Using the Fault Tree Analysis Profile

Installation

The profile should be installed in the Rhapsody installation directory folder, under Share/ Profiles.

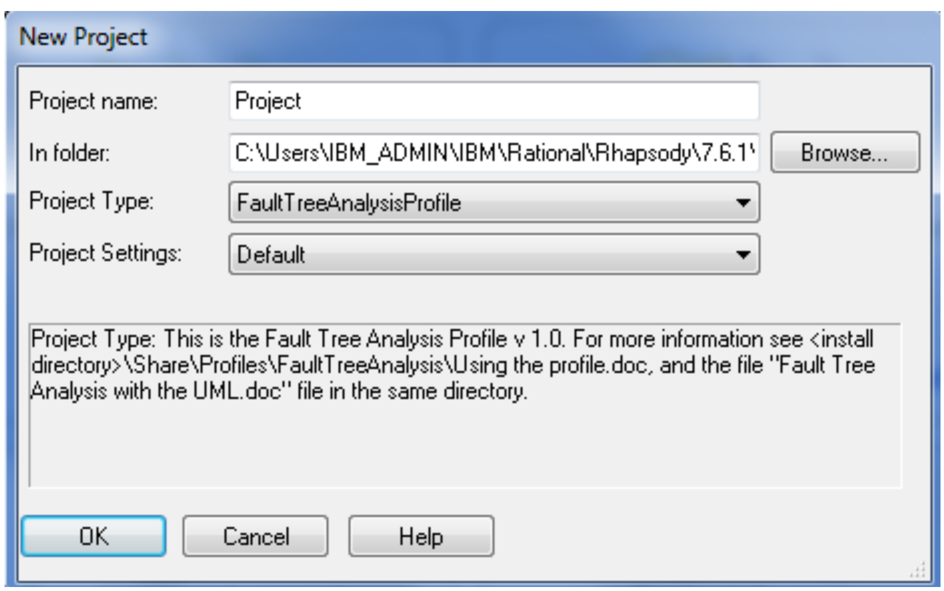
1. Copy the FaultTreeAnalysisProfile.zip file to the <installation directory>/Share/ Profiles directory
2. Note. Microsoft Windows 7 users will find the share directory located in their home directory, along with Rhapsody samples.
3. Unzip the file with the create directories option on.
   This will create a directory called FaultTreeAnalysis

That's it!

Creating a model with the profile

Use the File→New menu option in Rhapsody to create a Fault Tree analysis project.

1. Add the project name and locations you want
2. In the Type drop-down list, select FaultTreeAnalysisProfile

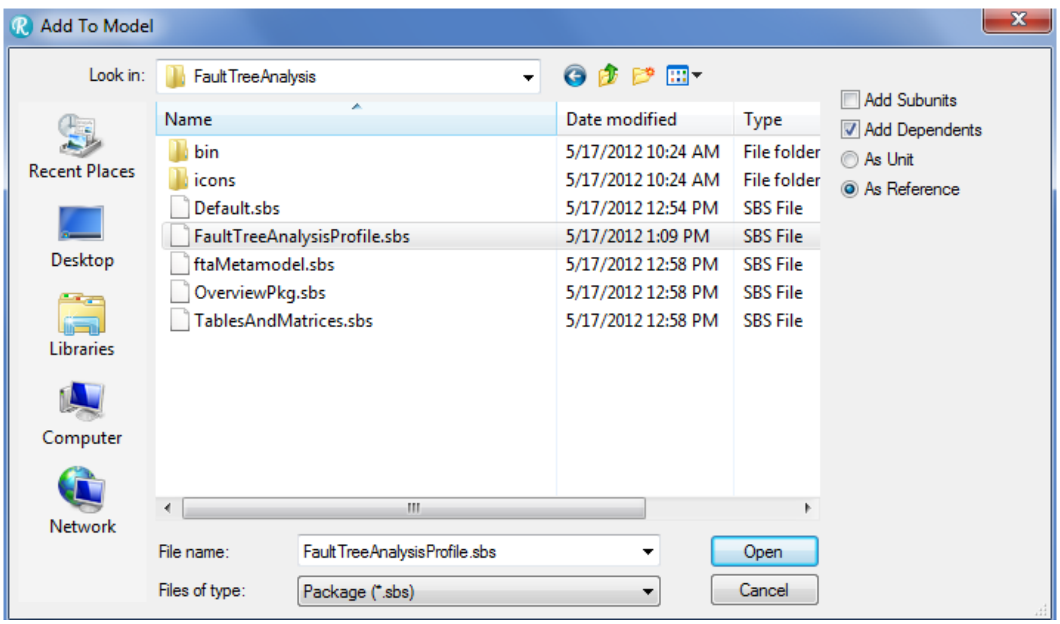


This will create a new model with the profile.

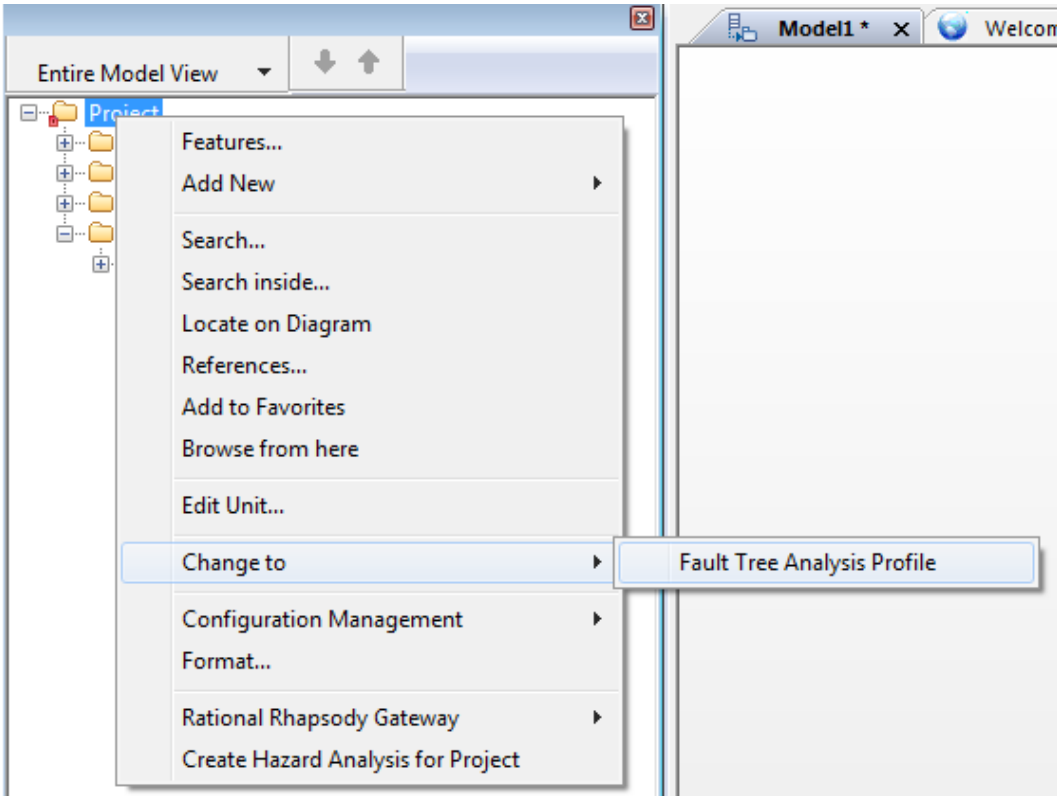
Adding the profile to an existing model

Use Rhapsody's Add To Model feature to add the profile, then change the project type to FaultTreeAnalysisProfile type.

1. Use File->Add To Model.. to open the Add To Model dialog
2. Navigate to the directory into which the profile has been installed (e.g. <install directory>\share\profiles\FaultTreeAnalysis
3. In the Add to Model dialog, using the Files of Type drop down list, select Package (*.sbs)
4. Select FaultTreeAnalysisProfile.sbs
5. Check Add Dependents checklist
6. Click on As Reference radio button



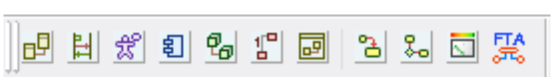
7. Click on Open
8. Once the profile is added, navigate to the project in the browser window (very first line).
9. Right click on the project, select Change To->FaultTreeAnalysis



Adding a Fault Tree Analysis Model

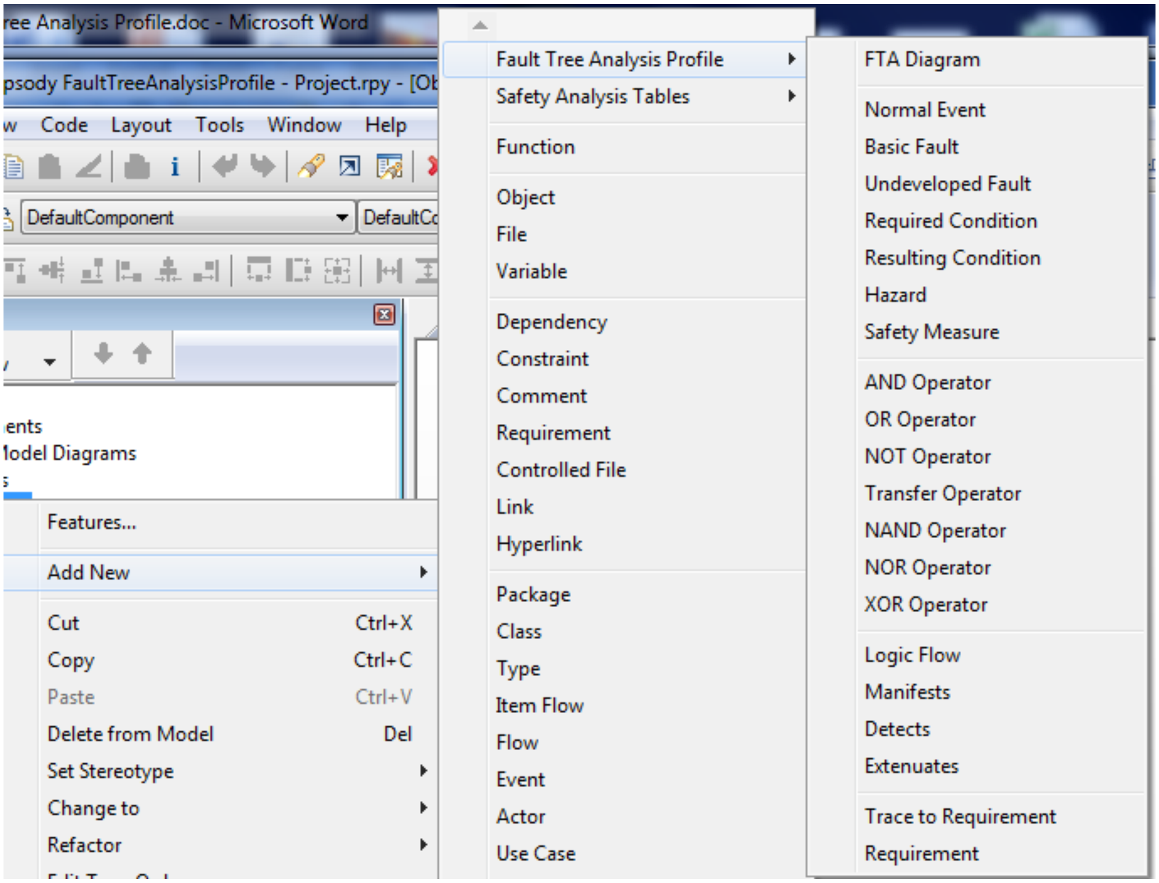
Once you've created a Fault Tree Analysis model, you have the full power of UML *plus* the ability to add Fault Tree diagrams and analyze them. We recommend creating a separate package in your model to hold your fault tree analysis elements and diagrams.

The diagram toolbar (normally located at the top of the Rhapsody window), should now have an FTA diagram option:

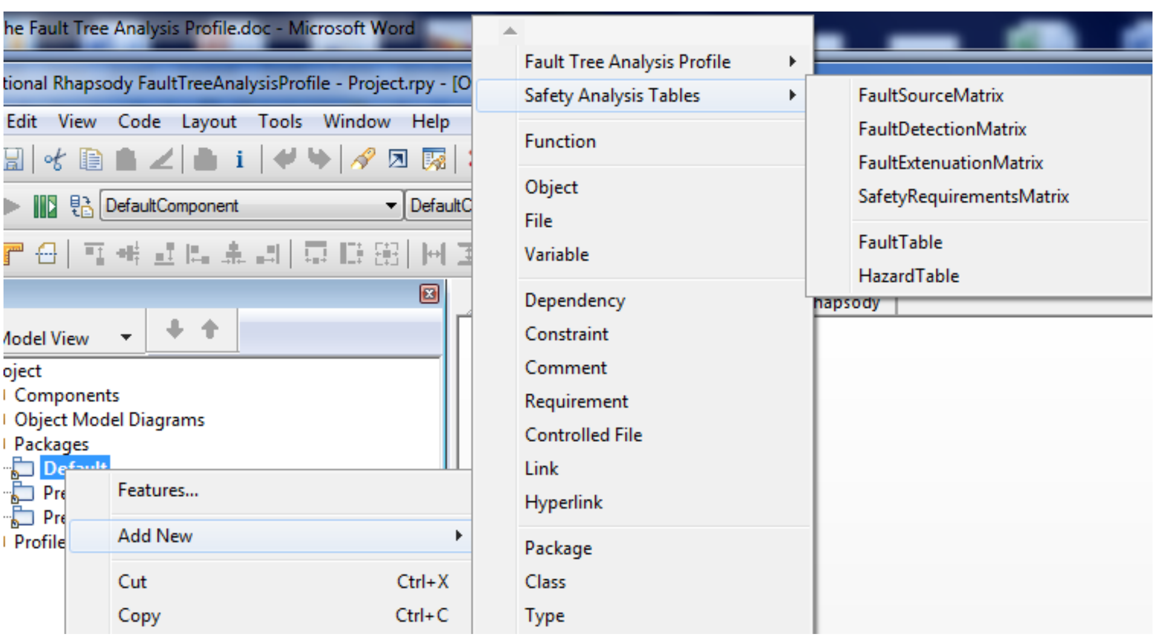


Clicking on the FTA Diagram button will create a new FTA diagram. In addition, the Add New right click menu has been extended. If you select a package and right click you will see two new primary categories added; one of these adds semantic elements (e.g. hazards, faults, etc) and FTA diagrams while the other adds various summary tables and matrices.

The list of semantics elements includes FTA diagrams, semantic elements, logical operators, and various relations, seen below:



The other menu adds tables and matrices:



The key elements for the metamodel (along with their profile realizations) are:

- Hazard –a condition that will lead to an accident or loss. This is usually the top terminal element in an FTA. (Stereotype of Class)
- Fault – the non-conformance of an element to its specification or expectation. Faults are further subclassed into Basic Faults and Undeveloped Faults. These are usually the bottom terminal elements in an FTA. (Stereotype of Class)
- Resulting Condition – the condition resulting from a combination of faults and conditions, combined with logical operators. (Stereotype of Class)
- Required Condition – A condition required for the fault to interact. (Stereotype of Class)
- Logical Operator – one of several logic conjunctives, such as AND, NOT, OR, etc. Note that Transfer operator actually has no semantics of its own but is used as a "diagram connector", allowing large FTAs to be broken up across multiple diagrams. (Stereotype of Class)
- Logic Flow – the connection of a fault, condition or hazard to a Logical Operator. The logic flow can be an input or an output. For example, in the statement A || B → C, there is a flow output from A as an input to the || (OR) operator. There is also an output from flow the || operator to the resulting condition C. (Stereotype of Flow).
- Fault Source – this is a normal UML element that could manifest a fault, i.e. that could be the source of a fault. (Stereotype of Class)
- Safety Measure – this is a normal UML element that could detect or extenuate (i.e. mitigate) a fault. (Stereotype of Class)
- Manifest relation – this is a relationship from a Fault to a Fault Source that causes the fault (Stereotype of Dependency)
- Detect relation – this is a relation from a Fault or Hazard to a Safety Measure that can detect when the fault has occurred. (Stereotype of Dependency)
- Extenuates relation – this is a relation from a Fault or Hazard to a Safety Measure that reduces either the likelihood or severity of the hazard or fault. (Stereotype of Dependency)
- Trace To Requirement – this is a relation from a Fault or Hazard to a Requirement. (Stereotype of Dependency)

Faults and Hazards elements have important metadata characterizing them. The important metadata is summarized

Metaclass	Metadata	Description
Hazard	Fault Tolerance Time	This is the length of time the fault can be tolerated before it leads to an accident.
	Fault Tolerance Time Units	This is the units of time (e.g. ms, seconds, hours, days)
	Risk	Risk is the product of the severity times the probability
	Severity	The degree of damage the accident can cause

	Safety Integrity Level	For standards such as IEC65-1508, this is the identified SIL level
	Probability	The likelihood of occurrence of the hazardous condition, usually computed from the metadata of the faults
Fault	Probability	The likelihood the fault will occur
	MTBF	The Mean Time Between Failure for the element
	MFBF Time Units	The time units expressed in the MTBF meta-attribute
Fault Source	Fault Mechanism	A description of how the fault can occur
Safety Measure	Fault Action Time	The length of time the corrective action requires to complete once initiated
	Fault Detection Time	The length of time, from the occurrence of the fault to its detection
	Fault Time Units	The unit of time used in the Fault Action Time and the Fault Detection Time
	Safety Mechanism	A description of how the detection and/or safety action is performed

Table 1: Fault Tree Metadata

Tables, Matrices and Hazard Analyses

In addition to the elements of the profile, new tables and matrices are added in the profile as well.

Table or Matrix	Format	Description
Fault Table	Rhapsody Table View	This lists the faults and all their metadata
Hazard Table	Rhapsody Table View	This lists the hazards and all their metadata
Fault Source Matrix	Rhapsody Matrix View	This shows a fault x fault source matrix, as defined by the Manifests relations
Fault Detection Matrix	Rhapsody Matrix View	This shows a fault x safety measure matrix, as defined by the Detects relations
Fault Extenuation Matrix	Rhapsody Matrix View	This shows a fault x safety measure matrix, as defined by the Extenuates relations
Hazard Analysis	Tab-separated value text file (.tsv) intended to load into Excel	This is an external file generated by the profile helper macros summarizing the hazard and fault information.

Table 2: Tables and Matrix summary views

The Hazard analysis is generated as an external file with a helper macro. This macro scans the entire model and generates the tab-separated value file[1] that can be loaded into most spreadsheet programs. The macro generates the name from the current date and time so that multiple versions of the hazard analysis can be kept. The output is divided into three sections.

The first section lists the hazards and their metadata, including the description, fault tolerance time, fault tolerance time units, probability, severity, risk, and safety integrity level.

The second section lists the relations between the faults and the hazards as defined by multiple intervening logical operators and logic flows. Each fault is identified with is name, description and other metadata.

The third section lists the relations between the faults and the "normal" UML model elements – requirements and classes related with the manifests, detects, extenuates, and traceToReqs relations.

For example, a Fault Table looks like this:

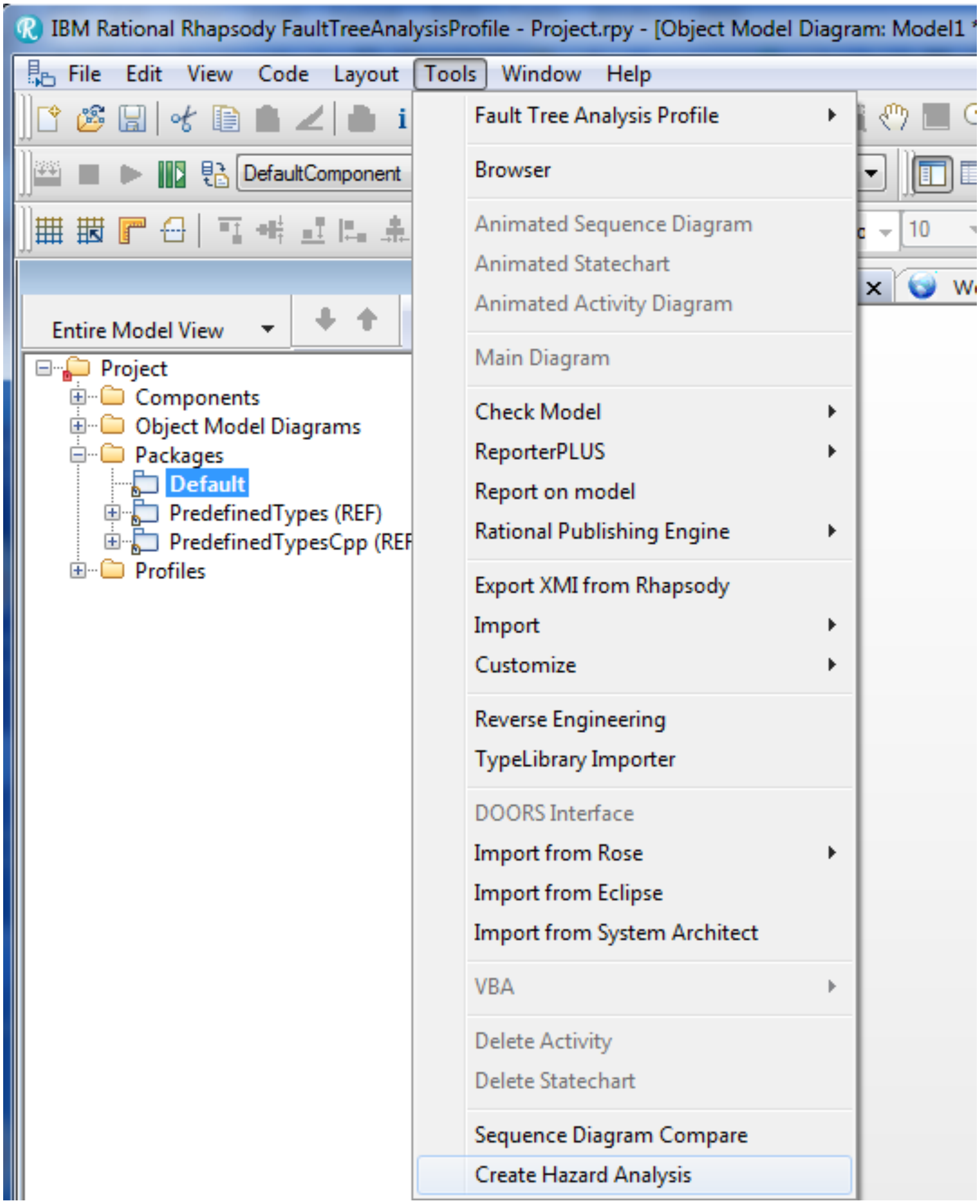
Name	Description	MTBF	MTBF_TimeUnits	Probability
Gas Supply Fault	This fault occurs when gas from a required source (e.g. O2 air N2 or He). This may be to any number of root causes such as a stuck or closed valve, running out of gas, a leak_	1e6	minutes	1e-6
Breathing Circuit Leak	This fault occurs when a significant amount of gas leaks from the breathing circuit into the	1e3	minutes	1e-3
Ventilator Pump Fault	This fault occurs when the pump internal to the ventilator no longer functions to shape the	1e6	seconds	1e-6
Ventilator Parameter Setting wrong	This fault occurs when a ventilator parameter is out of range. This includes: I:E ratio Tidal Volume Respiration Rate Inspiratory Pause Maximum inspiratory pressure Inspiration time	1e4	seconds	1e-4
Ventilator Computation Incorrect	This fault occurs when an error in the software or a fault in a necessary resource (e.g.	1e5	seconds	1e-5
Esophageal Intubation	This is a user-fault, but is common. This is mitigated by a CO2 sensor on the expiratory	1e5	minutes	1e-4
Patient disconnect from Breathing Circuit	This fault can occur as a result of jostling the breathing circuit during a surgical procedure.	1e4	minutes	1e-4
Power Supply Fault	The mains can fail because of a source power supply fault or if the power cord becomes	1e5	minutes	1e-5
Failure to Alarm	The alarm system is a system that exists solely for safety reasons. Therefore, it need not	1e5	minutes	1e-5
O2 Supply Fault	The O2 supply fault can occur because of a exhaustion of the supply itself, stuck or	1e4	seconds	1e-4
Breathing Circuit Problem				
Ventilator Problem				
Power Supply Problem				
Connection problem				
O2 Concentration Problem				
Redundant computational Channel fails	The redundant computational channel uses a heterogeneous algorithm to compute the	1e5	seconds	1e-5
Ventilator Parameter Limiting Fails	This fault occurs if the limit checks on the setting of ventilator parameters fail, i.e. allow a	1e6	seconds	1e-6
Gas Flow Sensor Fault	This fault occurs if the gas flow sensor fails to correctly measure the gas flow in the	1e-7	minutes	1e-7
Ventilator Parameter CRC check fails	Ventilator parameters are protected with a 32-bit CRC algorithm. This is specifically	1e5	seconds	1e-5
Backup Power Fails	The battery backup exists as a safety means to enable the system to continue to provide	1e4	minutes	1e-4
Physician unable to manually ventilate	The anesthesiologist is required to have a manual ventilation system available in the case	1e10	minutes	1e-10
SpO2 Sensor Fault	The SpO2 sensor is a fingercuff O2 sensor. This fault occurs if the sensor does not	1e7	seconds	1e-7
Breathing Circuit O2 Sensor Fault	The breathing circuit O2 sensor is provided to ensure that the O2 delivered from the	1e7	seconds	1e-7
Inspiratory Pressure Sensor Fault	The inspiratory pressure sensor is used to determine that the pressures delivered to the	1e7	seconds	1e-7
Expiratory Limb CO2 sensor fault	The expiratory limb CO2 sensor exists to ensure that the breathing circuit is properly	1e7	seconds	1e-7

[1] Tab-separated value format was used because Excel™ has defects in its interpretation of the more-common comma-separated value (CSV) file format.

The hazard analysis is a generated external provides a summary with enough information to trace from the safety requirements to the model elements realizing those requirements, as well as from the faults and hazards to the requirements and design.

Creating a Hazard Analysis

Creating a hazard analysis is easy. A fault tree analysis project as a new feature under the Tools menu, called Create Hazard Analysis.



Selecting this menu item will invoke a helper plug-in (written in Java, so the Java run-time environment is required to run the plug-in). This plug-in walks over the entire model and creates a tab-separated value (.tsv) file that can be loaded into a spreadsheet program. This file does not contain formatting codes, so you will need to set the columns widths and word wrap (recommend for the third column since it has descriptions) yourself in the spreadsheet program.

The plug-in places the file in the project directory and names it using the date and time. This allows you to keep multiple versions of the file if you desire. You can also add this file into your Rhapsody project as a Controlled File, if desired.

The hazard analysis consists of three sections. The first shows the hazards and the metadata from the fault tree model. The second part of the hazard analysis summarizes the relations between the faults and the hazards. This involves the tracing of multiple levels of logic flows connecting the faults with the hazards. Lastly, the hazard analysis contains the relations between all faults and the elements of the model, including requirements, and classes that manifest, detect, or extenuate faults. This view is crucial for a detailed understanding of the correctness and safety of a design model.

For more information, see the white paper "Fault Tree Analysis with the UML".

Disclaimer

The Fault Tree Analysis Profile provided here can be used to help Licensee meet compliance obligations, which may be based on laws, regulations, standards or additional practices. Any directions, suggested usage, or guidance provided with the Fault Tree Analysis profile does not constitute legal, accounting, or other professional advice, and Licensee is cautioned to obtain its own legal or other expert counsel. Licensee is solely responsible for ensuring that Licensee and Licensee's activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Fault Tree Analysis Profile does not guarantee compliance with any law, regulation, standard or additional practice.