CALIFORNIA PATH

CALIFORNIA PATH HEADQUARTERS
UNIVERSITY OF CALIFORNIA, BERKELEY
INSTITUTE OF TRANSPORTATION STUDIES
RICHMOND FIELD STATION
1357 S. 46TH STREET, BUILDING 452
RICHMOND, CA 94804-4698
TEL: (510) 231-9495 FAX: (510) 231-9565

Date: 22 Aug 96

Number of pages to follow: 9

To Confirm: (510) 231-9495
Fax: (510) 231-9565

To: Phil Koopman

Fax Number: (412)268-5229

Agency/Department: CMU

FAX FROM: Jim Misener

COMMENTS: ① Re Hughes AEFT, per your request. Please heed to my admonition in the e-mail, as Hughes is sensitive that any use be for NAHSC purposes.

② Glad to hear you're in dialog with Bret Michael. Be sure to ask Rim about the software safety and verification project that he's involved with. His colleague, Andy Segal, is more into it, but Bret is familiar with it.

③ The first guy to talk to @ Hughes re: AEFT is Jim Lewis (ph. 714-446-2790, e-mail jlewis4@msmail3.hac.com)

ACTIVE ELEMENT FAULT TREE (AEFT)

Users Manual

TABLE OF CONTENTS

LIST OF FIGURES

1.0 Introduction

The Hughes developed tool named Active Element Fault Tree (AEFT) provides a graphical interface for hazard tree development and a simulation program for calculating the Mean Time to Hazard (MTTH) for the root node of the hazard tree. The hazard tree is used not only for top-down safety analysis but serves as a vehicle for organizing and archiving the results of the safety analysis. Documents can be linked to each leaf event to show how the leaf event was mitigated. The user can double-click on a leaf to view these documents. The AEFT tool runs on both Mac and (soon) Windows platforms.

2.0 Configuration and Installation

2.1 Configuration. The configuration needed to run the AEFT tool is listed below:

a. Macintosh Computer
b. MacFlow 4.0.5
c. AEFT 2.0

2.2 Installation. Installation consists of installing MacFlow on the computer, coping the AEFT simulation application and the AEFT Starter Fault Tree from the disk to a folder on your Macintosh, and coping the AEFT extraction plugin from the disk to the MacFlow plugin folder.

3.0 Hazard Tree Development

3.1 General Hazard Tree Conventions. The tree is conventionally drawn upside down, with the root at the top and the leaves at the bottom. Refer to Figure 1 for a diagram of a sample hazard tree. An event or condition is indicated by a rectangle. The event is labeled with an Event Lable and a description of the event/condition. The logical cause-and-effect interrelationships between events are indicated by interconnecting the events/conditions by means of OR and AND gates, culminating in the root event. An OR gate is represented by a shield. An AND gate is represented by a semicircle. Each gate has one or more events/conditions as inputs and a single event condition as output. The output event occurs if and only if the input events occur (according to the logic). The input events/conditions are drawn directly beneath the gate and are each connected to the gate by a line. The output event/condition is drawn directly above the gate and connected to the gate by a line. An OR gate means that the input events/conditions can each cause the output event condition or that the input events/conditions describe the output event/condition with greater specificity. An AND gate means that all of the input events/conditions have to occur—at the same time—in order for the output event/condition to occur.

The top event is a Root Hazard. The second level events are the Top-Level Hazards. All other levels contain Input and Output events. An event which has no input events connected to it is a Leaf event. An event which has input events connected to it is an Output event.

Leaf events can be grouped into sets. Each leaf belonging to a set is treated as occuring at the same time. The event lable is used to specifiy the sets. Refer to Figure 2 for the Event labeling conventions.

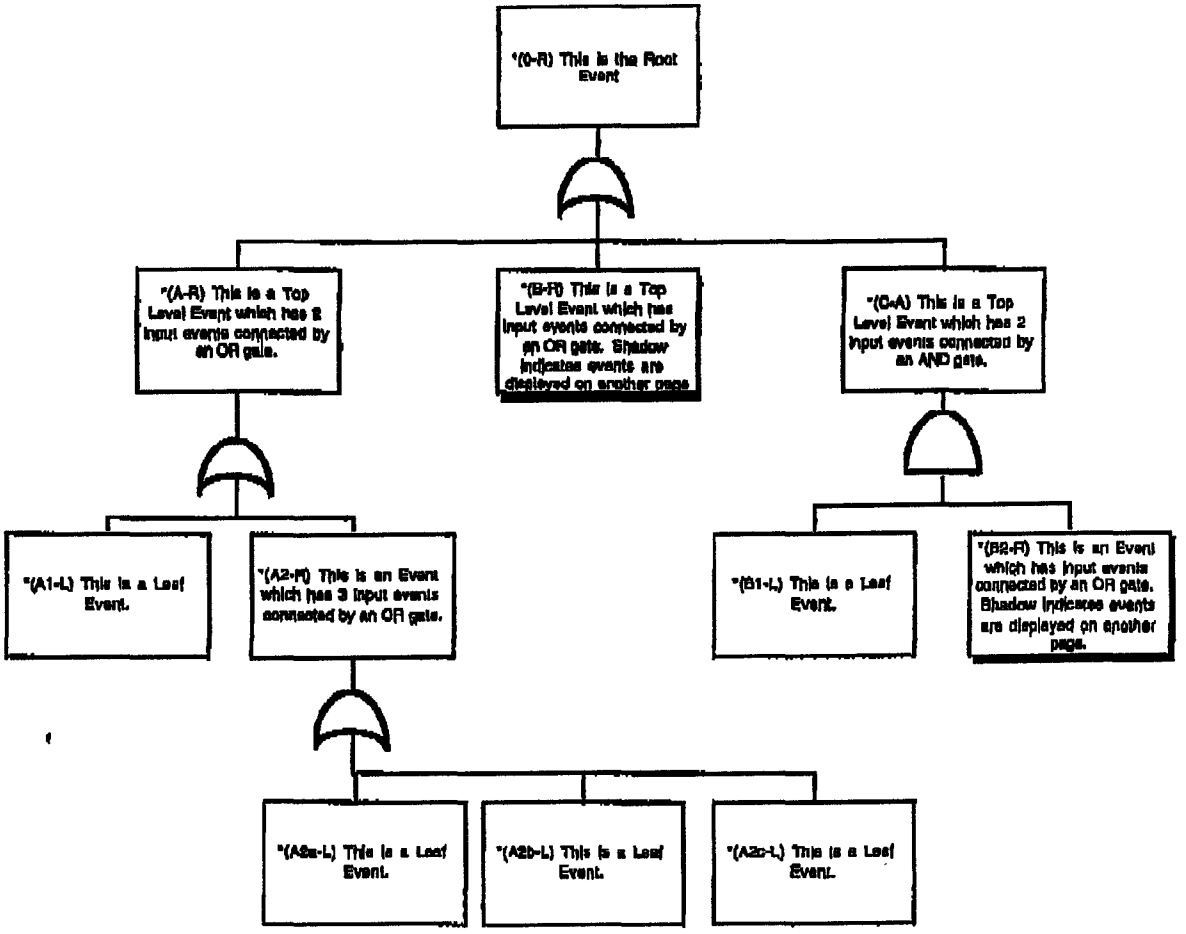

Figure 1 Sample Hazard Tree

3.2 Using MacFlow

3.2.1 Manual Limitations. This manual is not intended to provide a detailed description on how to use MacFlow. Refer to the MacFlow user documentation for this type of information. Certain features of MacFlow will be discussed in this manual as they relate to using the AEFT tool. Any features of MacFlow can and should be used to enhance the understanding of the hazard tree.

3.2.2 Link Modes. The three link modes used by MacFlow (Chart, Comment and Application) are described below.

3.2.2.1 Chart Mode. The chart mode is used to display the various pages of the hazard tree. Most of the entry and modification of the tree will be done using this mode. An event drawn with the chart symbol means that that branch of the tree indicated by the chart symbol is continued on another page. Double clicking the chart symbol displays the next page.

3.2.2.2 Comment Mode. The comment mode is used to display comments associated with the event. An event drawn with the comment symbol means that the event has associated comments.

Double clicking the comment symbol displays the comments. AEFT requires that MTTO and MD quantification data for the leaf events be contained in the event comments. See Section 3.4 for a description of this type of comment data. Optionally other brief comments about the quantification data or mitigation for the event should be entered in the event comment.

3.2.2.3 Application Mode. The application mode is used to launch documents in other applications such as Word or Excel. These documents would contain more detailed or formatted information about the mitigation of the event or other related information. Refer to MacFlow documentation for question on how to set up and use this mode. Once the application is set up for an event, double clicking the application symbol will launch the application and open the document specified. Quiting the application or document will return control back to the MacFlow document.

3.3 Event Labeling Conventions. Each event on the tree must contain a label. The Event label consists of the Event Code and the Gate Type. Refer to Figure 2 for a detailed description of the event label.

3.4 Quantification Data. Each input leaf event of the tree must contain a comment containing quantification data. Comments are entered using the Shadow Comment mode. See Section 3.2.2.2 for details on entering event comments. Only leaf input events need associated quantification data. Output events do not contain quantification data. The quantification data consists of the MTTO and MD data. Refer to Figure 3 for a detailed description of the MTTO and MD formatting standards.

4.0 Simulation

The simulation program quantitatively analyzes the hazard tree to arrive at the mean time between hazards (MTBH) figure of merit.

The input consists of a hazard tree whose leaf events are each associated with a pair of values, a mean time between occurrence of that event and a mean duration for that event. The top (root) event of the fault is the occurrence of any hazardous event for the system.

The program works by performing a discrete event simulation. Because time jumps discontinuously from the occurrence of one event to the next, many thousands or even millions of years of operation can be simulated

Each event can be in one of two logical states: TRUE (the event is happening) and FALSE (the event is not happening). When the simulation satrts, all events are in the FALSE state. From time to time during the simulation, events transition from the FALSE state to the TRUE state and back again. The transition from FALSE to TRUE is called OCCURRENCE. The transition from TRUE to FALSE is called RESTORATION. The duration of an event is the period of time that passes between OCCURRENCE and RESTORATION.

The period of time between an event's successive OCCURRENCEs is modeled by a negative exponential distribution. Likewise, the duration of time between OCCURRENCE and RESTORATION is also modeled by a negative exponential distribution.

Each leaf event's mean time to event occurrence and mean duration are each used as the value of the mean parameter of a negative exponential distribution. Random numbers are generated from the distribution to simulate successive inter-occurrence times and event durations. After every

change of any leaf event's state, every higher-level event (i.e., non-leaf event) in the hazard tree is evaluated as to whether ther higher-level event enters a TRUE state or a FALSE state. The output event of an OR gate is TRUE only when one or more of its input events is TRUE. The output event of an AND gate is TRUE only when all of its input events are simultaneously TRUE. For each higher-level event, the program keeps track of the mean time to event occurrence and mean duration.

The most important output is the mean time to occurrence of the root event after the time the simulation is concluded. This is the system's mean time between hazards (MTBH).

5.0 Starting AEFT.

5.1 Required Files. One file must be present to run AEFT, the (MacFlow) hazard tree document. Refer to Figure 4 for a diagram of the Extraction/Simulation box.

5.2 Running the Extraction. Double clicking the extraction plugin symbol on the Extraction/Simulation box reads the hazard tree and stores pertinent information about the tree in temporary files located in the directory containing the MacFlow application. These files are used as input to the simulation program.

5.2 Running the Simulation. Once the extraction has been run double clicking the simulation application symbol on the Extraction/Simulation box will run the simulation.

6.0 Results Analysis.

If an error has been detected during the analysis the error message will be written to the console display and written to a file named aeft.log. All other report will be displayed to the console screen.

Sample Event Labels:

*(A2c - L)
*(A2d1c3-L01)
*(B1a4-R)
*(C4b2-A)

Event Label Format: *(Event Code-Gate Type)

*( ) - The astorisk, open parenthesis and closed parenthesis are mandatory and required for the AEFT to process the hazard tree.

Event Code - The Event Code for the Root Event is the number zero "0". Refer to Figure 1 for an example of Root Event labeling.

The Event Code for the Top Level Hazards are upper case alphabetic starting with an "A" for the top left Top Level Hazard and proceeding with the next alphabitic letter in sequence labeling the Top Level Hazard events from left to right and top to bottom. Refer to Figure 1 for an example of Top Level Event labeling.

Each Input Event contains the Event Code of its output event plus an alpha or numeric starting with a lower case "a" if the output Event Code ends in numeric or "1" if the output Event Code ends in an alpha. The "a" or "1" is appended to the output event code and put on the input event at the top left side of the input events. The other related input events are assigned the next alpha or numeric in sequence labeling the input events from left to right and top to bottom. Refer to Figure 1 for an example of input event labeling.

Gate Type - The only three valid gate types are the upper case letters listed below. Refer to Figure 1 for an example of event Gate Type labeling.

"R" - If the input events are connected to the output event by an OR gate.

"A" - If the input events are connected to the output event by an AND gate.

"L" - If the event is a Leaf event (has no input events). Leaf sets can be created by appending up to 2 digits to the "L". Each leaf event containing the same leaf set identifier will belong to that leaf set.

Figure 2 Event Labeling Conventions

Sample Quantification Data

MTTO:(1.0e3)
MD:(ONE_FRAME)

MTTO Data	MTTO:(Number or Symbol)
MTTO	Uniquely identifies this events comment data as Mean Time To Occurrence data.
:( ) -	The colon, open parenthesis and closed parenthesis are mandatory and required for the AEFT to process the hazard tree.
Number or Symbol	In its simplest form this is a number in hours which represents how often this event or condition will occur. If desired the number can be represented by a symbol which is assigned a number in the AEFT Simulation document. Symbols are case sensitive.

MD Data	MD:(Number or Symbol)
MD	Uniquely identifies this events comment data as Mean Duration data.
:( ) -	The colon, open parenthesis and closed parenthesis are mandatory and required for the AEFT to process the hazard tree.
Number or Symbol	In its simplest form this is a number in hours which represents how often this event or condition will occur. If desired the number can be represented by a symbol which is assigned a number in the AEFT Simulation document. Symbols are case sensitive.

Figure 3 MTTO and MD Conventions

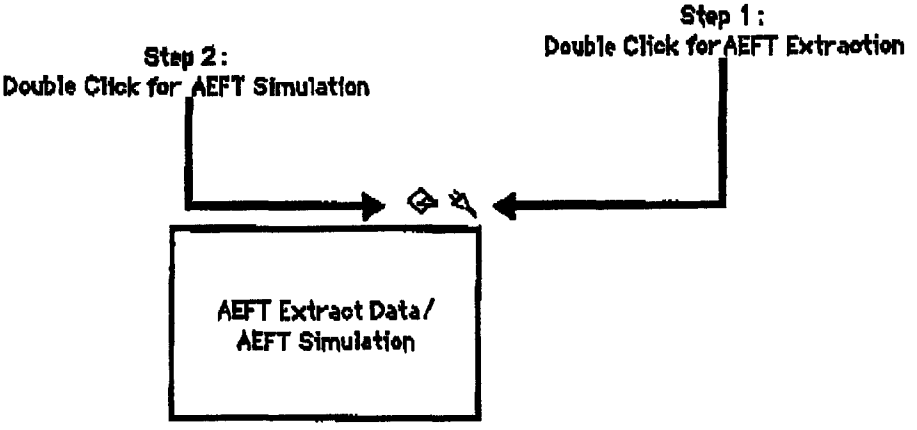

Figure 4 AEFT Extraction/Simulation