# Table of Contents

FT, FTPLUS ........................................................................................................................................ 3

INPUTS & OUTPUTS ............................................................................................................................. 3

MENUS & BUTTONS ............................................................................................................................. 4

**FIGURE 1. MENUS AND BUTTONS OF FAULT TREE ANALYSIS** .................................................. 5
**FILE MENU** ................................................................................................................................. 6
**SETTINGS DIALOG** .................................................................................................................... 7
**EXAMPLES MENU** ....................................................................................................................... 8
**WINDOW MENU** ............................................................................................................................ 8
**FIGURE 2. ALLOCATION STRATEGY SELECTION BUTTONS** ......................................................... 8

**ALLOCATING RESOURCES** ............................................................................................................. 9

**OBJECTIVE** .................................................................................................................................. 9
**DISPLAY** ..................................................................................................................................... 9
**STRATEGY** .................................................................................................................................... 10
**MANUAL** ...................................................................................................................................... 10
**RANKED** ...................................................................................................................................... 11
**APPORTIONED** ........................................................................................................................... 11
**MINIMAL (OPTIMAL)** ................................................................................................................. 12

**THE EVENT TREE** .......................................................................................................................... 13

**FIGURE 3. EVENT TREE DISPLAY** .............................................................................................. 13

**SUMMARY WINDOW** .................................................................................................................... 14

**GO/CLEAR** ................................................................................................................................... 15

**SENSITIVITY ANALYSIS** .............................................................................................................. 15

**FIGURE 4. EDIT BUTTONS** ........................................................................................................... 16

**ENTERING AND EDITING A FAULT TREE** .................................................................................. 16

**EDIT** ............................................................................................................................................ 16
**FT, FTplus**

Program *FT.jar* is the desktop version of Fault Tree Analysis. Program *FTplus.html* is the browser version of Network Analysis. These programs are identical except for:

*FTplus.html* cannot save or open files from your local computer. It also requires a browser.

*FT.jar* is a stand-alone desktop application that runs on Macs and PCs, and does not need a browser. However, like all PC applications, *FT.jar* must be properly installed on your computer before it is launched. It requires the latest Java Virtual Machine. Installation requires an administrative password under Windows XP.

Fault Tree Analysis is copyleft software, which means it is open source. All changes must be returned to the author for re-distribution as open source. The Java source code of Fault Tree Analysis is available from the author. It may be used for research and educational purposes, but it cannot be sold.

**INPUTS & OUTPUTS**

In general, you input the fault tree consisting of budget, components, logic gates, and threat, and the program computes the appropriate allocation of dollars to reduce threat risk or vulnerability. The purpose of FTplus is to compute the allocation of resources across a system modeled as a fault tree.

You will need the following information prior to using this program:

List of Components and Threats  
Budget Estimate  
For each Threat:  
  T : Probability of an attack (Threat)  
  V : Probability of successful attack (Vulnerability)  
  C : Cost to Eliminate the threat (Cost)  
  D : Damage estimate if attack is successful (D)

You will also need to know the shape of your fault tree – what are the components and how are they connected together by logic gates. Most of the time, the logic gates will be OR gates. Use AND gates to express redundancy.

FTplus produces an allocation (A) for each Threat. It also produces an Event Tree, and performs sensitivity analysis. Sensitivity analysis tells you how sensitive the results of the calculations are relative to changes in input values.
Menus & Buttons

Figure 1 shows the menus and buttons of the main window of Fault Tree Analysis. There are two windows: the one shown in Figure 1 and another one called Event Tree Analysis, which is obtained from selecting the EVENT TREE item from the Window menu.

The menus and buttons in the top panel control the fault tree itself, while the buttons in the bottom panel control the processing algorithms used to analyze a fault tree. The message area always appears in the upper left-hand portion of the display screen. A current fault tree always appears in the middle of the display screen – showing a single block when the program initially starts to run.

FILE, EXAMPLES, and WINDOW menus perform the file input and output operations typical of any application. WINDOW allows you to switch between the main (Fault Tree) display, a summary of results window, and the auxiliary (Event Tree) window.

The current fault tree can be modified or a new tree constructed using the colored buttons: ERASE, THREAT, COMPONENT, LOGIC AND/OR, and EDIT. In every case, they are used by first selecting a fault tree block and then pressing one of the buttons.

The lower panel contains an array of radio buttons and three control buttons. The radio buttons are arranged in four groups: OBJECTIVE, which determines what the objective of the analysis is: to reduce fault probability (a.k.a. vulnerability), or to reduce risk (vulnerability times damage). You may select %VULNERABILITY REDUCTION, or $RISK REDUCTION.

The DISPLAY group of radios determines what is displayed in the chart and histogram area, which will appear, during processing, in the upper right hand portion of the display. You may select $ALLOC V. THREAT, which shows the result of each strategy calculation, or $RISK V. $BUDGET, which shows the reduction in vulnerability or risk versus budget (total investment).

The final two groups are actually one group: STRATEGY contains four allocation strategies: MANUAL: you provide the allocation manually; RANKED: Fault Tree Analysis computes the allocation based on Ranked Order; APPORTIONED: minimize the sum of squared error difference between allocations and non-allocation of the budget; and MINIMAL: compute the mathematical optimum reduction in vulnerability or risk.

The ALLOCATE button is used to activate the allocation after you have selected which strategy to employ.

The SENSITIVITY button calculates the sensitivity of the result – either vulnerability or risk – versus the inputs to the threats – V (vulnerability), C (cost), and D (damage). The results of sensitivity analysis are displayed as a bar chart versus threat number for all threats in the fault tree.
GO/CLEAR starts and stops the program. Always press GO to activate the other buttons and menus. Pressing CLEAR erases the current fault tree and starts the program over again, with a single “root block” of a generic fault tree.

The current fault tree is defined as the fault tree that is currently displayed on the screen. The message area is where errors are reported and is updated during processing to lead you through the proper use of the program.

**Figure 1. Menus and Buttons of Fault Tree Analysis.**

![Image of menus and buttons](image)

---

Objective:
- [ ] $V$ulnerability Reduction
- [x] $R$isk Reduction

Display:
- [ ] $S$Alloc v. Threat
- [ ] $S$Risk v. $B$udget

Strategy:
- [ ] Manual
- [ ] Ranked
- [ ] Minimal

Strategy, cont'd:
- [ ] Apportioned

Control:
- [ ] Allocate
- [ ] Sensitivity
- [ ] Clear
FILE MENU

File contains the ABOUT, OPEN, SAVE, SAVE AS, SETTINGS…, and QUIT menu items. When running Fault Tree Analysis from within a browser, the OPEN, SAVE, SAVE AS.. items are disabled, because Java does not allow you to access local disk drives via the Web.

ABOUT presents the user with information about the program: the Creators, Copyleft information, etc.

OPEN allows you to read a previously saved fault tree file from your local disk.

SAVE allows you to store the current fault tree to your local disk. If previously saved, using the SAVE AS… item, you will not be prompted for the name of the file, but the current fault tree will be saved over the current file – erasing it and replacing it with the current fault tree.

SAVE AS allows you to name the current fault tree and place it in a directory of your choosing. SAVE AS can be used to save multiple versions of the current fault tree under different names.

SETTINGS… displays a dialog that allows you to set global program parameters: step size, maximum number of iterations – both used by the MINIMAL allocation organizing principle; and SENSITIVITY, which is used to bound the sensitivity calculation. See SETTINGS DIALOG.

Program parameters stay set to the values you provide in the SETTINGS DIALOG. They assume a default value, which remain in effect until you change them using this option. Default options work for almost all situations, except for small budget values, or unusual sensitivity settings.

QUIT will cause the program to stop and exit.
**Settings Dialog**

SETTINGS… causes the following dialog to appear so you can change program-wide parameters: step size, sensitivity, and number of iterations used for emergence algorithms.

![Fault Tree Default Settings](image)

**STEP SIZE:** The organizing principle used to emerge the minimum value or risk or vulnerability subtracts STEP SIZE from a DONOR threat’s allocation and gives it to a RECIPIENT threat’s allocation – both selected at random. For some problems, a STEP SIZE = 1.0 is too coarse. For example, if the budget is $10.5 or the cost values are small, e.g. 1, 2, 3, or 4, the emergence process will overshoot the optimal value. In such cases, use a smaller STEP SIZE. For example, for a budget of $10.5, a STEP SIZE = 0.1 may be appropriate.

The smaller the STEP SIZE, the more time it takes to calculate the solution. The larger it is, the less accurate is the solution. STEP SIZE is set to 1.0 by the program, but you can change it to obtain results quickly, or accurately, as needed.

**EMERGENCE.** The default value of 100 iterations means that the optimum allocation strategy calculations are computed 100 times to obtain the answer by emergence. This may be too many or not enough for the correct value of risk or vulnerability to emerge. Increasing this parameter results in many more iterations, which means the program runs slowly. Decreasing it, means the answers are inaccurate. Typical values of 100 to 200 should give enough accuracy for most applications. This parameter only affects the MINIMAL strategy calculation used by ALLOCATE and SENSITIVITY.

**SENSITIVITY** is a percentage that represents the amount of change in each input value, V, C, and D, for every threat. The default value of 10% means that each V, C, and D are increased by 10% and then decreased by 10% in turn. The ALLOCATE calculation is done for each of these values, and then compared with the results obtained without sensitivity analysis. The resulting bar chart plots the percentage of change in the answer versus each value of C, V, and D. In this way you can study the effect of a change in an input value versus the answer obtained by ALLOCATE.
**EXAMPLES MENU**

The EXAMPLES menu contains a list of built-in example fault trees that illustrate the value of Fault Tree Analysis. This list may vary depending on the version of the program you have. The examples can be saved to your local disk (FT.jar, only) and modified to create similar fault trees.

**WINDOW MENU**

The WINDOW menu is used to select which display you see: the FAULT TREE display is the default or main display. The SUMMARY item causes a window containing all results up to this point to appear. The EVENT TREE item displays the event tree corresponding to the current fault tree.

**Figure 2. Allocation Strategy Selection Buttons**

![Allocation Strategy Selection Buttons](image)
Allocating Resources

Once a current fault tree is loaded from a file, the EXAMPLES menu, or constructed by the user, there are three steps to compute a resource allocation, see Figure 2:

1. Objective Selection
2. Strategy Selection
3. Pressing the ALLOCATE button

Figure 2 shows the radio buttons used to set up a calculation prior to pressing the ALLOCATE or SENSITIVITY button.

The ALLOCATE/PAUSE button alternates between ALLOCATE and PAUSE. After each allocation, press PAUSE to see the updated results in the message window. An example is shown below. V = vulnerability. R = risk. This message will appear only when the PAUSE button is pressed, which also terminates the allocation process.

The SENSITIVITY/OFF button alternates between SENSITIVITY and OFF. After each sensitivity calculation and display, press OFF to revert to other options. You cannot operate the program while sensitivity analysis is being performed. In large fault trees, it may take many minutes to complete sensitivity analysis of the OPTIMAL allocation strategy because it uses emergence.

OBJECTIVE

There are two high-level objectives: either you want to allocate for the purpose of reducing vulnerability, or you want to reduce risk. \( \text{%VULNERABILITY REDUCTION} \) is selected to reduce vulnerability (fault reduction), or \( \text{$RISK REDUCTION} \) is selected to reduce risk (risk reduction).

DISPLAY

There are two display types available: \( \text{$ALLOC V. THREAT} \) produces a bar chart of the budget allocation versus threat number calculated by FT. The \( \text{$ALLOC V. THREAT} \) radio produces a bar chart of risk/vulnerability versus budget as shown below.
The purpose of this option is to help you determine the effect of an investment on risk or vulnerability. This information can be used to investigate the level of risk that is acceptable versus the investment that may be required to achieve the acceptable risk level.

**STRATEGY**

There is no single “best” investment strategy. Instead, there are strategies that achieve specific goals. The MANUAL strategy may achieve political or economic goals; the RANKED strategy reduces the worst-case vulnerability/risk; the APPORTIONED strategy achieves a compromise between RANKED and MINIMAL; the MINIMAL strategy tells you what is absolutely, the mathematically minimum risk/vulnerability for the current fault tree, given the budget.

All strategies, except the OPTIMAL strategy calculate quickly. The OPTIMAL strategy may require some time, because it uses the organizing principle to find the optimal allocation through emergence. This calculation can be sped up by setting STEP SIZE to 2.0, 3.0, 4.0, or 5.0, but this may produce inaccurate results. Setting STEP SIZE to a fraction less than 1.0 will generate a better result, but this can take a desktop computer many minutes to compute. STEP SIZE is changed by entering values through the FILE>SETTINGS… menu.

**MANUAL**

When MANUAL is selected and then ALLOCATE is pressed, a table appears as shown here. The first column of this table is the THREAT number; the second column is the THREAT name, and the third column is the current allocation corresponding with each threat.
The $Allocation entries can be changed by selecting them with the mouse, deleting the current value, and typing in a new value. These values are instantly substituted into the fault tree and used to compute a new value of fault tree vulnerability and risk.

After dismissing this dialog, you must press the PAUSE button to see the updated value of risk and vulnerability. The message is always the result of the previous allocation.

Note: Be careful with the last $Allocation entry in this table. You must press the ENTER or RETURN key on your keyboard upon entering values in this table, and before dismissing this table dialog. Otherwise, the new entry will be lost. It is tempting to enter the last value in this table, and then dismiss it without pressing RETURN or ENTER, first.

This dialog can only be dismissed by closing it using its controls (RED gum drop on a Macintosh, and X box on a PC). There is no OK button. It can also be left open while doing other things, but it will not be updated with new results until you close and re-open it.

**RANKED**

Select the RANKED strategy radio button and press ALLOCATE. The Ranked Order allocation will be performed and the results displayed in the upper right-hand portion of the display as shown here. This display summarizes the allocation: $Allocation versus Threat#.

Press PAUSE to see the resulting vulnerability and risk, in the message area.

**APPORTIONED**

Select the RANKED strategy radio button and press ALLOCATE. The Ranked Order allocation will be performed and the results displayed in the upper right-hand portion of the display as shown here. This display summarizes the allocation: $Allocation versus Threat#.
Select the APPORTIONED strategy radio button and press ALLOCATE. The Apportioned allocation will be performed and the results displayed in the upper right-hand portion of the display as shown here. This display summarizes the allocation: $Allocation versus Threat#.

Press PAUSE to see the resulting vulnerability and risk, in the message area.

**MINIMAL (OPTIMAL)**

Select the OPTIMAL strategy radio button and press ALLOCATE. The Optimal allocation will be performed and the results displayed in the upper right-hand portion of the display as shown here. This display changes as the organizing principle is applied many times. The bars will move, showing how the organizing principle works its way toward the minimum value, iteration by iteration. After some time, these changes should cease, which means the solution has been found.

Press PAUSE to see the final vulnerability and risk, in the message area.
The Event Tree

The Event Tree replaces the fault tree in the display area when the WINDOW>EVENT TREE item is selected from the WINDOW menu. Figure 3(a) shows one of two display methods used by EVENT TREE. The second method is shown in Figure 3(b).

Figure 3. Event Tree Display.

(a) First Event Tree Display Method

(b). Second Event Tree Display Method

Figure 3 shows both methods of display. In the first method, each single and combination event is shown as a bar chart containing the before and after vulnerabilities corresponding with each event. The gray bar charts refer to vulnerability when the budget is evenly distributed to all events; the red bars refer to the vulnerabilities after the allocation has been made according to the selected strategy.

Events are numbered according to the threats involved: a 1 means threat number one, only. A bar labeled with 2 3 signifies that threats 2 and 3 are both involved in the event. A bar with 1 2 3 4 means threats 1 2 3 and 4 are part of the combination event.

Figure 3(b) shows how the EVENT TREE is displayed when there are too many events to show in the bar-chart format. Recall that the number of events grows as a power of 2, so a fault tree with 5 threats will have 32 events, and a fault tree with 6 threats will have 64 events! Therefore, method two displays a compressed representation of all possible events.

The compression is very terse: \( V = 5(T: 2 \ 3) \) means the vulnerability is 5% and the combination threats involved in this event are threats 2 and 3. Similarly, \( V = 1(T: 5) \) means that threat 5 is the only threat involved in the event and its fault probability is 1%.
In the second method, the compressed display only shows the non-zero events. Hence, it is the most compact form of event tree that Fault Tree Analysis can display!

To return to the current fault tree display, select WINDOW>FAULT TREE.

Note: The **Before Risk** value is the risk of the fault tree prior to allocation. This value corresponds to when the budget is initially distributed evenly to all threats, regardless of their vulnerability or damage values. The **After Risk** value is the risk of the fault tree after the selected allocation strategy has been applied. If you want to discover the risk with zero investment, use the MANUAL strategy to enter zero allocations, and then observe the **After Risk** value in the Event Tree display.

### Summary Window

The SUMMARY window shown above is obtained by selection menu WINDOW > SUMMARY. It hovers above the default Fault Tree/Event Tree window, but you must close and re-open it to obtain the most-recent results.

**SUMMARY** does one simple, but useful thing: it displays all results of all strategy allocations in a tabular format. The top half of this table displays results of **%VULNERABILITY REDUCTION**, while the bottom half shows results of **$RISK REDUCTION**.

The number and name of each threat is listed in the first two columns. The fault probability (vulnerability) is shown in the third column. The remaining columns summarize the results obtained from each allocation strategy. Fault probability and risk values are given for each of MANUAL, RANKED, APPORTIONED, and OPTIMAL (MINIMAL).
**GO/CLEAR**

GO must be pressed to start Fault Tree Analysis. Once started, the program changes this button to CLEAR. Do not press CLEAR unless you want to start all over again, because CLEAR erases the current fault tree and starts a new one. Be sure to SAVE your current fault tree before CLEARing the program.

**Sensitivity Analysis**

Sensitivity analysis is the process of determining the sensitivity of allocation to input values. In this case, the input values are V (fault probability), C (cost to remove the vulnerability), and D (damage due to successful attack), for each threat. There are 30 inputs to a fault tree with 10 threats. Therefore, sensitivity analysis must explore the sensitivity of the vulnerability or risk calculation due to change in each of the 30 input values.

Sensitivity uses the SENSITIVITY setting in FILE > SETTINGS… to calculate each value in the analysis. The default setting is 10%, which means that each input value is varied by 110% and 90%, respectively. Then, each changed value of V, C, and D is used to calculate an allocation that results in a fault tree vulnerability (%VULNERABILITY REDUCTION) or risk ($RISK REDUCTION).

Sensitivity is expressed as a percentage: the percentage change in risk/vulnerability for each change in V, C, and D. These are displayed in a bar chart, see the display, below.

Sensitivity analysis tells you how sensitive an allocation result is to change in inputs. A change of 20% when an input changes by 10% indicates a high degree of sensitivity.
Conversely, a change of 5% when an input changes by 10% suggests that the result of allocation is rather stable relative to inputs.

Once again, the OPTIMAL emergence calculation can take considerable time. When multiplied by the much higher demands of repeated calculations needed to compute sensitivity, emergence can take many minutes. For this reason, the MESSAGE display area will report on the progress of SENSITIVITY analysis on OPTIMAL allocation results. Be patient.

**Figure 4. Edit Buttons**

[Image showing edit buttons]

**-entering and editing a fault tree**

Figure 4 shows the editing buttons used to enter a new fault tree or modify an existing one. These all work the same way: first select a block to change, and then press one of the editing buttons in the top panel.

Blocks change to a gray color when selected by clicking on the EDIT field in the upper left-hand corner of a block. Blocks can be moved around and re-positioned on the display screen by dragging them with the mouse. These positions will be remembered when you save the fault tree.

**EDIT**

The EDIT button is used to change the name or values associated with any block in the fault tree. Select a box, then press EDIT, and the appropriate EDIT dialog will appear. The dialog will contain fields for values that can be altered.

**Changing the Budget**

For example, the budget is stored in the root box of the fault tree. The only way to change it is to edit the root node. The example below shows the dialog box that pops up when you select the root box and then press EDIT. Select the Budget field and enter a new value into the field. Press OK, and the fault tree now has a new budget.
ERASE

Select a block to be erased. Click on the ERASE button. The block and all of the blocks below it will disappear.

THREAT

Threat boxes contain the name of the threat, the probability of an attack taking place (T), probability of success, assuming the attack takes place (V), reduced probability of success after allocation (P), cost to eliminate the threat (C), damage expected in the event of a successful attack (D), and the computed allocation of budget to this threat (A). The user inputs T, V, C, and D, and the software computes P and A.

To add a new threat to the current fault tree, select the block that you want to connect the new threat to and press THREAT. Threats can only be attached to components (blue boxes) or logic gates (green diamonds). Threats cannot be connected to other threats.

When the THREAT or EDIT button is pressed, the following threat dialog box will appear:
The first field in this dialog (Threat) is the probability that an attack will take place. It is the intelligence information needed to estimate the likelihood of an attack. Typically, it is set to the default value of 100%. It affects the calculations because the probability of an incident is the product of Threat * Vulnerability.

The second field (V) Vulnerability is the fault probability, which equals the probability of a successful attack, assuming an attack takes place. It should be a number greater than zero and is a percentage between 0.1% and 100%.

The next field (COST) is the cost of entirely removing the vulnerability. It must be a positive number, expressed in dollars, millions of dollars, billions, etc.

The fourth field (Damage) is the estimated damage or target value should a successful attack take place. It should be a positive number measured in the same units as COST.

The final field (Name) is optional – it is the name associated with the threat, e.g. BOMB, EARTHQUAKE, etc.

Press the OK button and the threat box will appear with these inputs. Press CANCEL and your changes are ignored.

**COMPONENT**

A sector component is any asset or group of assets that may be threatened. It has a name, and at least one threat or logic gate connected to it. Each threat connected to a component contains vulnerability, cost, and damage estimates that pertain to the component. Components are targets of threats, but we must connect them via a logic gate. Figure 5 shows an incomplete multi-level fault tree containing four components.
Components are added and edited just like all other boxes in a fault tree. Select a component and press EDIT to change its name. Select the box that you want a new component to be connected to, and press COMPONENT to add the new component. A dialog will appear:

![Component dialog](image)

It is possible to construct a fault tree with several layers of components, but they must be layered via logic gates as shown in Figure 5. A component cannot be connected to another component. Components can be connected to a logic gate, or a single THREAT box. Symmetrically, a logic gate can be connected only to one or more components or one or more THREATs.

The root box of the tree (at the top) is a special component that contains the budget to be allocated. To change the budget, you must edit this special component. Select it and press EDIT.

If you attempt to form an improper fault tree, an error message will appear in the message area. This program will not process an improper fault tree, but it will allow you to temporarily form an improper fault tree during construction of the tree.

**Color Coding**

The following color codes are used to remind you of what box is being edited:

- Blue: Sector and Component box.
- Green: Logic Gate (AND/OR)
- Red: Threat box.
Figure 5. A Fault Tree with several layers.

**LOGIC AND/OR**

A logic block can be either an OR-gate or an AND-gate. Therefore, a new logic block is added to the fault tree by selecting the block to connect it to, followed by selecting either the AND or OR radio button in the logic block dialog:

Logic blocks can be attached to components, but not threats. Only one logic block may be attached to each component. Components or threats can be attached to a logic gate.

Press OK and the new logic block will be attached to the fault tree. Cancel ignores your inputs.