
User's Manual for

CARA-FaultTree v4.1

by Sydvest Software

This manual was produced using *Doc-To-Help*[®], by WexTech Systems, Inc.

Contents

1. Introduction	1
1.1 About CARA-FaultTree	1
1.2 About the Manual	1
1.3 Getting more Information	2
1.4 Installing and Uninstalling	2
1.4.1 System Requirements	2
1.4.2 Starting Setup	3
1.4.3 Installing CARA-FaultTree to run from a Network	3
1.4.4 Uninstalling CARA-FaultTree	3
1.5 Capacities of a CARA-FaultTree Document	4
2. Getting Started	5
2.1 The CARA-FaultTree Window	5
2.1.1 Program Window Layout	5
2.1.2 Standard versus Expert User Level	6
2.1.3 Open a New Fault Tree	6
2.1.4 Open Existing Fault Tree	6
2.1.5 Save Fault Tree	7
2.1.6 The Toolbar	7
2.2 Drawing your First Fault Tree – A Quick Tour	8
2.3 Fault Tree Construction	11
2.3.1 Drawing a Fault Tree	11
2.3.2 Fault Tree Symbols	14
2.3.3 The Fault Tree Page	22
2.4 The Fault Tree Overview	26
2.5 Running an Analysis	27
2.5.1 Starting an analysis	27
2.5.2 The Analysis Report	28
2.5.3 Verification and Consistency Check	28
2.6 Importing Graphics to other Windows-programs	31
3. CARA-FaultTree Menus	33
3.1 General	33
3.2 File menu	33
3.2.1 Command Summary	34
3.2.2 Importing and Exporting Failure Data	36
3.2.3 Printing Fault Trees and Reports	39

3.3 Edit menu	41
3.4 Symbols menu	43
3.4.1 Command Summary	44
3.4.2 Edit Event Classes...	45
3.4.3 Edit events...	46
3.5 Tree menu.....	46
3.6 Analysis menu	51
3.6.1 General	51
3.6.2 Standard User Mode	51
3.6.3 Expert User Mode	59
3.7 View menu	72
3.8 Window menu.....	74
3.9 Help menu.....	75
4. Method Description	77
4.1 Introduction to the Fault Tree Method.....	77
4.1.1 History.....	77
4.1.2 The Fault Tree Technique	77
4.2 Fault Tree Construction.....	78
4.2.1 Fault Tree Diagram, Symbols and Logic.....	78
4.2.2 Definition of the Problem and the Boundary Conditions.....	80
4.2.3 Construction of the Fault Tree	81
4.2.4 Using the House event.....	82
4.3 Identification of Minimal Cut and Path Sets	83
4.3.1 Definition of Cut- and Path Sets	83
4.3.2 MOCUS - method for obtaining cut sets	84
4.4 Qualitative Evaluation of the Fault Tree.....	86
4.4.1 Conditions for Qualitative Evaluation of the Fault Tree.....	86
4.4.2 Criticality Ranking of Minimal Cut Sets	87
4.5 Quantitative Analysis of the Fault Tree	87
4.5.1 Available System Reliability Measures in CARA- FaultTree.....	87
4.5.2 The probability that the TOP event occurs at time t - $Q_0(t)$	88
4.5.3 The probability that the TOP event does not occur in $[0,t)$ - $R_0(t)$	89
4.5.4 Mean time to first system failure - MTTF.....	89
4.5.5 $E(\# \text{ failures})/Freq(\text{TOP})/Freq \text{ distr}$	90
4.5.6 Average system availability in $[0,t)$ - $A_{0,av}(t)$	91
4.5.7 Quantitative ranking of minimal cut sets.....	91
4.5.8 Notation for Describing Reliability Measures.....	91
4.6 Input Data to the Fault Tree	92
4.6.1 Category of Failure Data for Input Events.....	92
4.6.2 Frequency	93

4.6.3 On Demand Probability.....	93
4.6.4 Test interval	93
4.6.5 Repairable Unit	94
4.6.6 Non repairable unit	94
4.7 TOP Event Calculations	95
4.7.1 Methods for Calculating the Reliability Measures	95
4.7.2 Calculation of $Q_0(t)$ Using Exact Calculation (ERAC) and Upper Bound Approximation.....	96
4.7.3 Calculation of $R_0(t)$, MTTF and $Freq(TOP)$ Using Monte Carlo (Stochastic) Simulation.....	98
4.7.4 Calculation of $R_0(t)$, MTTF and $E(\#failures)$ Using Numerical Integration	99
4.7.5 Calculation of $Freq(TOP)$ Using the Hand Calculation Method	101
4.8 Modular Decomposition.....	102
4.8.1 Modular Decomposition of the Fault Tree	102
4.8.2 The Modularization Technique	103
4.8.3 Guidance on selecting Modularization Level.....	104
4.8.4 Advantages using Modularization	104
4.9 Measures of Importance	105
4.9.1 Available Measures of Importance.....	105
4.9.2 Vesely-Fussell's Measure of Reliability Importance ..	105
4.9.3 Birnbaum's Measure of Reliability Importance.....	106
4.9.4 Improvement potential	107
4.9.5 Criticality Importance.....	107
4.9.6 Order of smallest cut set	107
4.9.7 Birnbaum's Measure of Structural Importance.....	108
4.9.8 Cut set importance	108
4.10 Uncertainty Analysis	109
4.10.1 Required input for the Uncertainty Analysis.....	109
4.10.2 Uncertainty Analysis – Simulations	109
4.10.3 Uncertainty Analysis - Example	110
5. References	113
5.1 List of References	113
6. Glossary of Terms	115
7. Index	121

1. Introduction

1.1 About CARA-FaultTree

CARA-FaultTree is a program for fault tree construction and analysis.

Fault Tree Construction involves building the fault tree consisting of logical gates and input events, and entering data (identifiers, descriptive text as well as reliability data).

After construction of the fault tree you may run different analyses, e.g. calculations of mean time to failure (MTTF), unavailability, survival probability, measures of reliability importance and uncertainty analysis. For further information about the Fault Tree methodology, please refer to the "Method Description" on page 77.

"Drawing your First Fault Tree – A Quick Tour" on page 8 helps you draw your first fault tree, enter some input data and run an analysis.


1.2 About the Manual

Help on fault tree construction

The first part of the user's manual will show you how to create a fault tree, manipulate symbols, analyse the fault tree and print reports. Refer to "Drawing your First Fault Tree" on page 8 for a short introduction on how to draw your first fault tree, enter some input data and run an analysis. For a more thorough description, refer to "Fault Tree Construction" on page 11. Further, the "CARA-FaultTree Menus" section on page 33 gives a complete reference to all the menu options in the program.

Limitations to a fault tree

Refer to "Capacities of a CARA-FaultTree Document" on page 4 for information about the different limitations that apply to a fault tree in CARA-FaultTree.

<i>Method description</i>	Refer to the "Method Description" on page 77 for an introduction to the fault tree methodology and the various advanced options included in the analysis.
<i>Figure appearance</i>	All figures described are taken from Windows NT 4.0. With Windows 9x or Windows 2000 the appearance will differ slightly.
<i>Typing conventions</i>	The typing conventions for this guide are bold text for menus. The main menu name is put first and the menu in the drop-down list, the menu command, is last, separated by a “ ”. E.g. to create a new fault tree you must first click on the File menu and then select the New command. This command is also described as the File New command.
<i>Shortcuts</i>	Shortcuts for menu commands are available through keyboard combinations, the toolbar and the symbols palette. These shortcuts are put in the left margin of the text describing the menu command or operation. E.g.:
 <i>or Ctrl+N</i>	The File New command has two shortcuts.

1.3 Getting more Information

This user's manual, including information on Installing and Uninstalling as well as the Method Description, is always the first place to look for help. The User's Manual is also available within CARA-FaultTree through the help menu and "Help"-buttons.

If you still need help, then contact your distributor or visit our Web-site:

www.sydvest.com

1.4 Installing and Uninstalling

1.4.1 System Requirements

- Windows 9x/NT or Windows 2000
- 486DX66 minimum, Pentium recommended
- 12 Mb RAM minimum
- 10 Mb free disk space
- Available on CD or disks

1.4.2 Starting Setup

CARA-FaultTree may be delivered both on disks as well as a CD. Follow the steps below, and use disks or CD depending on the medium relevant for you.

Before you begin the installation, it is recommended to close all programs running on your computer.

1. Place the CARA-FaultTree installation CD or installation disk 1 in your PC's CD-ROM drive or disk station.
 - If you install from a CD, and your CD-ROM has AutoPlay enabled, the CARA-FaultTree Setup will start automatically. In this case, skip to step 4.
 - If Setup does not start automatically, continue with step 2.
2. Open the **Run** dialog box by opening the **Start** menu and choose **Run**.
3. Start the CARA-FaultTree Setup program by typing **d:\setup** (where **d:** is the drive containing the CARA-FaultTree CD or installation disk) and press **Enter**.
4. The CARA-FaultTree Setup screen appears. Follow the instructions on your screen.

1.4.3 Installing CARA-FaultTree to run from a Network

Although CARA-FaultTree can be run from a network, the installation procedure is not optimised for network installation. During the installation, some changes are made to the Windows setup, and hence *the installation program must be run on every PC that will be used to run CARA-FaultTree*. The program may be installed to the same network directory each time.

1.4.4 Uninstalling CARA-FaultTree

You can use the uninstall feature of CARA-FaultTree to remove CARA-FaultTree from your system.

1. Click the **Start** button, select **Settings**, and click **Control Panel**. The Control Panel opens.

2. Open the Add/Remove Programs control. The Add/Remove Program Properties dialog box appears.
3. In the list of programs that can be removed, select CARA-FaultTree, then click the **Add/Remove** button.
4. Click **Yes** to confirm that you want to remove CARA-FaultTree

1.5 Capacities of a CARA-FaultTree Document

The following capacities apply to a fault tree in CARA-FaultTree:

- Up to *50 symbols* on each page (i.e. AND/OR-gates, Input events, Comment rectangles and Transfer symbols).
- Up to *12 inputs* to each gate.
- Up to *200 fault tree pages*.
- Up to *1 000 unique Input events* totally.
- Up to *1 000 unique gates* totally.
- Up to *800 Transfer symbols* (i.e. you may include references to max. 800 fault tree pages totally within one fault tree file). Note that if one fault tree page is referred several times, this will count as several references.
- Up to *5 500 cut sets*.
- Up to *32 000 Input events* totally in all cut sets. Note that if one Input event is found in several cut sets, this Input event will count several times.

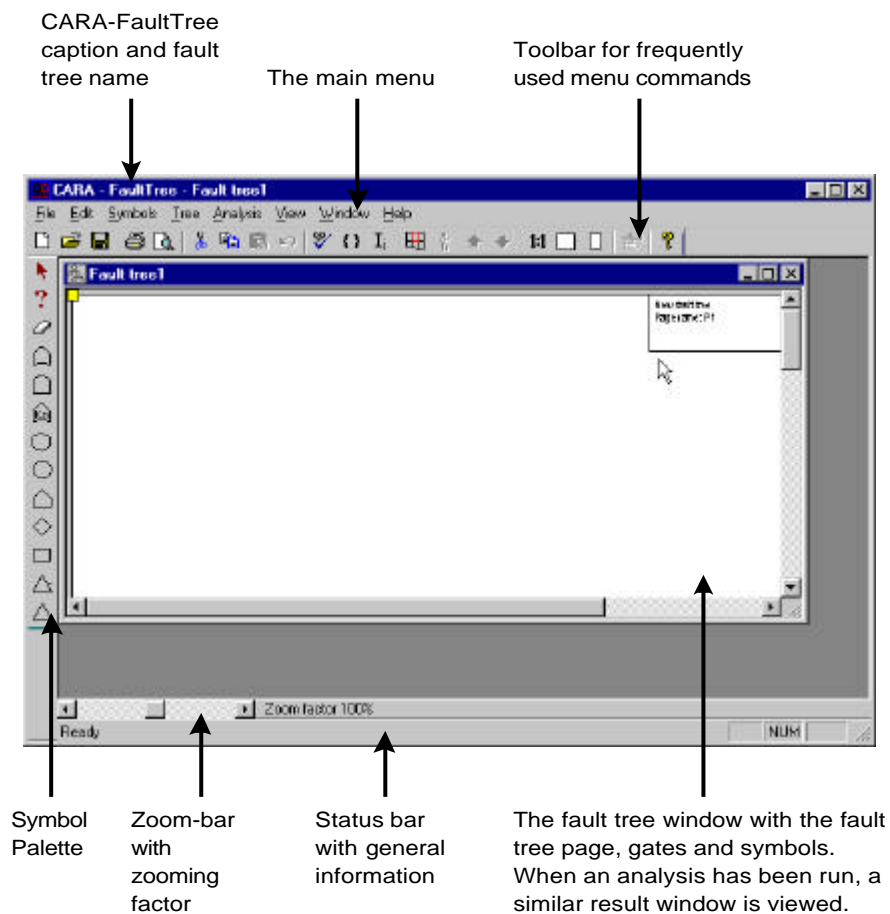
Note! During identification of the minimal cut sets, the structure of the fault tree is copied into internal arrays of the program. A very complex fault tree may then cause the size of the arrays to be insufficient (even if the fault tree as such is within the above limitations). If so happens, the message "*Memory overflow, cannot proceed*" will be displayed, and the calculation terminates.

2. Getting Started

2.1 The CARA-FaultTree Window

2.1.1 Program Window Layout

The CARA-FaultTree window has a menu, a toolbar for menu shortcuts, a symbol palette and an area for fault trees and reports, see figure and description below:



Status line A status line is displayed at the bottom of the main window. When the mouse cursor moves over a menu item or a toolbar icon, short descriptions are given on this status line.

Zoom bar A zoom-bar is found above the status line, and the current page zoom value is displayed in percent. By dragging the knob to the left or to the right on the bar, the active fault tree is zoomed in or out.

Move toolbar or symbol palette The toolbar and the symbol palette can be dragged from their default location and placed anywhere in the CARA-FaultTree window. Press down the left mouse button on one of the toolbars (not on a button) and drag the toolbar to a new position. If the toolbar is dragged to another side of the CARA-FaultTree window it will be automatically integrated with the closest window side. If the toolbar is not dragged over a window edge the toolbar will become a window of its own; a floating toolbar.

2.1.2 Standard versus Expert User Level

CARA-FaultTree has an option to simplify the selections and choices you must make when performing an analysis. See File | User level on page 36 for more information.

2.1.3 Open a New Fault Tree

Upon start of the program, a new fault tree file is opened.

Create a new fault tree



To create another new fault tree, use the **File | New** command. This command opens a new fault tree in a new window.

When you save a newly created fault tree, a default file name "Fault.cft" is suggested. You may accept this name or enter a different one as desired.

2.1.4 Open Existing Fault Tree



Import from DOS-version

Open an existing fault tree with the **File | Open...** command.

You may import a fault tree created with the former DOS-version, CARA-CAFTAN (version 3.0 or newer). See "File | CAFTAN Import..." on page 35 for more information.

2.1.5 Save Fault Tree



To save a fault tree use the **File | Save** command. If the fault tree is just created, you will be asked for a name and where you want to save the file.

If you have several fault trees (several windows) open you can save them all at once by the menu command **File | Save All**.

Save a fault tree using the **File | Save As...** if you want to save the fault tree to a file with a different file name.

2.1.6 The Toolbar

The horizontal toolbar below the menu line is a short cut to frequently used menu commands in CARA-FaultTree.




Drag the mouse cursor over any of the buttons to see its functionality in the status line (at the bottom of CARA-FaultTree window).

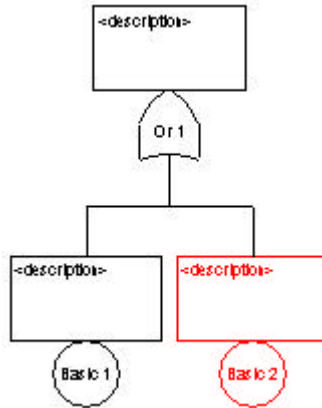
Button	Menu command	Button	Menu command
	File New		Tree Overview
	File Open...		Edit Goto Page...
	File Save		Edit Goto Previous
	File Print		Edit Goto Next
	Print preview		View 1:1
	Edit Cut		View Full width
	Edit Copy		View Fit to view
	Edit Paste		Symbols Symbol Data...
	Edit Undo		Help About CARA-FaultTree...
	Tree Verify		
	Analysis List cut sets...		
	Analysis Component Importance...		

2.2 Drawing your First Fault Tree – A Quick Tour

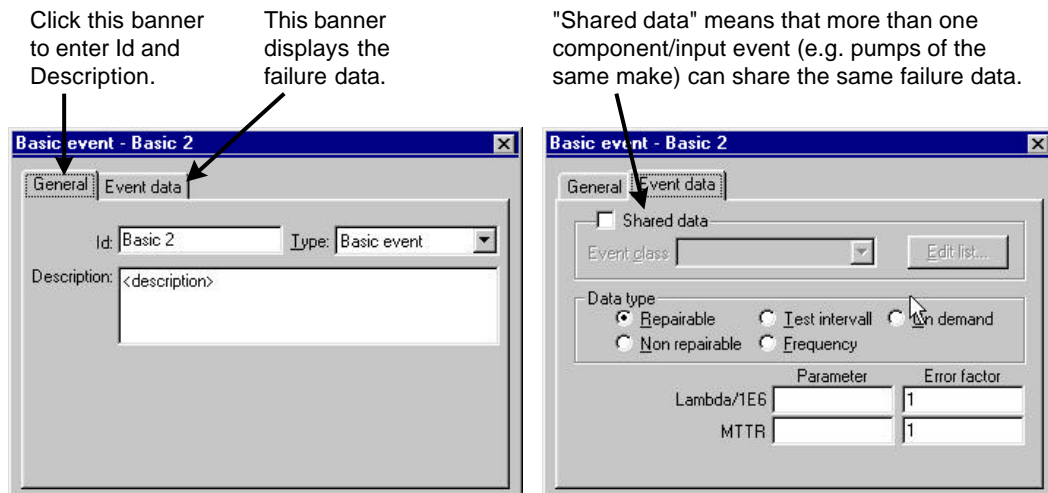
A quick tour through drawing a new fault tree, enter input data and run a simple analysis is given below. For a more thorough description, refer to "Fault Tree Construction" on page 11.

1. Create a new fault tree using the **File | New** command (or simply start with the new fault tree opened when the program is started).
2. Add an OR-gate as TOP event in your new fault tree as follows: Click the mouse on the OR-gate button in the Fault Tree Symbol Palette (see "Fault Tree Symbols" on page 14 for details). The mouse pointer is now "loaded", this is indicated by an OR-gate shown at the side of the cursor. Drop the OR-gate on the fault tree page by clicking on the position where you want the gate to be drawn (preferably near the top of the fault tree page).
3. Add two Basic events below the OR-gate you have inserted as follows: Load the cursor with a Basic event symbol by clicking the Basic event-button in the Fault Tree Symbol Palette. Try moving the cursor around the fault tree page. Observe that as long as you are pointing outside the OR-gate, the cursor will be accompanied by a stop sign , and you are not able to add the Basic event. If you move the cursor over the OR-gate, however, the cursor again shows the Basic event symbol. Drop the Basic event on the OR-gate by simultaneously pressing the **Shift** key and clicking on the OR-gate. The Basic event is automatically connected to the gate, and given the default name "Basic 1". The reason for pressing down the **Shift** key is that the cursor then remains loaded with the Basic event symbol. Click on the OR-gate once more, but this time do not hold the **Shift** key. A new Basic event (named "Basic 2") is inserted below the OR-gate. Since you did not hold down the **Shift** key this time, the cursor is reset and loaded with the pointer.

- The fault tree should now look like this:








- To edit the input data, double-click on the Basic event “Basic 1”. A property dialog is opened, where you may enter an event ID (set by default to “Basic 1”, “Basic 2”, etc.), a description, as well as Failure data, see below:



- Enter an appropriate set of failure data into the Event data tab of the dialog.
- While leaving the property dialog open, click on the Basic event named “Basic 2”. The property dialog is updated to display information about the new active component “Basic 2”. Enter some failure data for this component as well. If you removed the property dialog by accident, just double-click on “Basic 2” to create it again.
- The fault tree page and the OR-gate both have “properties” as well. By double-clicking on a blank part of the page, you are allowed to enter a page id and a description as well as determining the page layout. In the description field you may add text as you like, or enter one of the supported codes, e.g.

^Date to print the current date or ^Page to print the name of the page

9. By clicking the right mouse button on a gate or an event, a quick menu is available. This menu change depending on the type of component selected. E.g. if you add a Transfer down-symbol to your tree you can, by right-clicking this transfer symbol, create a new page to which the transfer symbol is connected. Further, you can connect it to an already existing page, or (if the transfer symbol is already linked to a page) move to the connected page.
10. Select the Look-at tool  from the Symbol Palette, and move the cursor over one of the components. All the failure data is displayed in a yellow sticker on the screen. This utility, which is also available in tree overview, makes it quick to view and verify the data input.
11. Run an analysis, e.g. by selecting **Analysis | Failure frequency distribution...** You will be prompted to enter some settings to run the analysis, then press **OK** to perform the calculations. A result window is displayed. This report may be saved in RTF-format (readable for all standard word processors running under Windows). You can also mark text or graphics in the result window, copy the text to the clipboard (e.g. using the standard Windows **Ctrl+C** key) and paste it into your word processor (e.g. using the standard Windows **Ctrl+V** key).
12. To run a new analysis, you must first make the fault tree the active window, e.g. by selecting **Fault tree 1** in the **Window** menu. Then all analyses options are again available.
13. Now, select the **Tree | Overview** command or press the Overview button  in the toolbar. In the Overview window all pages of your fault tree are displayed tied together (here, having only one fault tree page, only this single page is shown). If you select the Look-at tool  from the Symbol Palette, and place the cursor over a fault tree page, the structure of that page is displayed.
14. Use the zoom scrollbar on the bottom of the window to increase the zoom factor. Zoom up to

15%. Now, the structure of the fault tree is displayed within the overview window, and the Look-at tool  will display properties for all gates and events. If you want to, you can even edit the fault tree in this view (add or remove components, utilise drag and drop etc.). Go to a different page by selecting **Edit | Goto Page** () in the toolbar, or **Ctrl+G**) and select the desired page from the displayed list.

2.3 Fault Tree Construction

2.3.1 Drawing a Fault Tree

Drawing a fault tree always starts with the identification of a critical TOP event. Thereafter you must carefully try to identify all failure events that are immediate, necessary and sufficient to cause the TOP event to occur. These failure events are connected to the TOP event by means of a logic gate. You then proceed like this, level by level, until all failure events are developed to the required level of detail. The analysis is deductive and is carried out by repeatedly asking, "What may cause this event to occur?"

CARA-FaultTree is a program for top-down construction of fault trees. The TOP event should thus be placed on top of the first fault tree page with the rest of the symbols, level by level, towards the bottom of the page. If a fault tree is too large to fit on one page, the Transfer symbol is used to establish a link to another page, refer to "Transfer symbols" on page 20.

More information on the fault tree construction methodology is found in "Fault Tree Construction" section in the Method Description (page 78).

Connecting and Moving Symbols

*Start with the TOP event
of the tree*

When a new fault tree is created, you choose a TOP event from the symbol palette and drop it on the fault tree page where you want the top of the fault tree to start. Note that a TOP event must be a Gate event.

You may move the tree simply by dragging the TOP event symbol to the desired position.

Add events

Add the next event (Gate or Input event) below the TOP event simply by dropping it onto the TOP event. The new event is then connected and placed below the existing symbol.

Hold down Shift to enter several instances of the same symbol

If you want to put several instances of the same symbol type in one operation, hold down the Shift-key when you drop the symbol.

Tree building rules

You cannot drop symbols anywhere on the fault tree page. Apart from the first symbol on the page, all symbols must be connected to existing symbols. As long as the mouse cursor is in a place where you cannot drop the symbol, a stop-sign (⊘) is displayed at the cursor. Some symbols must also be dropped on specific symbol types, e.g. no symbols on an input event.

Symbols in the fault tree can be selected for editing, deleting or moving. A selected symbol is marked with red, and becomes the active or current symbol. If a gate at the top of a sub-tree is selected, the whole sub-tree is selected. The selected branch of symbols turns into grey while the active symbol turns into red.

Delete tool



To delete a symbol or a sub-tree select the symbol and select the **Edit | Cut** or **Edit | Delete** commands. The first command deletes the symbol but also places a copy of it on the clipboard. You can also first select the Delete-tool from the Symbol Palette and click on the symbol/sub-tree you want to delete.

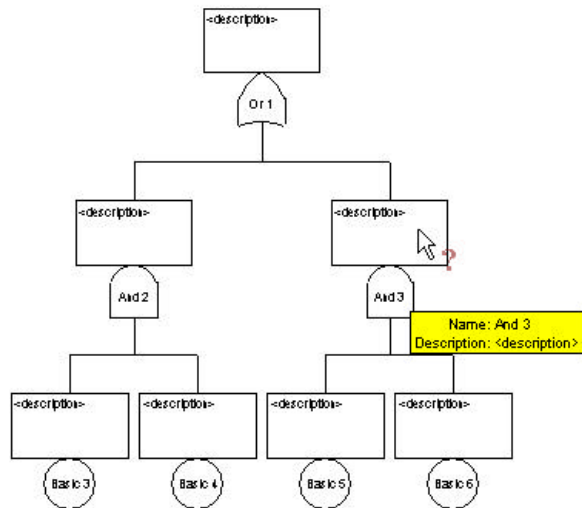
Move symbol or sub-tree

If you want to move a symbol or sub-tree, simply drag the symbol to where you want it moved (i.e. onto the symbol you want it connected to).

Look-at tool



To have a quick look at the information in a symbol first select the Look-at tool from the Symbol Palette. Then, move the cursor over symbols in the fault tree. A yellow note will be viewed displaying the symbol information:



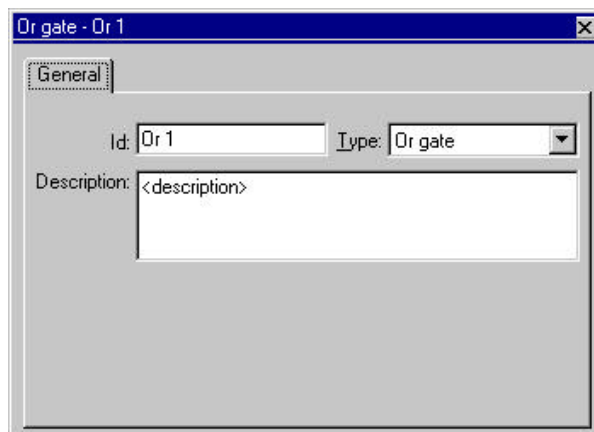
Symbol properties

Each Gate and Input event in the fault tree has an identifier and a description, as well as an indication of type of Gate/Input event. Input events have in addition various input data, depending on the type of Input event. All this information is referred to as the properties of the symbol, or the symbol data. Note that new symbols are given default identifiers and description that should be replaced by the user.

Properties/Symbol Data



To edit the symbol properties select **Symbols | Symbol Data...** command, double-click on the symbol, or right-click on the symbol and select **Properties...** from the command menu.



The example above shows the properties of an OR-gate. The identifier is “Or 1”, gate type is OR-gate, and the description is “<description>”.

The property dialog will remain open also when clicking on other symbols in the tree, or even the background of the fault tree page, as this also has properties. The contents of the

property dialog will change to show the properties of the current symbol or item.

*Symbol identifiers,
The Id property*

All Gate and Input event symbols have unique identifiers (or names) in order to be able to refer to the symbol.

When a symbol is inserted in the fault tree, a default identifier is given to the symbol. The identifier given is prefixed with a text depending on the symbol type (e.g. "Or") and suffixed with a serial number. In CARA-FaultTree the Gate and Input event identifiers may contain up to 16 characters. However, depending on the parameter given in the **General** tab in **Tree I Setup**, only a specified part of the identifier is displayed in reports and print-outs. By default, all the characters of the identifier are displayed (see the "**General tab**" on page 47 for details).

If two or more Gates have the same Id, the underlying subtree must be identical. This is checked by the fault tree verification function.

If two or more Input events have the same identifier, they are treated as the same Input event, and shares the same input data.

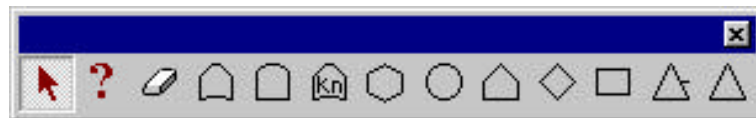
The Description property

Description is a descriptive text which may be entered (not mandatory) in order to give a supplementing description. The length is up to 255 characters, however depending on the font size and symbol size, how much of the description is visible may vary (see "The Fault Tree Page" on page 22 for more information on the page layout).

The symbol-specific properties are described for each symbol in the Fault Tree Symbols section below.

2.3.2 Fault Tree Symbols

In the **Symbols** menu, as well as in the Symbol Palette (see below), all symbols you need to build a complete fault tree are given:



The Symbol Palette is initially given at the left side of the CARA-FaultTree main window, but it can be moved and placed anywhere in the main window.

The **Symbols** menu contains the same set of symbols as in the Symbol Palette, except for the first three command buttons in the Palette.

General Tools in the Symbol Palette



The tool is for selecting symbols and branches of symbols. If you have selected a symbol to be placed in the fault tree this can be cancelled by selecting this arrow.



The question-mark tool is for easily browsing the properties of the symbols. Select the question-mark tool and move the cursor over the fault tree symbols to view the symbol properties.



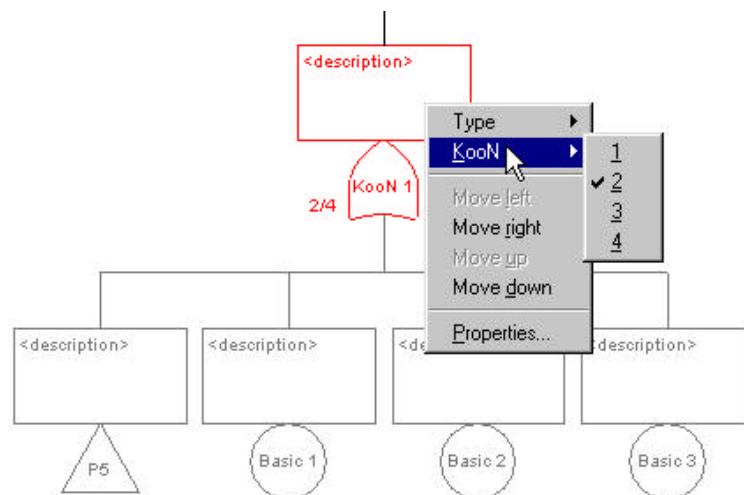
The rubber-tool deletes the symbol or sub-tree that you select.

Gate and Input events

In the sections below, the various Gate and Input event symbols are explained. Here, the term Input event is used as a common term for Basic events, House events, and Undeveloped events.

Right-clicking on a symbol

Right-clicking on a symbol on the fault tree page gives you access to several useful commands. The commands offered vary depending on which symbol is selected, as well as on what location it has in the tree. An example for the KooN-gate is given in the figure below.



Move left / right / up / down

Note that the **Move left/right/up/down** commands are only available when right-clicking on a symbol. Use **Move left/right** to shift the symbol to left or right compared to the other in-going symbols at the same level. If you **Move down** a symbol, it is graphically shifted one level downward (keeping its out-going connection). **Move up** will move the symbol up one level.

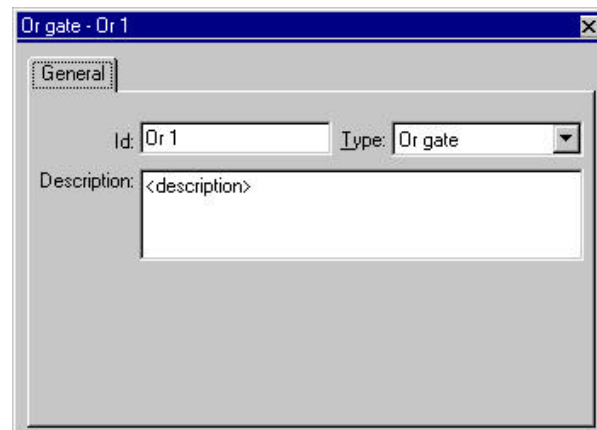
OR-gate

An OR-gate is used to indicate that the event will occur if any of the in-going events occur.

An OR-gate accepts one out-going connection (top of symbol) and up to twelve in-going connections.

Select the OR-gate with the **Symbols | OR-gate** command or the corresponding Symbol palette button.

The properties for the OR-gate is identifier, description and type (see figure below). The type is a dropdown-list for selecting if the event is an OR-gate, AND-gate, Inhibit-gate or KooN-gate.



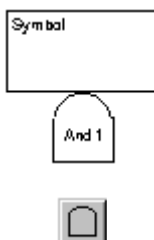
AND-gate

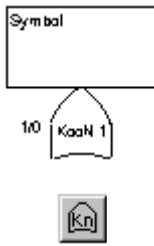
An AND-gate is used to indicate that the event will occur if all the in-going events occur simultaneously.

An AND-gate accepts one out-going connection (top of symbol) and up to twelve in-going connections.

Select the AND-gate with the **Symbols | AND-gate** command or the corresponding Symbol palette button.

As for the OR-gate (see figure above), the properties for the AND-gate are identifier, description and type. The type is a dropdown-list for selecting if the event is an OR-gate, AND-gate, Inhibit-gate or KooN-gate.





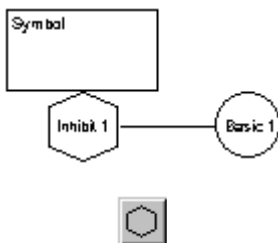
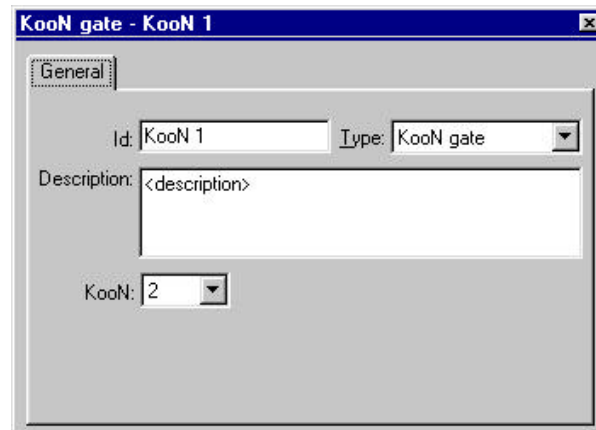
KooN-gate

The KooN-gate is used to indicate that the event will occur if *any* K of the N in-going events occurs.

A KooN-gate accepts one out-going connection (top of symbol) and up to twenty in-going connections.

Select the KooN-gate with the **Symbols | KooN-gate** command or the corresponding Symbol palette button.

The properties for the KooN-gate (see figure below) are similar to the other gates, however in addition to identifier, description and type comes the specification of the k -value. The type is a dropdown-list for selecting if the event is an OR-gate, AND-gate, Inhibit-gate or KooN-gate.



Inhibit-gate

The Inhibit-gate is used to indicate that the event occurs if both the conditional event and the in-going event occur.

An Inhibit-gate accepts one out-going connection (top of symbol) and one in-going event.

Select the Inhibit-gate with the **Symbols | Inhibit-gate** command or the corresponding Symbol palette button.

The properties for the Inhibit gate itself are identifier and description. In addition comes the properties of the conditional event, which are identical to those for a Basic event, see below.

Basic event

The Basic event represents a basic equipment fault or failure that requires no further development into more detailed Basic events or failures.

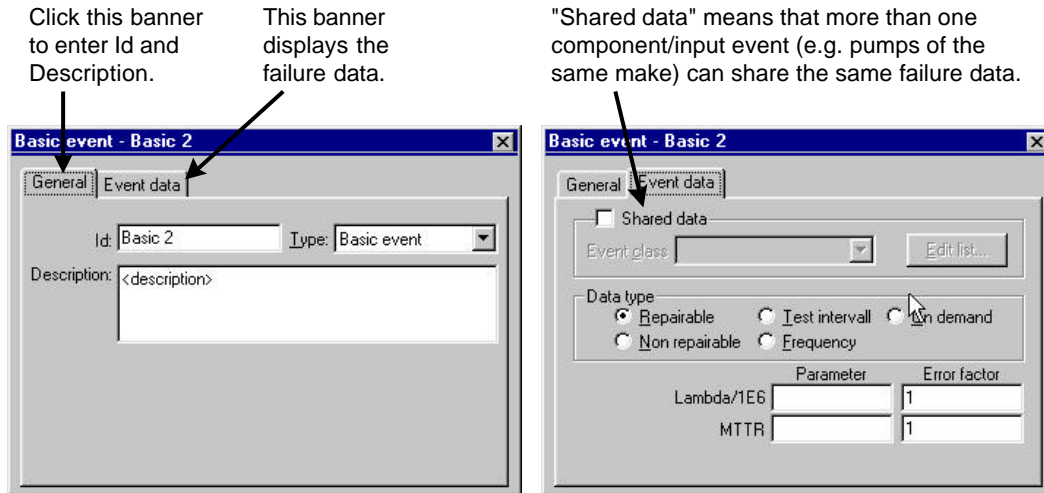
A Basic event accepts one out-going connection (top of symbol) and has no in-going connections.





Select the Basic event with the **Symbols | Basic event** command or the corresponding Symbol palette button.

The properties for the Basic event have two tabs, **General** and **Event data** (see figure below)



As for the Gate events, the **General** tab includes identifier, description and type. The type is a dropdown-list for selecting if the Input event is a Basic or Undeveloped event.

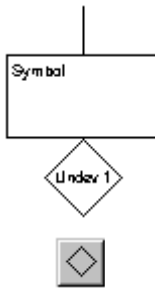
Note that if you enter an already existing identifier, the failure data and descriptive text that has been assigned to that identifier, will be displayed. If you edit the data of a repeated identifier, the changes will be made to all the events with the same identifier.

The **Event data** tab (see figure above) includes the type of input event and the failure data, in addition to the shared data option.

If you want this Input event to refer to an Event class defined as shared data, select Shared data and choose the desired Event class from the drop-down list. Please refer to "Edit Event Classes..." on page 45 for more information.

If you want to use individual data for the input event, you choose between the five different input data types, and enter the required reliability parameters. Please refer to "Input Data to the Fault Tree" on page 92 for more information on data types and reliability parameters.

Undeveloped event



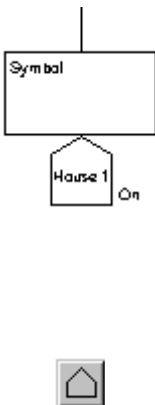
The Undeveloped event represents a fault or failure that is not examined any further because information is unavailable or because it is insignificant to the result of the analysis.

An Undeveloped event accepts one out-going connection (top of symbol) and has no in-going connections.

Select the Undeveloped event with the **Symbols | Undeveloped event** command or the corresponding Symbol palette button.

As for the Basic event, the properties for the Undeveloped event have two tabs, **General** and **Event data**, and the properties are identical to those for the Basic event. Thus, please refer to Basic event above for more information.

House event

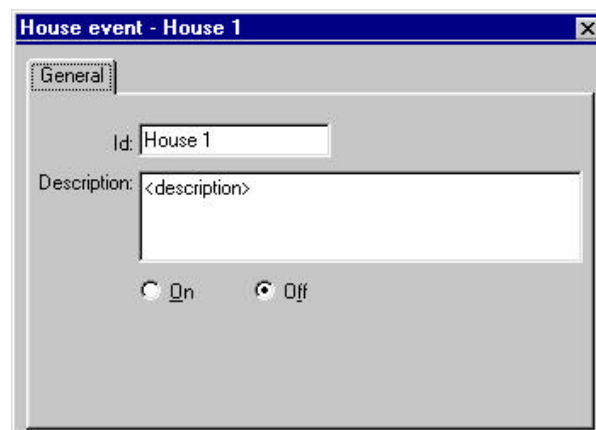


The House event represents a condition or an event that is either True or False. The House event may be used to include or exclude the part of the fault tree that is connected to the event. Please refer to "Using the House event" on page 82 for more information on how you apply the House event in your fault tree.

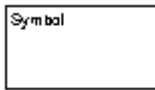
A House event accepts one out-going connection (top of symbol) and has no in-going connections.

Select the House event with the **Symbols | House event** command or the corresponding Symbol palette button.

The properties for the House event (see figure below) include identifier and description, in addition to radio buttons where you select if the House event is On (i.e. True) or Off (i.e. False).



Comment rectangle



The Comment rectangle provides a possibility for entering supplementary information. It will accept one out-going and one in-going connection.

A Comment rectangle accepts one out-going connection (top of symbol) and one in-going event.



Select the Comment rectangle event with the **Symbols | Comment rectangle** command or the corresponding Symbol palette button.

The properties for the Comment rectangle include only the descriptive text.

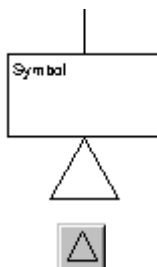
Transfer symbols

Transfer symbols are used to indicate that the fault tree is developed further at another fault tree page. The page referring the further development contains a Transfer down symbol at the bottom of a sub-tree on that page, whereas the page where the fault tree is further developed starts with a Transfer up symbol on the top of the page. The identifier of the Transfer down symbol must then be identical to the name of the page referred to.

The reason for splitting up the fault tree on several pages may be that there is not enough space on one page for the whole fault tree (which is almost always the case), or that you want to separate a part of the fault tree containing a subsystem or similar.

Note that the referenced page might be referenced from several places in the fault tree. This will e.g. be relevant if the page contains a subsystem used by several parts of the system.

Transfer down



Add a Transfer down symbol if you want to develop the fault tree further at another page.

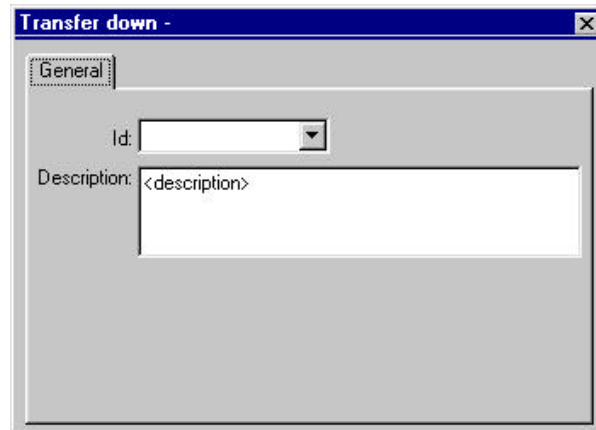
Select a Transfer down symbol with the **Symbols | Transfer down** or the corresponding Symbol palette button.

The properties for the Transfer down symbol (see figure below) are identifier and description. Note that the identifier for the Transfer symbols is different from the other symbol

types. The reason for this is that the Transfer symbols refer to names of fault tree pages. Thus, the identifier for the Transfer down symbol is selected from a drop-down list of the available pages in the fault tree.

*Transfer symbol Id
up to four characters long*

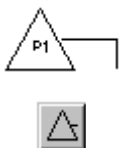
Note that the length of the Transfer symbol identifiers differs from the other symbol types. A fault tree page identifier in CARA-FaultTree, and thus also the Transfer symbol identifier, may be up to four characters long.



Insert new page

To continue constructing the fault tree on a new page, you need to insert a new page with **Edit | New page**. You may also simply right-click on the Transfer down symbol and select **New page**. This will create a new page, link the Transfer down symbol to this page, and move to the new page.

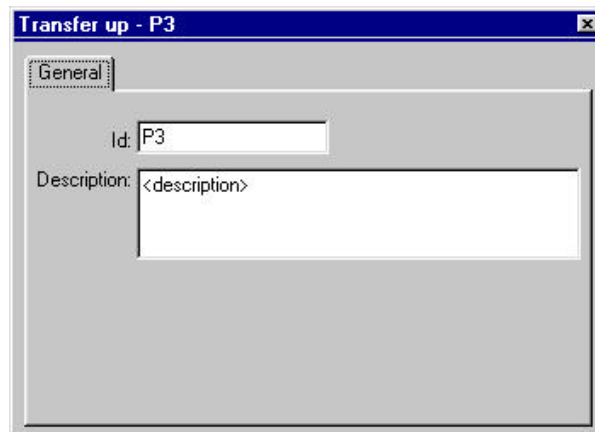
Transfer up



After having inserted a blank page, you add the Transfer up symbol on the new fault tree page.

Select a Transfer up symbol with the **Symbols | Transfer up** or the corresponding Symbol palette button.

The properties for the Transfer up symbol (see figure below) are identifier and description. The property dialog looks identical to the property dialog for the Transfer down symbol, however there is a difference for the identifier. Whereas the identifier for the Transfer down symbol was selected from a drop-down list of the available pages in the fault tree, the identifier of the Transfer up symbol is identical to the Page identifier (Page name) for the fault tree page it is placed on. Thus changing the Transfer up identifier also changes the name of the fault tree page, and vice versa.

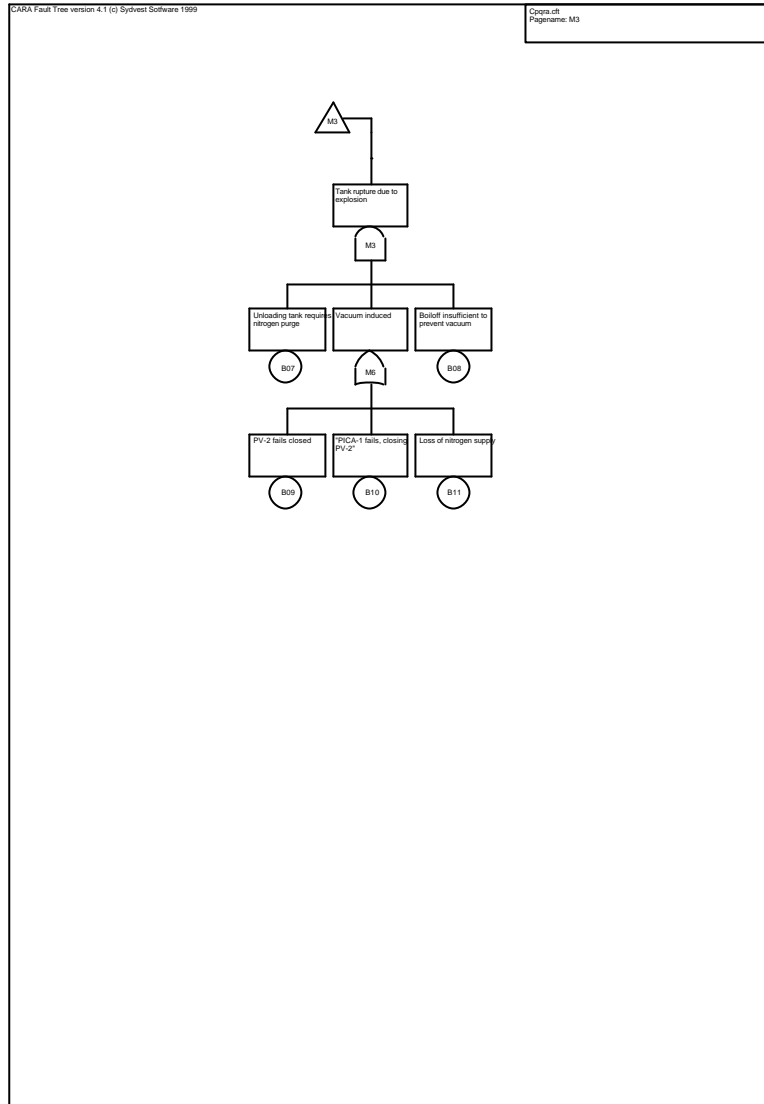


2.3.3 The Fault Tree Page

The fault tree is displayed in a window in CARA-FaultTree. Several fault tree windows, as well as several fault trees, can be open at the same time. The well-known **Window** command helps you to organise the fault tree windows as well as the analysis result windows, where the reports from the analyses are presented.

A fault tree window may view either a single fault tree page, or it can view an overview of the complete fault tree, where the various fault tree pages are connected. A fault tree page is by default set to A4 size with portrait orientation, however this can be altered individually on the various fault tree pages.

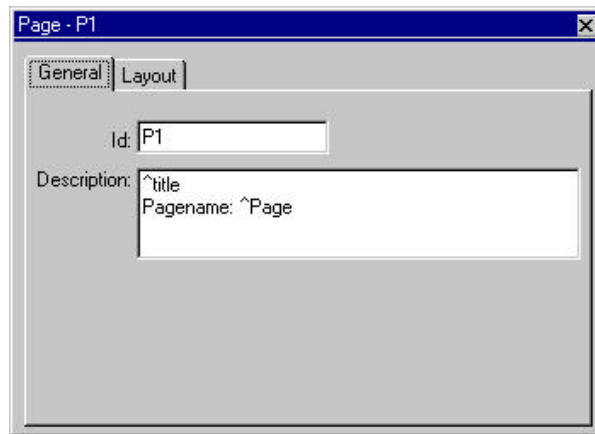
Fault tree page



Page properties

Similar to the Event and Gate symbols, the fault tree page also has properties. Select a page you want to change the properties for and double-click on a blank part of the fault tree page. The properties dialog of the page will open, having two tabs; **General** and **Layout**.

The parameters on the **General** tab (see figure below) are identifier and description.



Page Id The page identifier is the same as the page name, and may contain up to four characters.

Page Description The page description is an optional descriptive text displayed in the upper right corner of the page. Codes can be inserted to display e.g. page name and fault tree title, see table below. You may force a new line by entering **Ctrl+Enter**.

Code	Description
^page	The page identifier
^title	The fault tree title
^time	Current time as set in the Control Panel
^date	Current date as set in the Control Panel ("short" date)
^file	Path and file name
^computer	Computer name (if running on a Windows network)

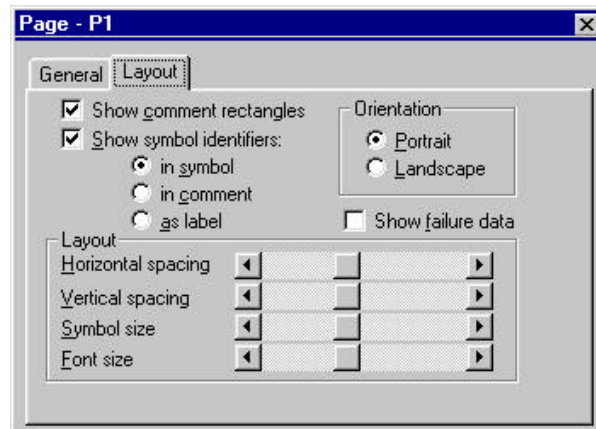
As given in the table above, the date and time codes use the format set in the Windows Control Panel. Observe that, if you change these settings while you are running CARA-FaultTree, the new settings will not affect CARA-FaultTree until you start up the program again.

Page Layout

The **Layout** tab (see figure below) defines how the fault tree page is displayed (both on screen and print).

CARA-FaultTree supports individual properties on all the different fault tree pages constituting the fault tree. Thus note that when you change the layout in the properties of the current page, the changes only affect this page. If you want to change the layout of all pages simultaneously, or only to new

fault tree pages to be added, please refer to the **Layout tab** in the "Tree menu" on page 46.



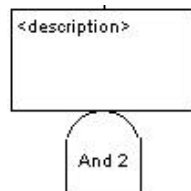
Show comment rectangles

If the **Show comment rectangles** is checked, the descriptive text on each symbol is displayed (i.e. the rectangles above each symbol).

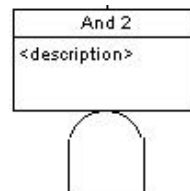
Show symbol identifiers

The **Show symbol identifiers** option rules if – and how – the identifiers for each symbol is displayed. If you select to show the identifiers, you may select between the three options **in symbol**, **in comment**, and **as label**. The differences between these options are as follows:

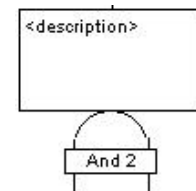
"in symbol"



"in comment"



"as label"



Show failure data

If the **Show failure data** option is selected, the failure data of the Input events are displayed.

Page orientation

Each fault tree page can be oriented as **Portrait** (vertical) or as **Landscape** (horizontal).

Layout

The four different **Layout**-controls define the presentation of symbols on the page. The **Horizontal spacing** and **Vertical spacing** sets the space between the symbols. The **Symbol size** sets the size of the symbols, whereas **Font size** sets the font used both for the symbols and the page description (increasing the font size also increases the size of the page description field).

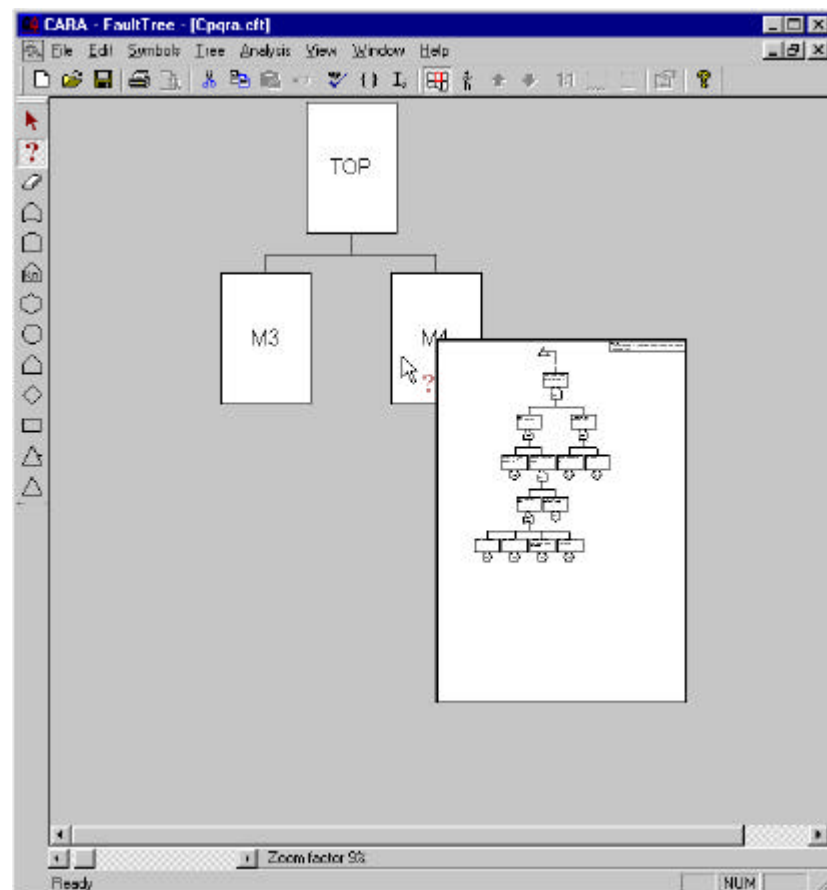
2.4 The Fault Tree Overview

The fault tree window may have two different views; Page view for viewing a single fault tree page, or Overview to display how the various fault tree pages are connected together to form the complete fault tree.



Select **Tree | Overview** to display the fault tree overview. Selecting **Tree | Overview** again will return to the fault tree page view.

Depending on the zoom factor selected in the zoom-bar at the window bottom, the fault tree pages are viewed showing page names only, or also – or only – showing the content of each fault tree page. In the example below, the pages are displayed with names only. However in the example, the Look-at tool has been selected from the Symbol Palette, and when the cursor is moved over one of the fault tree pages, the details of this page are displayed.



Note that you may alter the settings for when the fault tree page names and/or the fault tree page contents are viewed. This is defined in **Tree overview** tab of the **Tree | Setup**

dialog. Please refer to "**Tree Overview tab**" on page 48 for more information.

2.5 Running an Analysis

CARA-FaultTree offers a variety of analysis types, and both qualitative and quantitative analyses are supported. Note that this section only discusses the general aspects of starting and running an analysis.

A description of the available system performance measures as well as presentation of the methods used for calculations is given in the "Method Description" on page 77.

All analyses are available from the **Analysis** menu. Refer to the "Analysis menu" section on page 51 where the required input parameters and other information related to the various analyses are discussed.

2.5.1 Starting an analysis

When you have finished constructing a version of your fault tree, you may run an analysis.

Fault tree verification

However, before the analysis is run, CARA-FaultTree will automatically run a verification of the fault tree. The verification will among other things check for illegal couplings in the fault tree, look for components without failure data etc.

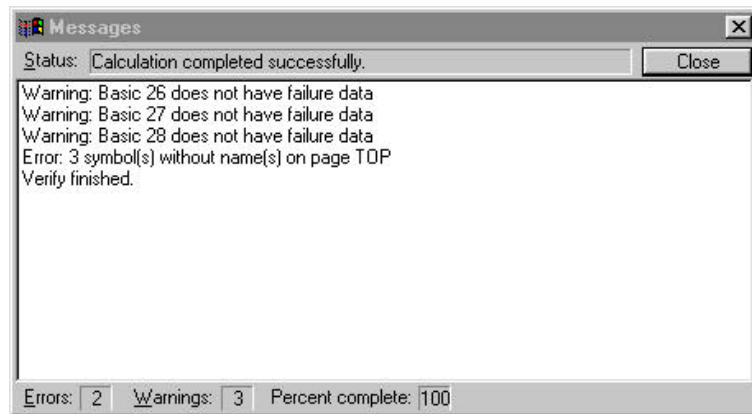
Note that if no changes have been made to the fault tree since last time verification was run, CARA-FaultTree will skip the verification.



You may also run the verification manually at any time by selecting **Tree | Verify** command.

Please refer to "Verification and Consistency Check" on page 28 for more information.

After you have started an analysis you will see a status box (see figure below), indicating both the result from the possible verification, and the percent completion of the calculation.



Note that the status box will be displayed only while the calculation is running. However, if errors were encountered during the verification, the analysis will not continue, and the status box will remain open.

By pressing the **Close** button you can terminate an ongoing calculation.

2.5.2 The Analysis Report

When a calculation is completed, the results are presented in a report. The report is displayed in a separate window.

The report window is in fact a small text editor, in which you can customise the report, or send it to a printer. The report can also be saved to file in Rich Text Format (RTF), which is recognised by all Windows text editors.

The header of the analysis report includes information on among other things date and time for the analysis, file name and title of the fault tree.

Long vs. Short report

In the setup of the fault tree (the **Tree | Setup** command), you may select between **Long** and **Short** analysis report. If **Long** report is selected, you will get additional information like graphics and tables. See also **Analysis tab** in the "Tree menu" on page 46.

2.5.3 Verification and Consistency Check

CARA-FaultTree includes various online consistency checks, as well as a verification command.

Online Consistency Checking

When you are constructing the fault tree, CARA-FaultTree will monitor the fault tree layout, and check and prevent you from introducing e.g. loops in the fault tree, illegal identifiers, and similar. Further, warnings will be given in certain

situations, e.g. if you enter an Input event identifier that is already in use.

Fault Tree Verification



CARA-FaultTree includes a verify command, **Tree | Verify**. Verify will also be run automatically in CARA-FaultTree before the minimal cut sets are found. The verification will e.g. check for illegal couplings in the fault tree, look for components without failure data etc. (see details below).

Note that if no changes have been made to the fault tree since last time verification was run, CARA-FaultTree will skip the verification.

A table is given on the next page describing the various tests included in the verification. In the column "E/W", it is noted if the message given reflects an error (E), or a warning (W) only.

Note that some test may in some situations result in an error and sometimes in a warning. E.g. missing input data for some Input events will only be given as a warning if no quantitative analysis is to be run (i.e. if only the minimal cut sets are to be found or if the verification is run manually). For tests where this is the case, "E/W" is given in this column.

Test for	Message given	E/W	Comments
Empty fault tree page	"Page <page name> is empty."	E	Checks for totally empty fault tree page.
Missing symbol names	"<no. of> symbols without names on page <page name>."	E	Checks for symbols (i.e. gates, transfer symbols and input events) without identification.
Missing symbol text	"<symbol name> does not have texts, page <page name>."	W	Checks for symbols (i.e. gates, comment boxes and input events) without descriptive text.
Missing failure data	"<symbol name> does not have failure data."	W	Checks for input events without failure data.
Improper connections	"<symbol name> is not connected, page <page name>."	E	General test for symbols missing connections.
	"Gate <gate name> does not have any inputs, <page name>."	E	Checks for gates without "children".
	"Gate <gate name> has only one input, page <page name>."	E	Checks for gates with only one input.
	"Comment box not properly connected, page <page name>."	E	Checks for comment boxes with missing connection.
Improper content of fault tree page	"No gates or events on page <page name>."	E/W	Checks if the fault tree page totally lack gates or input events.
Non-identical subtrees or gates with same identifier	"Bad use of gate name <gate name>." Followed by either of:	E	Error message followed by one of the four additional messages:
	"<gate name> occurs as both AND" and "OR" gate on page <page name>."	E	Checks if a gate is used as both "AND" and "OR" gate on the same fault tree page.
	"<gate name> occurs as both AND" and "OR" gate on page <page name> and <page name>."	E	Checks if a gate is used as both "AND" and "OR" gate on different fault tree pages.
	"<gate name> occurs as top of different subtrees on page <page name>."	E	Checks if a gate is top of non-identical subtrees on the same fault tree page.
	"<gate name> occurs as top of different subtrees on page <page name> and <page name>."	E	Checks if a gate is top of non-identical subtrees on different fault tree pages.
Non-referenced fault tree pages	"Page <page name> is not referenced from others."	W	Checks for non-referenced fault tree pages.
More than one top event	"Duplicate top event <symbol name> found on page <page name>. First top event found was <symbol name> on <page name>."	E	Checks if there are more than one top event in the fault tree. If found, the symbol names of the different top events and the location (page name) is listed.

2.6 Importing Graphics to other Windows-programs

Generally, all graphics in CARA-FaultTree can be imported into other Windows-programs via the Windows clipboard (note that this is also the case for text e.g. in the analysis reports). When a subtree, a single symbol or other is copied or cut from a fault tree or report window, the graphic is placed on the clipboard, and you may “pick it up” in another Windows-program. There are, however, some useful hints on available options. These are explained below.

Inserting a Fault Tree Page

Fault tree page with title field

When a fault tree window is open, you may place a copy of the whole fault tree page on the clipboard by selecting the **Edit | Copy page** command. The fault tree page copied to the clipboard will be identical to the printed fault tree page, which include the page title and license information.

Next, move to the Windows-program where you want to insert the fault tree page. Here, you may paste from the clipboard using the standard **Edit | Paste** command (**Ctrl+V**).

Paste special preferred

It is recommended, however, to select the **Edit | Paste Special...** command where available (the command is common in most word processors and drawing programs). Using this command, you will be able to specify the format of the pasted object. Here, you are advised to select the picture format (that is overriding the default “fault tree object”).

Inserting a Sub-Tree or an Input event

Similar to copying and pasting a whole fault tree page, you may insert a sub-tree or a single Input event. Simply activate the top gate of the sub-tree or the Input event you want to copy, and select the **Edit | Copy** command (**Ctrl+C**) to copy it to the clipboard.

Next, move to the Windows-program where you want to insert the graphics and follow the steps described above.

Inserting Graphics from an Analysis Report

Some of the analysis reports contain results presented in graphs. These graphs may also be copied and pasted into other Windows-programs. Simply activate the graph you want to copy, and select the **Edit | Copy** command (**Ctrl+C**) to copy it to the clipboard.

Next, move to the Windows-program where you want to insert the graphics and follow the steps described above.

3. CARA-FaultTree Menus

3.1 General

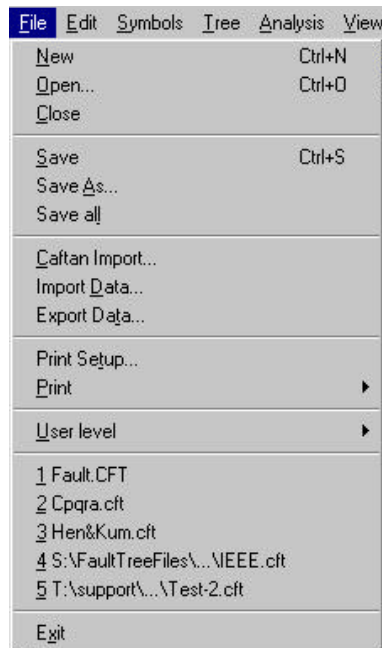
The CARA-FaultTree menu structure is organised similar to a typical Windows program, and should thus be easily understood. When you select or drag the mouse over any menu there is a short description in the status bar.

The menu options will vary depending on if the active window is a fault tree window or a report window, as some of the menu options are not available from a report window. The descriptions in this chapter will explain the full menu options, i.e. the menu options available from a fault tree window.

3.2 File menu

The **File** menu contains common file-commands for creating, opening, saving and printing. Also available are import and export options, see below.

The File menu is available both from the fault tree and report windows, however the available options are fewer from a report window (the example below is the File menu from the fault tree window).



3.2.1 Command Summary

File | New



or *Ctrl+N*

The **File | New** command is used to create a new fault tree. The new fault tree is displayed in a separate blank window.

File | Open...



or *Ctrl+O*

Select the **File | Open** command to open an existing fault tree for editing. A dialog box for selecting the fault tree file will be displayed. If you work on a network and another user already has opened the fault tree file you select, the file will be opened as read only (changes cannot be saved).

File | Close

The **File | Close** command closes the active fault tree. If the fault tree has changed since the last time you saved it, you will be asked if you would like to save the fault tree.

File | Save



or *Ctrl+S*

Use the **File | Save** command to save the active fault tree or report (if selected from a report window). If this is the first time you save the file, you will be asked for a file name.

Choose the **File | Save As...** command if you want to change the name or location of an existing fault tree.

File | Save As...

Use the **File | Save as...** command to save and name the active fault tree or report (if selected from a report window) with a different file name and/or location. To save a fault tree with its existing name and location, use the Save command.

File | Save All

Use the **File | Save all** command to save all open windows. If there are any new fault trees or any new report windows, you will be asked for a file name for the new files.

File | CAFTAN Import...

The **File | CAFTAN import...** command makes it possible to import a fault tree from the former DOS-version of CARA-FaultTree, i.e. CARA-CAFTAN v3.0 or newer (for simplicity denoted only “CAFTAN” in the following). In CAFTAN, each fault tree was stored in five different files (please refer to page 53 in the CAFTAN User’s Manual). CARA-FaultTree searches for CAFTAN fault tree header files, with the file extension “.FTR”, however for the import to be successful also the files with extensions “.FT1” and “.FT3” must be available.

File | Import Data / Export Data

Use the **File | Import data / Export data** commands for importing/exporting failure data – both Basic events and Event classes – as well as error factors from/to a tab-separated text file. See "Importing and Exporting Failure Data" on page 36 for more information.

File | Print Setup...

Use the **File | Print setup...** command to select a printer, a printer connection, paper size etc.

File | Print



or *Ctrl+P*

Use the **File | Print** command to print the active fault tree or analysis report. The **Print** command works on the currently active window, and the available print options depends on whether the active window is a fault tree page window, a fault tree overview window, or an analysis report window. Please refer to "Printing Fault Trees and Reports" on page 39 for more information.

File | User level

With the **File | User level** command you are given the opportunity to select between Standard and Expert mode of CARA-FaultTree. In the Standard mode (which is set by default) some parameters on the **Analysis** dialogs are set to default values, while in Expert mode you must specify these values yourself. Please refer to "Analysis menu" on page 51 for more information on the differences when running an analysis.

Recently used File List

Select a file from this list if you want to open one of the fault trees you have used recently.

File | Exit

Selects the **File | Exit** command to end the CARA-FaultTree session. You can also use the **Close** command on the application Control menu. You will be prompted to save fault trees having unsaved changes.

3.2.2 Importing and Exporting Failure Data

Use the **Import data / Export data** commands for importing/exporting failure data – both Basic events and Event classes/shared data – as well as error factors. The data is imported from/exported to a text file with columns separated by tabulator characters (in short known as a “tab-separated” text file). The combined features of exporting and importing data allows the user to manipulate data in a familiar environment, to do sensitivity analyses and to export data from e.g. a database.

A tab-separated text file is easily opened in, or saved from, a spreadsheet. A good way of using this feature is thus to edit the text file using your standard spreadsheet program.

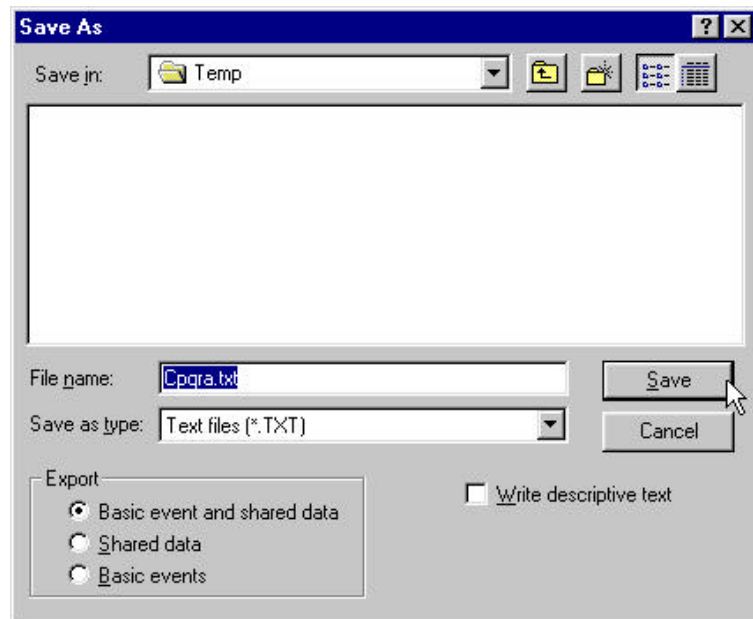
By selecting to import/export Shared data (i.e. Event classes) only, you have an effective way applying and maintaining a library of “typical” components.

Exporting Data

When **File | Export data...** is selected, a dialog is opened (see below) where you may specify if you want to export both data for Input/Basic event as well as data from shared events (i.e. the Event classes). You may also specify whether or not

to include the descriptions (the “Write descriptive text” option).

Select the desired options, select where to save the data, enter a file name, and save the text file.



The format of the resulting tab-separated file is as follows:

Column	Contents
1	Input event identifier
2	Name of Event class referred to. - If Input event does not refer to an Event class, “<not shared>” is indicated. - If the event data is for an Event class, “<event class>” is indicated.
3	Failure category code: R = Repairable unit N = Non repairable unit T = Test interval O = On demand probability F = Frequency H = House event
4	First reliability parameter
5	Error factor first parameter
6	Second reliability parameter
7	Error factor second parameter
8	Third reliability parameter
9	<not used>
10	Descriptive text

Which reliability parameters are used depends on the failure category type, see table below. Further, an example export data file is given below.

Important notes!

Important notes:

- All rates/frequencies are entered per hour.
- All times/intervals are entered in hours.
- You may use both regular decimal number as well as an exponential number.
- The period, “.” is used as decimal-format. If you e.g. are using a spreadsheet to edit the exported text file, you should thus be aware that period should be used as decimal-format also in the spreadsheet.
- Thus, a failure rate of 2 per 10^6 hours may be entered as “2e-6”, “2.00E-6”, “0.000002” or similar.
- For parameters not entered a value, the value “-1” is set.

Category of failure data		Reliability parameter		
Code	Description	First	Second	Third
R	Repairable unit	Failure rate	Repair time	
N	Non repairable unit	Failure rate		
T	Test interval	Failure rate	Repair time	Test interval
O	On demand probability	Probability		
F	Frequency	Frequency		
H	House event	On/Off		

In the text box below, an example of an exported data file is given. Here the “→”-symbol indicates a tab-character.

```

B01 → TypA → R→ 4.00E-06 → 2 → 4 → 2→ -1 → → <description>
B02 → TypB → T→ 4.00E-06 → 3 → 6 → 3→ 8760 → → <description>
B03 → <not shared> → F→ 0.00114 → 1 → -1 → 1→ -1 → → <description>
B04 → <not shared> → O→ 0.01 → 1 → -1 → 1→ -1 → → <description>
B05 → <not shared> → N→ 2.00E-06 → 4 → -1 → 1→ -1 → → <description>
TypA → <event class> → R→ 4.00E-06 → 2 → 4 → 2→ -1
TypB → <event class> → T→ 4.00E-06 → 3 → 6 → 3→ 8760

```

Importing Data

Choosing the **File | Import data...** you will see a dialog almost identical to the **File | Export data...** dialog. Please refer to "Exporting Data" above for more information on the **Import data...** dialog, as well as the format of the tab-separated text file.

A hint on the use is first to export data to a text file, and then to edit or append the exported file.

Important notes!

Important notes:

- If you enter an Input event referring to an Event class ("shared data"), and also the reliability parameters are entered in the same line in the text file, these parameters will not be read. The reason for this is that the reliability parameters for a "shared Input event" will be taken from the data for the referenced Event class.
- If you enter the same identifier in more than one line in the text file, only the last line will be imported and used by CARA-FaultTree.

3.2.3 Printing Fault Trees and Reports

The Print command works on the currently active window, and the available print options depend on whether the active window is a fault tree page window, a fault tree overview window, or an analysis report window. Note that the shortcut keys also depend on the window type you are in.

Print from a Fault Tree Page Window

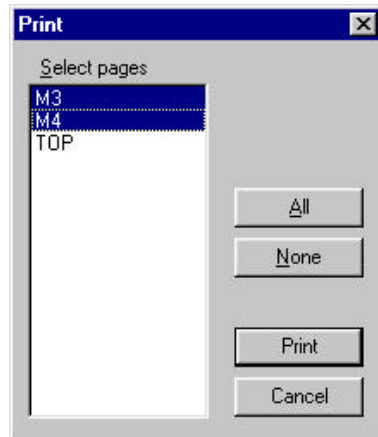
If a fault tree page window is active, the **File | Print** command will have two options available; **Current page** and **Selected pages...**



or Ctrl+P

Print | Current page sends a copy of the current fault tree page to the selected printer.

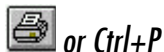
Print | Selected pages... opens a dialog where you may specify which of the fault tree pages to send to the printer (see example below). Click on the fault tree pages in the list to select/deselect which pages to print.



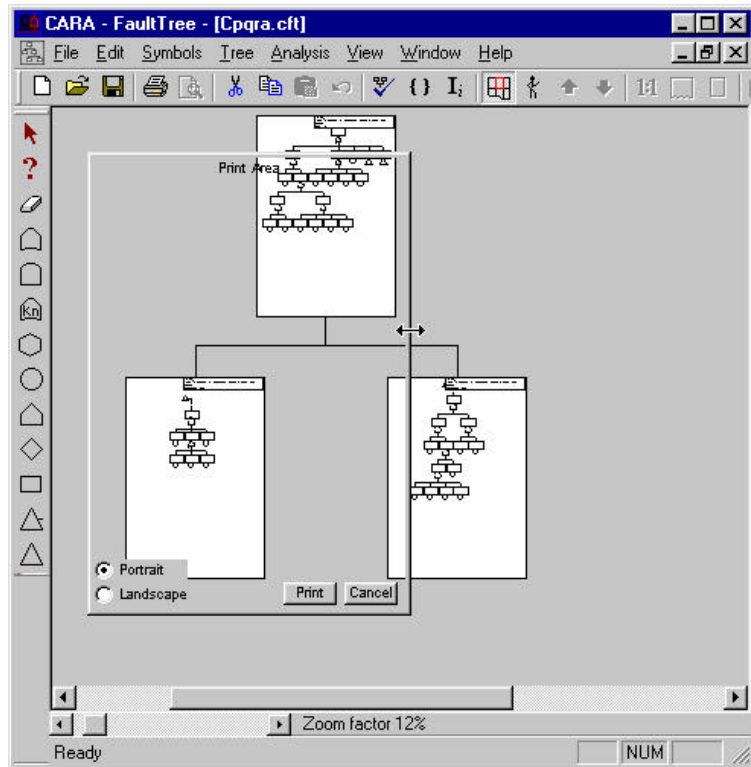
Print from a Fault Tree Overview Window

If a fault tree overview window is active, the **File | Print** command will have two options available; **Selected pages...** and **Overview...**

From **Print | Selected pages...** opens a dialog where you may specify which of the fault tree pages to send to the printer (see above).



Selecting **Print | Overview** places a frame in the overview window, indicating which segment of the window that will be printed, see figure below. Drag the border of the frame in order to increase or decrease the frame, or drag inside the frame to move it. You may also select between a **Portrait** and **Landscape** orientation of the frame. Click on the **Print** button to complete the print, or **Cancel** the operation.



Print from an Analysis Report Window

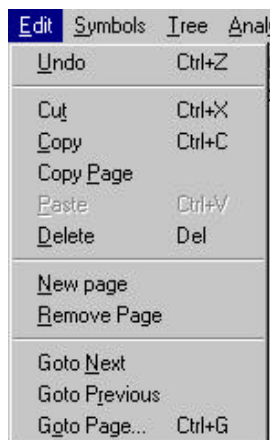


or *Ctrl+P*

Selecting the **File | Print** command opens the Windows Print dialog, and the report may be sent to the default printer.

3.3 Edit menu

The **Edit** menu contains the standard Windows undo, cut, copy, and paste commands, as well as commands operating on fault tree pages.

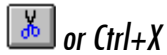


Edit | Undo



Use the **Edit | Undo** command to undo the last operation or last operations.

Edit | Cut



Use the **Edit | Cut** command to delete items in the currently selected window, and place it on the Windows clipboard. First, activate the symbol, text or other to be deleted, then activate the command. The deleted item may be inserted again by selecting **Edit | Paste**

Edit | Copy



Use the **Edit | Copy** command to copy items in the currently selected window. First, activate the symbol, text or other to be copied, then activate the command. The item will be placed on the Windows clipboard and is inserted by selecting **Edit | Paste**. The copy command can be used in the fault tree window to duplicate a symbol with its corresponding data. In the analysis window it can be used to copy results from the table into a word processor.

Edit | Copy Page

Use the **Edit | Copy page** command to place a copy of the entire fault tree page on the Windows clipboard. You may then insert the fault tree page e.g. in the word processor for documenting a fault tree analysis.

Please refer to “Importing Graphics to other Windows-programs” on page 31 for more information on how to import graphics.

Edit | Paste



Use the **Edit | Paste** command to paste the content of the Windows clipboard into the currently selected window.

Edit | Delete

Delete-key

Use the **Edit | Delete** command to delete items in the currently selected window. First, activate the symbol, text or other to be deleted, then activate the command.

Edit | New Page

Use the **Edit | New page** command to insert a new page to your current fault tree. The new page is opened in the fault tree page window.

Edit | Remove Page

Use the **Edit | Remove page** to delete the current fault tree page from the fault tree. You may **Undo** the page removal, however note that the deleted page will not be opened as the current fault tree page again. You must thus open the page again manually after having inserted the page again.

Edit | Goto Next

 or
*right-click on a transfer
symbol*

The **Edit | Goto next** command will be available if there is a Transfer down symbol in the drawing area (note that the Transfer down symbol also must be connected to a fault tree page).

If the fault tree page contains more than one connected Transfer down symbol, a list of the connected fault tree pages will be displayed.

Edit | Goto Previous

 or
*right-click on a transfer
symbol*

The **Edit | Goto previous** command will be available if the fault tree page is below the TOP level of the fault tree.

If the fault tree page is referred to from more than one fault tree page, a list of all the referencing fault tree pages will be displayed.

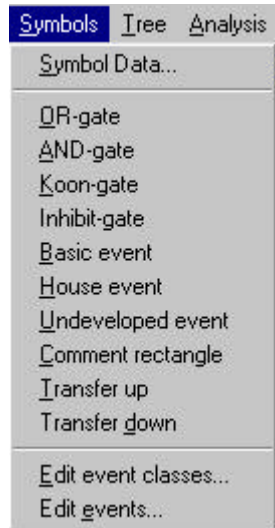
Edit | Goto Page...

 or *Ctrl+G*

The **Edit | Goto page...** command will be available if there are more than one page in the fault tree. A list of all pages in the fault tree is displayed, and you select which page to go to.

3.4 Symbols menu

The **Symbols** menu contains a list of the various symbol types that can be added to the fault tree, as well as commands related to Gates and Input events. See menu below.



3.4.1 Command Summary

Symbols | Symbol Data...



or double-click on symbol

Use the **Symbols | Symbol data...** command to open the properties dialog for a symbol in the fault tree page. First activate the symbol, then choose **Symbols | Symbol data...**

Please refer to "Fault Tree Symbols" on page 14 for details on the parameters for each symbol type.

Symbols | List of Symbols

The list of symbol types in the **Symbols** menu is identical to the fault tree symbols available from the Symbols Palette. Please refer to "Fault Tree Symbols" on page 14 for more information.

The other options on the **Symbols** menu are explained in the following sections.

Symbols | Edit Event Classes..

The **Symbols | Edit event classes...** command opens the Event classes dialog. Please refer to "Edit Event Classes..." on page 45 for more information.

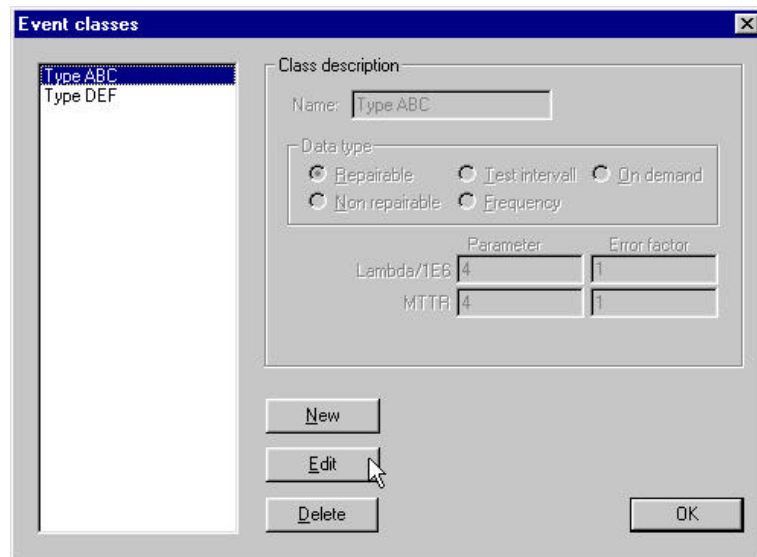
Symbols | Edit Events...

The **Symbols | Edit events...** command opens the Event data window. Please refer to "Edit events..." on page 46 for more information.

3.4.2 Edit Event Classes...

CARA-FaultTree offers an option for defining Event classes for Input events. Say, as an example, that your system includes several electric motors of one specific make. You may then define an Event class for this electric motor, enter the relevant failure data, and simply refer to this Event class from the various instances of the Input events in the fault tree. In this way, you only need to enter the failure data once, and also make possible changes in the data only once.

Select the **Symbols | Edit event classes...** command to open a dialog (see example below) where you may edit the list of Event classes. The Event classes dialog can also be opened from the Event data tab of the Input event property dialog.



All the defined Event classes are listed in the Event class dialog, and you may enter new classes, and edit or delete a defined Event class. Note that the class description (name and data) is shaded out as long as the class is not opened for editing.

Enter new Event class

To enter a new Event class, select **New** and type the desired name for the new Event class, select data type and enter data. Click on one of the other Event classes on the list or select **OK** to complete entering the new class.

Edit Event class description

To edit the name or data of an Event class, select the class and click **Edit**. Edit the desired fields and click on one of the other Event classes on the list or select **OK** to complete.

Delete Event class

To delete an Event class, select the class and click **Delete**. Note that to be able to delete an Event class, no Input events must refer to the class.

3.4.3 Edit events...

Select the **Symbols | Edit events...** command to open the Edit event window (see example below). The Edit event window lists all the Input events in a table, and you may edit the data directly in the table.

All the non-shaded fields are available to edit, and drop-down lists are offered for relevant data fields. Use the mouse to select a field to edit, or use **Tab** to move between fields.

The shaded fields, that is the Input event identifier as well as failure data fields for possible Input events applying Event classes, are not available to edit.



Name	Shared	Type	Parameter	Value	Error	Parameter	Value	Error	Parameter	Value	Description
E01	Type ABC	Repeatable	Lambda*1E6	4.0000e+000	1.0000e+000	MTTF	4.0000e+000	1.0000e+000			Tank drain break
E02	cut shared	Frequency	Frequency/SES	1.4200e+001	1.0000e+000						Tank truck unloading
E03	cut shared	Frequency	Frequency/SES	1.1400e+003	1.0000e+000						Vehicle impact
E04	Type DEF	Test interval	Lambda*1E6	4.0000e+000	5.0000e+000	Tau	5.0000e+000	5.0000e+000	Test in.	0.7000e+002	Aircraft impact
E05	Type ABC	Repeatable	Lambda*1E6	4.0000e+000	1.0000e+000	MTTF	4.0000e+000	1.0000e+000			Collision
E06	Type DEF	Test interval	Lambda*1E6	4.0000e+000	5.0000e+000	Tau	5.0000e+000	5.0000e+000	Test in.	0.7000e+002	Tornado
E07	cut shared	Frequency	Frequency/SES	1.1400e+003	1.0000e+000						Unloading tank leak
E08	cut shared	On demand	q	1.0000e+002	1.0000e+000						Boiloff insufficient to p
E09	cut shared	On demand	q	1.0000e+002	1.0000e+000						PU-2 tank closed
E10	cut shared	On demand	q	1.0000e+002	1.0000e+000						PU-1 tank closing
E11	cut shared	On demand	q	1.0000e+004	1.0000e+000						Loss of nitrogen succ
E12	cut shared	Frequency	Frequency/SES	1.1400e+000	1.0000e+000						Failure of PU-1, dc
E13	cut shared	On demand	q	1.0000e+003	1.0000e+000						Exceed capacity of R
E14	cut shared	On demand	q	1.0000e+003	1.0000e+000						V-1 closed
E15	cut shared	On demand	q	1.0000e+002	1.0000e+000						Insufficient volume in
E16	cut shared	On demand	q	1.0000e+002	1.0000e+000						Failure of, or ignoring
E17	cut shared	On demand	q	1.0000e+003	1.0000e+000						Wrong material in tank
E18	cut shared	On demand	q	1.0000e+002	1.0000e+000						Tank truck not scrapp
E19	cut shared	On demand	q	1.0000e+001	1.0000e+000						Reagent reacts with v
E20	cut shared	On demand	q	1.0000e+001	1.0000e+000						Pressure too exceede
E21	cut shared	On demand	q	1.0000e+002	1.0000e+000						Failure of, or ignoring
E22	cut shared	Frequency	Frequency/SES	1.1500e+001	1.0000e+000						PU-1 tank closed
E23	cut shared	Frequency	Frequency/SES	1.1500e+001	1.0000e+000						V-2 closed
E24	cut shared	Frequency	Frequency/SES	1.1500e+001	1.0000e+000						Temperature of inlet f
E25	cut shared	Frequency	Frequency/SES	1.1500e+001	1.0000e+000						High pressure in floe

3.5 Tree menu

The **Tree** menu contains general handling of the fault tree, see below.



Tree | Verify



Activate the **Tree | Verify** command to verify the completeness and consistency of the fault tree.

Please refer to "Verification and Consistency Check" on page 28 for more information on the **Verify** command.

Tree | List events

The **Edit | List events** generates a report listing all the Input events in the fault tree, as well as their related reliability data. The report can be saved to an RTF-file or printed.

Tree | Overview



Activate the **Tree | Overview** command to display how the various fault tree pages are connected together to form the complete fault tree.

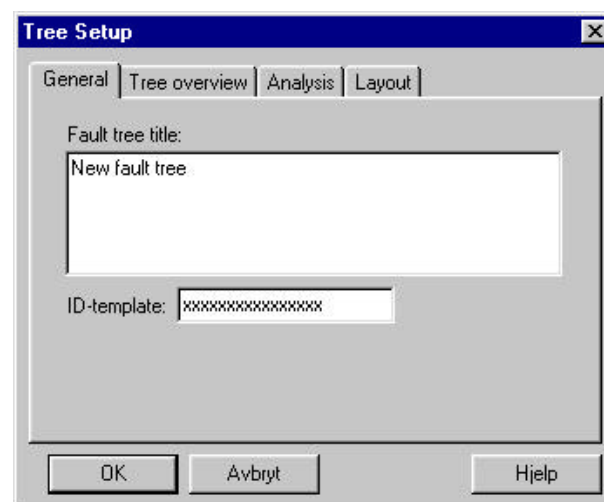
Please refer to "The Fault Tree Overview" on page 26 for more information on the Overview command.

Tree | Setup...

The **Tree | Setup...** command activates a dialog where the user can set options for the fault tree. The dialog contains four tabs: General, Tree overview, Analysis and Layout.

General tab

In the **General** tab of the **Tree | Setup** dialog (see below) you specify the fault tree title as well as what part of the up to 16 character long symbol identifier that shall be displayed, see below.



Fault tree title The fault tree title is printed on analysis reports, and may also be displayed in the fault tree page description (see "Page properties" on page 23). You may also use keywords in the fault tree title as given in "Page properties". The available keywords here are ^time, ^date, ^file and ^computer. See "Page properties" (page 23) for more information on keywords.

ID-template The ID-template is a way to filter the displayed Gate and Input event identifier. In the fault tree page window and printouts, CARA-FaultTree displays the characters of the identifier in positions where a "x" is given. If there is a space (" ") in the ID-template, the corresponding character in the symbol identifier is not displayed.

E.g. the symbol identifier "SYS-20-PT012" has twelve characters. Say, e.g., that the reason for including the first seven characters ("SYS-20-") is that you want to maintain the full tag number for easy import/export from an equipment database. At the same time you want, however, also to limit the space taken up on the printouts by excluding this prefix. You should then start the ID-template with seven spaces followed by nine or more "x"-es.

Tree Overview tab

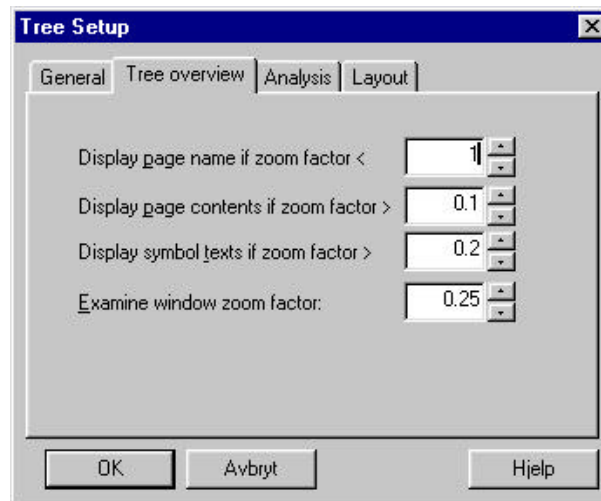
The **Tree overview**-tab of the **Tree | Setup** dialog (see figure below) determines how the Tree overview window is displayed. Depending on how much the window is zoomed, the Overview window displays:

- Page names (page identifier)
- Page contents (the symbols on the page)
- Symbol text (symbol identifiers and description)

The first three factors set in the Tree overview tab determines the limit with respect to zoom factor when these three information types are displayed. E.g., page names are displayed only if the zoom factor is less than specified. By default, the page name display factor is set to 1, in order for the page names always being displayed. Note however, that in versions prior to version 4.1 this was set to 0.1.

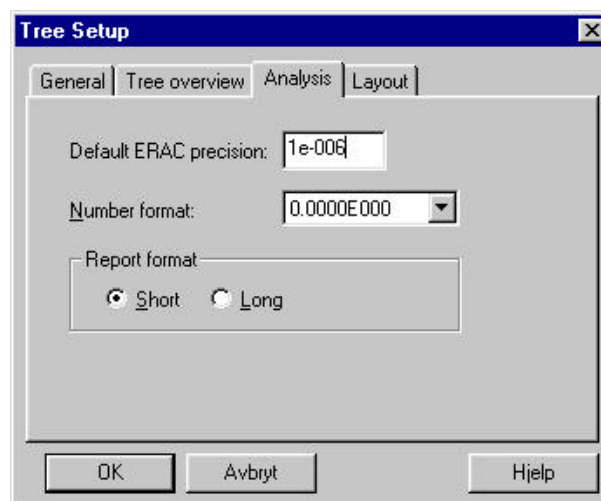


"Examine window zoom factor" is the last parameter specified in the Tree overview tab. This determines the size of the window displayed when the Look-at tool is selected and moved over a fault tree page (see "The Fault Tree Overview" on page 26 for more information on using the Look-at tool in the Overview window).



Analysis tab

In the **Analysis** tab of the **Tree | Setup** dialog (see figure below) you specify the default precision of one of the CARA-FaultTree analyses, the number format used in reports, and to select between long and short analysis reports, see below.



ERAC precision

The **Default ERAC precision** is the default value used as cut-off criterion in ERAC calculations. Please refer to "Exact Calculation of $Q_0(t)$; the ERAC Algorithm" on page 97.

Number format

The **Number format** specifies the format of the analysis used for presenting analyses numbers.

Short vs. Long report

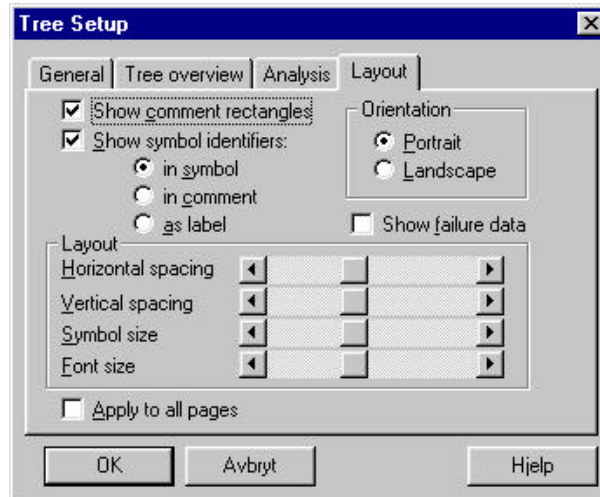
The **Report format** can be set to **Short** or **Long**. Selecting the long format will give you analysis reports with additional information compared to the short format.

The additional information varies depending on which analysis you run. In general, the short report shows only the

performance measure/parameter you specify to be calculated, however the long report also includes some other parameters as well as the minimal cut set listing. Also, a graphical presentation of the result is included in some of the analysis reports in long format.

Layout tab

The **Layout**-tab of the **Tree | Setup** dialog (see figure below) defines the default values for the fault tree page display (both on screen and print).



You will notice that this dialog looks almost identical to the **Layout** dialog for individual pages, please refer to "Page Layout" on page 24. It looks as if the only difference is that the current dialog includes the additional **Apply to all pages** option. However, the actual difference goes beyond this: Whereas the page layout properties set on individual pages affect the current page only, this is not the case for the values set here. Here, the values set either affect only new fault tree pages to be added, or, if **Apply to all pages** is selected, it affects all pages in the fault tree.

Please refer to "Page Layout" on page 24 for further details on the meaning of the various parameters to be set, as these are the same for the two dialogs.

3.6 Analysis menu

3.6.1 General

Standard and Expert user modes

CARA-FaultTree supports two user modes; Standard and Expert user mode. The reason for this is to be able to offer also a less complicated user interface, where some capabilities not required for standard calculations, are hidden. Note that the differences in user interface are in the analysis menu only.

Standard user mode

Running an analysis in Standard user mode, you will not be prompted e.g. for the calculation method to be used in the analysis, nor will you be able to specify some more advanced options. The good thing with this is that the program will supply default choices both regarding calculation parameters and method.

Expert user mode

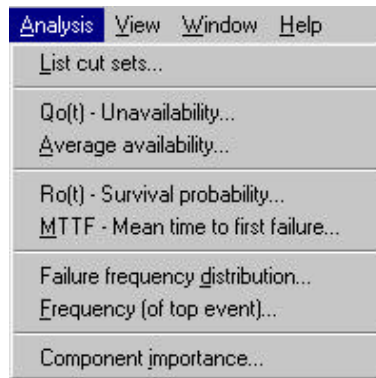
You should, however, select the Expert user mode if you want to take full control of all available options and parameters. Applying the Expert user mode, you should be familiar with the theoretical foundation for the various analyses as described in the "Method Description" (especially the section on "TOP Event Calculations" on page 95).

In the following, the Analysis menu both for Standard and Expert user mode is explained, together with a description of the required input to the analyses. The description is split in two sections, one for each of the user modes. These sections are independent, so you need to read only the section that is relevant for you.

Have also in mind that some options relating to the analyses are set in the **Analysis tab** of the **Tree | Setup** dialog (please refer to page 49).

3.6.2 Standard User Mode

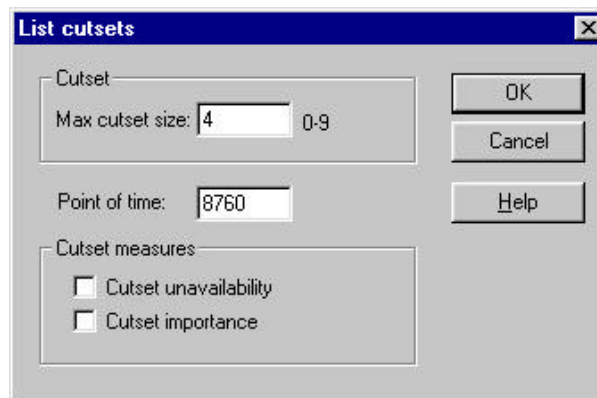
The Analysis menu in Standard user mode contains easy access to the most common system analyses methods available in CARA-FaultTree, see below.



Analysis | List cut sets...



Select the **Analysis | List cut sets...** command to obtain the minimal cut sets of your fault tree. The “List cut sets” dialog will be displayed, see below.



Max. cut set size

You are asked to specify the maximum size of the minimal cut sets to be obtained (**Max. cut set size**), with the default value set to four. Cut sets of higher order will be discarded from the cut set listing, and from the later calculations which are based on the cut set representation of the fault tree. Please refer to "Identification of Minimal Cut and Path Sets" on page 83 for an introduction to minimal cut sets.

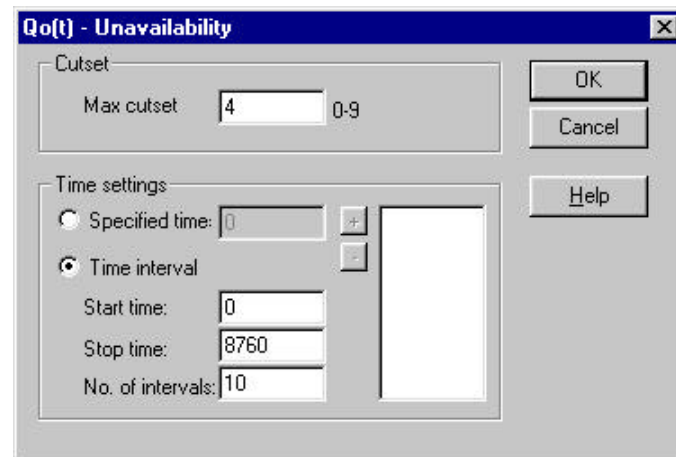
Point of time / Cut set measures

You may also include the **Cut set unavailability** and **Cut set importance** in the cut set listing. In this case you also need to enter the **Point of time** for these measures to be calculated (simply keep the point of time unchanged if this is not relevant for you). Please refer to "Quantitative ranking of minimal cut sets" on page 91 for information on the cut set unavailability and cut set importance.

Analysis | $Q_0(t)$ - Unavailability...

Select the **Analysis | $Q_0(t)$ - Unavailability...** command to calculate the probability of the TOP event occurring at a given

point in time. The “ $Q_0(t)$ – Unavailability” dialog will be displayed:



Max. cut set size

First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Time settings

Next, you need to specify the **Time settings**, that is to calculate the (time dependent) fault tree unavailability $Q_0(t)$, you must specify the different points of time for which $Q_0(t)$ should be calculated. You have two options; **Specified time** or **Time interval**.

Specified time

When **Specified time** is selected, you enter the points of time one by one, separated by pushing the “+”-button (the plus sign). The points of time are added to the list of calculation values. To remove a selection from the list, make the point of time active, and press the “-”-button (the minus sign).

Time interval

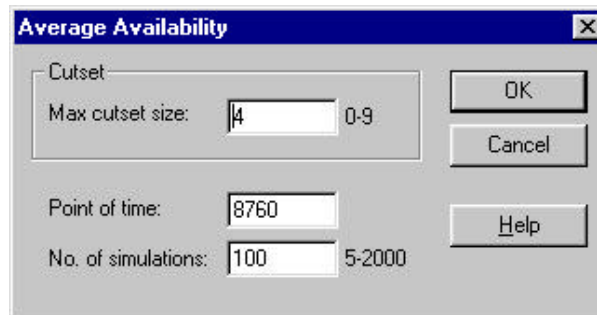
When **Time interval** is selected, you enter a the start and end of the interval (**Start time** and **Stop time**), and the **No. of intervals** to be calculated.

Calculation method

When running in the Standard user mode, the calculation method used is the Exact calculation (ERAC). Please refer to "Calculation of $Q_0(t)$ Using Exact Calculation (ERAC) and Upper Bound Approximation" on page 96 for more information.

Analysis | Average Availability...

Select the **Analysis | Average Availability...** command to calculate the average system availability up to a given point in time. The “Average Availability” dialog will be displayed, see below.



Max. cut set size

First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Calculation method

The calculation of the **Average Availability** is done by Monte Carlo (Stochastic) simulation. Thus, you also need to specify the **Point of time** and the **No. of simulations**. Please refer to "Calculation of $R_0(t)$, MTTF and $Freq(TOP)$ Using Monte Carlo (Stochastic) Simulation" on page 98 for a description of the method used.

Point of time

No. of simulations

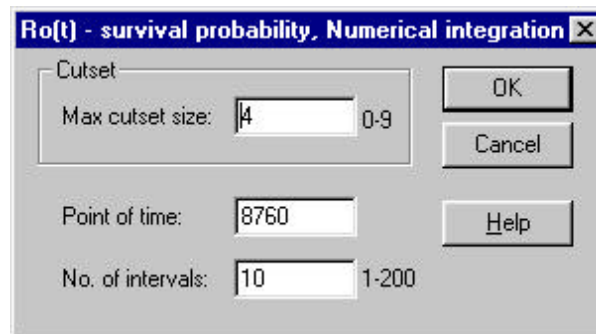
All component failure and repair times are drawn from their respective distributions, and the system behaviour is simulated through the interval from $t=0$ to $t = \mathbf{Point\ of\ time}$. This is repeated **No. of simulations** times, and the quantity is calculated as the average over all replications.

The results are presented with a standard error to reflect the uncertainty of the estimates. The standard error should be low relative to the estimate. A standard error of less than 1 % of the estimate should in most cases be regarded as acceptable. If the standard error is significantly larger than 1 %, consider re-running the calculations with a larger number of simulations.

Analysis | $R_0(t)$ - Survival probability...

Select the **Analysis | $R_0(t)$ - Survival probability...** command to calculate the probability of not having

experienced any system failure up to a given point in time. The “ $R_0(t)$ – Survival probability” dialog will be displayed, see below:



Max. cut set size

First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Calculation method

The calculation of the **Survival Probability** is done by Numerical integration. Thus, you also need to specify the **Point of time** and the **No. of intervals**. Please refer to "Calculation of $R_0(t)$, MTTF and $E(\#failures)$ Using Numerical Integration" on page 99 for a description of the method used.

Point of time

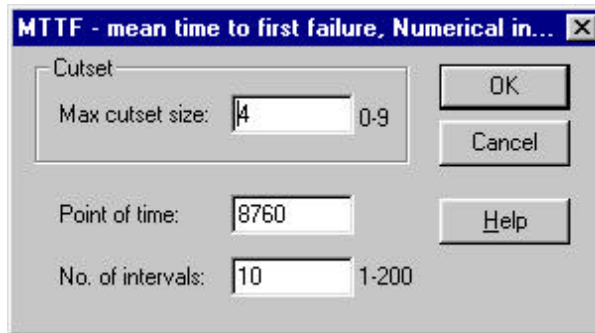
No. of simulations

All component failure and repair times are drawn from their respective distributions, and the system behaviour is simulated through the interval from $t=0$ to $t = \mathbf{Point\ of\ time}$. This is repeated **No. of simulations** times, and the quantity is calculated as the average over all replications.

The results are presented with a standard error to reflect the uncertainty of the estimates. The standard error should be low relative to the estimate. A standard error of less than 1 % of the estimate should in most cases be regarded as acceptable. If the standard error is significantly larger than 1 %, consider re-running the calculations with a larger number of simulations.

Analysis | MTTF - Mean time to first failure...

Select the **Analysis | MTTF – Mean time to first failure...** command to calculate the mean time to first system failure. The “MTTF – Mean time to first failure” dialog will be displayed, see below:



Max. cut set size

First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Calculation method

The calculation of the **Mean time to first failure** is done by Numerical integration. Thus, you also need to specify the **Point of time** and the **No. of intervals**. Please refer to "Calculation of $R_0(t)$, MTTF and $E(\#failures)$ Using Numerical Integration" on page 99 for a description of the method used.

Point of time

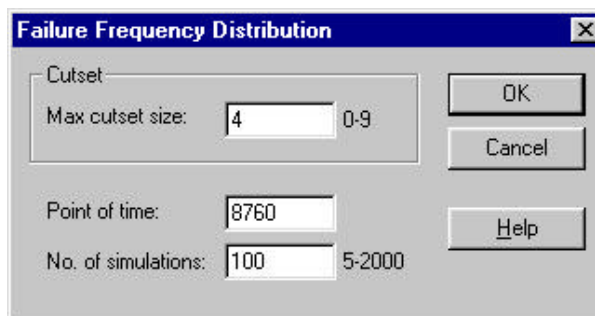
The system is investigated at times from $t=0$ to $t = \text{Point of time}$. This time period is separated into **No. of intervals**.

No. of intervals

The number of intervals determines the precision; a higher number of intervals give good precision on the expense of calculation time.

Analysis | Failure Frequency Distribution...

Select the **Analysis | Failure Frequency Distribution...** command to calculate the distribution of the TOP event frequency. The "Failure Frequency Distribution" dialog will be displayed, see below:



Max. cut set size

First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Calculation method

Calculation of the **Failure Frequency Distribution** is done by Monte Carlo (Stochastic) simulation. Thus, you also need to specify the **Point of time** and the **No. of simulations**. Please refer to "Calculation of $R0(t)$, MTTF and $Freq(TOP)$ Using Monte Carlo (Stochastic) Simulation" on page 98 for a description of the method used.

Point of time

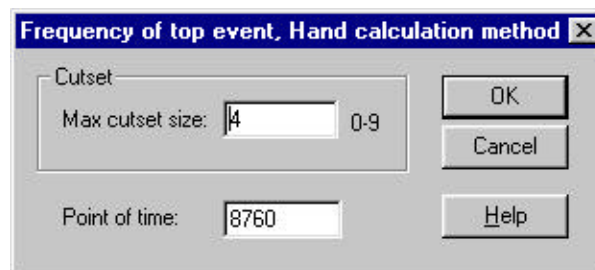
No. of simulations

All component failure and repair times are drawn from their respective distributions, and the system behaviour is simulated through the interval from $t=0$ to $t = \mathbf{Point\ of\ time}$. This is repeated **No. of simulations** times, and the quantity is calculated as the average over all replications.

The results are presented with a standard error to reflect the uncertainty of the estimates. The standard error should be low relative to the estimate. A standard error of less than 1 % of the estimate should in most cases be regarded as acceptable. If the standard error is significantly larger than 1 %, consider re-running the calculations with a larger number of simulations.

Analysis | Frequency of TOP event...

Select the **Analysis | Frequency of TOP event...** command to calculate the mean time to first system failure. The "MTTF – Mean time to first failure" dialog will be displayed, see below:



Max. cut set size First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

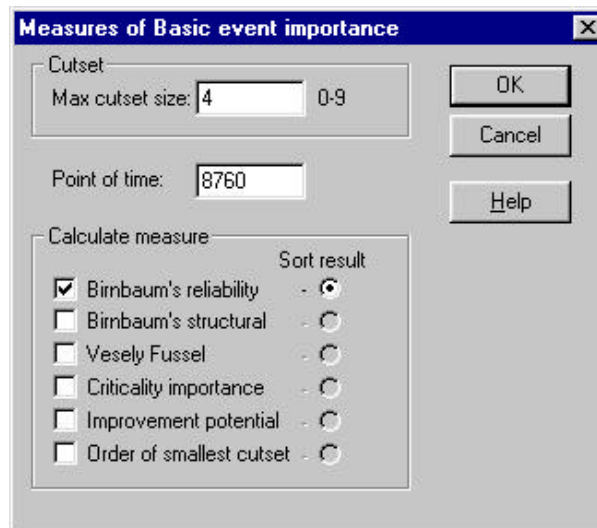
Calculation method Calculation of the **Frequency of the TOP event** is done by the Hand calculation method. Thus, you also need to specify the **Point of time**. Please refer to "Calculation of *Freq(TOP)* Using the Hand Calculation Method" on page 101 for a description of the method used.

Analysis | Component Importance...



Select the **Analysis | Component Importance...** command to calculate various importance measures for the Basic/Input events. An introduction to the various importance measures is given in "Measures of Importance" on page 105.

Selecting this command the "Measures of Basic event importance" dialog will be displayed:



Max. cut set size First, you need to specify the **Max. cut set size** in order to obtain the cut sets to base the calculation on. Please refer to "Analysis | List cut sets..." on page 52 for further information on minimal cut sets.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

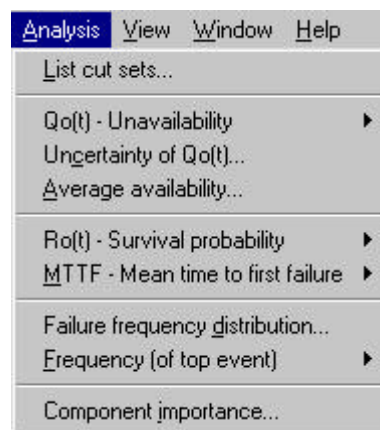
Point of time To calculate reliability measures (i.e. measures also dependent on failure data), a **Point of time** is required.

Calculate measure In the **Calculate measure** options you specify which of the offered measures to include in the calculations. Selecting more than one measure, you are allowed to specify which of the measures to **Sort results** on.

3.6.3 Expert User Mode

The Analysis menu for the Expert user contains easy access to all the system analyses methods available in CARA-FaultTree, see below.

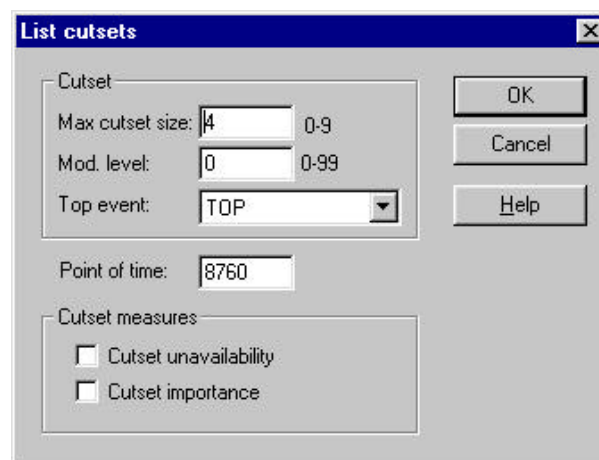
The various analysis methods are described in the "Method Description" on page 77.



Analysis | List cut sets...



Select the **Analysis | List cut sets...** command to obtain the minimal cut sets of your fault tree. The "List cut sets" dialog will be displayed, see below.



- Max. cut set size* You are asked to specify the maximum size of the minimal cut sets to be obtained (**Max. cut set size**), with the default value set to four. Cut sets of higher order will be discarded from the cut set listing, and from the later calculations which are based on the cut set representation of the fault tree. Please refer to "Identification of Minimal Cut and Path Sets" on page 83 for an introduction to minimal cut sets.
- Mod. level* Specify the **Mod. level** if you want to use the modularization technique when obtaining the minimal cut sets (leaving it with the value "0" means that modularization is not applied). When analysing very complex fault trees (e.g. having many AND-gates and repeated events), obtaining the minimal cut sets can be quite time consuming. CARA-FaultTree offers a modularization technique which may reduce the computing time drastically, please refer to "Modular Decomposition" on page 102 for more information.
- Note that when using modularization, the minimal cut sets will not be expressed explicitly, as the super modules will appear as Basic events. The events that constitute a super module will also be displayed but you will not know the structure of the module.
- TOP event* You may analyse any subtree of your fault tree in a given analysis, not just the entire fault tree. Select the desired **TOP event** for the current analysis from the drop-down list. The drop-down contains a list of all gates in the fault tree, with the actual TOP event in the fault tree as default.
- Point of time / Cut set measures* You may also include the **Cut set unavailability** and **Cut set importance** in the cut set listing. In this case you also need to enter the **Point of time** for these measures to be calculated (simply keep the point of time unchanged if this is not relevant for you). Please refer to "Quantitative ranking of minimal cut sets" on page 91 for information on the cut set unavailability and cut set importance.

Analysis Methods and Input Parameters

CARA-FaultTree offers five different calculation methods to be applied when obtaining the different performance measures:

- Exact calculation (ERAC)
- Upper bound approximation
- Monte Carlo (stochastic) simulation
- Numerical integration

- Hand calculation method

The methods are introduced below, however, the theory behind the various methods is described in the "Method Description", please refer to "TOP Event Calculations" on page 95. There, also the pros and cons with the different methods are discussed.

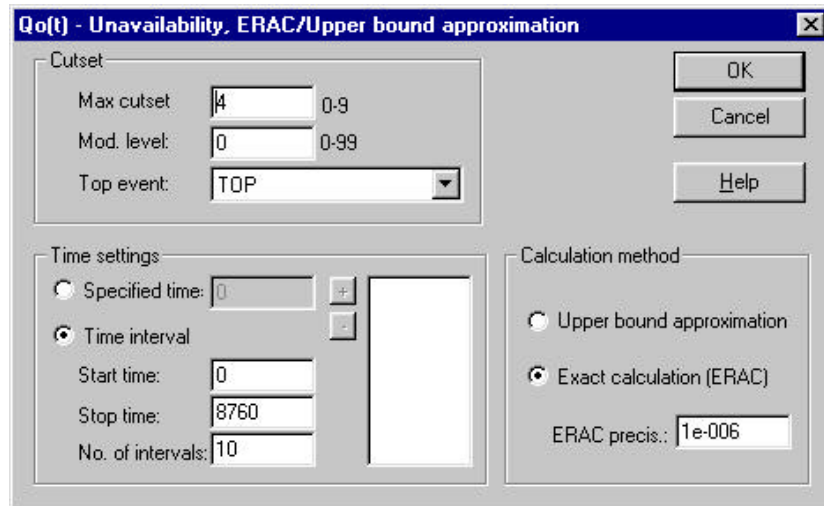
Each of the performance measures can typically be obtained using two or even three of the available calculation methods. "Methods for Calculating the Reliability Measures" on page 95 give an overview of the available combination of measures and methods.

When running in Expert user mode you need to select which of the methods to use. The required input parameters for the analyses depend on the selected calculation method only (that is not on the performance measure to be calculated). Thus, in the sections below the dialogs for the different methods are explained.

Have also in mind that some options relating to the analyses are set in the **Analysis tab** of the **Tree | Setup** dialog (please refer to page 49). Especially note the option for selecting between **Short** and **Long** report format. If the **Long** report format is selected, e.g. all the performance measures that can be found using the selected calculation method will be listed.

Exact Calculation (ERAC)/Upper Bound Approximation

The exact calculation (ERAC) and the upper bound approximation methods may be used to calculate the (time dependent) fault tree unavailability $Q_0(t)$ only. Both methods are explained in "Calculation of $Q_0(t)$ Using Exact Calculation (ERAC) and Upper Bound Approximation" on page 96. When you select either of these methods, the same dialog is given, see below.



Max. cut set size
Mod. level
TOP event

First, you need to specify the **Max. cut set size**, **Mod. level** and **TOP event** in order to obtain the cut sets to base the calculation on. The parameters required are identical to the ones for the **Analysis | List cut sets...** command, please refer to "Analysis | List cut sets..." on page 59.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Time settings

Next, you need to specify the **Time settings**, that is to calculate the (time dependent) fault tree unavailability $Q_0(t)$, you must specify the different points of time for which $Q_0(t)$ should be calculated. You have two options; **Specified time** or **Time interval**.

Specified time

When **Specified time** is selected, you enter the points of time one by one, separated by pushing the "+"-button (the plus sign). The points of time are added to the list of calculation values. To remove a selection from the list, make the point of time active, and press the "-"-button (the minus sign).

Time interval

When **Time interval** is selected, you enter the start and end time of the interval (**Start time** and **Stop time**), and the **No. of intervals** to be calculated.

Calculation method

Finally, you select which **Calculation method** to apply, either **Upper bound approximation** or **Exact calculation (ERAC)**. When running exact calculations, an upper and lower limit for $Q_0(t)$ is calculated. You may specify the **ERAC precision**, which is the acceptable relative error of the two. Note that the computing time will increase with a smaller relative error.

Monte Carlo (Stochastic) Simulation

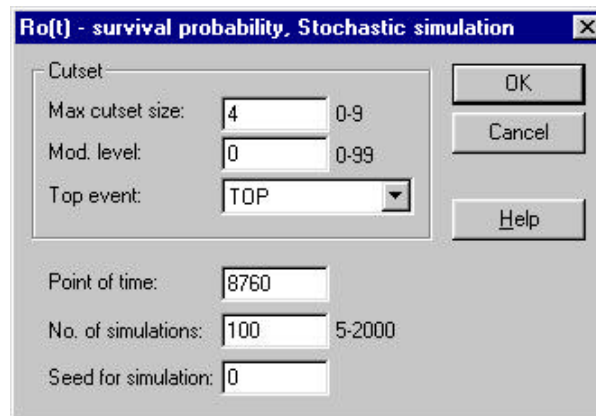
By Monte Carlo (stochastic) simulation you may among others calculate the survival probability - $R_0(t)$, the mean time to first failure (MTTF) and the relative frequencies of the TOP event.

Note! Dynamic tree required!

Note that to run the Monte Carlo simulation the fault tree must be dynamic (all the minimal cut sets must contain at least one Basic event with a time dependent q_i).

Please refer to "Calculation of $R_0(t)$, MTTF and $Freq(TOP)$ Using Monte Carlo (Stochastic) Simulation" on page 98 for a description of Monte Carlo (stochastic) simulation.

When you select the Monte Carlo simulation, the following dialog below is opened (here, assuming that you have selected it for calculating $R_0(t)$):



The dialog box is titled "Ro(t) - survival probability, Stochastic simulation". It contains the following fields and buttons:

- Cutset:**
 - Max cutset size: 4 (range 0-9)
 - Mod. level: 0 (range 0-99)
 - Top event: TOP (dropdown menu)
- Point of time:** 8760
- No. of simulations:** 100 (range 5-2000)
- Seed for simulation:** 0
- Buttons: OK, Cancel, Help

Max. cut set size

Mod. level

TOP event

First, you need to specify the **Max. cut set size**, **Mod. level** and **TOP event** in order to obtain the cut sets to base the calculation on. The parameters required are identical to the ones for the **Analysis | List cut sets...** command, please refer to "Analysis | List cut sets..." on page 59.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Next, you need to specify the **Point of time**, **No. of simulations** and the **Seed for simulation**.

Point of time

No. of simulations

All component failure and repair times are drawn from their respective distributions, and the system behaviour is simulated through the interval from $t=0$ to $t = \mathbf{Point\ of\ time}$. This is repeated **No. of simulations** times, and the quantity is calculated as the average over all replications.

Seed for simulation

The **Seed for simulation** determines the start up value for the random number generator when the failure and repair times are drawn. If the same calculation is performed twice with the same seed value, the exact same results will be calculated. If the seed values differ, the results will not be identical. Note that the default value for the seed will change each time a simulation is performed.

The results are presented with a standard error to reflect the uncertainty of the estimates. The standard error should be low relative to the estimate. A standard error of less than 1 % of the estimate should in most cases be regarded as acceptable. If the standard error is significantly larger than 1 %, consider re-running the calculations with a larger number of simulations.

Numerical Integration

Numerical integration may be used to calculate the survival probability - $R_0(t)$, the mean time to first failure (MTTF) and the expected number of failures within a time period - $E(\#fail.)$.

Note! Dynamic tree required!

Note that to run numerical integration, the fault tree must be dynamic (all the minimal cut sets must contain at least one component with a time dependent q_i).

Please refer to "Calculation of $R_0(t)$, MTTF and $E(\#failures)$ Using Numerical Integration" on page 99 for a description of the numerical integration method.

When you select the numerical integration method, the following dialog is opened (here, assuming that you have selected it for calculating $R_0(t)$):

The dialog box is titled "Ro(t) - survival probability. Numerical integration". It contains the following fields and controls:

- Cutset section:**
 - Max cutset size: 4 (range 0-9)
 - Mod. level: 0 (range 0-99)
 - Top event: TOP (dropdown menu)
- Buttons:** OK, Cancel, Help
- Point of time:** 8760
- No. of intervals:** 10 (range 1-200)
- Interval incr. ratio:** 1.1

Max. cut set size
Mod. level
TOP event

First, you need to specify the **Max. cut set size**, **Mod. level** and **TOP event** in order to obtain the cut sets to base the calculation on. The parameters required are identical to the ones for the **Analysis | List cut sets...** command, please refer to "Analysis | List cut sets..." on page 59.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Next, you need to specify the **Point of time**, **No. of intervals** and the **Interval incr. ratio**.

Point of time
No. of intervals

The system is investigated at times from $t=0$ to $t =$ **Point of time**. This time period is separated into **No. of intervals**. The number of intervals determines the precision; a higher number of intervals give good precision on the expense of calculation time.

Interval incr. ratio

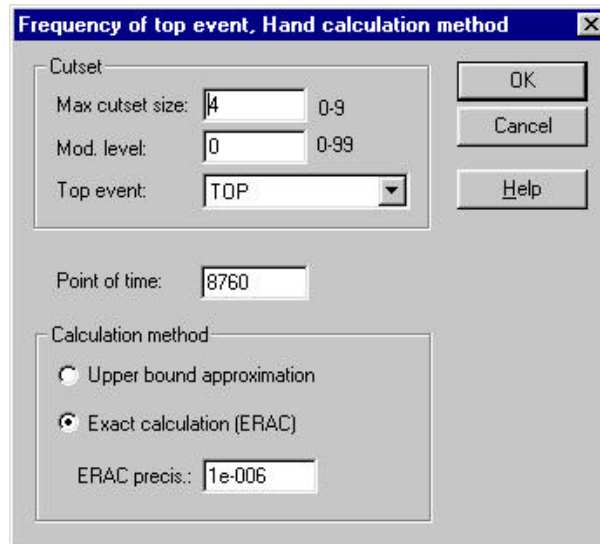
The integration kernel often changes rapidly in the beginning, and as t increases, it converges to its asymptotic constant value. The **Interval incr. ratio** controls the length of each interval, so that the intervals are shorter for small t - values, thus giving higher computation accuracy. A recommended value is 1.1 for the increase factor.

Hand Calculation Method

The Hand calculation method is used to calculate the frequency of the TOP event, $Freq(TOP)$.

Please refer to "Calculation of $Freq(TOP)$ Using the Hand Calculation Method" on page 101 for a description of the Hand calculation method.

When you select the Hand calculation method, the following dialog is opened:



Max. cut set size

Mod. level

TOP event

As for the other calculation methods, you need to specify the **Max. cut set size**, **Mod. level** and **TOP event** in order to obtain the cut sets to base the calculation on. The parameters required are identical to the ones for the **Analysis | List cut sets...** command, please refer to "Analysis | List cut sets..." on page 59.

Note that if you have already obtained the minimal cut sets in an analysis, and you specify identically the same cut sets to be found for the current analysis, the existing cut set listing will be used, saving calculation time.

Modularization not recommended

Note that it is recommended not to use modularization when using the hand calculation method. This is because complete cut sets are not obtained, and CARA-FaultTree can therefore not verify that the input data types are as required.

Point of time

The Hand calculation method is based on calculation of $Q_0(t)$. Hence, you next need to specify the **Point of time**.

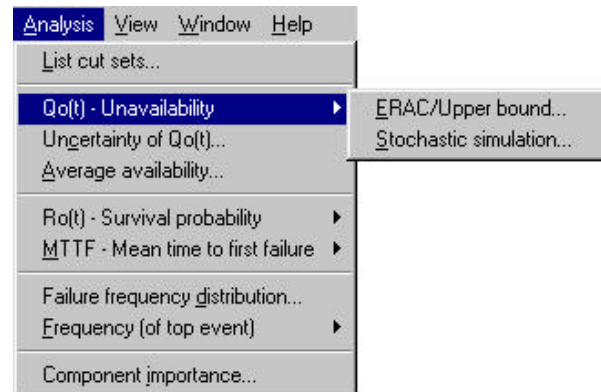
Calculation method

As explained in the method description (see "Calculation of $Freq(TOP)$ Using the Hand Calculation Method" on page 101), CARA-FaultTree offers two alternative methods for the situation when the minimal cut sets are not disjoint. Thus, you need to specify to use either the **Upper bound approximation** or **Exact calculation (ERAC)**. If the ERAC method is to be used, you also need to specify the **ERAC precision**.

Analysis | $Q_0(t)$ - Unavailability...

Select the **Analysis | $Q_0(t)$ - Unavailability...** command to calculate the probability of the TOP event occurring at a given point in time. Three alternative methods are available; Exact

calculation (ERAC), Upper bound approximation, or Monte Carlo (Stochastic) simulation, as seen from the analysis menu:



Please refer to “Analysis Methods and Input Parameters” on page 60 regarding the input parameter dialog when using the **ERAC/Upper bound...** or **Monte Carlo (Stochastic) simulation** respectively.

Normally the best method to use for calculation of $Q_0(t)$ is the Exact calculation, however also using the Upper bound approximation is widespread. Below, some further considerations regarding both these methods are given.

When using either of these two methods, the calculation of $Q_0(t)$, will be presented as a listing. Further, if you have selected Long report format (please refer to "Tree | Setup..." on page 47), also a plot of the TOP event probability as a function of mission time is presented.

If the fault tree that is analysed neither includes repairable components, nor components with on demand probabilities or frequencies, $Q_0(t)$ will converge on an unavailability of 1 as a function of time.

If either of these types of components are included in the fault tree, $Q_0(t)$ will converge on the mean unavailability of the system. The steady state performance of a system is typically reached for a mission time that is 3-5 times as long as the repair time of the critical components.

Analysis | Uncertainty of $Q_0(t)$...

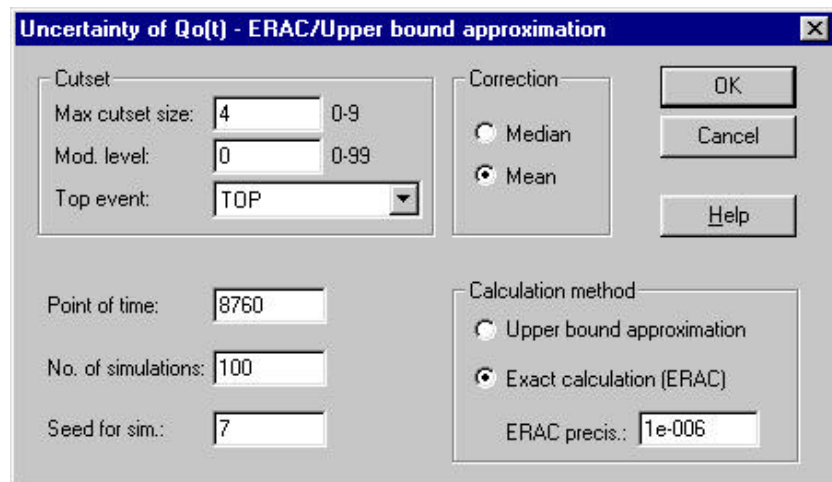
Select the **Analysis | Uncertainty of $Q_0(t)$...** command to calculate the effect the uncertainty in the failure data of the Input events has on the TOP event probability, $Q_0(t)$.

Generally, some kind of uncertainty will be associated with the failure data for the Input events. By means of Monte Carlo simulation, CARA-FaultTree calculates the resulting uncertainty in the TOP event probability. Refer to

"Uncertainty Analysis" on page 109 for detailed information on the calculation procedures.

Note that to be able to run the uncertainty analysis you must describe the uncertainty of the Input event data by means of the so-called error factors. Please refer to the method description, "Uncertainty Analysis" on page 109, regarding interpretation of the error factors. At least one error factor must be different from 1 if you want to run an uncertainty analysis.

Having selected the **Analysis | Uncertainty of $Q_0(t)$...** command, the following dialog is presented:



Cut set / Calculation method

You will see that the **Cut set** and **Calculation method** options are identical to the Exact calculation (ERAC)/Upper bound approximation. Thus, please refer to "**Exact Calculation (ERAC)/Upper Bound Approximation**" on page 61 for specification of these parameters.

*Point of time
No. of simulations
Seed for sim*

Further, the specification of the **Point of time**, **No. of simulations** and **Seed for sim.** are identical to the Monte Carlo simulation. Thus, please refer to "

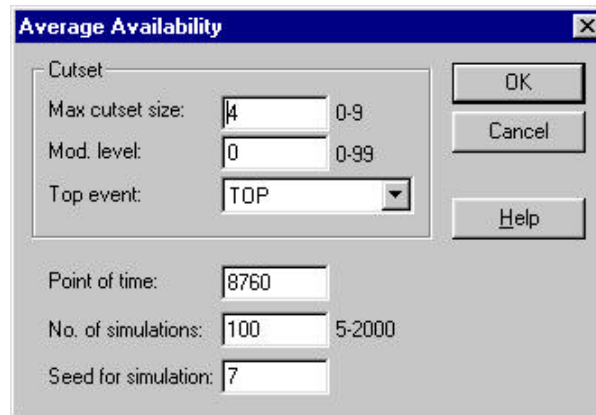
Monte Carlo (Stochastic) Simulation" on page 63 for specification of these parameters.

Correction

As explained in the method description, ("Uncertainty Analysis" on page 109), your estimates for the Input event data may be interpreted as either the **Median** or **Mean** of the log-normal distribution. Select the appropriate option for your data.

Analysis | Average Availability...

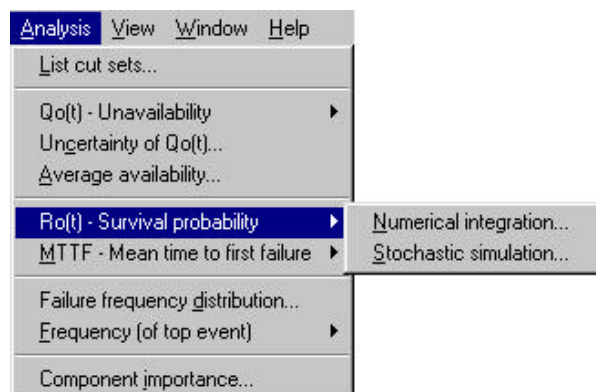
Select the **Analysis | Average Availability...** command to calculate the average system availability up to a given point in time. The “Average Availability” dialog will be displayed, see below:



The calculation of the **Average Availability** is done by Monte Carlo simulation. Thus, please refer to the “Monte Carlo (Stochastic) Simulation” section in “Analysis Methods and Input Parameters” on page 60 for a description of the input parameters.

Analysis | $R_0(t)$ - Survival probability...

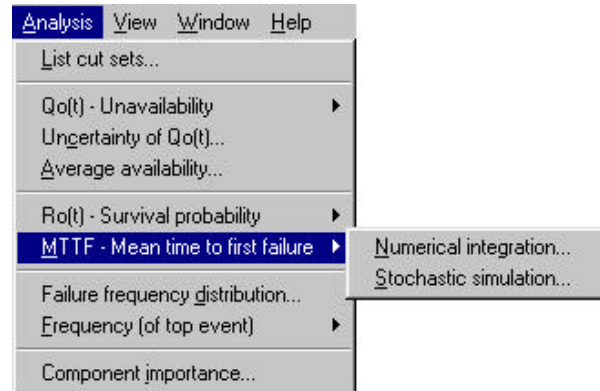
Select the **Analysis | $R_0(t)$ – Survival probability...** command to calculate the probability of not having experienced any system failure up to a given point in time. Two alternative methods are available; Numerical integration or Monte Carlo (Stochastic) simulation, as seen from the analysis menu:



Please refer to “Analysis Methods and Input Parameters” on page 60 regarding the input parameter dialog when using the **Numerical integration** or **Monte Carlo (Stochastic) simulation** respectively.

Analysis | MTTF - Mean time to first failure...

Select the **Analysis | MTTF – Mean time to first failure...** command to calculate the mean time to first system failure. Two alternative methods are available; Numerical integration or Monte Carlo (Stochastic) simulation, as seen from the analysis menu:

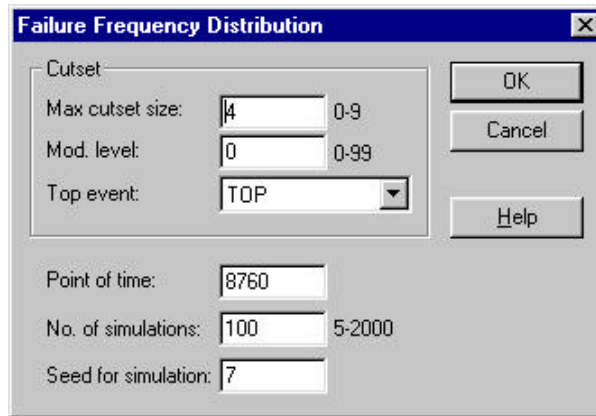


Please refer to “Analysis Methods and Input Parameters” on page 60 regarding the input parameter dialog when using the **Numerical integration** or **Monte Carlo (Stochastic) simulation** respectively.

If Monte Carlo (Stochastic) simulation is chosen, the average number of failures which occurred during the total number of simulations, should be close to or greater than 1 to get a robust estimate for MTTF. The estimated MTTF is based on an approximation formula if the mission time was too short for all the simulations to end with one or more failures. The formula will be displayed if a failure did not occur in more than 10% of the simulations.

Analysis | Failure Frequency Distribution...

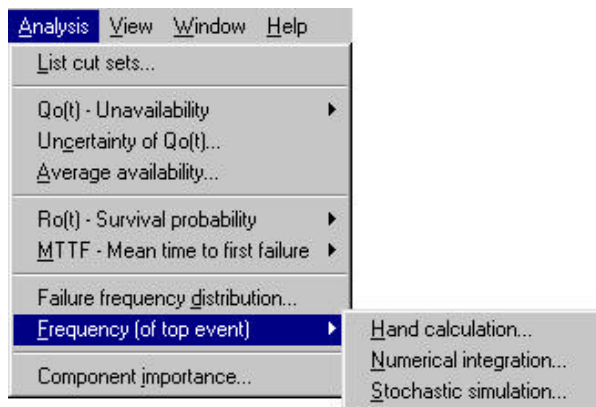
Select the **Analysis | Failure Frequency Distribution...** command to calculate the distribution of the TOP event frequency. The “Failure Frequency Distribution” dialog will be displayed, see below.



The calculation of the **Failure Frequency Distribution** is done by Monte Carlo simulation. Thus, please refer to the “Monte Carlo (Stochastic) Simulation” section in “Analysis Methods and Input Parameters” on page 60 for a description of the input parameters.

Analysis | Frequency of TOP event...

Select the **Analysis | Frequency of TOP event...** command to calculate the frequency of the TOP event. Three alternative methods are available; Hand calculation, Numerical integration or Monte Carlo (Stochastic) simulation, as seen from the analysis menu:



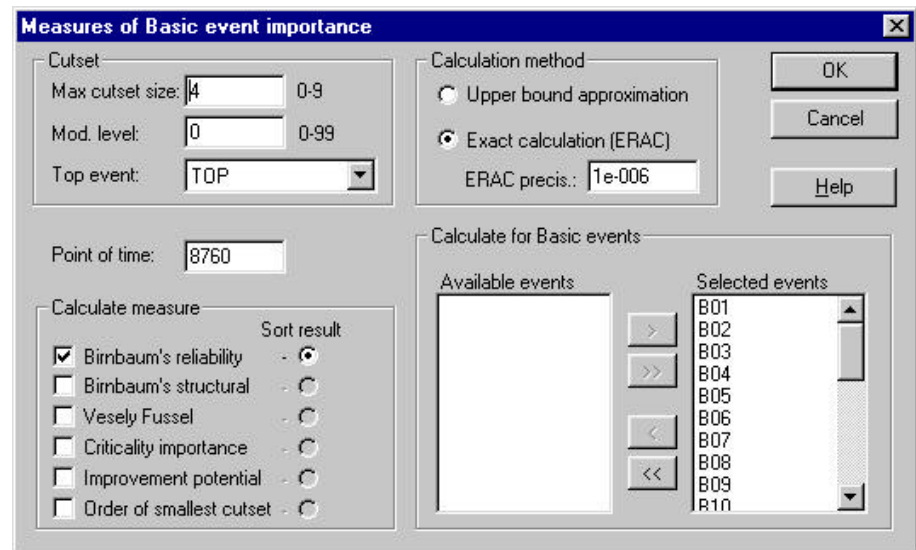
Please refer to “Analysis Methods and Input Parameters” on page 60 regarding the input parameter dialog when using the **Hand calculation method**, **Numerical integration** or **Monte Carlo (Stochastic) simulation** respectively.

Analysis | Component Importance...



Select the **Analysis | Component Importance...** command to calculate various importance measures for the Basic/Input events. An introduction to the various importance measures is given in "Measures of Importance" on page 105.

Selecting this command the “Measures of Basic event importance” dialog will be displayed:



Cut set / Calculation method

You will see that the **Cut set** and **Calculation method** options are identical to the Exact calculation (ERAC)/Upper bound approximation. Thus, please refer to the “Exact Calculation (ERAC)/Upper Bound Approximation” section in “Analysis Methods and Input Parameters” on page 60 for a description of the input parameters.

Point of time

To calculate reliability measures (i.e. measures also dependent on failure data), a **Point of time** is required.

Calculate measure

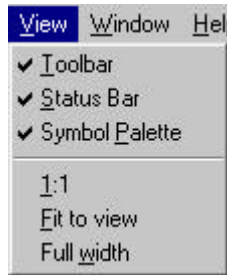
In the **Calculate measure** options you specify which of the offered measures to include in the calculations. Selecting more than one measure, you are allowed to specify which of the measures to **Sort results** on.

Calculate for Basic events

With the **Calculate for Basic events** option you are allowed to select whether to calculate the measures for all or only selected Basic/Input events. Initially all events are selected and listed **Selected events**. You may then select/deselect individual events or all the events, as you desire. The single arrow-buttons move the single selected event from one list to the other, whereas the double arrow-buttons move all events from one list to the other.

3.7 View menu

With the **View** menu you can show and hide the toolbar, status bar and symbol palette, and control how you want the fault tree window displayed, see below.



View | Toolbar

Select the **View | Toolbar** command to show or hide the Toolbar. Please refer to "The Toolbar" on page 7 for more information on the Toolbar.

View | Status bar

Select the **View | Status bar** command to show or hide the Status bar at the bottom of the CARA-FaultTree window. The status bar will show short descriptions of the menu items when the user moves the marker in the menus, or descriptions of the command buttons when the user moves the mouse over the buttons.

View | Symbol Palette

Select the **View | Symbol palette** command to show or hide the CARA-FaultTree Symbol palette. Please refer to "Fault Tree Symbols" on page 14 for more information on the Symbol palette.

View | 1:1



The **View | 1:1** command sizes the fault tree page to the actual physical size. This size is defined as the 100 % zoom factor.

View | Fit to view



With the **View | Fit to view** command the whole fault tree page is displayed inside your CARA-FaultTree window.

View | Full width



With the **View | Full width** command, the fault tree page is displayed with the side edges fitting inside the CARA-FaultTree window.

3.8 Window menu

The **Window** menu contains commands to arrange windows on the screen and to toggle between open windows (fault trees), see below. The user can also arrange individual windows in the workspace by dragging them with the mouse.



Window | New window

The **Window | New window** command opens a new window of the current fault tree. If the window you activated the command from was a fault tree window, a new window with the same contents is opened. You may, however, navigate in the fault tree so that the two windows show different views of the same fault tree. If the window you activated the command from was a report window, a new blank report window is opened.

Window | Cascade

The **Window | Cascade** command displays all windows. The window is displayed overlapping each other. Use this command to arrange all windows on the screen or to show windows that may have been hidden.

Window | Tile Horizontal

The **Window | Tile horizontal** command arranges open windows in small sizes to fit on the screen. The windows are stacked evenly in size from top to bottom.

Window | Tile Vertical

The **Window | Tile vertical** command arranges open windows in small sizes to fit on the screen. The windows are stacked evenly in size from left to right.

Window | Arrange Icons

The **Window | Arrange icons** command arranges all the minimised windows. The command is available only when a

minimised window is active. All icons will be arranged horizontally from left to right at the left bottom of the CARA-FaultTree window.

The 1, 2, 3 ... Window command

The **Window** menu also contains a list of all opened windows. You may switch to another window by selecting it from the list, or by typing the number preceding the window name.

3.9 Help menu

The help menu is the online Users Guide and Method Description, see below.



Help | Contents

The **Help | Contents** command opens the table of contents for the Help system. The Help content is almost identical to the Table of Contents of this User's Manual.

Help | Search...

The **Help | Search...** command opens a dialog for searching in the Help system. Start writing the command or word you are looking for and the help system will narrow your search while you write.

Help | Symbol Guide

The **Help | Symbol guide** command gives you online access to the symbol guide of this manual.

Help | About CARA-FaultTree...

The **Help | About CARA-FaultTree...** command shows the CARA-FaultTree about box. It gives information of Copyright and version numbers of CARA-FaultTree.

4. Method Description

4.1 Introduction to the Fault Tree Method

4.1.1 History

The fault tree technique was introduced in 1962 at the Bell Telephone Laboratories, in connection with a safety evaluation of the launching system for the intercontinental Minuteman missile. The Boeing Company improved the technique and introduced computer programs for both qualitative and quantitative fault tree analyses. Today fault tree analysis is by far the most commonly used technique of risk and reliability studies. Fault tree analysis has particularly been used with success to analyse safety systems in nuclear power stations, e.g. during the Reactor Safety Study, WASH-1400 (US Atomic Energy Commission, 1974).

4.1.2 The Fault Tree Technique

A fault tree is a logic diagram that displays the interrelationships between a potential critical event (accident) in a system and the reasons for this event. The reasons may be environmental conditions, human errors, normal events (events which are expected to occur during the life span of the system) and specific component failures. A properly constructed fault tree provides a good illustration of the various combinations of failures and other events that can lead to a specified critical event. The fault tree is easy to explain to engineers without prior experience of fault tree analysis.

An advantage with a fault tree analysis is that the analyst is forced to understand the failure possibilities of the system, to a detailed level. A lot of system weaknesses may thus be revealed and corrected during the fault tree construction

A fault tree is a *static* picture of the combinations of failures and events that can cause the TOP event to occur. Fault tree analysis is thus not a suitable technique for analysing dynamic systems, like switching systems, phased mission systems and systems subject to complex maintenance strategies.

A fault tree analysis may be qualitative, quantitative or both, depending on the objectives of the analysis. Possible results from the analysis may e.g. be:

- A listing of the possible combinations of environmental factors, human errors, normal events and component failures that can result in a critical event in the system.
- The probability that the critical event will occur during a specified time interval.

The analysis of a system by the fault tree technique is normally carried out in five steps:

1. Definition of the problem and the boundary conditions.
2. Construction of the fault tree.
3. Identification of minimal cut and/or path sets.
4. Qualitative analysis of the fault tree.
5. Quantitative analysis of the fault tree.

It is the purpose of this method description to describe main aspects of the theory and practice of fault trees, emphasising the options available in CARA-FaultTree.

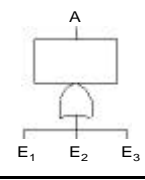
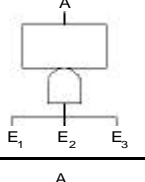
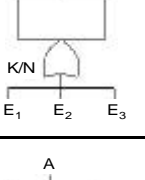
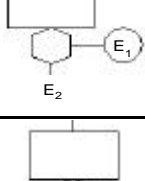






Fault tree analysis is thoroughly described in the literature, see "List of References" on page 113.

4.2 Fault Tree Construction

4.2.1 Fault Tree Diagram, Symbols and Logic

A fault tree is a logic diagram that displays the connections between a potential system failure (TOP event) and the reasons for this event. The reasons (Basic/Input events) may be environmental conditions, human errors, normal events and component failures. The graphical symbols used to illustrate these connections are called "logic gates". The output from a logic gate is determined by the input events.

The appearance of the fault tree symbols is dependent on what standard we choose to follow. Fault tree symbols shown in the table below are according to the most commonly used standard, and are also the symbols used in CARA-FaultTree.

	Symbol	Description
Logic gates	Or-gate 	The OR-gate indicates that the output event A occurs if any of the input events E_i occur.
	And-gate 	The AND-gate indicates that the output event A occurs only when all the input events E_i occur simultaneously.
	KooN-gate 	The KooN-gate indicates that the output event A occurs if K or more of the input events E_i occurs.
	Inhibit-gate 	The INHIBIT gate indicates that the output event A occurs if both the conditional event E_1 and the input event E_2 occur.
Input events	Basic event 	The Basic event represents a basic equipment fault or failure that requires no further development of failure causes.
	House event 	The House event represents a condition or an event which is TRUE (ON) or FALSE (OFF) (not true).
	Undeveloped event 	The Undeveloped event represents a fault event that is not examined further because information is unavailable or because its consequence is insignificant.
Description of state	Comment rectangle 	The Comment rectangle is for supplementary information.
Transfer symbols	Transfer down 	The Transfer down symbol indicates that the fault tree - - is developed further at the occurrence of the corresponding Transfer up symbol.
	Transfer up 	

4.2.2 Definition of the Problem and the Boundary Conditions

Definition of the problem and the boundary conditions consists of:

- Definition of the critical event (the accident) to be analysed.
- Definition of the boundary conditions for the analysis.

The critical event (accident) to be analysed is normally called the TOP event. It is very important that the TOP event is given a clear and unambiguous definition. If not, the analysis will often be of limited value. As an example, the event description “Fire in the plant” is far too general and vague. The description of the TOP event should always answer the questions: **What, where** and **when**.

- **What:** Describes what type of critical/undesired event that occurs, e.g. fire.
- **Where:** Describes where the critical/undesired event occurs, e.g. in the process oxidation reactor.
- **When:** Describes when the critical/undesired event occurs, e.g. during normal operation.

A more precise TOP event description is thus: “Fire in the process oxidation reactor during normal operation”.

To get a consistent analysis, it is important that the *boundary conditions* for the analysis are carefully defined. By boundary conditions we mean:

- **The physical boundaries of the system.** What parts of the system are to be included in the analysis, and what parts are not?
- **The initial conditions.** What is the operational state of the system when the TOP event occurs? Is the system running on full/reduced capacity? Which valves are open/closed, which pumps are functioning etc.?
- **Boundary conditions with respect to external stresses.** What type of external stresses should be included in the analysis? By external stresses we here mean stresses from war, sabotage, earthquake, lightning etc.

- **The level of resolution.** How far down in detail should we go to identify potential reasons for a failed state? Should we as an example be satisfied when we have identified the reason to be a “valve failure”, or should we break it further down to failures in the valve housing, valve stem, actuator etc.? When determining the required level of resolution, we should remember that the detail in the fault tree should be comparable to the detail of the information available.

4.2.3 Construction of the Fault Tree

The fault tree construction always starts with the TOP event. We must thereafter carefully try to identify all fault events that are the immediate, necessary and sufficient causes that result in the TOP event. These causes are connected to the TOP event via a logic gate. It is important that the first level of causes under the TOP event is developed in a structured way. This first level is often referred to as the TOP structure of the fault tree. The TOP structure causes are often taken to be failures in the prime modules of the system, or in the prime functions of the system. We then proceed, level by level, until all fault events have been developed to the required level of resolution. The analysis is in other words deductive and is carried out by repeated asking “*What are the reasons for...?*”

Rules for Fault Tree Construction

Description of the fault events

Each of the Basic/Input events must be carefully described (*what, where, when*) in a “rectangle”.

Evaluation of the fault events

Component failures may be divided in three groups: primary failures, secondary failures and command faults.

- A primary failure is a failure caused by natural ageing of the component. The primary failure occurs under conditions within the design envelope of the component. A repair action is necessary to return the component to a functioning state
- A secondary failure is a failure caused by excessive stresses outside the design envelope of the component. A repair action is necessary to return the component to a functioning state.

- A command fault is a failure caused by an improper control signal or noise. A repair action is usually not required to return the component to a functioning state. Command faults are often referred to as transient failures. The “normal” Basic/Input events in a fault tree are primary failures identifying the equipment that is responsible for the failure. Secondary failures and command faults are intermediate events that require a further investigation to identify the prime reasons.
- When evaluating a fault event, we ask the question “can this fault be a primary failure?”. If the answer is “yes”, we classify the fault event as a “normal” Basic event. If the answer is “no”, we classify the fault event as either an intermediate event which has to be further developed, or as a “secondary” Basic/Input event. The “secondary” Basic/Input event is often called an “Undeveloped” event and represents a fault event that is not examined further because information is unavailable or because its consequence is insignificant.

The gates shall be completed

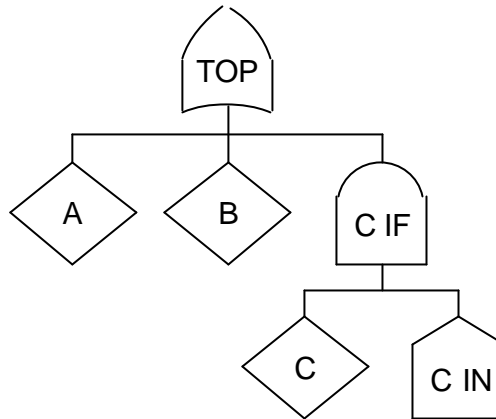
All inputs to a specific gate should be completely defined and described before proceeding downwards to the next level. The fault tree should be completed in levels, and each level should be completed before beginning the next level.

4.2.4 Using the House event

The House event is a special event type that needs some explanation and guidance. The House event represents a condition or an event that is either TRUE (ON) or FALSE (OFF).

The most typical use of this event type is as a “switch” in the fault tree, to switch parts of the tree on or off depending on which system state or operating condition to be analysed. Say, as an example, that a system consists of three subsystems (A, B and C), and that all subsystems normally need to work for the system to work. Assume further that the subsystem C is not required under some of the operating conditions.

To model the above situation requires two slightly different fault trees, however using a House event this may be obtained in the same fault tree, see example fault tree and explanation below.



In the fault tree above, the two subsystems A and B are connected directly to the TOP event (OR-gate). Here, each subsystem is simply represented by the Undeveloped events “A”, “B” and “C”. Subsystem C is connected via an AND-gate (“C IF”), and the AND-gate having a House event (“C IN”) as the other input.

The two different operating conditions, that is including/not including subsystem C, are now analysed by switching the House event ON or OFF. Having the House event switched ON (TRUE), the “C IF” gate (being an AND-gate) will be true if “C” is true, and false if “C” is false. Thus, having the House event switched ON, subsystem C is included identical to the subsystems A and B. Having the House event switched OFF (FALSE), the “C IF” gate will never be true since it is an AND-gate. Thus, having the House event switched OFF, subsystem C is not included in the analysis.

4.3 Identification of Minimal Cut and Path Sets

4.3.1 Definition of Cut- and Path Sets

A fault tree provides valuable information about possible combinations of fault events that can result in a critical failure (TOP event) of the system. Such a combination of fault events is called a cut set.

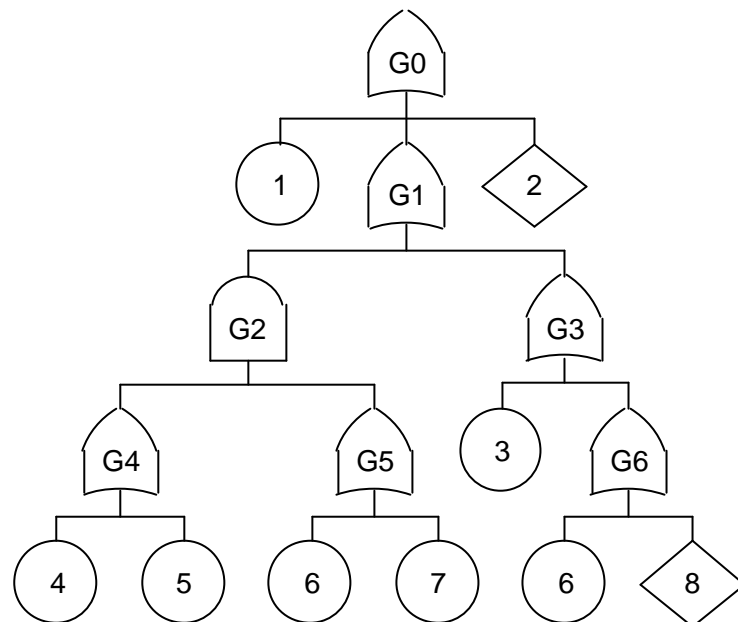
*A **cut set** in a fault tree is a set of Basic events whose (simultaneous) occurrence ensures that the TOP event occurs. A cut set is said to be **minimal** if the set cannot be reduced without losing its status as a cut set.*

*A **path set** in a fault tree is a set of Basic events whose non-occurrence (simultaneous) ensures that the TOP event does not occur. A path set is said to be **minimal** if the set cannot be reduced without losing its status as a path set.*

For small and simple fault trees, it is feasible to identify the minimal cut- and path sets by inspection without any formal procedure/algorithm. For large or complex fault trees we need an efficient algorithm. The algorithm MOCUS, to be described next, is used in an improved version [8] by CARA-FaultTree.

4.3.2 MOCUS - method for obtaining cut sets

MOCUS (*Method for obtaining cut sets*) is an algorithm that can be used to find the minimal cut and path sets in a fault tree. The simplest way to explain the algorithm is to demonstrate it on an example. In the fault tree below, all the gates are numbered from G0 to G6.



The algorithm starts with the gate G0 being the TOP event. If this is an OR-gate each input to the gate is written under each other (the inputs may be new gates).

In our example, G0 is an OR-gate and so we start writing:

```

1
G1
2
  
```

If G0 had been an AND-gate, we should have written the inputs as the first row in a matrix. We would then have started writing:

```

1, G1, 2
  
```

Since in the case with an AND-gate each of the three inputs, 1, G1 and 2 will cause the TOP event to occur, each of them will form a cut set.

The idea is to gradually replace each gate with its inputs (Basic events and new gates) until one has gone through the whole fault tree and is left with Basic events.

It is now easy to realise that the rows in the resulting matrix represent the cut sets in the fault tree.

Since G1 is an OR-gate, the next step is to write:

1
G2
G3
2

Since G2 is an AND-gate we now write:

1
G4, G5
G3
2

And since G3 is an OR-gate:

1
G4, G5
3
G6
2

Since G4 is an OR-gate:

1
4, G5
5, G5
3
G6
2

Since G5 is an OR-gate:

1
4, 6
4, 7
5, 6
5, 7
3
G6
2

Finally, since G6 is an OR-gate we write:

1
4, 6
4, 7
5, 6
5, 7
3
6
8
2

We are then left with the following 9 cut sets:

$\{1\}$, $\{2\}$, $\{3\}$, $\{6\}$, $\{8\}$, $\{4,6\}$, $\{4,7\}$, $\{5,6\}$ and $\{5,7\}$

Since $\{6\}$ is a cut set, the cut sets $\{4,6\}$ and $\{5,6\}$ are not minimal. If we leave these out, we are left with the following list of *minimal* cut sets:

$\{1\}$, $\{2\}$, $\{3\}$, $\{6\}$, $\{8\}$, $\{4,7\}$ and $\{5,7\}$.

The reason that the algorithm in this case leads to non-minimal cut sets is that the Basic event 6 occurs several places in the fault tree.

To find the minimal *path sets* in the fault tree, we may start with the so-called *dual fault tree*. This can be obtained by replacing all the AND-gates in the original fault tree with OR-gates and vice versa. In addition, we let the events in the dual fault tree be complements to the corresponding events in the original fault tree. The same procedure as described above applied on the dual fault tree will now yield the minimal path sets.

4.4 Qualitative Evaluation of the Fault Tree

4.4.1 Conditions for Qualitative Evaluation of the Fault Tree

A qualitative evaluation of the fault tree may be carried out on the basis of the minimal cut sets. The importance of a cut set depends obviously on the number of Basic events in the cut set. The number of different Basic events in a minimal cut set is called the *order* of the cut set. A cut set of order one is usually more critical than a cut set of order two, or higher. When we have a cut set with only one Basic event, and the TOP event will occur as soon as this Basic event occurs. If a cut set has two Basic events, both of these have to occur at the same time to cause the TOP event to occur.

Another important factor is the type of Basic events in a minimal cut set. We may rank the criticality of the various cut sets according to the following ranking of the Basic events:

1. Human error
2. Failure of active equipment
3. Failure of passive equipment

The ranking is based on the assumption that human errors occur more frequently than active equipment failures, and that active equipment is more failure-prone than passive equipment (an active or running pump is for example more exposed to failures than a passive standby pump).

4.4.2 Criticality Ranking of Minimal Cut Sets

Based on the ranking discussed above, we get the ranking of the criticality of minimal cut sets of order two as shown in the table below.

Rank	Basic event no. 1 (type)	Basic event no. 2 (type)
1	Human error	Human error
2	Human error	Active equipment failure
3	Human error	Passive equipment failure
4	Active equipment failure	Active equipment failure
5	Active equipment failure	Passive equipment failure
6	Passive equipment failure	Passive equipment failure

4.5 Quantitative Analysis of the Fault Tree

4.5.1 Available System Reliability Measures in CARA-FaultTree

When reliability data for each of the Basic events is available, it is possible to carry out a quantitative evaluation of the fault tree. Quantitative analyses of fault trees are available from the Analysis menu. In this section, an introduction to the various system reliability measures available in CARA-FaultTree is given.

To be able to calculate the system reliability measures it is necessary to enter reliability data for the Basic events. Please refer to "Input Data to the Fault Tree" on page 92 for more information on this. Further, "TOP Event Calculations" on

page 95 explains how CARA-FaultTree calculates the different system reliability measures. Please refer to [2], [4], and [7] in the "List of References" on page 113 for a more detailed introduction to quantitative fault tree analysis.

The different system reliability measures available in CARA-FaultTree are listed in the table below, and further discussed below.

Further, note that CARA-FaultTree also calculates the unavailability and importance at *cut set level*. This is explained in "Quantitative ranking of minimal cut sets" on page 91.

Reliability measure	Description
$Q_0(t)$	The probability that the TOP event occurs at time t
$R_0(t)$	The probability that the TOP event does not occur in $[0,t)$
MTTF	Mean time to first system failure
Freq distr.	Distribution of TOP event frequency
$Freq(TOP)$	Frequency of the TOP event
$E(\#failures)$	Expected number of failures within a time period
$A_{0,av}(t)$	Average system availability in $[0,t)$

4.5.2 The probability that the TOP event occurs at time t - $Q_0(t)$

$Q_0(t)$ is the probability that the TOP event occurs at time t . If the state of each component in the fault tree is known at time t , then the state of the TOP event can also be determined regardless of what has happened up to time t . Hence $Q_0(t)$ is uniquely determined by the $q_i(t)$'s.

Note here that we use the term *component* instead of *input event* because it is natural to think about the occurrence of an input event as a component failure. In other situations, e.g. when the input event represent a *human error*, this is not obvious, however.

If all components have failure data of the category *on demand probability*, the $q_i(t)$'s are constant with respect to the time, hence $Q_0(t)$ is also time invariant (please refer to "Input Data to the Fault Tree" on page 92 for information on failure data categories). If at least one component in each minimal cut set has data of the category *repairable unit* or *non-repairable*

unit, the corresponding $q_i(t)$'s will increase from $q_i(0) = 0$ to some asymptotic value $q_i(\infty) \leq 1$ implying $Q_0(t)$ to increase from $Q_0(0) = 0$ to $Q_0(\infty) \leq 1$.

It makes no sense to obtain values for $Q_0(t)$ when components with failure data of category *frequency* are used. Components with failure data of category *frequency* are assumed to function at time t with probability one (*duration* of occurrence equals zero). Thus minimal cut sets with such components are also assumed to function at time t with probability one.

4.5.3 The probability that the TOP event does not occur in $[0, t)$ - $R_0(t)$

$R_0(t)$ is the probability that the TOP event has *not* occurred in the time period from 0 to t , i.e. the probability that the system has survived up to time t .

Unlike $Q_0(t)$, $R_0(t)$ does depend on what has happened up to time t , and not only the situation at time t . We will illustrate this by considering a system with two components A and B in parallel. This corresponds to two components connected with an AND-gate. The TOP event occurs if both A and B occurs at time t , hence

$$Q_0(t) = q_A(t) \cdot q_B(t)$$

To determine whether the TOP event does occur one or several times up to time t , it is not sufficient to know that both components have failed one or several times up to time t . This because the TOP event will *not* occur if one of the components is functioning while the other is repaired.

As a special case, when *all* components have failure data of category *non-repairable unit*, we have

$$R_0(t) = 1 - Q_0(t)$$

It makes no sense to calculate $R_0(t)$ if one or more cut sets only contain components with failure data of category *on demand probability* or *test interval*.

4.5.4 Mean time to first system failure - MTF

MTTF is the mean time to the *first* occurrence of the TOP event. MTTF is always greater or equal to the mean time *between* failures, MTBF. This is because all components are assumed to function at time t , but this assumption cannot be made when the system has been restored after a system failure.

As for $R_0(t)$, it makes no sense to calculate MTTF if one or more cut sets only contains components with failure data of category *on demand probability* or *test interval*.

4.5.5 E(# failures)/Freq(TOP)/Freq distr

The frequency of the TOP event is the expected number of occurrences of the TOP event in a period of time, for example:

$$Freq(TOP) = 2 \text{ occurrences per year.}$$

Note that the number of occurrences of the TOP event, say X , in a given period of time, is a *random number*. We may be interested in obtaining the *distribution* of X as well as the *expected value* of X , $E(X)$. Thus the notation $Freq(TOP)$ is not always clear, in some situations we mean the distribution of X , in other situations we mean $E(X)$. The distribution of X is determined by the probabilities $P(X=0)$, $P(X=1)$, $P(X=2)$ etc., and the expected value of X is given by:

$$E(X) = \sum_{i=0}^{\infty} i \cdot P(X = i) \quad (1)$$

If the times between consecutive occurrences of the TOP event are *exponentially* distributed, then the number of failures X , in a unit period of time will be *Poisson* distributed with parameter $\lambda = 1/E(X)$ and the distribution of X is given by:

$$P(X = i) = \frac{\lambda^i}{i!} e^{-\lambda} \quad (2)$$

Note that it is *not* possible to obtain the frequency of the TOP event if one or more of the minimal cut sets only contain components with failure data of category *on demand probability* or *test interval*. In this situation the probability of occurrence of the minimal cut set is *constant*, and hence it does not make sense to speak about the frequency of failure of this cut set.

A common situation when the frequency of the TOP event applies, is when one and only one component in each minimal cut set has failure data of category *frequency*. As an example, consider a system with two components A and B in parallel. Component A has data of failure category *frequency*, say f_A , and component B has failure data of category *on demand probability*, say q_B . We then have:

$$Freq(TOP) = f_A \cdot q_B \quad (3)$$

This will be a typical situation when A is an undesired event and B is a barrier. Please refer to the Hand Calculation Method in "Calculation of $Freq(TOP)$ Using the Hand Calculation Method" on page 101 for further discussion of this situation.

4.5.6 Average system availability in $[0,t)$ - $A_{0,av}(t)$

$A_{0,av}(t)$ is the fraction of time the system is available in the time period from 0 to t . $A_{0,av}(t)$ will always be greater or equal to $1-Q_0(t)$ because the system is more available at time 0 than for a time greater than 0, thus the availability in the period up to t , is greater than the availability at time t , $1-Q_0(t)$.

4.5.7 Quantitative ranking of minimal cut sets

When cut sets are found, CARA-FaultTree also calculates some measures to rank the cut sets quantitatively.

Cut set Unavailability

The *cut set unavailability* quantifies the probability that a given cut set is in failed state at a time t .

The cut set unavailability is calculated as:

$$\check{Q}_j = \prod_{i \in K_j} q_i(t) \quad (4)$$

Here K_j denotes all components in the minimal cut set j .

Cut set Importance

The *cut set importance* can be interpreted as the conditional probability that minimal cut set j is failed at time t , given that the system is failed at time t .

The cut set importance is calculated as:

$$I^{CI}(j) = \frac{\check{Q}_j}{Q_0(t)} \quad (5)$$

4.5.8 Notation for Describing Reliability Measures

In the table below, an overview of the notation used when describing reliability measures is given:

Notation	Description
$Q_0(t)$	P(the TOP event occurs at time t)
$Q_j(t)$	P(cut set j occurs at time t)
$R_0(t)$	P(the TOP event does not occur in $[0,t)$)
MTTF	Mean time to first system failure
$Freq(TOP)$	Frequency of the TOP event
$E(\#fail.)$	Expected number of failures within a time period
$A_{0,av}(t)$	Average system availability in $[0,t)$
$q_i(t)$	P(i 'th component is not functioning at time t)
I_i	Failure rate, i 'th component, i.e. expected number of failures of i 'th component per 10^6 hours
f_i	Frequency of i 'th input event, i.e. expected number of occurrences of i 'th input event per 10^6 hours
τ_i	Mean time to repair, MTTR, for i 'th component (in hours)
t^*	Length of test interval for components periodically tested (in hours)
$I^B(i t)$	Birnbaum's Measure of Reliability Importance
$I^{VF}(i t)$	Vesely-Fussell's Measure of Reliability Importance
$I^P(i t)$	Improvement Potential Reliability Measure
$I^{CR}(i t)$	Criticality Importance Reliability Measure
$I^O(i)$	Order of smallest cut set
$B_\phi(i)$	Birnbaum's Measure of Structural Importance.
$I^{CI}(j)$	Cut set importance of cut set j

4.6 Input Data to the Fault Tree

4.6.1 Category of Failure Data for Input Events

The crucial factors in the quantitative evaluation of the fault tree are the reliability data for the Input events. CARA-FaultTree differentiates, in addition to the special House event, between five different categories of failure data for input events:

- Frequency
- On demand probability
- Test interval
- Repairable unit
- Non repairable unit

In the table below, the different categories are listed:

Failure data category	Reliability parameters
House event	ON/OFF
Frequency	$f = \text{Frequency}^{1)}$
On demand probability	$q = \text{Probability}$
Test interval	$t^* = \text{Test interval}^{2)}$, $\tau = \text{Repair time}^{2)}$ and $\lambda = \text{Failure rate}^{3)}$
Repairable unit	$\tau = \text{Repair time}^{2)}$ and $\lambda = \text{Failure rate}^{3)}$
Non repairable unit	$\lambda = \text{Failure rate}^{3)}$

- 1) Expected number of occurrences per hour.
- 2) To be specified in hours.
- 3) Expected number of failures per hours / per 10^6 hours

4.6.2 Frequency

Frequency is used to describe events occurring now and then, but with no duration. Thus the *probability* that the event occurs at time t , $q_i(t) = 0$. The reliability data entered to CARA-FaultTree is the expected number of times the event will occur in a time period of one hour.

Note! If there is a *duration* of the event, the event should be described as a *repairable unit*, where the failure rate equals the frequency of the event, and the repair time equals the duration.

4.6.3 On Demand Probability

On demand probability is usually used to describe components *not* activated during normal operation. The component is demanded only now and then. The reliability data entered to CARA-FaultTree is the probability that the component is not able to perform its function upon request. In safety systems, the *operator* is often modelled by an *on demand probability*, for example: *Operator fails to activate manual shut-down system.*

4.6.4 Test interval

Test interval is used to describe components that are tested periodically with test interval t^* . A failure may occur

anywhere in the test interval. The failure will, however, not be detected until the test is carried out or the component is needed. This is a typical situation for many types of detectors, process sensors and safety valves. The probability $q_i(t)$ in this situation often referred to as the mean fractional dead-time, MFDT. The reliability parameters entered are the failure rate λ (expected number of failures per hour), the test interval t^* (in hours) and the repair time τ (in hours). CARA-FaultTree calculates the MFDT by the formula:

$$q_i(t) \approx \frac{\lambda t^*}{2} + \frac{t}{t^*} \quad (6)$$

Note that this formula only is valid if we have *independent* testing of each component. If components are tested *simultaneously*, or if we have *staggered* testing, this formula will not be correct.

4.6.5 Repairable Unit

Repairable unit is used for components that are repaired when a failure occurs. If the failure rate is denoted λ and the mean time to repair (MTTR) is denoted τ , then CARA-FaultTree computes $q_i(t)$ by the formula:

$$q_i(t) = \frac{\lambda t}{1 + \lambda t} (1 - e^{-\frac{(1 + \lambda t)\tau}{t}}) \quad (7)$$

Note that by letting t tend to infinity, we obtain the well-known approximation:

$$q_i(t) = \frac{MTTR}{MTTR + MTTF} \quad (8)$$

where

$$MTTF = \frac{1}{\lambda} \quad (9)$$

The reliability parameters entered to CARA-FaultTree are the failure rate λ (expected number of failures per hour) and the mean time to repair, $MTTR = \tau$ (in hours).

4.6.6 Non repairable unit

Non repairable unit is used for components that are not repaired when a failure occurs. If the failure rate of the component is denoted by λ , then:

$$q_i(t) = 1 - e^{-\lambda t} \quad (10)$$

The reliability parameter entered to CARA-FaultTree is the failure rate λ (expected number of failures per hour).

4.7 TOP Event Calculations

4.7.1 Methods for Calculating the Reliability Measures

Available Methods for Calculation of Different Reliability Measures

The various system reliability measures available in CARA-FaultTree were discussed in "Available System Reliability Measures in CARA-FaultTree" on page 87. This section discusses how CARA-FaultTree calculates these various measures. An overview of combination of measures and methods is given in the table below. Note that the analysis in CARA-FaultTree is done under the assumption that *the input events are stochastically independent*.

Measure Method	$Q_0(t)$	$R_0(t)$	MTTF	Freq distr.	$Freq(TOP)$ $E(\#fail.)$	$A_{0,av}(t)$
Exact (ERAC)/ Upper bound	X					
Monte Carlo simulation	X	X	X	X	X	X
Numerical integration		X	X		X	
Hand calcula- tion method					X	

Legal Combinations of Reliability Measures and Failure Data Categories

When calculating the different reliability measures there are some limitations with respect to the categories of the input data. For example it does not make sense to calculate the mean time to failure of a system with only *on demand probability* type of data. The legal combinations are given in the table below.

Measure Method	$Q_0(t)$	$R_0(t)$	MTTF	Freq distr.	$Freq(TOP)$ $E(\#fail.)$	$A_{0,av}(t)$
Frequency		X ¹⁾	X ¹⁾	X ¹⁾	X ¹⁾	
On demand probability	X	X ²⁾	X ²⁾	X ²⁾	X ²⁾	X ²⁾
Test interval	X	X ²⁾	X ²⁾	X ²⁾	X ²⁾	X ²⁾
Repairable unit	X	X ¹⁾	X ¹⁾	X ¹⁾	X ¹⁾	X
Non repairable unit	X	X ¹⁾	X ¹⁾	X ¹⁾	X ¹⁾	X

- 1) Each minimal cut set must contain one or more components with failure data of category *frequency*, *repairable* or *non repairable* unit.
- 2) Each minimal cut set must contain at least one event with failure data of category different from *on demand probability* or *test interval*.

4.7.2 Calculation of $Q_0(t)$ Using Exact Calculation (ERAC) and Upper Bound Approximation

The probability of the TOP event is denoted by

$$Q_0(t) = P(\text{“The TOP event is occurring at time } t\text{”})$$

For a given point in time t , the value of $Q_0(t)$ of course depends on the structure of the fault tree and of the probabilities of occurrence of the input events at time t .

CARA-FaultTree supports two different methods for calculating $Q_0(t)$, the *upper bound approximation* and the exact *ERAC* algorithm. The upper bound approximation is very fast, but is inaccurate in some situations. The ERAC algorithm is exact, but much slower for large fault trees.

Upper Bound Approximation for $Q_0(t)$

The following formula provides an upper bound for $Q_0(t)$, and is usually a satisfactory approximation to $Q_0(t)$.

Let the minimal cut sets of the tree be denoted K_1, K_2, \dots, K_k . By the assumption of independence of input events, the probability that all input events in the minimal cut set K_j occur, is

$$\check{Q}_j(t) = \prod_{i \in K_j} q_i(t) \quad (11)$$

If the cut sets were disjoint, then they would be stochastically independent and we would have

$$Q_0(t) = 1 - \prod_{j=1}^k (1 - Q_j(t)) \quad (12)$$

In general, however, the minimal cut sets are not disjoint. In this case it may be shown that we always have

$$Q_0(t) \leq 1 - \prod_{j=1}^k (1 - Q_j(t)) \quad (13)$$

and that in fact $Q_0(t)$ approximately equals the right hand side of (13) at least when the $q_i(t)$'s are close to 0.

It should be noted that the inequality (13) for $Q_0(t)$ is also applicable when the input events in the fault tree are positively dependent (so-called *associated*) rather than independent.

Exact Calculation of $Q_0(t)$; the ERAC Algorithm

The upper bound approximation presented above may in some situations be rather inaccurate. A number of alternatives have therefore been proposed. One of these alternatives is the ERAC algorithm (Exact Reliability/Availability Calculation) which was developed by Aven [5].

The ERAC algorithm is based on a decomposition method by Doulliez and Jamouille [6], originally designed for transportation networks. A modification of Aven's approach is used in CARA-FaultTree.

To illustrate the ERAC algorithm, assume that we have a fault tree with n independent input events. Let $\underline{y} = (y_1, y_2, \dots, y_n)$ denote the random state vector of the input events, where y_i is equal to 1 when input event no. i occurs and 0 otherwise.

Now, let A denote all the states \underline{y} of the fault tree such that the TOP event occurs. The probability $Q_0(t)$ of the TOP event is thus determined by:

$$Q_0(t) = \sum_{\underline{y} \in A} P(\underline{Y}(t) = \underline{y}) \quad (14)$$

If we let

$$\begin{aligned} P(Y_i(t) = 1) &= q_i(t) \\ P(Y_i(t) = 0) &= 1 - q_i(t) = p_i(t) \end{aligned}$$

it is easy to verify that

$$P(\underline{Y}(t) = \underline{y}) = \prod_{i=1}^n p_i(t)^{l-y_i} q_i(t)^{y_i} \quad (15)$$

The ERAC algorithm and most of its competing algorithms are based on formula (15). The prime objective of all of these algorithms is to determine the set A as efficiently as possible. It is observed that A is always a subset of the vector interval $[0, \underline{1}]$. In ERAC the set A is determined by successive partitioning of this interval in so-called acceptable and non-acceptable states. This procedure is rather complicated and the reader is referred to [8] for further details.

4.7.3 Calculation of $R_0(t)$, MTTF and Freq(TOP) Using Monte Carlo (Stochastic) Simulation

The reliability function for the TOP event is defined as

$$R_0(t) = P(\text{“TOP event has not occurred in the time interval } [0,t]\text{”})$$

where it is assumed that the system is perfect at time 0, i.e. no input events have occurred by time 0.

Thus $R_0(t)$ is the *survival function* of the system with respect to the non-occurrence of TOP event.

The function $R_0(t)$ should not be confused with the function $U_0(t) = 1 - Q_0(t)$, which is the probability that the TOP event does not occur at time t , *without regard to whether the TOP event has occurred or not before time t* . Thus we always have $R_0(t) \leq 1 - Q_0(t)$.

A lower bound for $R_0(t)$ is obtained by putting all repair times equal to infinity and computing the resulting “ $Q_0(t)$ ” by one of the methods described above.

In CARA-FaultTree one may obtain an estimate of the exact value of $R_0(t)$, together with other information from a Monte Carlo simulation. The user then has to specify the time interval $[0,t]$, and the number of runs.

Each run constitutes a simulated realization of the system performance in the time interval $[0,t)$, and the times of occurrences of the TOP event are recorded for each run. The results are, after all runs have been done, summarized to obtain estimates for

- $R_0(t)$
- MTTF (= mean time to first occurrence of the TOP event)

- Frequency distribution for the number of occurrences of the TOP event in $[0,t)$
- $A_{0,av}(t)$ (= system availability in $[0,t)$)

$R_0(t)$ is estimated as the relative number of runs with no TOP event occurring in $[0,t)$.

In the case when all the runs result in at least one TOP event, the MTTF is estimated in a straightforward way as the arithmetic mean of the times to the first occurrence of the TOP event in each run. When there are one or more runs for which the TOP event does not occur in the time interval $[0,t)$, CARA-FaultTree estimates MTTF by the formula

$$MTTF = \frac{\sum_i T_i}{\text{Number of runs with at least one TOP event}} \quad (16)$$

where T_i for each run is set to the time of the first TOP event, if the TOP event occurred, and T_i is set to t otherwise. (This is the well-known formula “total time on test”/number of failures).

The simulation procedure is not of interest for *static* fault trees i.e. fault trees for which the $q_i(t)$ does not depend on t . Thus the analysis is restricted to *dynamic* trees, i.e. fault trees for which each minimal cut set contains at least one input event i with $q_i(t)$ depending on t .

The Monte Carlo simulation gives inaccurate values for very reliable systems. If reliable systems are considered, the numerical integration method described below should be used.

To run the Monte Carlo simulation sub-program in CARA-FaultTree, the user must enter a mission time, the number of simulations to run, and a seed. A good choice for the mission time will be 2-3 times the expected MTTF. The accuracy of the calculations increases with the number of simulations, but so does also the computing time. The seed needs only to be changed if one wants to reproduce calculations with one specific seed.

4.7.4 Calculation of $R_0(t)$, MTTF and E(#failures) Using Numerical Integration

We will now present a method for obtaining TOP event measures by using numerical integration. The method is due to

Vesely [2], who also wrote the computer program KITT where this method was implemented. This method is also referred to as Kinetic Tree Theory, KTT.

As in "Upper Bound Approximation for $Q_0(t)$ " on page 96 we denote the minimal cut sets by K_1, K_2, \dots, K_k . The probability of occurrence of cut set K_j is:

$$\overset{\vee}{Q}_j(t) = \prod_{i \in K_j} q_i(t) \quad (17)$$

Now introduce

$w_i(t)$ = failure frequency of the i 'th component

$w_{K_j}(t)$ = failure frequency of cut set K_j

$w_0(t)$ = system failure frequency

The system failure density can now be obtained by:

$$w_0(t) = \sum_{j=1}^k \frac{\partial Q_0(t)}{\partial \overset{\vee}{Q}_j(t)} w_{K_j}(t) \quad (18)$$

where

$$\frac{\partial Q_0(t)}{\partial \overset{\vee}{Q}_j(t)} \approx 1 - \sum_{\substack{l=1 \\ l \neq j}}^k \overset{\vee}{Q}_l(t) \quad (19)$$

and

$$w_{K_j}(t) = \sum_{i \in K_j} \frac{\overset{\vee}{Q}_j(t)}{q_i(t)} [1 - q_i(t)] I_i \quad (20)$$

(λ_i is the failure rate for the i 'th component, thus we do not sum for components with *on demand* failure data)

The system failure rate is defined by

$$I_0(t) = \frac{w_0(t)}{1 - Q_0(t)} \quad (21)$$

Finally we find by (numerical) integration:

$$R_0(t) = e^{-\int_0^t I_0(\tau) d\tau} \quad (22)$$

$$MTTF = \int_0^\infty R_0(t) dt \quad (23)$$

$$E(\text{no. fail up to } t) = \int_0^t w_0(\tau) d\tau \quad (24)$$

The above formulas only apply to very reliable systems. For unreliable systems, the formulas are inaccurate, and simulation should be considered.

To run the numerical integration sub-program in CARA-FaultTree, the user must enter a mission time, the number of intervals for the numerical integration and an increase factor. A good choice for the mission time will be 2-3 times the expected MTTF. The accuracy of the calculations increases with the number of intervals. The number of intervals should therefore be increased until the calculations do not depend on the number of intervals. The increase factor controls the length of each interval. The idea behind the increase factor is to make the numerical integration more accurate for small t -values. A recommended value is 1.1 for the increase factor.

4.7.5 Calculation of Freq(TOP) Using the Hand Calculation Method

The hand calculation method can be used to obtain the frequency of the TOP event. In the situation where each minimal cut set contains one and only one component with data type “frequency” and the renaming component in each cut set is of type “on demand probability” the formula is given by:

$$Freq(TOP) = \sum_{\text{all cut sets } K_j} \{ f_{k_j} \cdot \prod_{\substack{i \in K_j \\ i \neq k_j}} q_i(t) \} \quad (25)$$

where f_{k_j} is the frequency of the input event with “frequency” data in cut set K_j , and $q_i(t)$ is the probability that input event i in cut set K_j occurs at time t .

In the general situation the following formula may be used:

$$Freq(TOP) = \sum_{\text{all cut sets } K_j} \{ \sum_{i \in K_j} I_i \cdot \prod_{\substack{l \in K_j \\ l \neq i}} q_l(t) \} \quad (26)$$

where λ_i is the frequency/failure rate of component i and $q_l(t)$ is the probability that input event l occurs at time t .

If the minimal cut sets are not disjoint, CARA-FaultTree offers two alternative calculation methods.

The first method is to obtain a conservative value of the frequency of the TOP event by a similar method to the Upper bound approximation for calculating $Q_0(t)$. Please refer to "Upper Bound Approximation for $Q_0(t)$ " on page 96 for an introduction to the Upper bound approximation method.

CARA-FaultTree also offers an exact calculation method based on the ERAC algorithm, see below.

$Freq(TOP)$ can be found exactly by use of Birnbaum's measure of reliability importance, $I^B(i|t)$ (see "Birnbaum's Measure of Reliability Importance" on page 106 on how $I^B(i|t)$ can be calculated exact by using the ERAC algorithm):

$$Freq(TOP) = \sum_{\substack{\text{all basic} \\ \text{events } i}} I_i I^B(i|t) \quad (27)$$

Since $I^B(i|t)$ can be interpreted as the probability that the system is in such a state that component i is critical for the system, $I_i \cdot I^B(i|t) dt$ is the probability that the TOP event occurs due to component i in $[t, t+dt)$. The formula then follows directly since two components cannot fail simultaneously in $[t, t+dt)$.

4.8 Modular Decomposition

4.8.1 Modular Decomposition of the Fault Tree

In order to save computing time and improve the approximations, an option is provided in CARA-FaultTree to modularise the fault tree before performing the analysis. (For an introduction to modular decompositions of a fault tree, we refer to [4]).

The (optional) modularization used by CARA-FaultTree consists of seeking modules (i.e. subsets) of input events containing only non-repeated events inside the module, and where no input event in the module is found in the tree outside the module. In the modularised tree, the modules are treated as input events and the corresponding probabilities " $q_i(t)$ " are re-computed for each module by a simple recursive technique.

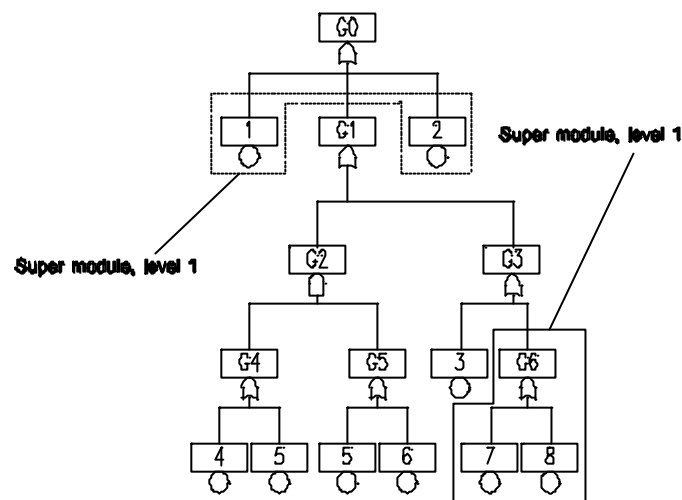
It should be noted that if the modularization option is chosen, then the MOCUS algorithm implemented in CARA-FaultTree will produce minimal cut sets only in terms of the input events of the modularised tree, i.e. the modules themselves will appear as input events in the minimal cut sets. Thus, if a list of all minimal cut sets is requested, then the modularization option should not be chosen.

Below, a short description of the modularization technique is given, together with some guidance on the use of modularization. Finally, the benefits using fault tree modularization are discussed.

4.8.2 The Modularization Technique

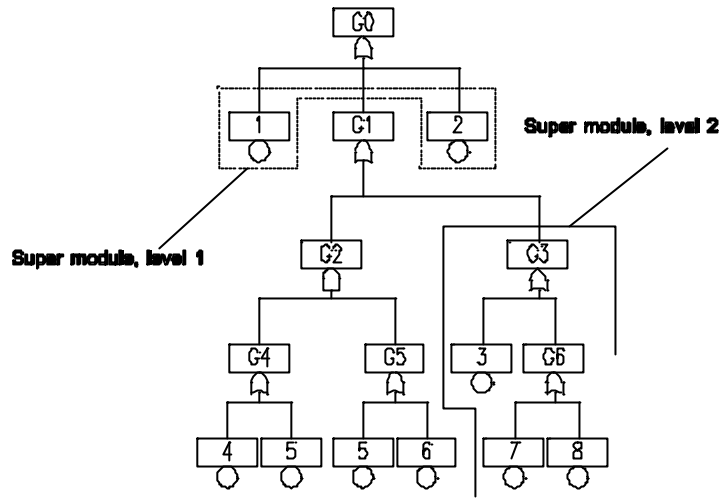
The modularization technique used by CARA-FaultTree consists of scanning the fault tree for so-called *super-modules*, that is, subtrees with input events that are not repeated inside or outside the subtree. In the modularised tree, the modules are treated as input events and the corresponding probabilities ($q_i(t)$) are re-computed for each module by a simple recursive (exact) technique.

A term used together with the CARA-FaultTree modularization option is modularization *level*. In the two figures below, *super-modules* for one example fault tree are illustrated.



In the figure above, CARA-FaultTree was run specifying modularization level 1, and two *super modules* were found. Note that the input events below gate G4 and G5 are not *super modules*, since input event 5 is repeated under both gates.

In the figure below, CARA-FaultTree was run specifying modularization level 2, and also here two *super modules* are found. Note that when specifying level 2 (or above), CARA-FaultTree also identifies *super modules* of lower levels. This is seen from the figure below, where one of the *super modules* is of level 1 and the other of level 2. Note also that the input events below gate G2 are not a *super module*, since input event 5 is repeated under both gate G4 and G5.



Note that when using modularization, the minimal cut sets will not be shown explicitly as the super modules will appear as Basic events. The events that constitute a super module will also be displayed but you will not know the structure of the module.

4.8.3 Guidance on selecting Modularization Level

If the user selects to run CARA-FaultTree with modularization, selecting level 1, 2 or 99 (i.e. the maximum level number) is recommended. Selecting level 1 and 2 gives *super modules* that will be of a "manageable size", and for most applications this will give a sufficient performance. If level 2 is not enough to give sufficient performance, the user might as well select level 99, allowing CARA-FaultTree to scan the tree for all levels of *super modules*.

4.8.4 Advantages using Modularization

First, note that if the modularization option is chosen, the MOCUS algorithm implemented in CARA-FaultTree will produce minimal cut sets only in terms of the input events of the modularised tree, i.e. the modules themselves will appear as input events in the minimal cut sets. Thus, if a list of all minimal cut sets is requested, then the modularization option should not be chosen.

The advantages using the CARA-FaultTree fault tree modularization are:

- Computing time for finding minimal cut sets is reduced. The reason for this is that computing time for finding *super modules* is proportional to the number of input events, whilst computing time for

finding the minimal cut sets may be of the order 2^n , where n is the number of input events.

- Calculations using approximations will be improved, since the calculations within the *super modules* are exact.
- Generally, the computing times for calculations are reduced.
- The exact calculation option in CARA-FaultTree (ERAC) is not available for fault trees having more than 64 input events. In order to overcome this problem, the modularization algorithm can be used to reduce the number of input events to a value less than 64.

4.9 Measures of Importance

4.9.1 Available Measures of Importance

CARA-FaultTree includes one measure of structural importance and two measures of reliability importance for Basic and Undeveloped events:

- Vesely-Fussell's measure of reliability importance.
- Birnbaum's measure of reliability importance.
- Improvement potential.
- Criticality Importance.
- Order of smallest cut set
- Birnbaum's measure of structural importance.

4.9.2 Vesely-Fussell's Measure of Reliability Importance

Vesely-Fussell's measure of reliability importance for component i is defined by:

$I^{VF}(i/t_0)$ = the conditional probability that at least one minimal cut set containing input event no. i is failed at time t_0 , given that the system fails at time t_0 .

(We say that a minimal cut set fails if all the input events in the set occur).

The following approximation, which is usually good, is used by CARA-FaultTree to compute I^{VF} for a non-modularised tree. For a modularised tree an improved version of this approximation is used. It should be noted that CARA-FaultTree provides the importance measures for each input event, even for a modularised tree.

The approximate formula is:

$$I^{VF}(i/t_0) \approx \frac{\sum_{j=1}^{m_i} Q_j^i(t)}{Q_0(t)} \quad (28)$$

where the upper index i means that, in the numerator, only the minimal cut sets containing input event no. i are considered. Then m_i is the number of minimal cut sets containing input event no. i .

Vesely-Fussell's measure of importance can be interpreted as the probability that the TOP event is *caused* by input event no. i , when it is given that the TOP event has occurred. Then by saying that "the TOP event is caused by input event no. i ", we mean that input event no. i occurs and the rest of the input events in the fault tree are in such states that the TOP event occurs if and only if input event no. i occurs.

As an example, consider a parallel system, with "system failure" as the TOP event. Then there is only one minimal cut set, namely the set containing all the input events, and therefore we get

$$I^{VF}(i/t) = 1 \text{ for all } i$$

It is clear that in this case, if there is a system failure, then all input events are contributing to the failure.

4.9.3 Birnbaum's Measure of Reliability Importance

Birnbaum's measure of reliability importance for component i is defined as follows:

$$I^B(i/t) = \text{the partial derivative of } Q_0(t) \text{ with respect to } q_i(t)$$

Thus an increase of $q_i(t)$ by a (small) amount a_i , say, will increase $Q_0(t)$ by an amount (approximately) a_i times $I^B(i/t)$.

CARA-FaultTree calculates Birnbaum's measure of reliability importance using another interpretation:

$$I^B(i/t) = P(\text{"TOP event occurs at } t_0\text{"} \mid q_i(t)=1) - P(\text{"TOP event occurs at } t\text{"} \mid q_i(t)=0) \quad (29)$$

i.e. the difference between the probabilities of the TOP event computed under the assumptions that input event no. i is known to occur and is known to not occur, respectively. This difference may be interpreted as the probability that input event no. i is *critical* at time t .

To give a simple example, consider a parallel system of two components. Then, for the TOP event "system failure" we have $Q_0(t) = q_1(t)q_2(t)$, so

$$I^B(1/t) = q_2(t), \quad I^B(2/t) = q_1(t)$$

4.9.4 Improvement potential

The improvement potential reliability measure for component i is defined by:

$$I^P(i/t) = \textit{the increase in system reliability if component } i \textit{ is replaced with a perfect component at time } t$$

The improvement potential measure is related to Birnbaum's measure by:

$$I^P(i/t) = I^B(i/t) \cdot q_i(t)$$

4.9.5 Criticality Importance

The criticality importance reliability measure for component i is defined by:

$$I^{CR}(i/t) = \textit{the probability that component } i \textit{ is critical for the system and is failed at time } t, \textit{ given that the system is failed at time } t$$

The criticality importance measure is related to Birnbaum's measure by:

$$I^{CR}(i/t) = \frac{I^B(i/t) \cdot q_i(t)}{Q_0(t)}$$

4.9.6 Order of smallest cut set

The order of smallest cut set importance measure is defined by:

$$I^O(i) = \textit{The order of the smallest cut set containing component } i$$

Note that this is a qualitative measure that does not depend on the component reliabilities.

4.9.7 Birnbaum's Measure of Structural Importance

Birnbaum's measure of structural importance for component i is defined as follows:

$$B_f(i) = \text{the relative number of system states for which component } i \text{ is } \mathbf{critical} \text{ for the system}$$

Component i is *critical* if the state of the system is such that the system functions if and only if component i functions. A more precise definition of this measure is:

$$B_f(i) = \frac{h_f(i)}{2^{n-1}} \quad (30)$$

where $h_f(i)$ is the total number of *critical path vectors* for component i . A critical path vector for component i is a state vector of the other components in the system such that the system functions if and only if the i 'th component functions. The idea behind this measure is to count the relative number of different states of the system (all *other* components than i) which cause component i to be *critical* for the system.

It can be shown that if all components have $q_i(t) = 0.5$, then $B_f(i) = I^B(i)$. CARA-FaultTree computes Birnbaum's measure of structural importance by means of this relation.

4.9.8 Cut set importance

The cut set importance for cut set j is defined by

$$I^{CI}(j) = \text{the conditional probability that at minimal cut set } j \text{ is failed at time } t, \text{ given that the system is failed at time } t$$

Cut set importance is calculated by the formula

$$\frac{\prod_{i \in K_j} q_i(t)}{Q_0(t)} \quad (31)$$

where $Q_0(t)$ is the probability that the TOP event occurs at time t .

4.10 Uncertainty Analysis

4.10.1 Required input for the Uncertainty Analysis

The input parameters to a quantitative fault tree evaluation are normally subject to some sort of uncertainties. It is therefore desirable to take these uncertainties into account in the analysis.

In the (optional) uncertainty analysis of CARA-FaultTree the user models his uncertainties of the input parameters by log-normal distributions.

The required input for each parameter (failure rate, repair time, probability of failure) are the *mean value* or the *median* m of the parameter, and in addition an *error factor* k which is supposed to measure the user's uncertainty about the value m . The error factor k should be chosen by the user so that, with a probability of 90%, the true value of the parameter is between m/k and $m \cdot k$.

It should be noted that the mean value and the median value do not coincide for a log-normal distribution, due to lack of symmetry in the probability density function. The *median* value of a random variable is the value such that in a large sample of realisations, about 50% of them exceed this value, and 50% of them fall below the value. On the other hand, the *mean* value of the random variable is the arithmetic mean of the sample of realisations.

In order to interpret the error factor k , consider as an example that the mean or median of a certain failure rate has been set to 0.6, and that one thinks that with a probability of 90% the true value of the failure rate is somewhere in the interval (0.4,0.9). Then put $m = 0.6$, $k = 1.5$.

In the above example, the values m and k were determined by subjective reasoning. Another possibility is that the failure rates are statistically estimated from available failure data. Then m may be set to the value of some point estimate for the true failure rate, and some 90% confidence interval for the failure rate may be used to compute k .

4.10.2 Uncertainty Analysis – Simulations

Given the values of m and k for each input parameter, their influence on the top event probability $Q_0(t)$ must be assessed. As the input parameters are now treated as random variables, $Q_0(t)$ is also a random variable. The uncertainty in $Q_0(t)$,

which is what we are after, should thus be represented by the *probability distribution* of $Q_0(t)$.

An analytical derivation of this probability distribution is in general not possible. To overcome this problem, CARA-FaultTree performs a Monte Carlo simulation in order to approximate the distribution of $Q_0(t)$. The simulation is done as follows:

In each of a user-specified number of runs, a set of values for the input parameters (failure rates, repair times etc.) is drawn at random according to the specified log-normal distributions. Then the TOP event probability $Q_0(t)$ is calculated for this set by the upper bound approximation (possibly adjusted by a constant factor if the ERAC option is chosen).

In this way a scattered set of values for $Q_0(t)$ is obtained, from which CARA-FaultTree estimates the mean value, the variance and the standard deviation of (the random variable) $Q_0(t)$. In addition, CARA-FaultTree provides a histogram and a table of quantiles of the estimated distribution for $Q_0(t)$.

In order to save computing time, the input parameters to a run are drawn from the log-normal distributions only for the 10 input events supposed to have the largest impact on $Q_0(t)$. For the remaining parameters the mean/median values m are chosen. This simplification usually has very little influence on the final result. The criterion used for selecting the 10 most important input events, is the product of the importance I^{VF} and the error factor k .

When interpreting the results of an uncertainty analysis, one should note that the mean value of $Q_0(t)$ in general does not exactly coincide with the value for $Q_0(t)$ obtained by exact computation by ERAC, when setting all parameters equal to their mean values (or median values). This is due to the fact that $Q_0(t)$ is a *non-linear* function of the input parameters (failure rates etc.)

4.10.3 Uncertainty Analysis - Example

For example, it may be theoretically proven that for a system of non-repairable components, the mean value of $Q_0(t)$ (as estimated by the uncertainty analysis) is always *below* the value of $Q_0(t)$ obtained by an exact computation using only the mean values of the failure rates.

As an illustration, consider a series system of 4 non-repairable components, each with mean/median failure rate $m = 1 \cdot 10^{-6}$, and error factor $k = 2$. At time $t = 8760$ we obtain:

$Q_0(t)$ computed by “upper bound” formula, all failure rates = $1 \cdot 10^{-6}$:

$$3.44 \cdot 10^{-2}$$

Expected value of $Q_0(t)$ in the uncertainty analysis, where $m = 1 \cdot 10^{-6}$ is interpreted as the *mean value*:

$$3.42 \cdot 10^{-2}$$

Expected value for $Q_0(t)$ in the uncertainty analysis, where $m = 1 \cdot 10^{-6}$ is interpreted as the *median value*:

$$3.73 \cdot 10^{-2}$$

As another illustration, consider a parallel system of the same 4 components, at time $t=10^5$. Then the three values above, computed for this situation, are respectively:

$$8.2 \cdot 10^{-5}$$

$$7.6 \cdot 10^{-5}$$

$$10.6 \cdot 10^{-5}$$

5. References

5.1 List of References

- [1] “Guidelines for Hazard Evaluation Procedures”, American Institute of Chemical Engineers, AIChE, 1985.
- [2] Henley, E. J. & Kumamoto, H.: “Reliability Engineering and Risk Assessment”, Prentice-Hall, 1981.
- [3] Vesely, W. E. & al.: “Fault Tree Handbook”, NUREG-0492, 1981.
- [4] Fussell, J. B.: “Fault Tree Analysis - Concepts and Techniques”. Article; “Generic Techniques in System Reliability Assessment”, Nordhoff-Leyden, 1976.
- [5] Aven, T.: “Reliability/Availability Evaluations of Coherent Systems Based on Minimal Cut Sets”, Reliability Engineering 13, 93-104, 1985.
- [6] Doulliez, P. and Jamouille, J. “Transportation Networks with Random Arc Capacities”, RAIRO, 3, 45-60, 1972.
- [7] Høyland, A. & Rausand, M.: “System Reliability Theory; Models and Statistical Methods”, John Wiley & Sons, New York, 1994, ISBN 0-471-59397-4.
- [8] Vatn, J: “Finding minimal cut sets in a fault tree”, Reliability Engineering and System Safety **36**, 59-62, 1992.

6. Glossary of Terms

$A_{0,av}(t)$

Average system availability in $[0,t)$.

AND-gate

The AND-gate indicates that the output event A occurs only when all the input events E_i occur simultaneously.

Basic event

The Basic event represents a basic equipment fault or failure that requires no further development into more basic faults or failures.

$B^f(i)$

Birnbaum's Measure of Structural Importance is defined as the relative number of system states for which component i is critical for the system.

Comment rectangle

The Comment rectangle is for supplementary information.

Cut set

A cut set in a fault tree is a set of Basic/Input events whose (simultaneous) occurrence ensures that the TOP event occurs. A cut set is said to be minimal if the set cannot be reduced without losing its status as a cut set.

$E(\#failures)$

Expected number of failures within a time period.

Fault tree

A fault tree is a logic diagram that displays the interrelationships between a potential critical event (accident)

in a system and the reasons for this event. The reasons may be environmental conditions, human errors, normal events (events which are expected to occur during the life span of the system) and specific component failures. A properly constructed fault tree provides a good illustration of the various combinations of failures and other events which can lead to a specified critical event. The fault tree is easy to explain to engineers without prior experience of fault tree analysis.

f_i

Frequency of i 'th input event, i.e. expected number of occurrences of i 'th input event per unit time.

Freq distr

Distribution of the TOP event frequency.

Freq(TOP)

Frequency of the TOP event.

Frequency

The Frequency input event data category is used to describe events occurring now and then, but with no duration. Thus the probability that the event occurs at time t , $q_i(t) = 0$. The reliability data entered to CARA-FaultTree is the expected number of times the event will occur in a time period of 10^6 hours.

House event

The House event represents a condition or an event that is TRUE (ON) or FALSE (OFF) (not true).

$I^B(i|t)$

Birnbaum's Measure of Reliability Importance of component i is defined as the partial derivative of $Q_0(t)$ with respect to $q_i(t)$.

$I^{CR}(i|t)$

The criticality importance of component i is defined as the probability that component i is critical for the system and is failed at time t , given that the system is failed at time t .

$I^{IP}(i|t)$

Improvement potential of component i is defined as the increase in system reliability if component i is replaced with a perfect component at time t .

$I^O(i)$

The order of the smallest cutset of component i is defined as the order of the smallest cutset containing component i .

$I^{VF}(i|t)$

Vesely-Fussell's Measure of Reliability Importance of component i is defined as the conditional probability that at least one minimal cut set containing input event no. i is failed at time t_0 , given that the system fails at time t .

λ_i

Failure rate, i 'th component, i.e. expected number of failures of i 'th component per hour.

MTTF

Mean time to first system failure.

Non repairable unit

The non repairable input event data category represents a component which is not repaired when a failure occurs.

On demand probability

On demand probability input event data category is used to describe components that are not activated during normal operation. The component is demanded only now and then. The reliability data entered to CARA-FaultTree is the probability that the component is not able to perform its function upon request. In safety systems, the operator is often modelled by an on demand probability, for example: Operator fails to activate manual shut-down system.

OR-gate

The OR-gate indicates that the output event A occurs if any of the input events E_i occur.

Path set

A path set in a fault tree is a set of Basic events whose simultaneous non-occurrence ensures that the TOP event does

not occur. A path set is said to be minimal if the set cannot be reduced without losing its status as a path set.

$Q_0(t)$

The probability of the TOP event is denoted by

$$Q_0(t) = P(\text{“The TOP event occurs at time } t\text{”})$$

For a given point in time t , the value of $Q_0(t)$ depends on the structure of the fault tree and of the probabilities of occurrence of the input events at time t .

$q_i(t)$

The probability that the i 'th component does not function at time t

$R_0(t)$

The reliability function for the TOP event is defined as

$$R_0(t) = P(\text{“TOP event has not occurred in the time interval } [0, t]\text{”})$$

Repairable unit

The repairable input event data category represents a component which is repaired (or replaced) when a failure occurs.

Test interval

The Test Interval input event data category is used to describe components that are tested periodically with test interval. A failure may occur anywhere in the test interval. The failure will, however, not be detected until the test is carried out or the component is demanded. This is a typical situation for many types of detectors, process sensors and safety valves.

t_i

Mean time to repair, MTTR, for i 'th component (in hours).

TOP event

The undesired event (e.g. accident) to be analysed is normally called the TOP event. It is very important that the TOP event is given a clear and unambiguous definition. The description of the TOP event should always describe what type of undesired event that occur, where the undesired event occurs, and when (e.g. in what operational mode) the undesired event occurs.

Transfer down

The Transfer down symbol indicates that the fault tree is developed further at the occurrence of the corresponding Transfer up symbol.

Transfer up

At the occurrence of the Transfer up symbol, the fault tree is developed further. The Transfer up symbol is referred to from one or more Transfer down symbols found on other fault tree pages.

Uncertainty Analysis

The input parameters to a quantitative fault tree evaluation are normally subject to some sort of uncertainties. It is therefore desirable to take these uncertainties into account in the analysis. In the (optional) uncertainty analysis of CARA-FaultTree the user models his uncertainties of the input parameters by regarding them as stochastic.

Undeveloped event

The input event data category Undeveloped event represents a fault event that is not examined further because information is unavailable or because its consequence is insignificant.

7. Index

A

AND-gate 16–17, 83–85, 89
Average system availability 54, 69, 88, 91–92

B

Basic event 8–9, 17–19, 36, 55–56, 63, 72, 82, 86–87
Boundary 78, 80

C

CARA-CAFTAN 6, 35
Comment rectangle 20
Cut set 50, 51–52, 63–66, 68, 72, 83, 85–92, 96, 99–101, 105, 107

E

E(#failures) 55, 56, 64, 88, 99
ERAC 49, 53, 60–62, 66–68, 72, 95–98, 101, 105, 110

F

Failure data 9–10, 18, 25, 27, 29, 35–36, 38, 45–46, 59, 67, 72, 88–93, 95, 100, 109
Fault tree title 24, 47–48
Freq(TOP) 95–96
Frequency 10, 37–38, 56–58, 65, 70, 88–92, 96, 99–100, 101

H

House event 19, 82–83, 37–38, 82–83, 92

I

Import 6, 35–36, 33, 35–36, 39, 42, 48
Inhibit-gate 16–17
Input event 4, 12–15, 18, 29, 31, 37, 39, 45–46, 48, 68, 82, 88, 92, 97, 99, 101–3, 105–6

K

KooN-gate 15–17

M

Modular decomposition 60, 102

O

OR-gate 8–9, 13, 16–17, 83–85

P

Print 1, 10, 14, 24, 35, 39–41, 50
Property 9, 13–14, 21, 45

T

TOP event 8, 11–12, 51, 56–58, 60–67, 61, 70, 78, 80–81, 83–85, 86–92, 87, 95, 96–99, 101–2, 106–10
Transfer down 10, 20–21, 43
Transfer symbol 4, 10–11, 20, 43
Transfer up 20–21

U

Undeveloped event 18–19

W

Web-site 2