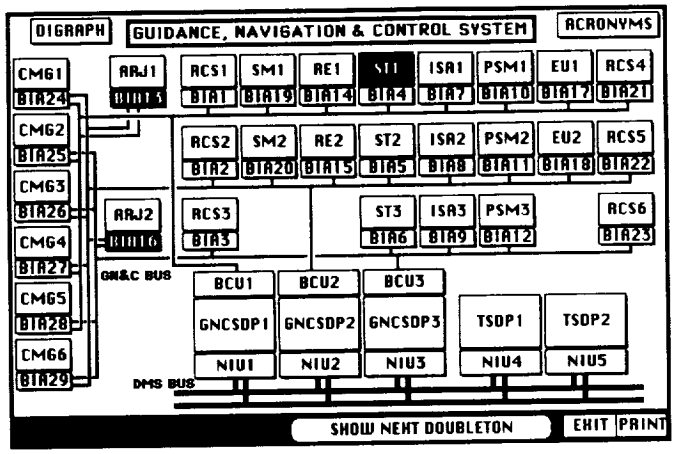

Figure 10
BIA13 AND BIA16 COMPRISE A
DOUBLETON TO ST1

However, when a double-point failure involves components on separate cards, another button, GO TO OTHER DOUBLET, will appear to allow the user to view the other half of the doubleton (a doubleton is made up of two "doublets"). As shown in **Figure 11**, the user has cycled through viewing doubletons until BIA16 is highlighted. BIA16 plus some other component off-screen are a double-point failure which can reach the target, ST1.

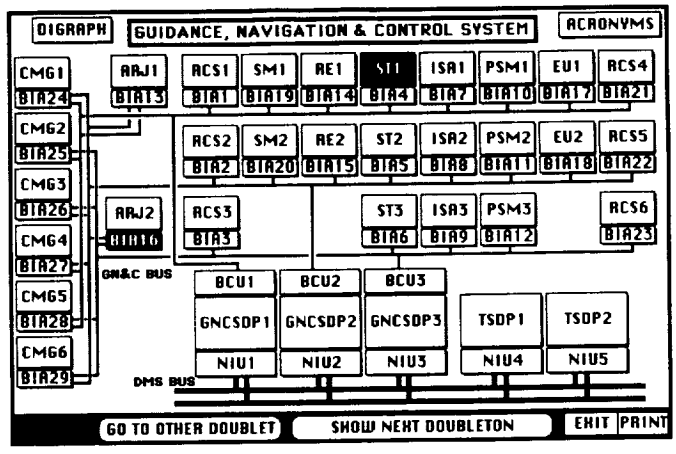

Figure 11
DISPLAY FOR AN OFF-SCREEN DOUBLET

By clicking on GO TO OTHER DOUBLET, the user will see the Electrical Power System block diagram with a single component highlighted, as shown in **Figure 12**. In this example, the alpha joint #1 (AJ1) is the second component of the pair. Thus BIA16 plus AJ1 failing together, will cause loss of ST1. A little inspection will show that BIA16 causes loss of Alpha Rotary Joint Driver #2 (ARJ2) which in turn causes loss of Alpha Joint #2 (AJ2). So the failure propagation path here involves loss of both

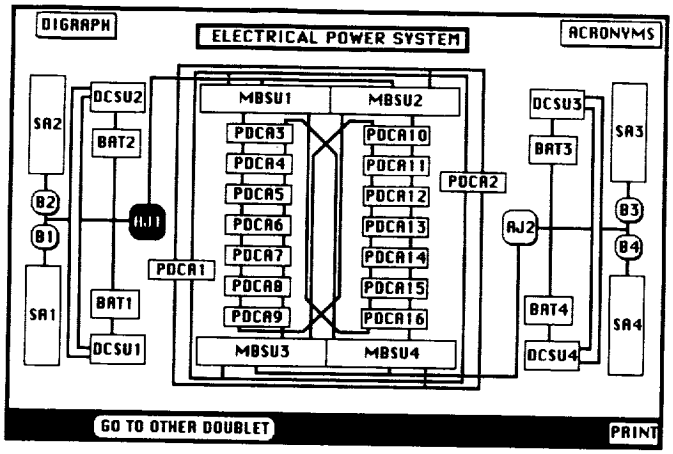

Figure 12
AJ1 IS THE OTHER DOUBLET

alpha joints and hence eventual total loss of power--which will naturally fail ST2. More complicated failure paths for other targets and sources might require viewing the entire fault model, as explained later.

There are other singletons and doubletons which reach ST1, not all shown here. These are viewed in the same way. At any point, the user can exit the process and choose another target. This is accomplished by clicking on EXIT until everything has been progressively reset. When the user is ready, clicking on RETURN will return him or her to the opening card.

4.3 Viewing the Fault Model

While running the demonstration, the user might be surprised that a particular singleton or doubleton can reach a given target. Failure tolerance is not always intuitively obvious. This demonstration allows the user to investigate a particular failure scenario further by viewing the fault model directly and rapidly tracing a failure path back from the target to the singleton or doubleton. Eventually, an understanding of the particular fault model contained in this demonstration can be attained. The speed with which the path can be traced demonstrates some of the advantages of computer graphical fault modeling.

The digraph topview card used for this purpose is shown in **Figure 13**. This card contains a guide to viewing the Space Station Freedom fault model drawings and source listings. It is reached by clicking on the VIEW MODEL button on the opening card, or the VIEW DIGRAPHS button on either the systems hardware or functions cards.

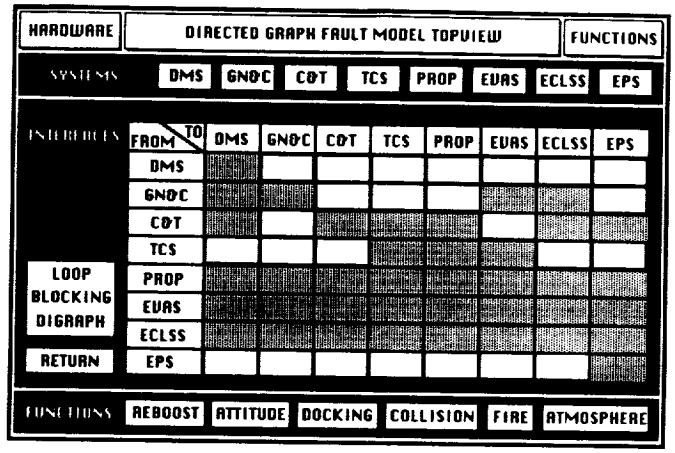

Figure 13
FAULT MODEL TOPVIEW CARD

The card contains a number of buttons which identify portions of the digraph. By clicking on any of these buttons, the user can view the associated portion of the digraph. This is useful for understanding how the fault model really works. The user can look through the digraphs to find the target chosen on a previous run, and trace back the failure propagation along the directed graph.

The systems buttons are across the top of the card. Interfaces between systems are identified in a matrix in the center of the card. Critical functions buttons are found across the bottom of the card. The loop blockage digraph has a dedicated button. The HARDWARE and FUNCTIONS buttons at the top will return the user back to the original cards. RETURN will take the user back to the opening card.

As an example, suppose the user wanted to trace the failure path from the doubleton pair BIA16, AJ1 to the target, ST1 as encountered in one of the examples above (**Figures 11 and 12**).

Figure 14 shows one of the digraph portion illustrations from which to start, in this case part of

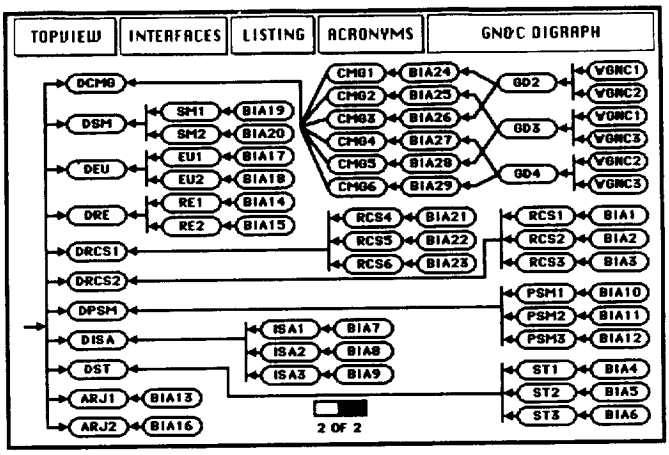

Figure 14
GN&C DIRECTED GRAPH

the GN&C system. A short-cut from the GN&C block diagram would have been to use the DIGRAPH button from that card (not available while the demonstration is active).

There are several active buttons across the top of **Figure 14**. The TOPVIEW button allows the user to return to the TOPVIEW card. ACRONYMS lists the acronyms found on this card. INTERFACES goes to the interface digraph for the GN&C System, and LISTING links to the digraph text listing.

Note from this figure that BIA16 fails ARJ2. On this drawing, ARJ2 fails nothing else. To see if ARJ2 fails anything in any other systems, the user will click on INTERFACES.

Figure 15 shows the result. In this case, all the GN&C interfaces fit on one card.

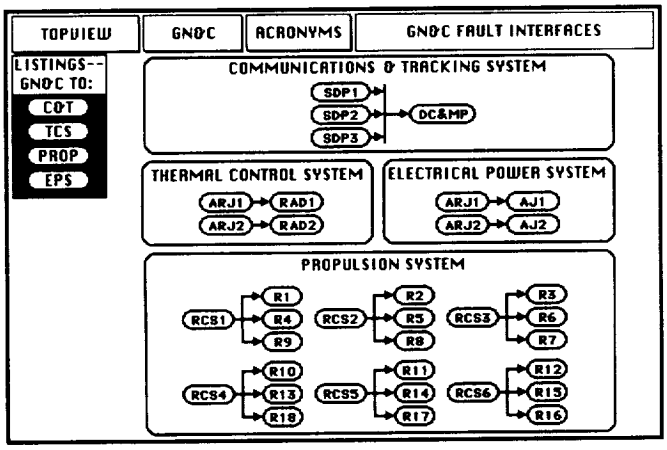

Figure 15
GN&C INTERFACES DIRECTED GRAPH

The interface digraphs such as this allow the user to gain a visual understanding of failure propagation paths between systems. A system button (GN&C here) allows the user to jump back to the source system digraph, if needed. To go to one of the interfacing systems, the user just clicks on the desired component belonging to that system.

ARJ2 can be found on the GN&C to EPS interface digraph. Here it is seen that that ARJ2 fails AJ2. It is also found in the GN&C to Thermal Control System (TCS) digraph. In this case, the user first tries the EPS digraph, and clicks on the AJ2 component to go there.

Figure 16 shows the EPS digraph. It can be seen that AJ1--one of the doubletons--is on this card as well as AJ2. By inspection, it can be seen that AJ1

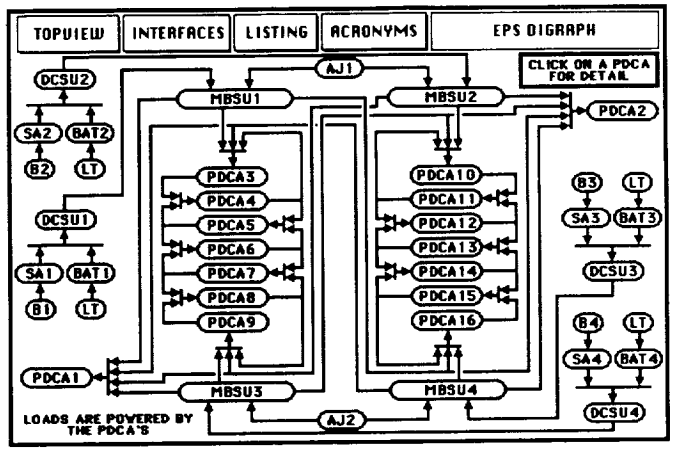

Figure 16
EPS DIRECTED GRAPH

and AJ2 failing will cause failure of Main Bus Switching Units (MBSU's) 1 through 4. Loss of all these will cause loss of power flow to all the Power Distribution and Control Assemblies (PDCA's). By clicking on EPS TO GN&C from the topview card, the card shown in **Figure 17** reveals that several BIA's are failed by losses of various PDCA's.

Going back to the GN&C digraph, **Figure 14**, it is seen that the target, ST1, is failed by loss of BIA4. Then, by going back to **Figure 17**, it is seen that BIA4 is indeed powered by PDCA1. Thus, the path from AJ1, BIA16 to ST1 has been found.

A check of the TCS and TCS interfaces digraphs does not find any such direct paths (**Figures 18 and 19**).

In a more developed tool, it would be useful to provide for automated tracing of these failure

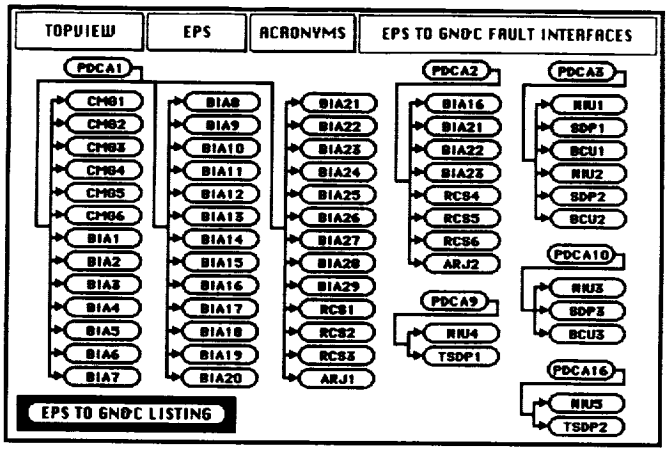

Figure 17
EPS TO GN&C INTERFACES
DIRECTED GRAPH

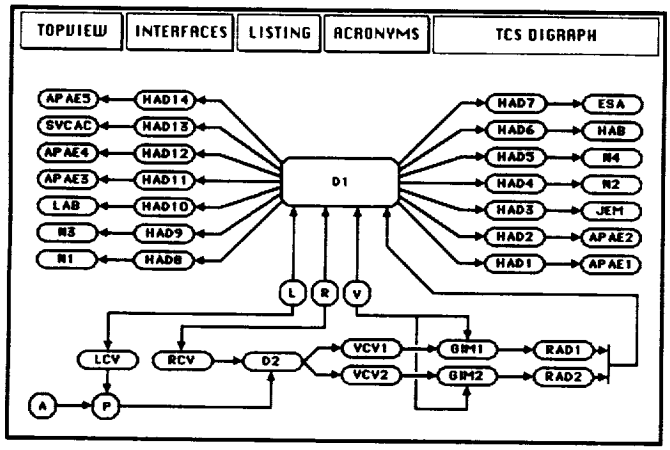

Figure 18
TCS DIRECTED GRAPH

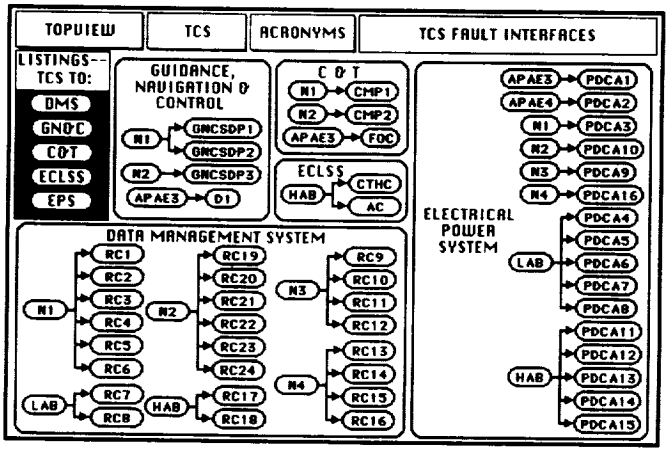

Figure 19
TCS INTERFACES DIRECTED GRAPH

propagation paths, known commonly as "cutsets."

A typical function digraph is shown in **Figure 20**. The function digraphs contain small "pushbuttons" which allow the user to go to the associated system card containing that object. The function digraphs are drawn in a fault tree structure. The linkage to digraphs shows one way that hardware failure modeling can be used in conjunction with functional modeling.

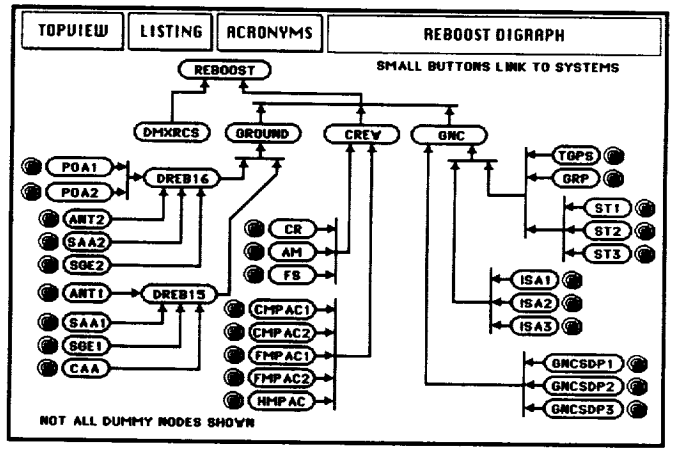

Figure 20
REBOOST FUNCTION DIRECTED GRAPH

Figure 21 shows one of the digraph listings cards. These cards contain the actual text listings of the Space Station Freedom fault model directed graph. The button highlighting seen in the demonstrations is driven by the failure propagation modeled in the total set of such listings. The syntax for these listings is of the form "A,B,C", meaning that A can reach B with C. If C is a "1", then the node A is a singleton

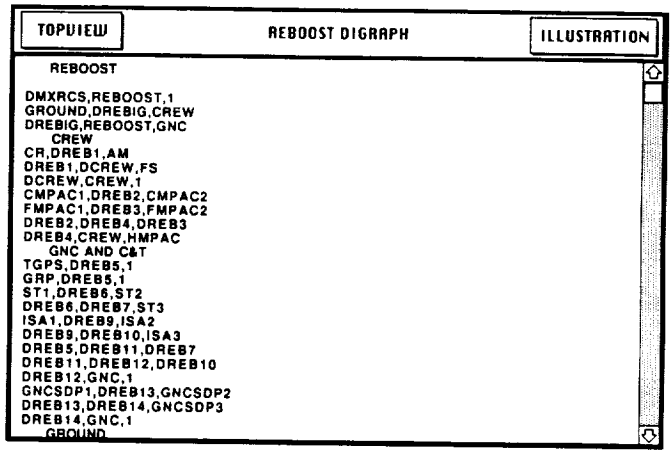

Figure 21
DIRECTED GRAPH LISTING EXAMPLE

to node B. The field can be scrolled up and down, using the scroll bar on the right, to view various portions of the listing. The ILLUSTRATION button will display an illustration of the digraph associated with this card, and the TOPVIEW button will return the user to the digraph topview card.

5.0 HYPERCARD DEMONSTRATION WORKINGS

This project had three separate phases: creating the HyperCard block diagrams and special button scripts to allow the demonstration to run, running the digraphs using Digraph Matrix Analysis (DMA) codes, and formatting the DMA results so they could be used by the HyperCard graphics demonstration. Reference 1 details the development of the demonstration. Reference 2 provides more information on DMA.

There are actually three HyperCard stacks used in the demonstration: one for the Introduction, one for Running the Demonstration, and one for Viewing the Model. This conserves the active memory in use by the Macintosh at any one time. The total memory occupied by all three stacks is about 670 kilobytes.

There are 98 cards in total: six for navigating, four for tutorials, 12 for system block diagrams, one for the functions demonstration, three for utility purposes, 14 for system digraphs, 11 for interface digraphs, seven for function digraphs, and 40 for digraph text listings.

The demonstration runs by accessing data stored in separate files on the Macintosh. The 1056 singleton and doubleton files are stored in a folder called "STATION_DATA." This folder occupies about 2.2 MB. In the demonstration, each time the user clicks on a target object, two of these files are copied into the HyperCard stack for use in highlighting the correct objects to show single and double-point failures.

6.0 FAILURE MODELING IN THE SPACE STATION FREEDOM PROGRAM

The distributed nature of the Space Station Freedom Program makes the system integration problem different from that on any previous NASA program. There is no longer a simple division of work by large hardware elements. Rather, work is divided into both hardware elements and distributed functional systems. The interfaces between the functional systems are more varied and complex than those between distinct elements.

In view of this, there is a need for new approaches to satisfying the program failure tolerance requirements and capturing the knowledge of how redundancy management evolves in various systems--both during design and operations. Failure modeling is one way to accomplish these goals.

7.0 CONCLUSIONS

The HyperCard tool has proven valuable as a means for prototyping various graphics concepts and for interfacing displays to fault modeling tools. The demonstration shows the basic methodology which would be performed in doing more detailed and accurate fault modeling. It contains a tutorial section, a block diagram section from which failure tolerance can be interactively displayed, and an illustration section by which the large directed graph fault model can be viewed. The Space Station Freedom systems, as modeled here, are indeed highly interdependent.

ACKNOWLEDGEMENTS

The fault modeling and demonstration was a joint effort by F. J. Becker and D. M. De Vos, a Lockheed summer-hire. D. M. De Vos's contributions were particularly essential for developing the software which interfaces the DMA files to the HyperCard stack and for co-creating the HyperCard script which drives the demonstration.

Thanks go to our NASA task monitor, J. T. Edge, and Lockheed task manager, W. H. Geissler, for their leadership in guiding this project.

REFERENCES

1. Becker, Fred, "Space Station Freedom Integrated Fault Model Report," LESC-26314, Lockheed Engineering and Sciences Company, Houston, Texas, December, 1988.

2. Sacks, Ivan, "Digraph Matrix Analysis," Analytic Information Processing, Inc., November, 1988.