



## **a medini™ solutions application report**

### **fault tree analysis for model based development of safety critical functions**

#### **background**

Over the past years, more and more safety critical functions in cars, trains and aircrafts are becoming realized by software. Participants in the development process need to be aware of the safety criticality and have to apply specific methods to make sure that the function developed is not harmful to the environment in both normal and mal-functional operation. Qualitative and quantitative risk and effects analysis methods are applied at the system and component configuration level in order to identify and eliminate harmful behavior or at least reduce it to a tolerable level. One popular quantitative risk analysis method is fault tree analysis (FTA).

#### **how can one apply FTA in software development processes?**

Modern development processes put software models in the center of all system engineering activities; one prominent development tool here is certainly MATLAB/Simulink. Quantitative risk analysis for software functions means first to translate the potentially harmful and undesired situations, which have been identified, into combinations of output signals of the model. Thereafter, the design model can be analyzed in order to find the potential sources of such undesired output signal combinations. The probability and frequency of such source events are used to compute the resulting probability/frequency of the harmful situation.

#### **supporting medini™ solution for the process**

Targeting the improvement of potentially iterative development, we have tightly integrated our medini™ FTA tool with MATLAB/Simulink for the customer in order to provide fine-grained traceability, automated mappings between MATLAB/Simulink model elements and FTA elements as well as automatic re-runs of analysis steps in case of changes to the models.

**we automate system creation –  
with medini™ solutions**

we automate your processes with medini™

we analyze your development process activities and procedures jointly with your process experts.

we identify candidate activities which would profit from introducing automation.

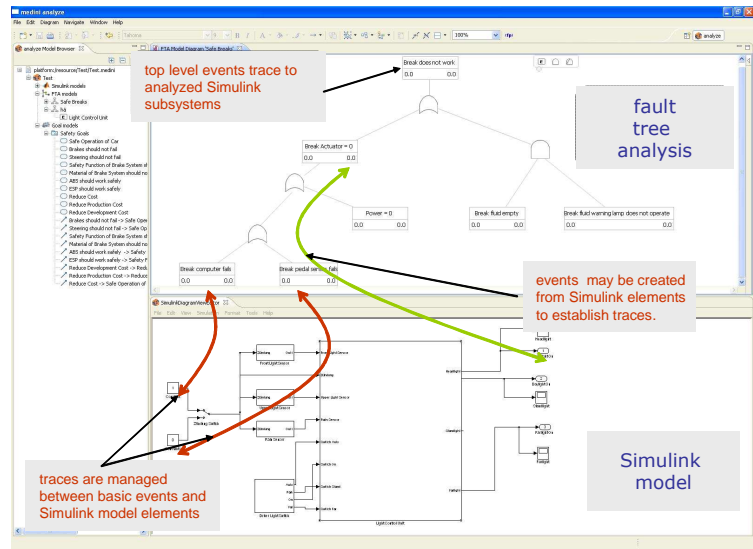
we configure available components from our medini tool box and create automated tool chains, customized to your process.

you benefit from automation,  
consistency and artifact validation.

## and the engineer's view?

The engineer uses an integrated development environment based on the medini™ cockpit user interface framework, that provides a combined view of the FTA and the Simulink model under investigation.

For additional customization, the cockpit is embedded in the eclipse environment, allowing Simulink model elements to be accessed and manipulated from other eclipse based tools. The figure on the right gives an impression.



## customer advantages

The advantages of such an integrated approach have become most significant during the following scenarios:

- creation of basic events in the FTA from design model elements, specifically from system and subsystem inputs and outputs, and keeping traceability between them,
- change impact analysis, i.e. traceability between FTA and design model elements is facilitated to point to those parts of the FTA that need reconsideration in the event of model changes,
- partially automated creation of FTA from design model, i.e. by analyzing the data flow and operator logic in the design model we can create parts of the FTA
- configuration optimization, i.e. if the FTA is used with a given probability for the top level event (typically determining the safety integrity requirement), and alternative configurations of subsystems exist, the FTA together with probabilistic evaluation can be used to calculate the most effective configuration to meet the safety requirement.

*do you need more information?  
do you have questions?  
how can we automate your process?*

**contact us at**

[www.ikv.de](http://www.ikv.de)

tel +49 (30) 3480 770

email [information@ikv.de](mailto:information@ikv.de)



ikv++ technologies ag