

---

# Safety and Reliability of Embedded Systems

## (Sicherheit und Zuverlässigkeit eingebetteter Systeme)

### Fault Tree Analysis Selected Tools

### Content

---

- ☐ Tool Selection
- ☐ Tool Overview
  - Faulttree+
  - Relex
  - BlockSim
  - Galileo
  - UWG3 / ESSaRel
- ☐ Other Tools

## Selection Criteria

---

- ☐ Purpose / Characteristics
  - Drawing Tool
  - Pure FT Analyzer
  - Integrated Analyzer (e.g. Markov, Event Tree Analyzer, FMEA)
- ☐ Expressiveness
  - Supported Types of Gates
  - Support of Repeated Events
- ☐ Analysis Capabilities
  - Fast Algorithm (BDD)
  - Limits (Number of Nodes etc.)
  - Useful and Justified Approximations
  - Minimal Cut-Set Listing
  - Importance Measures

## Selection Criteria

---

- ☐ Presentation of Results
  - Exportable Tables for Numerical Results and MCS Lists
  - Report Generation
  - Graphical Highlighting of Cut Sets etc.
- ☐ Handling / Ergonomics
  - Project Explorer / Structuring / Search Capabilities
  - Positioning and Routing Aids
  - Table Input for Large Amounts of Numerical Data
  - Reuse of Trees and Partial Trees from the Same / Other Projects
- ☐ Side Conditions
  - Licensing / Prices
  - Operating Systems
  - Required Hardware

## Tool Selection

---



**Claim a (full) trial version!**

**Do a small example FTA that you prepared ahead.**

**Let the final users judge the usability!**

**Try some test cases (e.g. for repeated event correctness)**

## Tool Overview

---

- ☐ Faulttree+
- ☐ Relex
- ☐ BlockSim
- ☐ Galileo
- ☐ UWG3 / ESSaRel

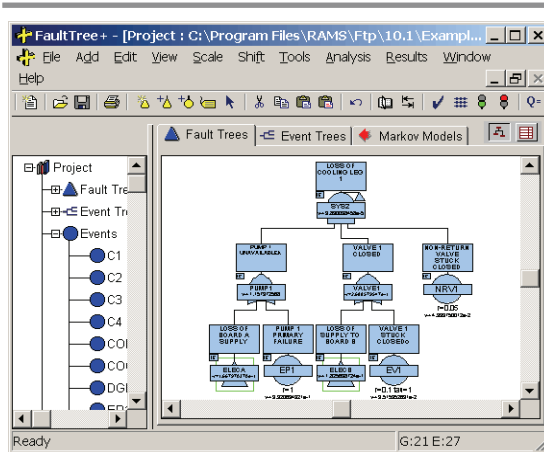
... are shown in more detail as examples.

Others are listed at the end of the presentation



**The features lists are based on material supplied by the vendors!**

## FaultTree+



[www.isograph-software.com](http://www.isograph-software.com)

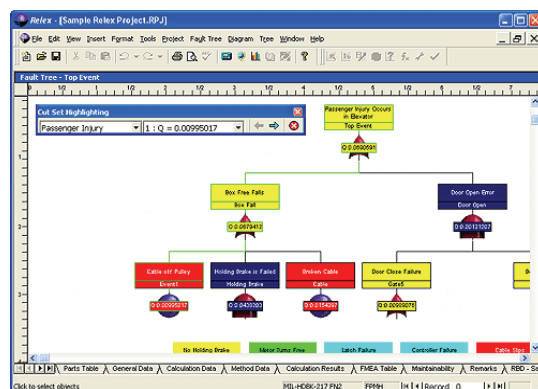
- ☐ By Isograph Software
- ☐ Popular Tool
- ☐ Tree Construction by Drag-and-Drop
- ☐ Includes Event Tree Analysis and Markov Analysis
- ☐ Different Failure Models
- ☐ Enabler / Initiator Events
- ☐ Common Cause Failures
- ☐ Can be integrated into a workbench

Safety and Reliability of Embedded Systems

ENGINEERING  
SOFTWARE  
DEPENDABILITY

Prof. Dr. Liggesmeyer, 6

## Relex



[www.relexsoftware.com](http://www.relexsoftware.com)

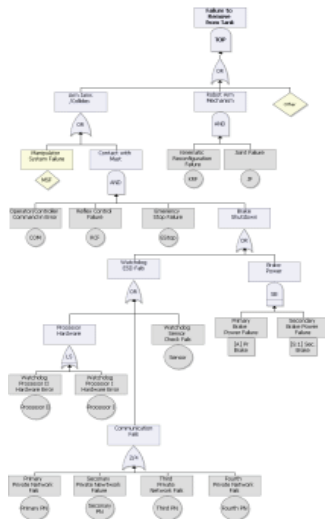
- ☐ By Relex Software
- ☐ Popular Tool
- ☐ Extended Standard Gates Set (e.g. Priority AND, Spare, Sequence Enforcing...)
- ☐ Different Analysis Algorithms
- ☐ Fast MCS Algorithm
- ☐ MCS Highlighting
- ☐ Different Common Cause Failure Models
- ☐ Also for Event Trees

Safety and Reliability of Embedded Systems

ENGINEERING  
SOFTWARE  
DEPENDABILITY

Prof. Dr. Liggesmeyer, 7

## BlockSim 6 FTI Edition



- ☐ By Reliasoft
- ☐ Recent FTA extension for an existing RBD tool
- ☐ Can convert between both models
- ☐ Specific gates (Standby, Load Sharing)

[www.reliasoft.com](http://www.reliasoft.com)

ENGINEERING  
**SOFTWARE**  
DEPENDABILITY

• Prof. Dr. Liggesmeyer, 8

## Safety and Reliability of Embedded Systems

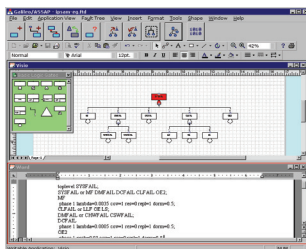


## Galileo/ASSAP Dynamic Fault Tree Analysis Tool



## Fault Trees

- ◆ Versatile mathematical reliability models
- ◆ A graphical representation of a logical function
- ◆ Can model both static or dynamic failure criteria
- ◆ Provides a logical framework for:
  - Combinations of component failures leading to system failure
  - Showing relationship between an event (failure) and its causes



## Dynamic Fault Tree Methodology

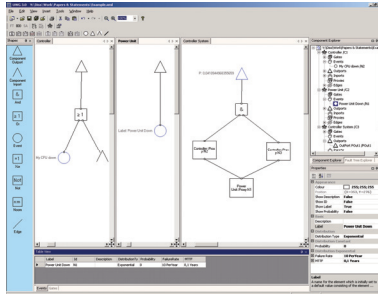
- ◆ Automatic modularization of fault trees &
- ◆ Independent solution of modules
- ◆ Efficient solution for
  - Static fault tree modules using binary decision diagrams
  - Dynamic fault tree modules using Markov-based techniques
- ◆ Multiple time-to-failure distributions
- ◆ Static and dynamic coverage modeling
- ◆ Sensitivity analysis and uncertainty analysis of basic events
- ◆ Special gates for modeling sequential behavior
  - Conversion of DFT into a Markov chain for solution
  - Modularization of complex fault trees
- ◆ Modeling and analysis of phased missions
- ◆ Diagnostic map to help determine cause of failure and optimize repair

## Package Oriented Programming (POP)

- ◆ COTS-based user interface *i.e.* built from widely used components
  - MS Word Editor interface
  - MS Visio Graphical interface
- ◆ Capability to edit fault tree in either textual or graphical representation
- ◆ Automatic rendering from textual view to graphical view, or vice-versa.
- ◆ Fault trees spanning multiple pages
- ◆ Enhanced graphical editing capability

[www.cs.virginia.edu/~ftree/](http://www.cs.virginia.edu/~ftree/)

## UWG3 / ESSaRel



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

- ☐ Windows based GUI Tools under .NET
  - Intuitive Use (Drag&Drop, Project Explorer...)
  - XML File-Format for Collaboration and Reuse
- ☐ **UWG3**
  - Supports Component Fault Trees
  - First Version in 2003
  - Successful Evaluation in Industry Projects
- ☐ **ESSaRel** (Embedded Systems Safety and Reliability Analyser)
  - Available Spring 2005
  - Integrates State-Event-Fault-Trees, Markov Chains and State Diagrams
  - Analysis by Translation to Petri Nets (DSPNs)

## Other Tools

- ☐ CAFTA
- ☐ FaulttrEASE
- ☐ CARA
- ☐ CARE
- ☐ SAPHIRE
- ☐ Item
- ☐ TTREE
- ☐ Risk Spectrum Fault Tree
- ☐ Tree Master
- ☐ Formal-FTA
- ☐ Logan



Good Overview: <http://www.enre.umd.edu/ftap.htm>