Software Fault Tree Analysis Tool User's Manual

Craig Rolandelli
Timothy J. Shimeall
Christi Genung
Nancy Leveson

Department of Information and Computer Science
University of California, Irvine
Irvine, CA 92717
(714) 856-5517

Technical Report #86-06

ABSTRACT

The Software Fault Tree Analysis Tool allows the user to interactively modify the graphic representation of a fault tree. This manual describes the user interface of the tool. The tool is currently available only for Sun-2 workstations running 4.2 BSD Unix.

1. Overview of Software Fault Tree Analysis

The Software Fault Tree Analysis Tool is designed to aid the user in the construction of software fault trees, identifying fault sequences which could lead to hazards. The tool is based on techniques of software fault tree analysis. The user unfamilar with these techniques should consult "Fault-Tree Analysis of Software"[1], the "Fault Tree Handbook"[2], and "Using Fault Trees to Find Design Errors in Real Time Software"[3].

1.1. Fault Tree Symbols

Software fault trees are constructed through the use of the below mentioned symbols. These symbols comprise a subset of those used in hardware, so as to create an intergration between hardware and software fault tree techniques. The symbols can be classified into two groups, the Event Descriptor Symbols (EDS) and the Event Requirement Symbols (ERS). Event Descriptor Symbols are used to describe system events and their analysis requirements. The Event Requirement Symbols are used to specify the requisite system state or input events to trigger a system output event.

1.1.1. Event Descriptor Symbols - Ref. Mil-Std-882a

Rectangle: Indicates an event to be further analyed.

Diamond: Used for nonprimal events which are not developed further for lack of information of insufficient consequences.

Circle: Indicates an elementary event or primary failure of a component; no further development is required.

House: Used for events which normally occur in the system. It represents the continued operation of the component, and its probability is the reliability of the component.

1.1.2. Event Requirement Symbols

Oval: Used to indicate a state of the system that permits a fault sequence to occur. This system state may be normal or a result of failures.

And : This gate serves to indicate that all input events are required in order to cause the output event.

Or : This gate indicates that one or more of the input events are required to produce the gated event.

Null: The ouput event is a direct consequence of a single input event.

2. The Mouse

The mouse has three functions:

Position : It allows you to move the pointer on the screen to point to the object you want.

Selection : By moving the pointer from subwindow to subwindow you pick the currently active subwindow; by pressing the buttons, you may select objects to be modified.

Command : By pressing the buttons, you may select commands or pop-up menu options. Buttons, commands, objects, and menus are discussed below.

2.1. The Buttons

The three buttons on the mouse are used as follows:

Left button : To select a command or object, move the mouse so that the pointer is close to the command or object then press the left mouse button. When selecting and object such as a node in the tree, you may move the node around by holding down the left button and moving the mouse pointer.

Right button : If there is a list of options that accompanies a command or you are in the graphics subwindow, pressing this button will give you a “pop-up” menu of options.

Center button : (only used in the graphics subwindow) It is used to add child or parent nodes to the current node.

3. The Screen and Pop Up Menus

3.1. Overview of the windows

The tool is made up of one main window and six subwindows. The main window may be moved, closed, opened, stretched, etc... using the standard Suntools menu and the mouse. Subwindows can not be rearranged within the tool.

3.2. Subwindows

3.2.1. Status Subwindow

The status subwindow is located in the top subwindow of the tool. It contains six fields. To select one of them, move the mouse pointer close to the field and press the selection (left) button. To change the selected field, type on the keyboard. Keyboard input to the status subwindow is only available if the mouse pointer is in the status subwindow or the graphics subwindow. The six fields are:

Node Label: This is the name that will be assigned to the current node. It's default is 'Root Node' for the top node, and 'blank' for all other nodes. If it is 'blank', then no label will be assigned to the current node. If the current node label has been changed, then that value will be present in this field.

Node Fault: This contains the fault associated with the current node.

Root Fault: This is the fault that is associated with the root node. (ie. The fault associated with the tree.)

Fault Tree Name: This is the file that contains the current fault tree. Both the 'store' and 'load' commands use this field. Its default is 'Tree'.

Session Name: This is the session name that is associated with fault tree. Its default is your login ID.

Author: This is the author of the current fault tree. Its default is your login ID.

3.2.2. Command Subwindow

The command subwindow is located just under the status subwindow. It has seven fields. To pick a command, move the mouse to the field of your choice, and press the left mouse button. The right mouse button will give you a one line description of the command. The commands are as follows:

Quit: This will exit the program. If you have not saved your last changes to the fault tree it tell you so, and ask for confirmation to quit.

Store: This will store the current fault tree in the fault tree file.

Load Tree: This will load the tree contained in the fault tree file.

Add Mode: This is a toggle switch to determine whether to add a a child node to the current node, or whether to make a new parent for the current node. Default is Add Child Node.

Help: Only the left hand button works for this field. It will display a short summary of all the commands and fields with in the subwindows.

Delete Node: Will delete the current node. No deletion is done if the current node has children, or it is the root.

Refresh: This will redraw the fault tree.

3.2.3. Mouse Button Subwindow

The mouse button subwindow is located under the command subwindow. This is just an information subwindow. No commands are available. It tells you what each mouse button will do when the mouse is inside of the graphics subwindow.

3.2.4. Message Subwindow

The message subwindow is located under the right hand half of the mouse subwindow. All error and confirmation messages will be displayed in this subwindow. No commands are available.

3.2.5. Print Subwindow

The print subwindow is located under the left hand half of the mouse subwindow. The print subwindow has three fields:

Form: This field has three options, PIC for output which can then be used with the pic, troff or tex processors; LPT for normal (80 column) line printer output; and WID for wide (132 column) line printer output. Pressing the left mouse button changes the value of Form, and the right button gives you help. Default is PIC.

File: This is the name of the output file which can then be sent to the printer. Default is the fault tree file name with the suffix '.out' appended.

Print: Command to cause the output to be generated.

3.2.6. Graphics Subwindow

This is the subwindow where the fault tree is drawn. The mouse is used to move the pointer around in the window. If the tree is taller than the window, a '(more)' prompt will be displayed where the tree goes out of the window. If the tree is wider than the window, then a '>' will be displayed if the tree goes out of the right hand side, or a '<' will be displayed if the tree goes out of the left hand side. By moving the pointer to one of these prompts, and pressing the left hand mouse button, you can move to the next 'page' of the tree. When the mouse pointer is in the graphics window, the three buttons have the following functions:

Left button: Selects the node closest to the mouse pointer as the new current node. If you hold the button down, a small window will appear around the node, you may then move this window around the screen. When you let go of the button, the current node will move to the current pointer location.

Middle button: This button will add a new node to the current node if Add Mode is set to Add Child Node, else it will add a new node between the current node and it's parent. If you try to add more than five children to a node, an error message is produced. It also will not let you add a parent to the root.

Right button: This button will produce the following menu of options:

Refresh tree: Redraws the fault tree.

Fix Position: Moves the current node to the level of its siblings. If the node is an only child, fix position moves it underneath its parent.

Change Parent: Changes the linkage between nodes in the tree.

Gate : There are three gate fields, OR, AND, and NULL. Picking one of these will add this gate to the current node. Only the rectangular nodes have gates, since only they have meaningful children.

Shape: There are five shape fields. Picking one of these will change the current node to that shape.

Delete node: This will delete the current node.

4. How To Create a Fault Tree.

To create a fault tree do the following:

1) Start the tool. It will initially look like figure 1.

2) To add a node, move the pointer to the root node, and press the left mouse button to select it as the current node, next press the middle button to add a child. Pressing this button again will add another child, up to five children. See figure 2.

3) To give a node a label, move to that node, and press the left mouse button to select it as the current node. Next move the pointer to the status subwindow, and type the new label. See figure 3.

4) To change the shape of a node, move the pointer to the node you wish to change, and press the left mouse button to select it as the current node. Next press the right mouse button and hold it down, a menu will appear on the screen. See figure 4. Next will holding the button down, slide the mouse pointer down to the shape you wish and let go of the button. See Figure 5.

5) To place an AND gate at the root, make it the current node, and press the right mouse button to get the menu. See figure 4. Select the AND gate option, and let go of the button. See figure 6.

5. Files

/users/safety/SFTA --Software Fault Tree Analysis Tool
or see System Administrator.

- currently the tool is available only on SUN-2 graphics workstations, running 4.2 BSD Unix*.

6. Acknowlegements

This program is a revision of an earlier program[4] written by Janice L. Stolzy, Jeffrey C. Thomas, Timothy J. Shimeall, Kenneth Geib, John Ritchie, and Thomas Jefferson. The earlier program was designed for non-graphic terminals, and has a completely different user interface.

7. Disclaimer

The Software Fault Tree Analysis Tool is the property of the Regents of the University of California. The Software Fault Tree Analysis Tool is provided by the Regents of the University of California on an "As Is" basis. The Regents of the University of California makes no warranty that the functions contained in the Software Fault Tree Analysis Tool will meet the user's requirements or will operate in the combinations which may be selected for use by the user, or that the operation of the Software Fault Tree Analysis Tool will be uninterrupted or error free. Additionally, the University of California makes NO warranty whatsoever as to merchantability or fitness for any particular purpose or use. Any implied warranties are hereby expressly disclaimed. The Regents of the University of California are under no obligation to provide either maintenance services, update services, notices of latent defects, or correction of defects for the Software Fault Tree Analysis Tool.

Bibliography

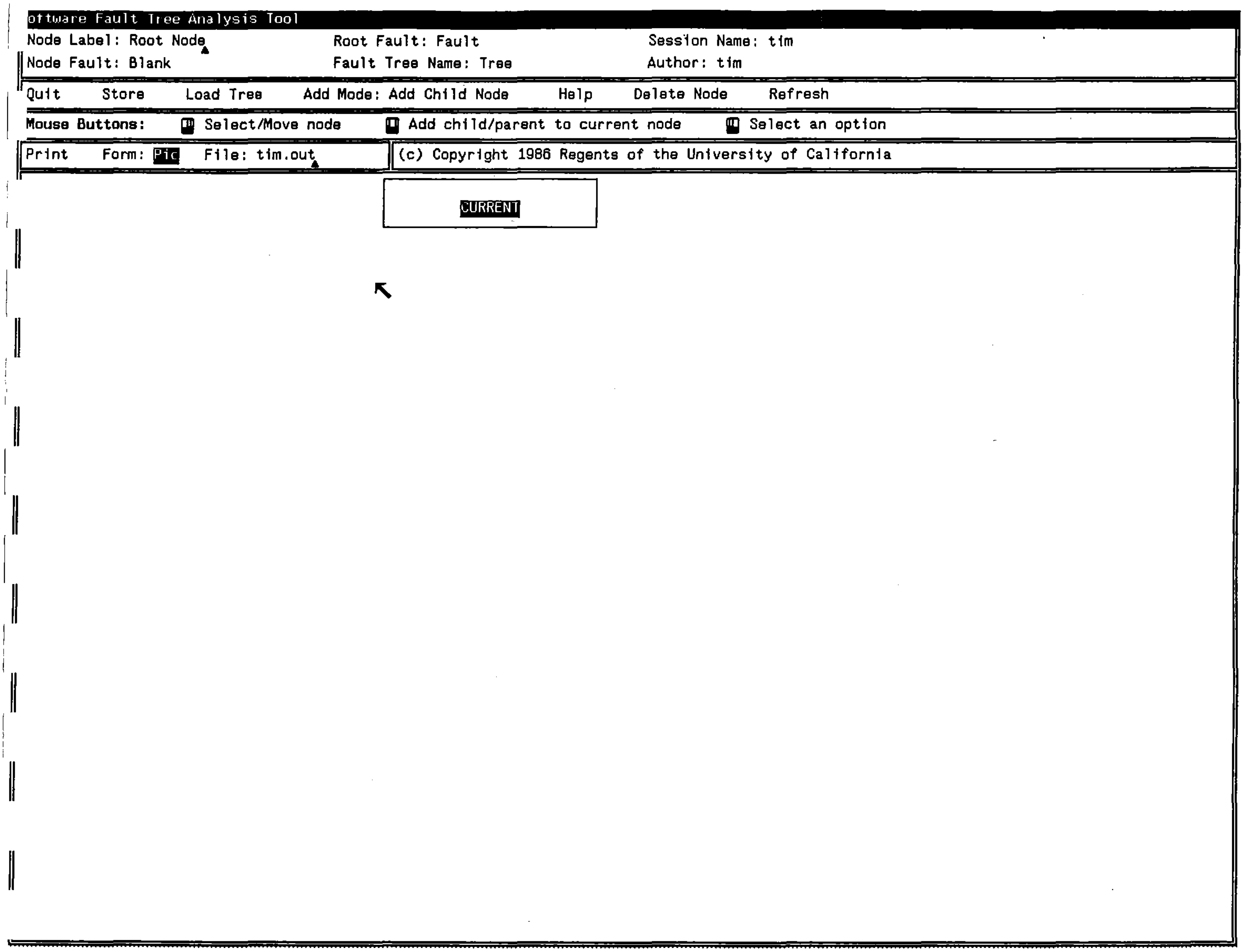
1. Harvey, P. "Fault-Tree Analysis of Software", Master's thesis, University of California, Irvine, January 1982.

2. Nuclear Regulatory Commission, "Fault Tree Handbook".

3. Leveson, N. and Stolzy J. "Using Fault Trees to Find Design Errors in Real Time Software", University of California, Irvine, January 1983.

*Unix is a trademark of AT&T.

4. Stolzy, J. "Software Fault Tree Analysis Tool", University of Califonia, Irvine, Dec. 1984.



oftware Fault Tree Analysis Tool

Node Label: Root Node   Root Fault: Fault   Session Name: tim

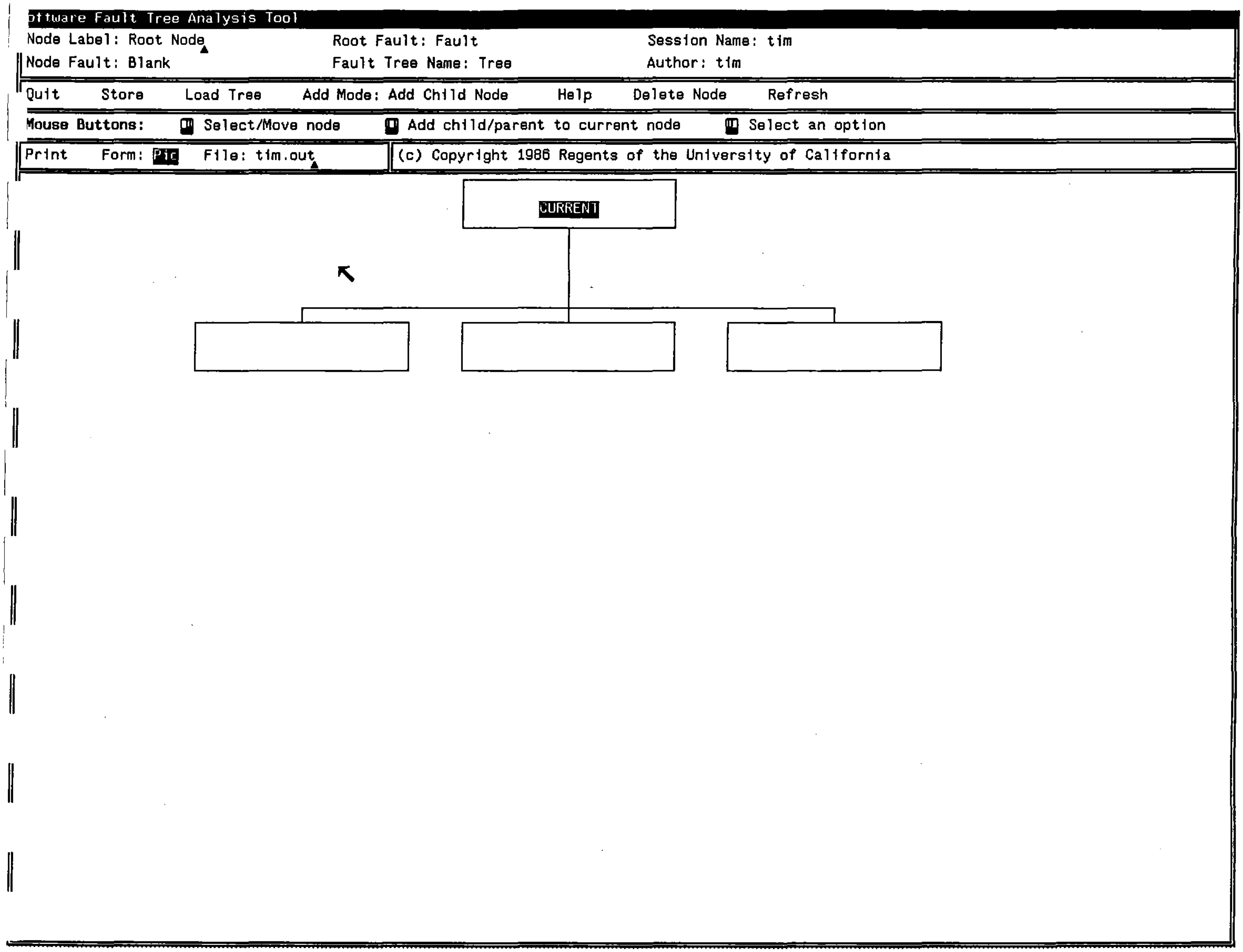
Node Fault: Blank   Fault Tree Name: Tree   Author: tim

Mouse Buttons: Select/Move node   Add child/parent to current node   Select an option

Form: Pic   File: tim.out

(c) Copyright 1986 Regents of the University of California

Figure 1



ottware Fault Tree Analysis Tool

Node Label: Root Node

Node Fault: Blank

Root Fault: Fault

Fault Tree Name: Tree

Session Name: tim

Author: tim

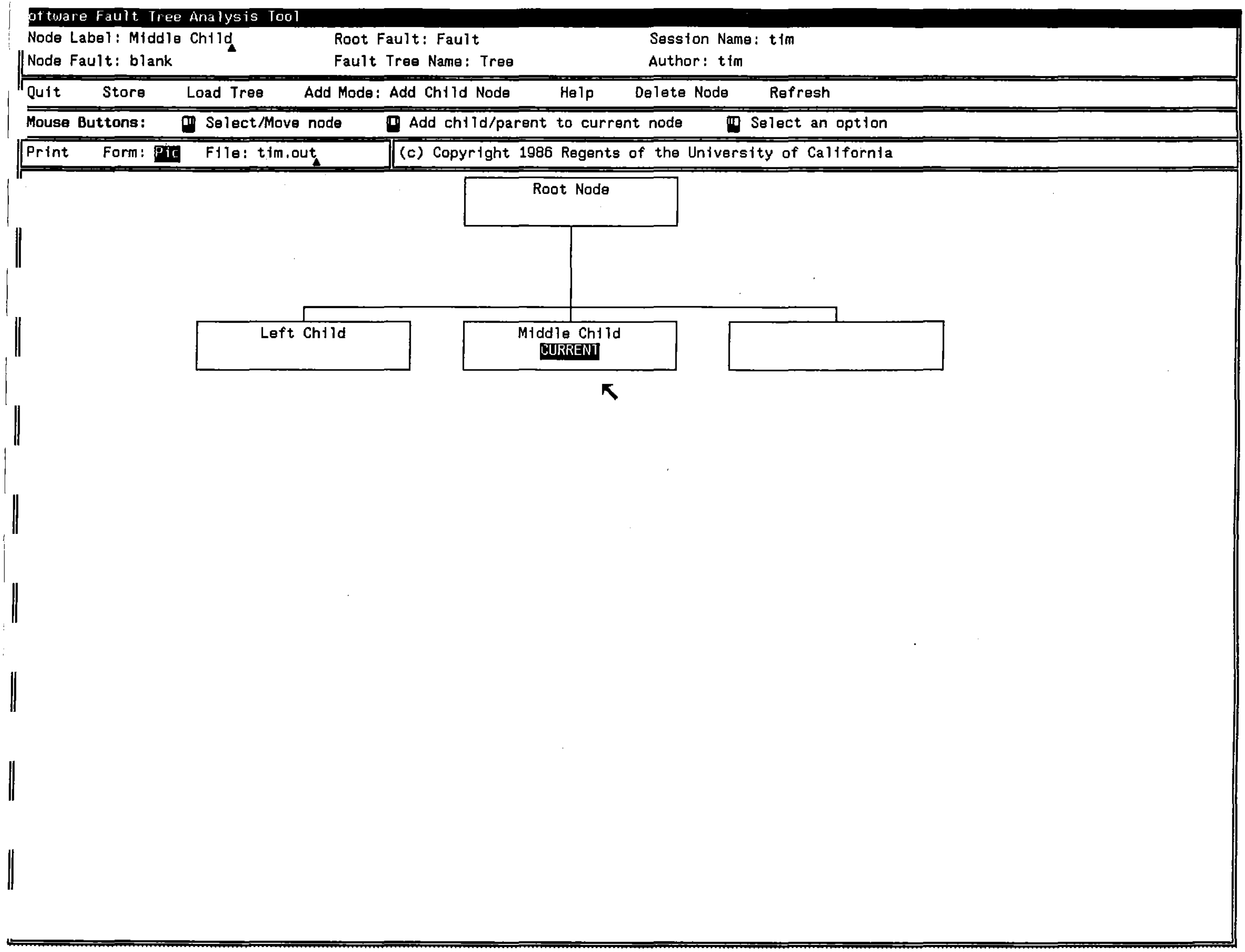
Add Mode: Add Child Node

Form: Pic

File: tim.out

(c) Copyright 1986 Regents of the University of California

Figure 2

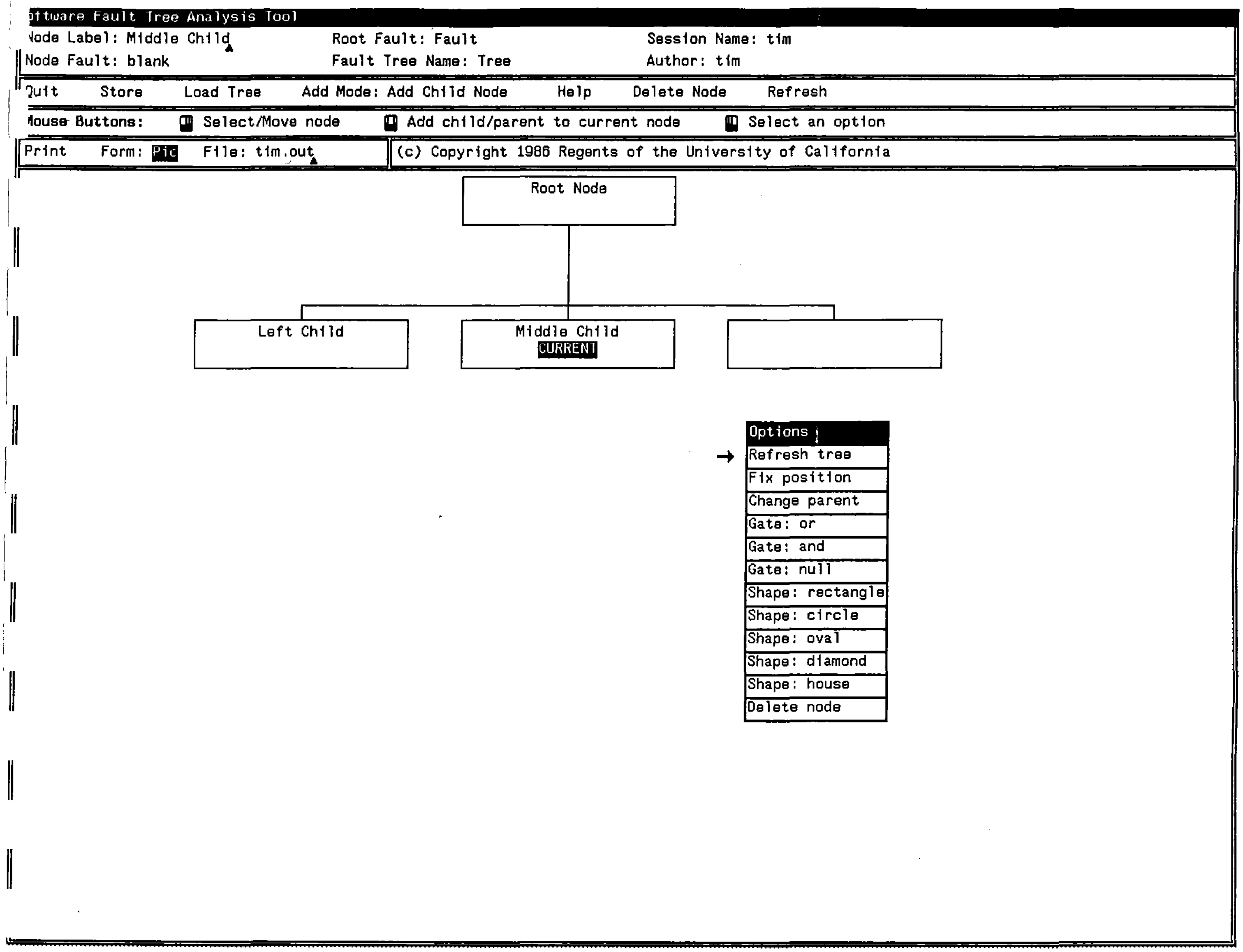


oftware Fault Tree Analysis Tool

```
Node Label: Middle Child        Root Fault: Fault              Session Name: tim
Node Fault: blank               Fault Tree Name: Tree          Author: tim
```

(c) Copyright 1986 Regents of the University of California

Figure 3

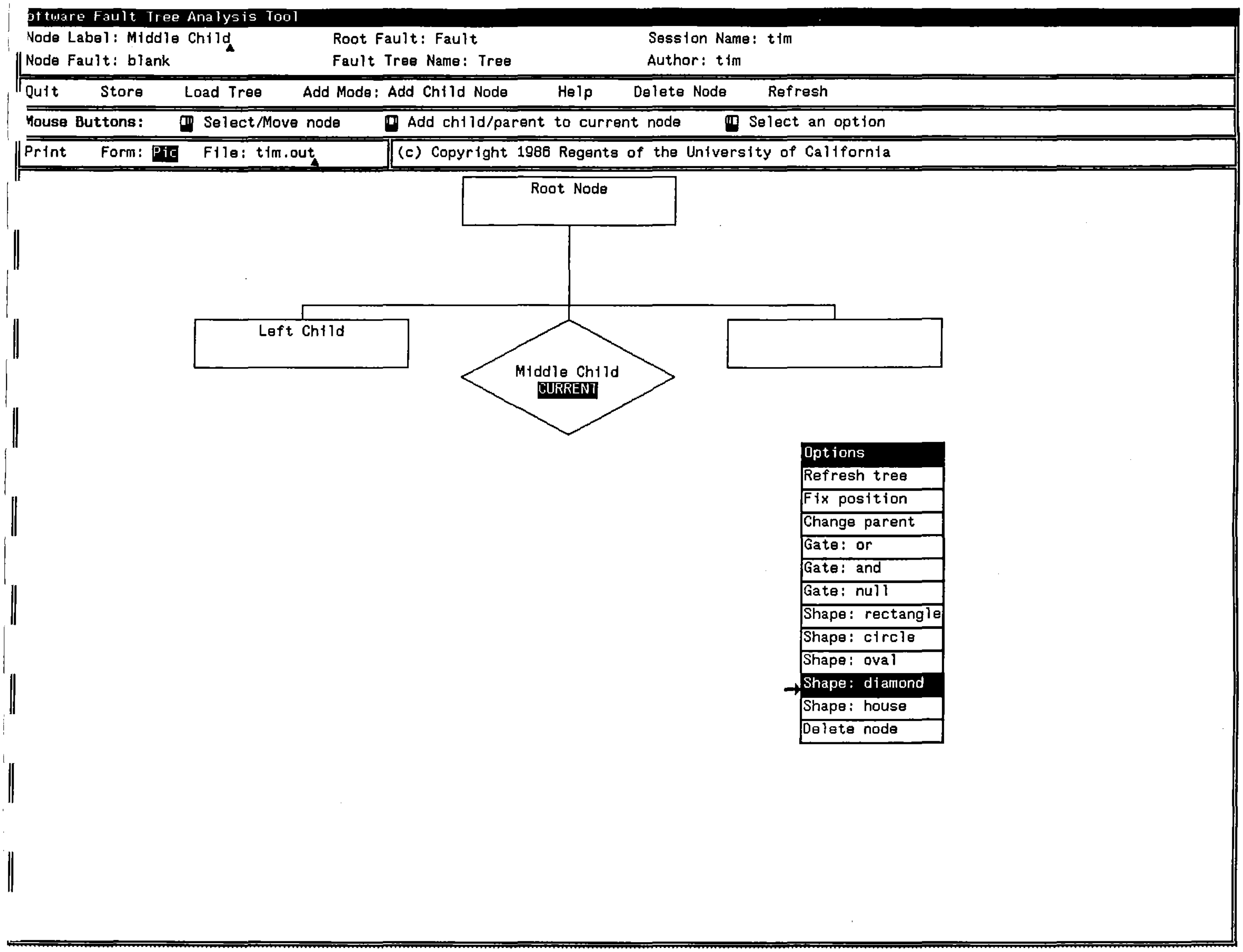

oftware Fault Tree Analysis Tool

Node Label: Middle Child   Root Fault: Fault   Session Name: tim
Node Fault: blank   Fault Tree Name: Tree   Author: tim

Print   Form: Pic   File: tim.out

(c) Copyright 1986 Regents of the University of California

Figure 4


oftware Fault Tree Analysis Tool

Node Label: Middle Child   Root Fault: Fault   Session Name: tim

Node Fault: blank   Fault Tree Name: Tree   Author: tim

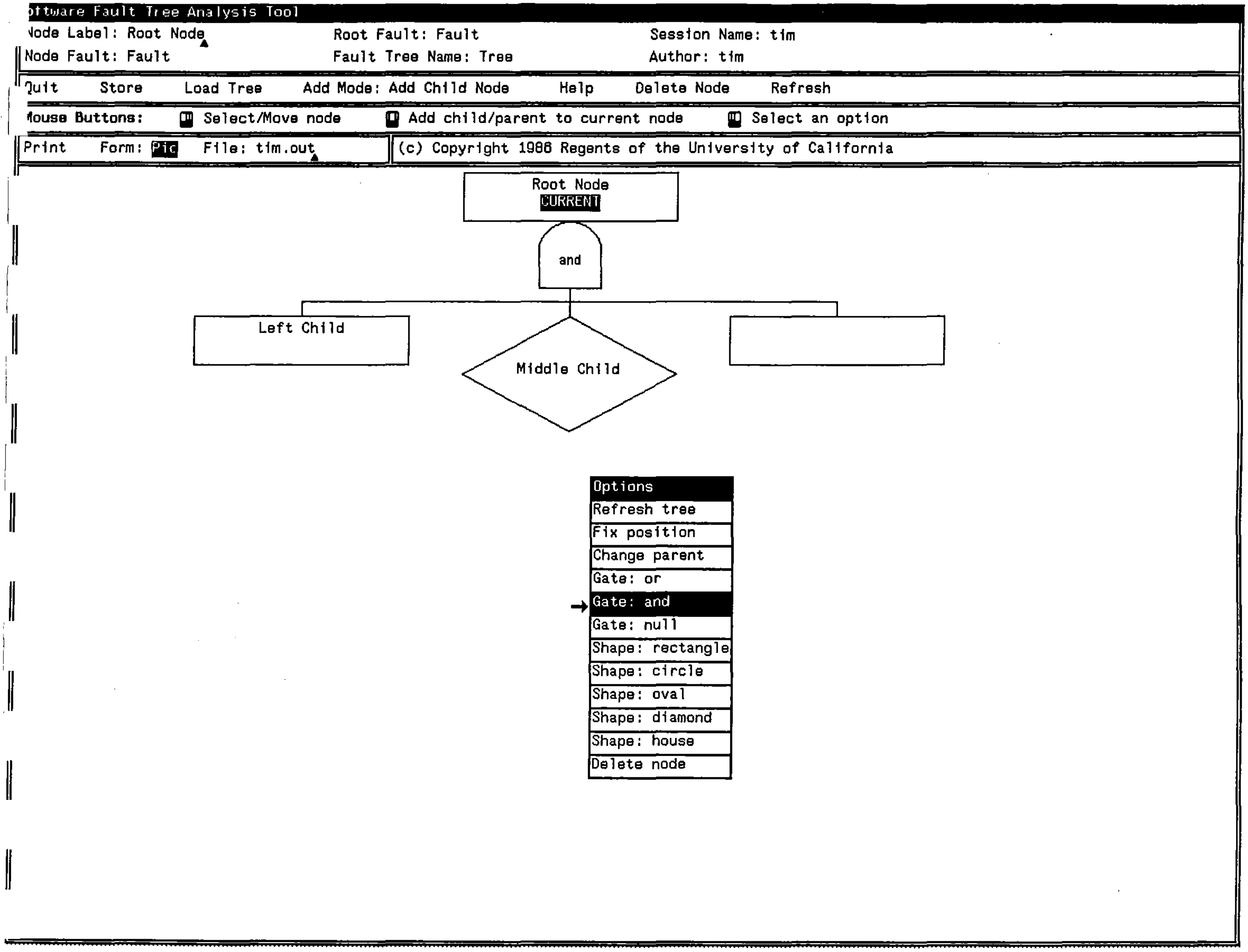
Add Mode: Add Child Node

Mouse Buttons: Select/Move node   Add child/parent to current node   Select an option

Form: Pic   File: tim.out

(c) Copyright 1986 Regents of the University of California

Figure 5



oftware Fault Tree Analysis Tool

lode Label: Root Node   Root Fault: Fault   Session Name: tim

Node Fault: Fault   Fault Tree Name: Tree   Author: tim

louse Buttons: ▯ Select/Move node ▯ Add child/parent to current node ▯ Select an option

Print Form: Pic File: tim.out

(c) Copyright 1986 Regents of the University of California

Figure 6