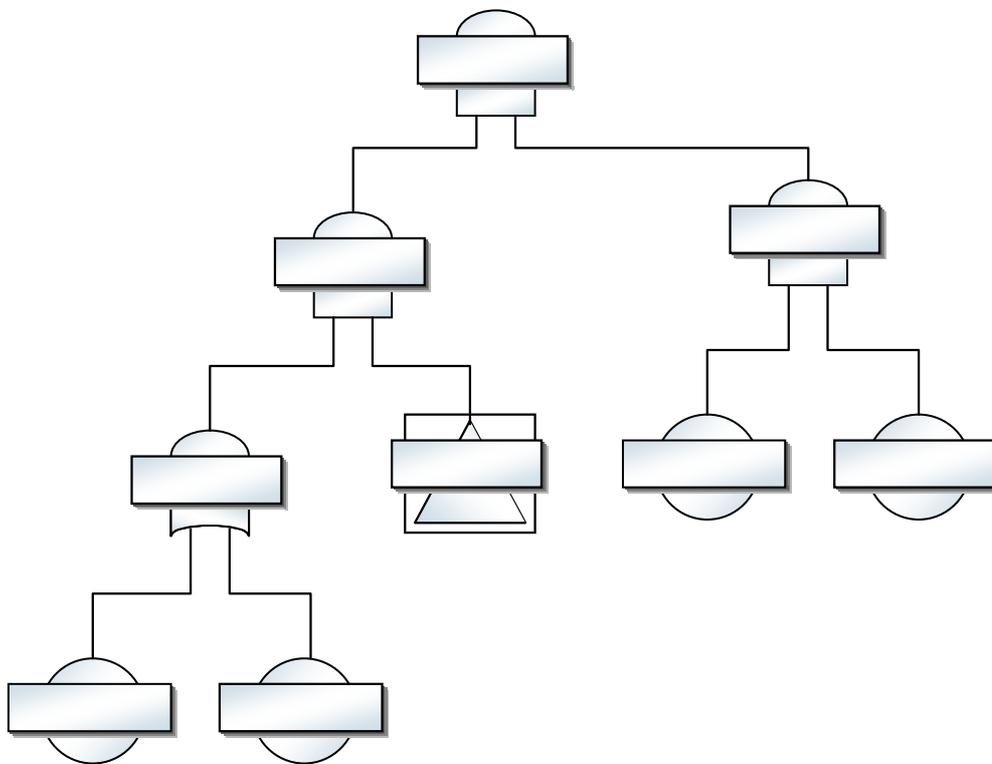


Fault Tree Analysis



1th Part

Bases

The Fault Tree Analysis, briefly FTA, was developed originally in the sixties in the area of the American telecommunication industry and aircraft industry. Only in the beginning of the eighties a formalisation of these methods occurred at the instigation of American authorities.

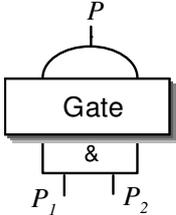
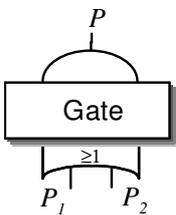
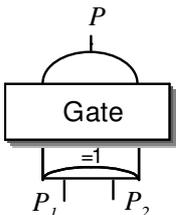
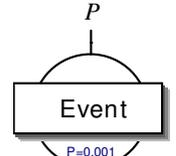
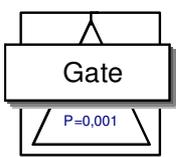
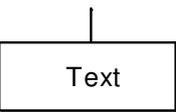
The Fault Tree Analysis is used for reliability- and safety security analyses. The proceeding is very similar to the Reliability Block Diagram RBD.

The aim is to determine possible combinations of causes which can lead to certain undesirable events (event), the so-called top level events. Furthermore is the job of a FTA:

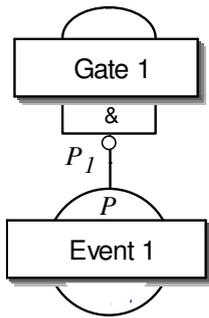
- *The generation of a graphic / logical tree structure to the understanding of the connections.*
- *Identification of possible failure causes and their combinations.*
- *Calculation of the probability of the undesirable event. Comparison of variations.*

Fault Tree Analysis

The link of the events is made in each case by different logical operators, the so-called gates. Device faults, operating faults and software faults which can cause with a certain probability to undesirable results belong to the events among other things. The following symbolism is used to the representation of the fault tree:

	<p>AND-Gate The output event enters only if all input events apply. The output probability P is calculated with:</p> $P = P_1 \cdot P_2 \cdot P \dots$	<table border="1" data-bbox="1173 510 1401 667"> <thead> <tr> <th>P₁</th> <th>P₂</th> <th>P</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>1</td> <td>0</td> <td>0</td> </tr> <tr> <td>0</td> <td>1</td> <td>0</td> </tr> <tr> <td>1</td> <td>1</td> <td>1</td> </tr> </tbody> </table>	P ₁	P ₂	P	0	0	0	1	0	0	0	1	0	1	1	1
P ₁	P ₂	P															
0	0	0															
1	0	0															
0	1	0															
1	1	1															
	<p>OR-Gate The output event enters if one of the input events applies. The output probability P is calculated with:</p> $P = 1 - (1 - P_1) \cdot (1 - P_2) \cdot (1 - P \dots)$	<table border="1" data-bbox="1173 743 1401 900"> <thead> <tr> <th>P₁</th> <th>P₂</th> <th>P</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>1</td> <td>0</td> <td>1</td> </tr> <tr> <td>0</td> <td>1</td> <td>1</td> </tr> <tr> <td>1</td> <td>1</td> <td>1</td> </tr> </tbody> </table>	P ₁	P ₂	P	0	0	0	1	0	1	0	1	1	1	1	1
P ₁	P ₂	P															
0	0	0															
1	0	1															
0	1	1															
1	1	1															
	<p>XOR-Gate (Exclusive-OR) The output event enters if only one of the input events apply but not both. The output probability P is calculated with:</p> $P = 1 - (1 - P_1) \cdot (1 - P_2) - P_1 \cdot P_2$	<table border="1" data-bbox="1173 999 1401 1155"> <thead> <tr> <th>P₁</th> <th>P₂</th> <th>P</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>1</td> <td>0</td> <td>1</td> </tr> <tr> <td>0</td> <td>1</td> <td>1</td> </tr> <tr> <td>1</td> <td>1</td> <td>0</td> </tr> </tbody> </table>	P ₁	P ₂	P	0	0	0	1	0	1	0	1	1	1	1	0
P ₁	P ₂	P															
0	0	0															
1	0	1															
0	1	1															
1	1	0															
	<p>Basic-Event Primary base event or failure. The probability P is defined directly and mostly comes from manufacturer's data of the component. As with the reliability block diagram P is dependent on the time (component age).</p>																
	<p>Sub-Gate At this point the other representation is interrupted. The given probability P represents the summary of other sub-elements which are not shown further.</p>																
	<p>Neutral text element Text elements can be inserted in paths to show additional information, or to insert other "creases". At several entrances this element works like an OR gate.</p>																

Hint: The symbolism is according to country and standards, as well as in software partly differently.

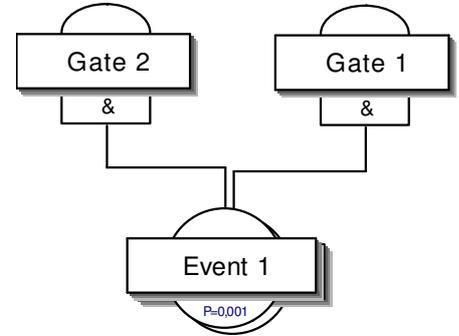


In addition to the OR gate there is still a seldom used OR2 gate with which at least 3 input events two must be fulfilled. This represents a hybrid between AND and OR gate.

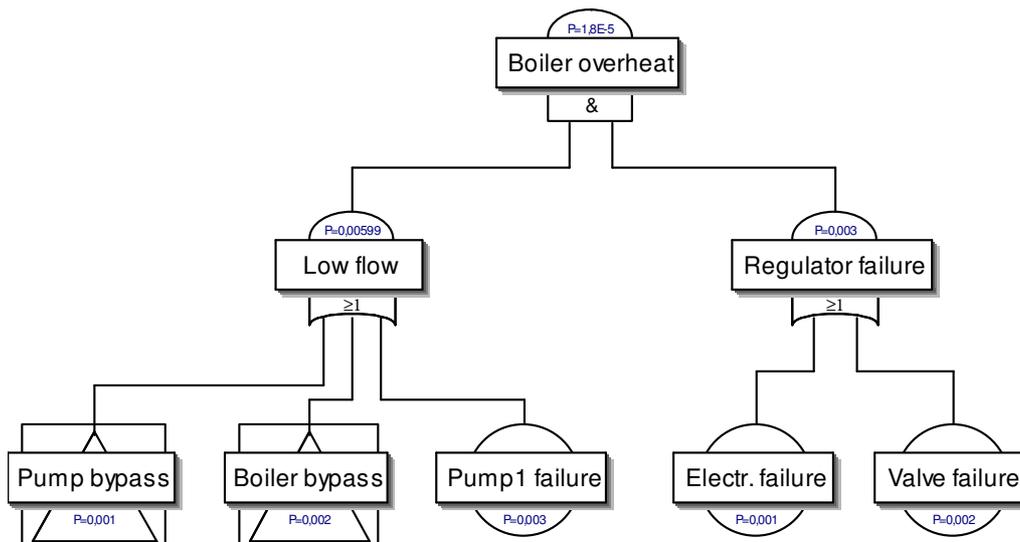
The exits from P can be negated (example on the left). Then P describes the probability that the event does not enter. This is marked by a symbol of a circle at the entrance of the following gate. The input probability of the following gate is: $P_1 = 1 - P$.

It can happen that an event applies for several gates (example on the right).

Because there is in each case only one exit, event 1 must be duplicated here. The arrangement can occur with the fact in such a way that both events 1 lie over an other to make clear that it is, actually, the same element. With the definition of the likelihood it manages in Visual-XSel on clicking an event. The duplicate takes over P if two elements are covered.

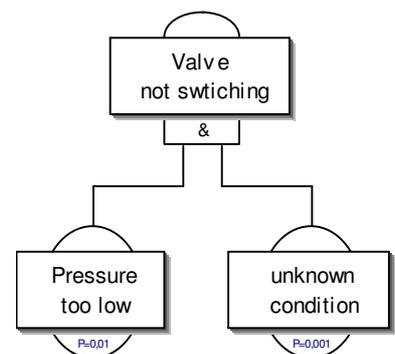


The following example shows a fault tree with calculated probabilities.



The advantage of the FTA is a easy to understanding tree structure as a basic documentation of the failure paths, even if the probability is not given. The consideration begins with the top event at the head. Down there the connections are specified more and more detailed, until one comes to the base events, or with the sub gates where the other structuring breaks off.

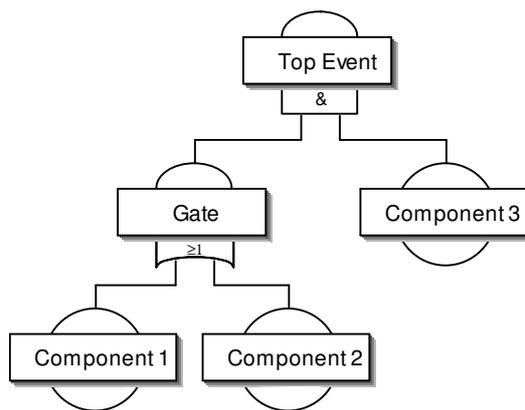
The complete production of the fault tree assumes that one can name all components and conditions. This is not always given under circumstances if, e.g., a failure appears as only temporary and is not known what condition must be still given here. This can be avoided first by a "place holder" who is to be determined later.



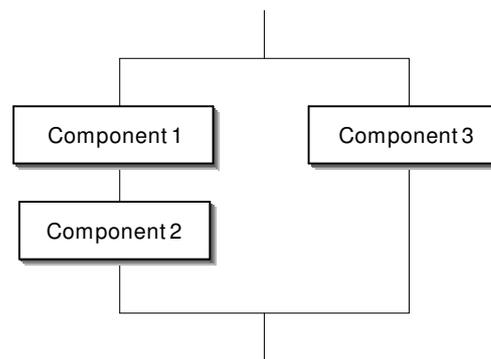
The FTA is suitable particularly for the electric / electronic area. Besides this, controls and software subjects can be also treated. Against it is not possible in the FTA to describe active connections quantitatively and to show mutual influences. Merely the appearance probability or the fault probability is settled here.

In the comparison no probability is treated moreover in a causes-effect diagram. One looks only at the "critical" moment when the fault occurs as a top event. As at the beginning described, the comparison with the reliability block diagram should be still shown (Reliability-block diagram = RBD).

Conspicuously is that here no gates are shown, but only the suitable components which are the base events in the FTA.



Fault - Tree



Reliability-Blockdiagram

While in the FTA a redundancy is shown merely as AND link, this seems more striking in the RBD by the parallel arrangement. The difference between OR / AND link is stronger emphasised here graphically. The advantage is also that here less elements are needed. However, the disadvantage of the RBD is that none Exclusive OR-links are possible.

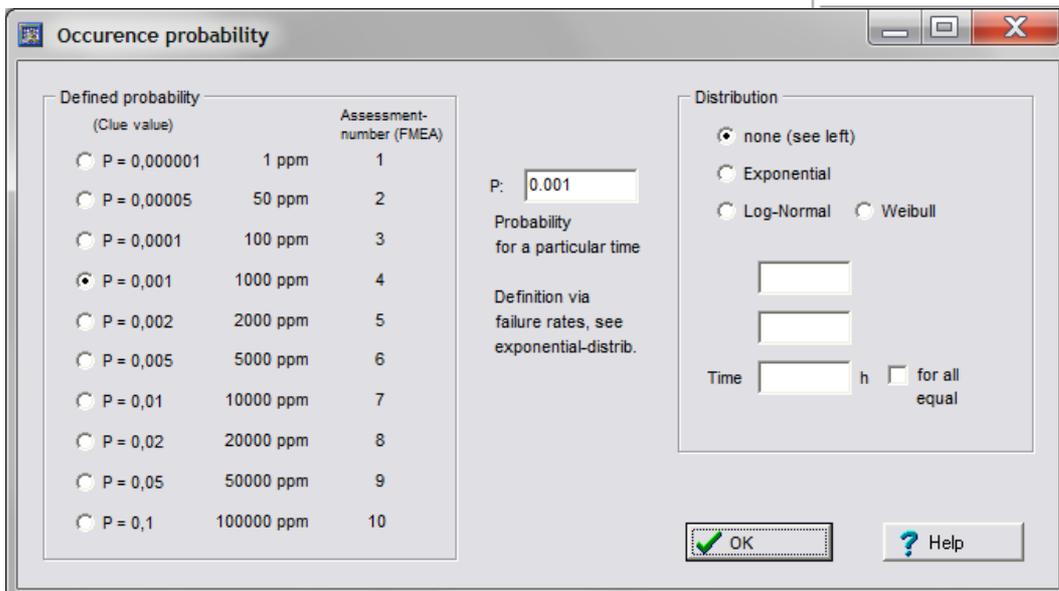
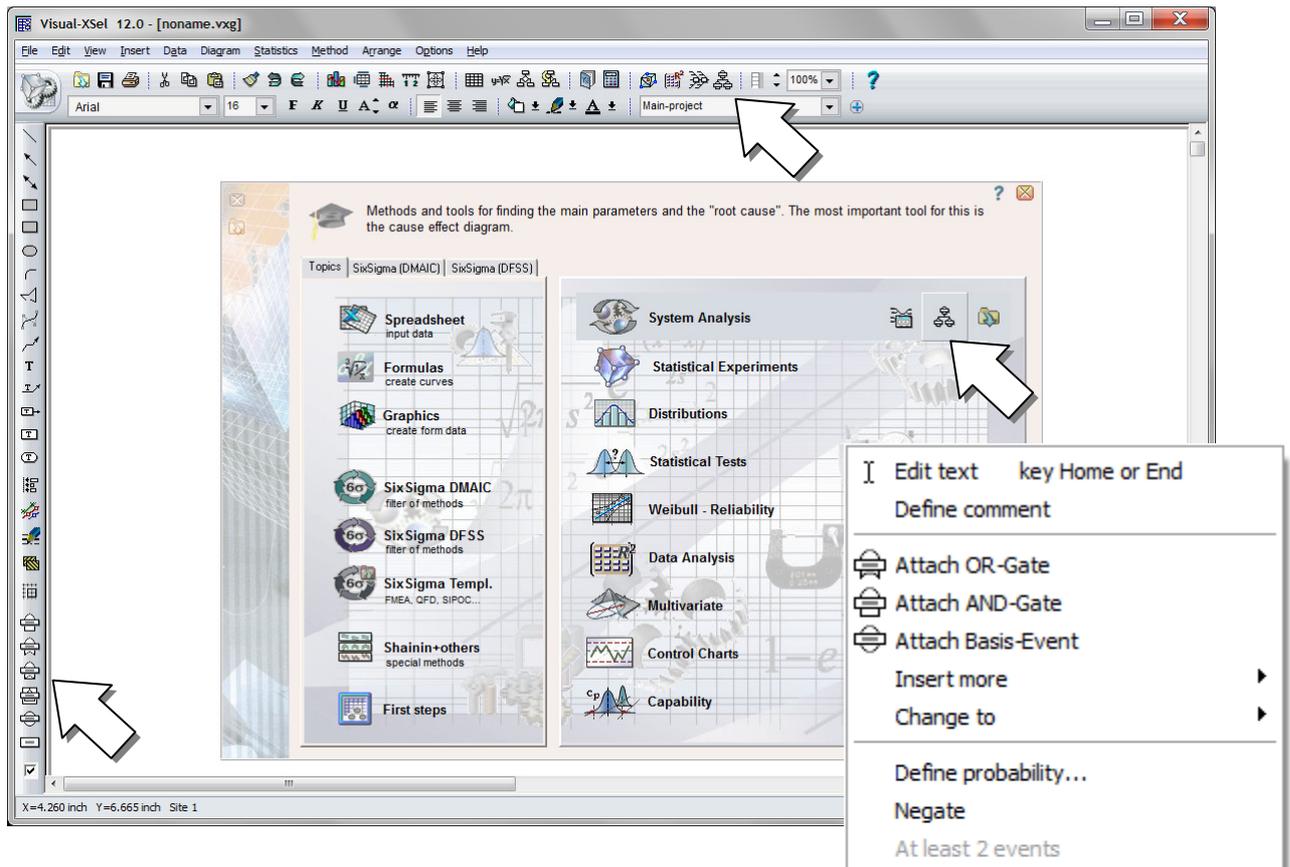
The advantage of the FTA is above all the hierarchical tree structure. Every gate shows a suitable level or a group. Through this a higher and higher level of detail is given from above down. By relatively few elements in the upper level a good entry is given to understand the "big points".

With the treatment of a problem, the comparison with a cause-effect-diagram is also looked often. If there are "conditions" or components which are not known yet, exists in the FTA the problem to name this. Here as a rule one places pseudo-elements which are to be determined even closer. In the cause-effect-diagram one is led there about the physical / technical active chain rather on the still missing connections. Further details to active diagram are described under systems-analysis.

2nd Part

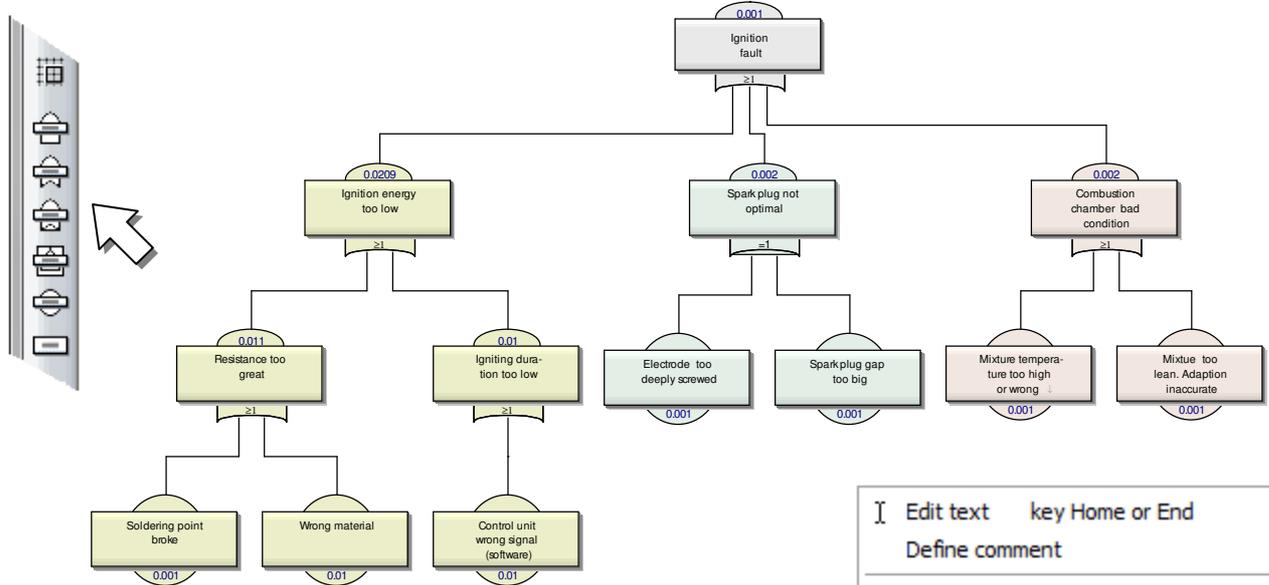
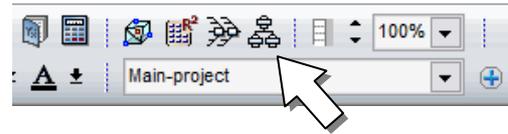
Program instructions

Visual-XSel 12.0



FTA with Visual-XSel 12.0 Multivar

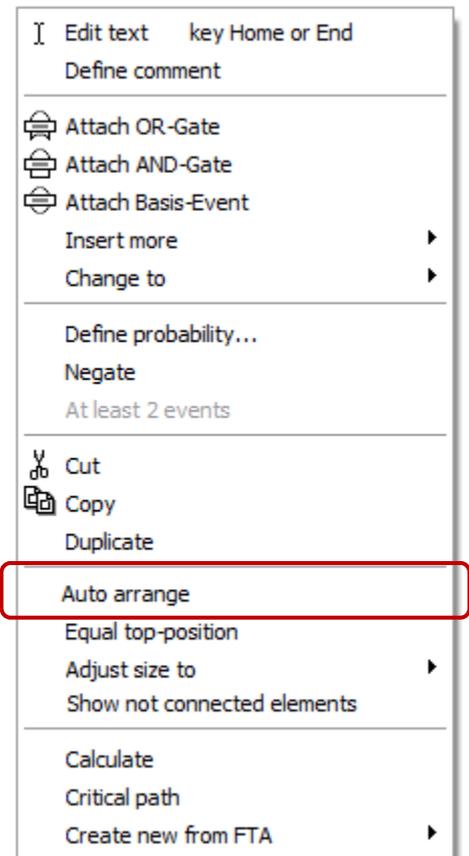
The fault tree analysis is provided in Visual-XSel 12.0 purely graphically. Moreover additional symbols appear in the icon bar on top, if the menu point Data / Fault Tree Analysis is used.



There are two kinds of representations. The first one is a free positioning of the FTA-elements. For this use the icons on the left side or better click in a FTA-element and use the right mouse button. Then select for example **Attach OR-Gate** in the popup-menu.

The second possibility is with **Auto arrange**, what is the fastest way to create FTA's. Here you have to use only the popup-menu via the right mouse button. Please note that the structure is aligned to the left of the main-window.

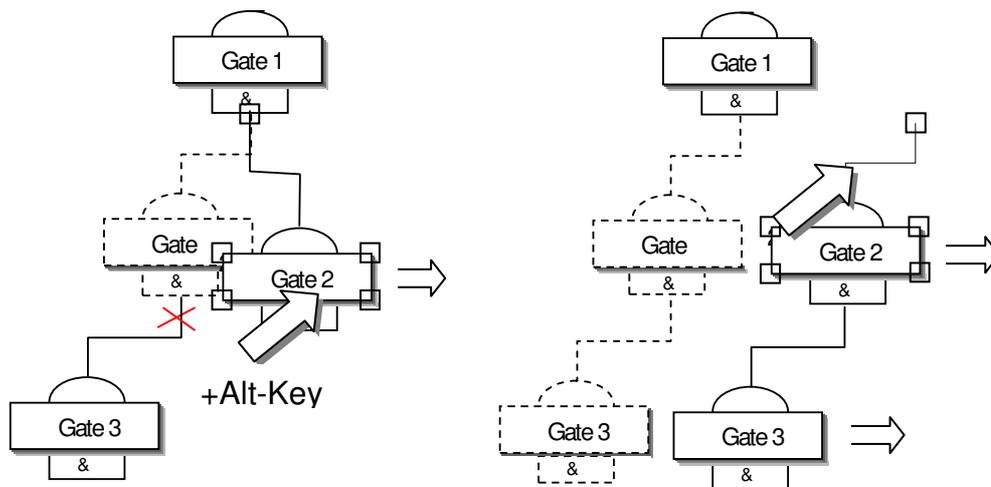
In case of printing it can happen that the paper size is not suitable. The border of the paper is shown in the main-window with a gray dotted line. Please use **Options/Format and Frames** and an adequate paper size. Normally the structure is overstepping the right border. Instead of printing side by side below each other, it will be used side by side to the right automatically. So the paper size must only inside the bottom limit.



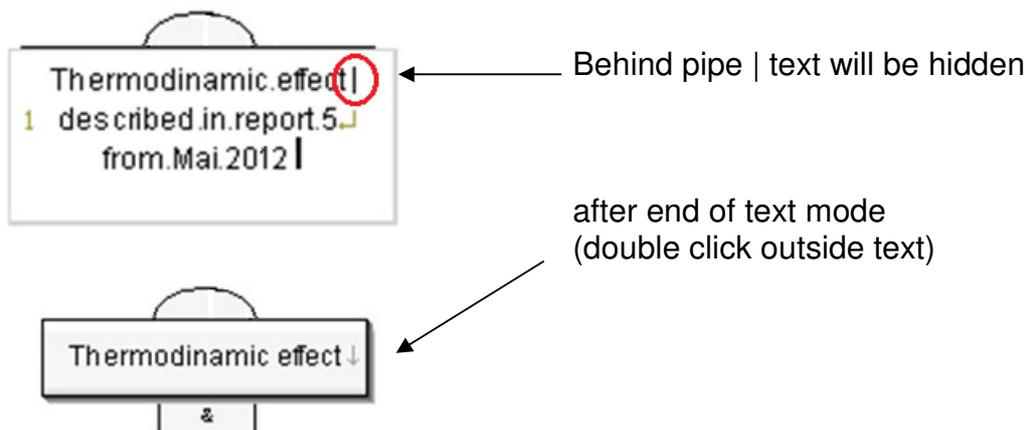
Elements can be moved by mouse, but after inserting a new element the structure will be positioned new. If this is not wanted, you can switch off the option **Auto arrange**.

Without **Auto arrange** and click to one of an element with the **Alt-key** it will be move alone. This concern also to double gates which lie on top of each other. With **Alt-key**, it is possible to separate elements. Otherwise all elements with an entrance are moved with the clicked element. Besides, own exit remains at the upper end on his

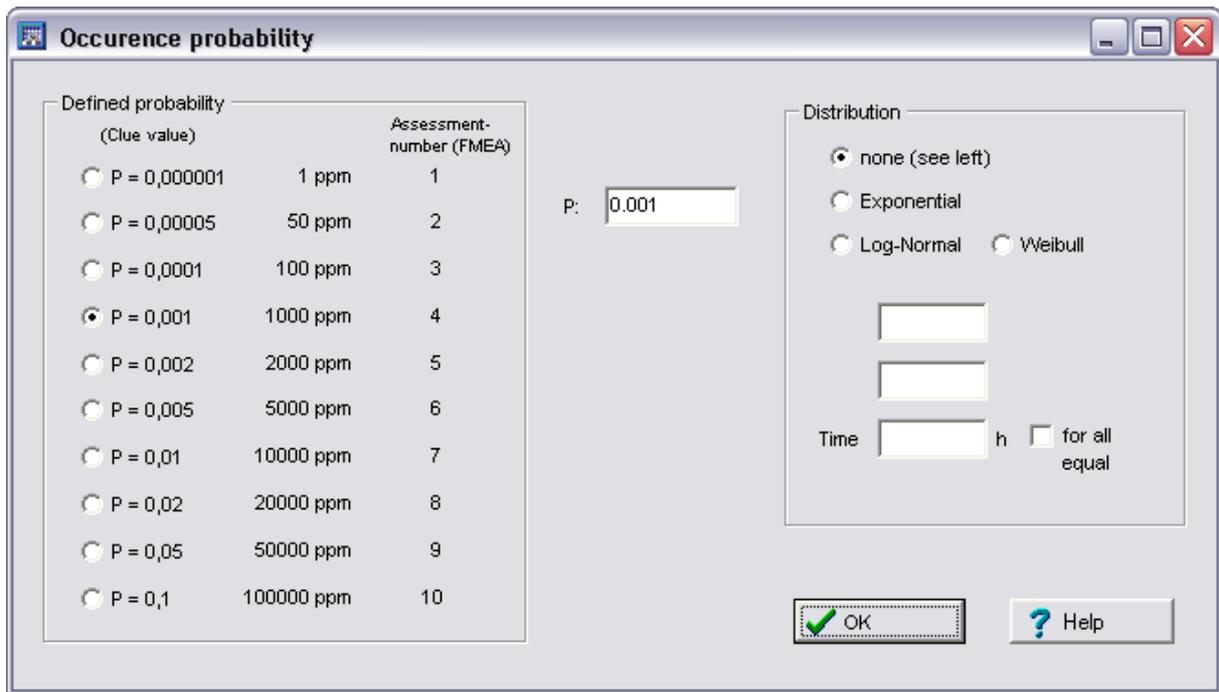
original position (picture on the left). If one goes with the mouse on the source connection, the subgroup will be moved (picture on the right).



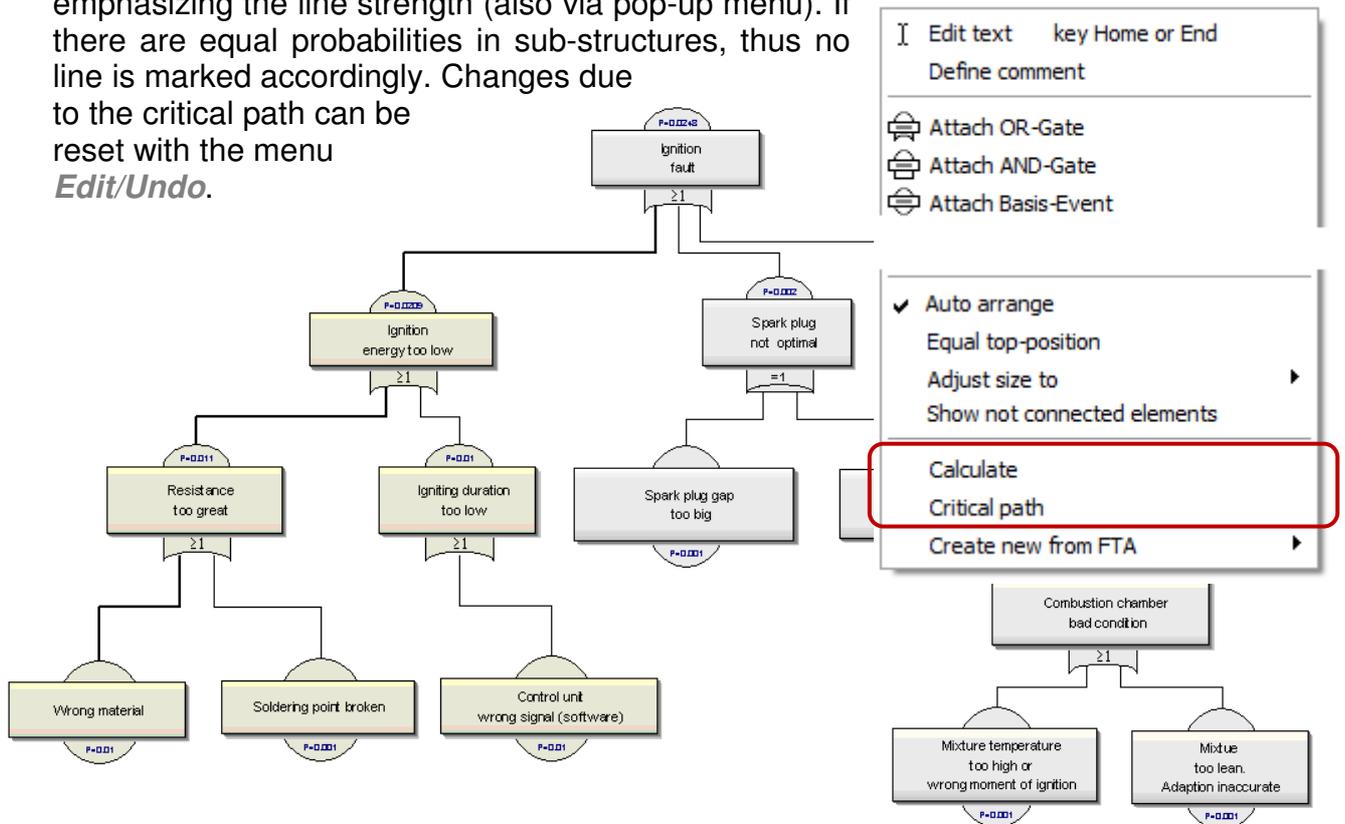
With the choice of the titles in the gates and events one should use a very clearly and exact description. However, because of less space it is not practicable to use too long text. Therefore, it is possible for a detailed description in an element to define hidden text. This not visible text becomes in the edit mode (double click or right mouse key) by the pipe sign | marked.



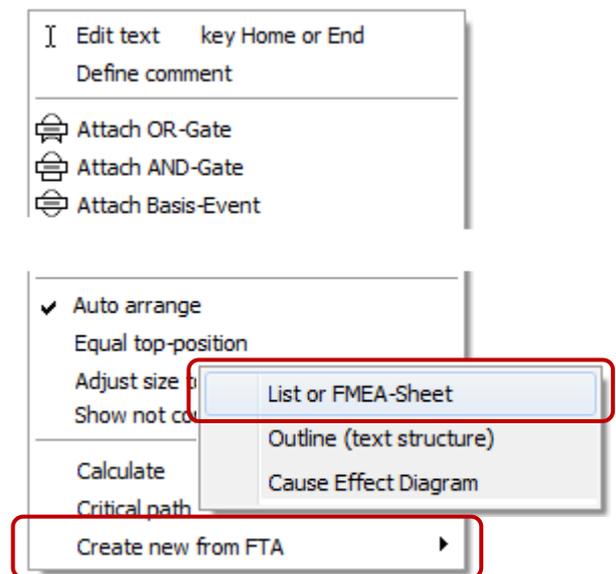
One can assign to the sub gates and base events an event or failure probability. This can be defined directly with a time independent value (left side), or about a distribution dependent on time (right side). The most-used distribution is here the exponential distribution with the failure rate λ . The time is to be understood in hours. Besides, different operating hours can be assigned to different elements. This makes sense, e.g. if in a system certain components are differently long in function and are loaded therefore calendrical differently. If the same operation duration is valid for all components, the option “for all equal” has to be selected. All FTA-elements will get the same value.



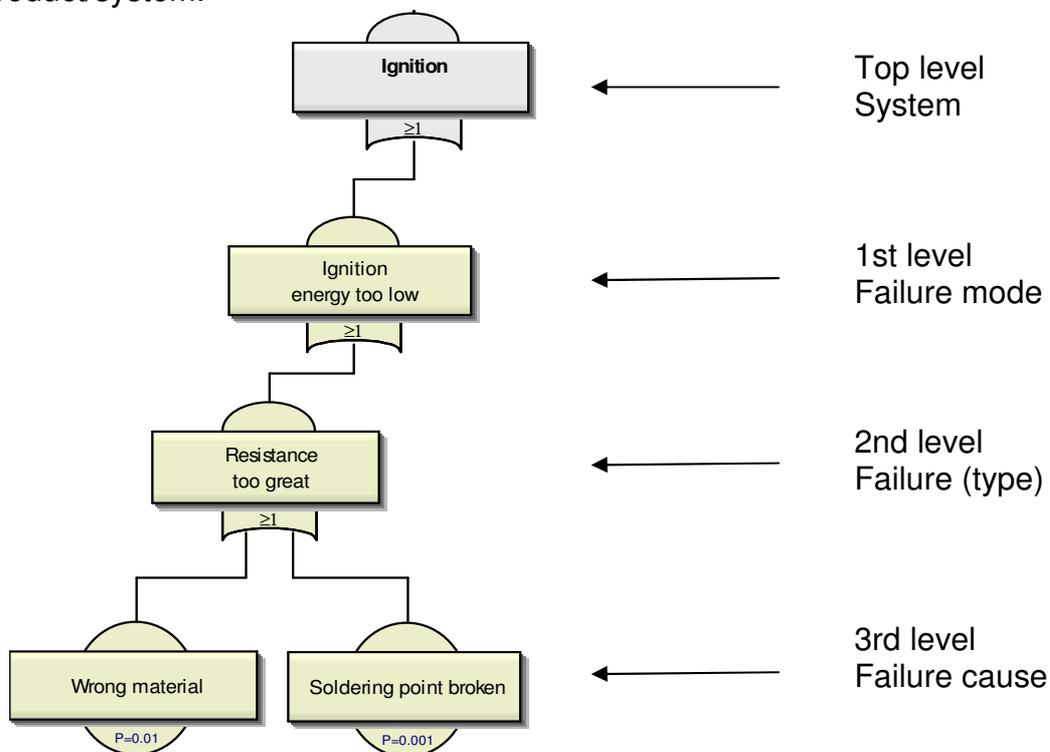
After the definition of all basis event probabilities the top-event probability can be calculated (use the pop-up menu via the right mouse button). If one liked to know, which path mostly influences the Top event, one can show this critical path by emphasizing the line strength (also via pop-up menu). If there are equal probabilities in sub-structures, thus no line is marked accordingly. Changes due to the critical path can be reset with the menu *Edit/Undo*.



The elements of the FTA can be exported in a list or a FEMA-form. For this click of an arbitrary element, and use the last choice of the pop-up menu (right mouse button).



Normally a FTA is derived from a FMEA. The shown function is a backward method. What is the advantage? At the beginning the graphically (FTA) overview is more understandable and clear, compared with a list of items. With this event based system analysis a good understanding can be approached very fast. For the export the FTA should be arranged in 3 levels. The top level, normally the top event, defines here the system. This makes sense for building up a system FTA. If using only a top event, the output is only a part of a complete product/system.



Below of the system the failure mode, the failure type and the failure cause are following. Between the system and the first level more structures (elements) can be defined, but this elements have no input in the Form. The defined probability P of the basic- or sub-gate event can be used optional as an occurrence probability (risk). This confirms also to an assessment-value.

	A	B	C	D	E	F	G	H	I
1									
2	Project:				FMEA: Form				
3									
4	System:				Process-FMEA		Product-FMEA		
5					Name / departure		Name of Process- / Product:		
6									
7	S-Severity			C-Attribute			O-Occurrence probability		
8									
9									
10		Failure mode	S	Failure	C	Failure cause	Avoidance action	O	Detection action
11	1	Ignition fault		Combustion chamber bad condition		Mixture temperature too high or wrong		4	
12									
13	2	Ignition fault		Combustion chamber bad condition		Mixture too lean. Adaption inaccurate		4	
14	3	Ignition fault		Spark plug not optimal		Spark plug gap too big		4	
15	4	Ignition fault		Spark plug not optimal		Electrode too deeply screwed		4	
16	5	Ignition energy too low		Igniting duration too low		Control unit wrong signal (software)		7	
17	6	Ignition energy too low		Resistance too great		Wrong material		7	
18	7	Ignition energy too low		Resistance too great		Soldering point broken		4	
19									
20									

All other fields in the FMEA-form must be filled in the table. If there are changes in the FTA a new table will be created the present entries are preserved. To combine the existing definitions with the new table, use copy and paste.

To learn about basics of the FMEA and getting continuing information here must be refer to the appropriate literature.

In Visual-XSel there can be build up a FTA and a cause-effect-diagram in the same file. This makes it possible to have different perspectives and to get specifically advantages of both methods. For more information to the cause-effect-diagram see Systemanalysis.pdf.

An alternative to the FTA is the Reliability-Block diagram which is defined in an own window (see menu Data/ Reliability-Block diagram).

Visual-XSel[®] 12.0

® Visual-XSel is a trademark of CRGRAPH