Lesson learnt from the Isograph Training Course
Winterthur 24th to 26th of July 2017

Miriam Blumenschein, Saskia Hurst and Estrella Vergara
- RAS Working Group Meeting -
31st of August 2017
1. Isograph for beginners

Estrella Vergara
Reliability Workbench

Available in CMF Packages: Isograph – RelWorkbench 13.01

Modules available

- Prediction Methods
- Failure Mode Effect and Criticality Analysis (FMECA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Markov Analysis
- Weibull
- Reliability Growth
- Reliability Allocation

CERN licenses

During installation...

Password needed for installation: cernvflxn07

Tutorials for each module:
Help → Getting Started → Tutorial
Prediction module

Provide consistent methods of estimating failure rates using Handbooks and standards

- Entering prediction data manually or using libraries (Project and Library must follow the same Standard or Handbook)
- Possibility to associate maintenance tasks in the prediction hierarchy
- Option to specify the phases if the ambient conditions change during the lifetime of the system

CERN license:
- Telecordia TR/SR
- MIL-217 Prediction
- NSWC Prediction

Only 1 license:
- 217 Plus Prediction
- FIDES Prediction

Environmental Properties

Parameters for the component type (defined by Handbook or Standard)
- External Category: entering data manually
Prediction module

Results

<table>
<thead>
<tr>
<th>ID</th>
<th>Part number</th>
<th>Description</th>
<th>Parent</th>
<th>Category</th>
<th>Sub category</th>
<th>Failure rate</th>
<th>MTTF</th>
<th>MTTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0-1</td>
<td>Motherboard 1</td>
<td>1</td>
<td>System Block</td>
<td></td>
<td>42.47</td>
<td>0.02354</td>
<td>6</td>
</tr>
<tr>
<td>1.1</td>
<td>0-1-1</td>
<td>CPU 1</td>
<td>1</td>
<td>Microprocessor</td>
<td>TTL</td>
<td>31.23</td>
<td>0.03202</td>
<td>0</td>
</tr>
<tr>
<td>1.2</td>
<td>0-1-2</td>
<td>Memory 1</td>
<td>1</td>
<td>Micro, Not EEPROM</td>
<td>ROM</td>
<td>7.935</td>
<td>0.126</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0-2</td>
<td>Motherboard 2</td>
<td>1</td>
<td>System Block</td>
<td></td>
<td>42.47</td>
<td>0.02354</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>0-2-1</td>
<td>CPU 2</td>
<td>2</td>
<td>Microprocessor</td>
<td>TTL</td>
<td>31.23</td>
<td>0.03202</td>
<td>0</td>
</tr>
<tr>
<td>2.2</td>
<td>0-2-2</td>
<td>Memory 2</td>
<td>2</td>
<td>Micro, Not EEPROM</td>
<td>ROM</td>
<td>7.935</td>
<td>0.126</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0-3</td>
<td>Memory 3</td>
<td>3</td>
<td>System Block</td>
<td></td>
<td>9.039</td>
<td>0.1106</td>
<td>6</td>
</tr>
<tr>
<td>3.1</td>
<td>0-3-1</td>
<td>Memory 3</td>
<td>3</td>
<td>Micro, Not EEPROM</td>
<td>ROM</td>
<td>7.935</td>
<td>0.126</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0-4</td>
<td>Disk 1</td>
<td>4</td>
<td>External</td>
<td></td>
<td>0.4</td>
<td>2.5</td>
<td>0</td>
</tr>
<tr>
<td>4.1</td>
<td>0-4-1</td>
<td>Disk 1</td>
<td>4</td>
<td>System Block</td>
<td></td>
<td>0.4</td>
<td>2.5</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0-5</td>
<td>Disk 2</td>
<td>5</td>
<td>System Block</td>
<td></td>
<td>0.807</td>
<td>1.647</td>
<td>12</td>
</tr>
<tr>
<td>5.1</td>
<td>0-5-1</td>
<td>Disk 2</td>
<td>5</td>
<td>External</td>
<td></td>
<td>0.4</td>
<td>2.5</td>
<td>0</td>
</tr>
</tbody>
</table>

Plots

![MTTF vs Temperature](chart1.png)

![Failure rate vs Temperature](chart2.png)
Fault Tree Analysis (FTA)

- Show interaction to failures
- Creation of fault trees manually

### Gates Types

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Meaning</th>
<th>Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>True if any input is True</td>
<td>≥2</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>True if all inputs are True</td>
<td>≥2</td>
<td></td>
</tr>
<tr>
<td>VOTE</td>
<td>True if $m$ inputs are True</td>
<td>≥3</td>
<td></td>
</tr>
<tr>
<td>EXCLUSIVE OR</td>
<td>True if one and only one input is True</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>INHIBIT GATE</td>
<td>True if all inputs are True; one input is conditional</td>
<td>≥2</td>
<td></td>
</tr>
<tr>
<td>PRIORITY AND</td>
<td>True if inputs occur in left to right order</td>
<td>≥2</td>
<td></td>
</tr>
<tr>
<td>NOT</td>
<td>True if inputs is FALSE</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Transfer In</td>
<td>Inputs appear elsewhere on same page or another page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer Out</td>
<td>Output appears elsewhere on same page or another page</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Event Types

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIC</td>
<td>BASIC</td>
<td>Basic event</td>
</tr>
<tr>
<td>UNDEVELOPED</td>
<td>A system event which is yet to be developed</td>
<td></td>
</tr>
<tr>
<td>CONDITIONAL</td>
<td>Conditional event connected to an inhibit gate</td>
<td></td>
</tr>
<tr>
<td>HOUSE</td>
<td>HOUSE</td>
<td>Definitely operating or definitely not operating</td>
</tr>
<tr>
<td>DORMANT</td>
<td>DORMANT</td>
<td>Failure not immediately revealed; latent/ hidden failure</td>
</tr>
</tbody>
</table>
Fault Tree Analysis (FTA)

- Show interaction to failures
- Creation of fault trees manually thought gates

Simple Cooling System

- No limit of gates or events ("Page" checkbox)
- Special Function: Multiple Project option:
  - ID must be coherent
  - Connection between gates (no events)
- Minimal Cut Set:
  - Minimum combination of events which cause TOP event
  - First step of Analysis
  - Produced using Boolean algebra
Reliability Block Diagram (RBD)

- Used to predict the **reliability** of entire systems
- Similar to FTA:
  - RBD → Process (availability) / FTA → Hazards

**Simplified Computer System Schematic**

- Flow from left to right – easy to read
- Blocks connected in series/parallel
- Option to Copy-Paste to duplicate a block (e.g. “MEM 3”)
- Special functions: RBD to FTA, Prediction to RBD and FMECA to RBD
Reliability Block Diagram (RBD)

ASSIGNING FAILURE MODELS TO BLOCKS

- Failure and repair date is entered in a failure model
  - Local Failure Model: attached to one block only
  - Generic Failure Model: can be attached to multiple blocks
- Applicable for FTA as well

Generic Failure Models

Assigning Generic Failure Model to a Block
Reliability Block Diagram (RBD)

PERFORMING AN ANALYSIS - Results

Summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Point Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unavailability</td>
<td>2.861E-12</td>
</tr>
<tr>
<td>Frequency</td>
<td>1.717E-06</td>
</tr>
<tr>
<td>CFI</td>
<td>1.717E-06</td>
</tr>
<tr>
<td>Number expected failure</td>
<td>1.717E-06</td>
</tr>
<tr>
<td>Unavailability</td>
<td>1.717E-06</td>
</tr>
<tr>
<td>MTTF</td>
<td>Not calculated</td>
</tr>
<tr>
<td>MTTR</td>
<td>Not calculated</td>
</tr>
<tr>
<td>Total downtime</td>
<td>2.861E-12</td>
</tr>
<tr>
<td>Mean unavailability</td>
<td>2.861E-12</td>
</tr>
<tr>
<td>Risk reduction factor</td>
<td>3.498E+11</td>
</tr>
<tr>
<td>Q/T</td>
<td>2.861E-12</td>
</tr>
<tr>
<td>Used method</td>
<td>Cross product</td>
</tr>
<tr>
<td>Number of compact states</td>
<td>5</td>
</tr>
</tbody>
</table>

Cut Sets: Combination of component block failures that will cause system failure

<table>
<thead>
<tr>
<th>No.</th>
<th>Q</th>
<th>Minimal cut set</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.778E-12</td>
<td>DISK 1, DISK 2</td>
</tr>
<tr>
<td>2</td>
<td>1.084E-12</td>
<td>CPU 1, CPU 2</td>
</tr>
<tr>
<td>3</td>
<td>9.662E-13</td>
<td>CPU 1, MEM 3, MEM 2</td>
</tr>
<tr>
<td>4</td>
<td>2.466E-17</td>
<td>MEM 1, MEM 3, MEM 2</td>
</tr>
<tr>
<td>5</td>
<td>9.662E-13</td>
<td>MEM 1, CPU 2, MEM 3</td>
</tr>
</tbody>
</table>

Importance: Block's contribution to the unavailability of the system
Event Tree Analysis (ETA)

- Identifies outcomes of initiating event
- ETA & FTA closely linked:
  - FTA can be used to quantify events in ETA sequence
  - Use cut sets and same quantitative methodology

Fault Tree created in FTA module

Event Tree Analysis

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Fatalities</td>
<td>0.1838</td>
</tr>
<tr>
<td>1 Fatality</td>
<td>0.01265</td>
</tr>
<tr>
<td>2 to 8 Fatalities</td>
<td>0.003335</td>
</tr>
<tr>
<td>Greater than 8 Fatalities</td>
<td>0.0002294</td>
</tr>
</tbody>
</table>
### Failure Mode Effect and Criticality Analysis (FMECA)

- Rates failure modes by danger

<table>
<thead>
<tr>
<th>Id</th>
<th>Component</th>
<th>FMEA CIBDS: Failure chain all levels</th>
<th>Date: 05/07/2017</th>
<th>Page 1 of 38</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Id Component FM</td>
<td>Effects immediate</td>
<td>Effects +1</td>
</tr>
<tr>
<td>1.1.1</td>
<td>P1</td>
<td>not considered</td>
<td>Effects +2</td>
<td>Effects +3</td>
</tr>
<tr>
<td>1.1.2</td>
<td>P2</td>
<td>not considered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3</td>
<td>IC26</td>
<td>Input open</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output open</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supply open</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output stuck low</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td>1.1.4</td>
<td>IC22</td>
<td>Input open</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output open</td>
<td>1.1.3 Incorrect monitoring information</td>
<td>1.1.6 Incorrect monitoring information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. **Compendium of useful features**

Miriam Blumenschein

Prediction – FMECA – Fault Tree
Prediction

1. **Component library**
   - Construct a project from a library:
     - *File ➤ Attach Library*
     - Drag and drop parts or structures to system structure
     - No automatic update if library is modified
   - Build a library: create components in prediction (blue fields)
   - Common CERN library?

![Diagram of a library in a project management tool with components listed and a library tab highlighted.](image)
2. **Import of bill of material:**
   - Easy to import: blue fields (component properties) part number, ID, quantity, description and category
   - Manual chapter “Importing a Bill of Materials”
   - Not (yet) easy to import: black fields (operating environment), filled in manually
   - Common Excel format of BOM?

<table>
<thead>
<tr>
<th>Id</th>
<th>PartNumber</th>
<th>Quantity</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0-1</td>
<td>1</td>
<td>OPL-Repeater_HW02</td>
<td>MIL-BK</td>
</tr>
<tr>
<td>2</td>
<td>0-2</td>
<td>1</td>
<td>OPL-Trans_1414_HW02</td>
<td>MIL-BK</td>
</tr>
<tr>
<td>3</td>
<td>0-3</td>
<td>1</td>
<td>OPL-REC-2418_HW02</td>
<td>MIL-BK</td>
</tr>
<tr>
<td>1.1</td>
<td>C-EUC0805_1000nF</td>
<td>1</td>
<td></td>
<td>MIL-CR</td>
</tr>
<tr>
<td>1.2</td>
<td>C-EUC0805_100nF</td>
<td>1</td>
<td></td>
<td>MIL-CR</td>
</tr>
<tr>
<td>1.3</td>
<td>C-EUC0805_100nF</td>
<td>1</td>
<td></td>
<td>MIL-CR</td>
</tr>
<tr>
<td>1.4</td>
<td>AFBR-2418</td>
<td>1</td>
<td></td>
<td>MIL-LB</td>
</tr>
<tr>
<td>1.5</td>
<td>C-EUC0805_100nF</td>
<td>1</td>
<td></td>
<td>MIL-CR</td>
</tr>
</tbody>
</table>
3. **Rename option**
   - Objects under the current tree control selection will be renamed based on the name of their parent
   - *Select parent block ➤ Tools ➤ Rename ➤ Blocks under selection*

4. **View option:**
   - Determination of the data which is displayed in the project tree control
   - *Project Options ➤ View ➤ check “Show category”; “Show component part; … number”*
Prediction

5. **Help option in dialog boxes**
   - “?” on the top right in each dialog opens corresponding chapter of the manual

6. **Part number**
   Several Functions are linked to the part number
   - Blue fields = component properties: same properties for same part number
   - Black fields = operating environment: independent of part number
   - Part Selection facility, Auto search project, auto search library, Auto Add Apportioned Failure Modes, Linked block, …
Prediction

7. **Unit of failure rate**
   - *Project Options ➤ General ➤ Units*

8. **Change component parameters**
   - Temperature, Environment, …
   - *Select section in tree control ➤ Special Functions ➤ change temperature/ MIL-217 environment*
   - OR
     - Export block properties to Excel (table PDBlocks; columns PartNumber, ParamValuesKey), find and replace properties in Excel, import Excel file

9. **Project Options, Special Functions and Tools**
   - change from one module to the other, always worth having a look at

10. **Recommendation:** Always create system structure in the prediction module, even if no prediction is performed
From one module to another

1. **Data conversion**
   - prediction hierarchy to FMECA, RBD, fault tree
   - FMECA hierarchy to RBD, fault tree
   - RBD to fault tree
   - Common way: Prediction to FMECA to Fault Tree
   - *Special Functions ➤ Convert pull-down menu*

2. **Data links**
   - Needs to be defined before the data conversion!
   - Data links will be automatically created between objects when copying between modules
   - Customize data conversion: *Project options ➤ Data links ➤ check “Assign data link on inter-module copy within project”*
   - Prediction to FMECA: Edit ➤ *Transfer linked data ➤ run the FMECA simulation*
   - *FMECA to Fault Tree: Run the FMECA simulation ➤ Edit ➤ Transfer linked data ➤ run the Fault Tree simulation*

3. **Update of system structure**
   - Failure modes remain
   - Prediction to FMECA: *Special Functions ➤ Convert pull-down menu*
FMECA-module

1. Apportionment table
   - Lists a component type (defined by the part number) and its failure modes and %
   - Apportionment table can be imported from excel
   - Add failure modes to existing blocks: Add ► Auto Add Apportioned Failure Modes
     OR
   - Add apportioned block
   - Common CERN apportionment table?
# FMECA-module

## 2. Severity matrix
- Tabulates the number of failure mode contributors in each severity category for each block in the system
- Exported as excel file
- If severity categories are defined as system failure modes: number of root contributors per system failure mode
- *Special Functions ➤ Export ➤ Severity Matrix*

## 3. Criticality matrix
- Tabulates the severity category and criticality for each failure mode
- *Special Functions ➤ Export ➤ Criticality Matrix*

<table>
<thead>
<tr>
<th>Block Name</th>
<th>Block Description</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>POWER SUPPLY</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>1.1</td>
<td>CAPACITOR, FIXED CK</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>1.2</td>
<td>CAPACITOR, FIXED CB</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>CAPACITOR, FIXED CK</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1.4</td>
<td>RESISTOR, FIXED RCR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1.5</td>
<td>RESISTOR, FIXED RC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1.6</td>
<td>I.C., DIGITAL</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>CPU BOARD</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>2.1</td>
<td>I.C., DIGITAL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2.2</td>
<td>CAPACITOR, FIXED CK</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block and Mode ID</th>
<th>Component Block Description</th>
<th>Failure Mode Description</th>
<th>Severity Category</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1</td>
<td>CAPACITOR, FIXED CK</td>
<td>Shorted (Electrical)</td>
<td>IV</td>
<td>0.069375</td>
</tr>
<tr>
<td>1.1.2</td>
<td>CAPACITOR, FIXED CK</td>
<td>Change of Value</td>
<td>IV</td>
<td>0.0555</td>
</tr>
<tr>
<td>1.1.3</td>
<td>CAPACITOR, FIXED CK</td>
<td>Open (Electrical)</td>
<td>III</td>
<td>0.006938</td>
</tr>
<tr>
<td>1.1.4</td>
<td>CAPACITOR, FIXED CK</td>
<td>Other</td>
<td>IV</td>
<td>0.006938</td>
</tr>
<tr>
<td>1.2.1</td>
<td>CAPACITOR, FIXED CB</td>
<td>Shorted (Electrical)</td>
<td>III</td>
<td>3.40543</td>
</tr>
<tr>
<td>1.2.2</td>
<td>CAPACITOR, FIXED CB</td>
<td>Open (Electrical)</td>
<td>III</td>
<td>0.729735</td>
</tr>
<tr>
<td>1.2.3</td>
<td>CAPACITOR, FIXED CB</td>
<td>Change of Value</td>
<td>IV</td>
<td>0.48649</td>
</tr>
<tr>
<td>1.2.4</td>
<td>CAPACITOR, FIXED CB</td>
<td>Other</td>
<td>IV</td>
<td>0.243245</td>
</tr>
<tr>
<td>1.3.1</td>
<td>CAPACITOR, FIXED CK</td>
<td>Shorted (Electrical)</td>
<td>III</td>
<td>0.055985</td>
</tr>
<tr>
<td>1.3.2</td>
<td>CAPACITOR, FIXED CK</td>
<td>Change of Value</td>
<td>IV</td>
<td>0.044788</td>
</tr>
</tbody>
</table>
Fault Tree

1. **System lifetime**
   - Unit of system lifetime corresponds to unit of failure
   - *Project Options ➤ Calculation*

2. **Failure and repair models**
   - 17 model types with different failure and repair characteristics
   - *Rate models: Constant failure and repair rate*
     - Input *Rate Model*: failure rate $\lambda$ and repair rate $\mu$
       - $\mu = 0$: non-repairable components
     - Input *Rate/MTTR*: failure rate $\lambda$ and MTTR
       - MTTR = 0: failures are immediately repaired
   - *Dormant failure model: non repairable components between inspections*
     - Three methods: mean (default), max (worst case), IEC 61508
   - Local failure model (for one event): Primary Event Properties ➤ Local Failure Model ➤ Failure Model Properties
   - Generic failure model (for any event): Add ➤ Failure model ➤ Failure Model Properties
Fault Tree

3. Calculation methods:
   • Cross Product, Esary-Proshan (Bertsche), Rare, Optimum Upper Bound (default), Lower Bound
   • Project Options ► Set Generations ► Custom Options

<table>
<thead>
<tr>
<th>Event Q</th>
<th>Cross Product</th>
<th>Esary-Proshan</th>
<th>Rare</th>
<th>Lower Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>0%</td>
<td>4.5%</td>
<td>45%</td>
<td>9.1%</td>
</tr>
<tr>
<td>0.1</td>
<td>0%</td>
<td>0.69%</td>
<td>2.5%</td>
<td>0.085%</td>
</tr>
<tr>
<td>0.01</td>
<td>0%</td>
<td>0.0096%</td>
<td>0.029%</td>
<td>0.000098%</td>
</tr>
</tbody>
</table>

4. Result Summary
   • CFI: Conditional Failure Intensity corresponds to $\lambda (t)$ (Bertsche):
     • probability per unit time that the component or system experiences a failure at time $t$, (operating, or was repaired to be as good as new, at time zero and operating at time $t$).
   • Unconditional Failure Intensity or Failure Frequency $\omega(t)$ Frequency:
     • probability per unit time that the component or system experiences a failure at time $t$, (operating at time zero).
   ➢ CFI-$\lambda(t)$, $\omega(t)$ Difference: the CFI has an additional condition that the component or system has survived to time $t$. 
5. **Quantity of gates**
   - Specifying a quantity of \( n \) is equivalent to including \( n \) identical gates underneath an gate, with no common cause failures, in the fault tree diagram.
   - Quantity values may only be specified for gates that have Modularization set to “Forced on” (default = automatic).

6. **House event**
   - Used for “what if”: switches branches on (Q = 1) and off (Q = 0)
   - **Primary event properties** ► **Type** ► **House; logic mode True or False**
Fault Tree

7. Event symbols dormant
   • Option to visualize the failure model
   • Primary event properties ► Type ► Dormant

8. Append facility
   • Alternative to library
   • Batch append: transfer all the fault tree structures from a group of projects in one go
   • Partial append: append parts of a single project by selecting individual gates
   • If branches need to be combined in different fault trees and the event ID needs to remain
     • Special Functions ► Append

9. MTTF
   • By default not calculated
   • Calculation requires numerical integration methods to be employed and may be time consuming for large numbers of minimal cut sets
   • Project Options ► Calculation ► MTTF/MTBF/MTTR calculations ► Method ► Standard
10. **Importance analysis**
   - Helps determine:
     - Event contribution to TOP event
     - TOP event sensitivity to event changes
     - Weak areas in the system
   - 6 different importance measures, most useful (?) Fussell-Vesely Importance (contribution to system Q)

11. **Confidence analysis**
    - Introduces uncertainty in component Q
    - *Project Options ➤ Confidence*
3. Isograph and the IEC 61508 Standard
Saskia Hurst
IEC 61508 - General SIL Verification

Three Barriers:

1. PFH/PFD Calculation
2. Architectural Constraints SFF/HFT
3. Systematic Capability/Integrity

→ Barrier 1 and barrier 2 can be calculated in Isograph
IEC 61508 - SIL Quantitative Calculation

Reliability Prediction

FMEDA Analysis

$\lambda_{safe}, \lambda_{dangerous}, \text{DC}$

PFD/PFH

SFF/HFT

SIL Evaluation IEC 61508

Prediction module

FMECA module

FMEA module

FTA/ RBD module

FTA/ RBD module
FMEDA (Failure Modes, Effects and Detectability Analysis)

- Takes into account:
  - Failure rates of components,
  - Failure mode probabilities,
  - Failure effect of each failure mode,
  - Diagnostic coverage:

  \[ \text{SC (Safe Coverage)} = \frac{\lambda_{SD}}{\lambda_{SD} + \lambda_{SU}}; \text{DC (Dangerous Coverage)} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}, \]

- Division into safe \( \lambda_S \) and dangerous \( \lambda_D \) and detectable and undetectable failure rates \( (\lambda_{SD}, \lambda_{SU}, \lambda_{DD}, \lambda_{DU}) \)
IEC 61508 - SFF Calculation

- Calculation in the FMECA module of Isograph by doing a FMEDA
- SFF is the ratio of safe and dangerous detected failures to the total failure rate
- Safe Failure Fraction (SFF) for a component:
  \[ SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \]
- Safe Failure Fraction (SFF) for a subsystem (safety function):
  \[ SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD} + \sum \lambda_{DU}} \]
IEC 61508 - HFT Calculation

- Calculation in the Fault Tree module of Isograph

- Hardware Fault Tolerance (HFT) is the maximum number of faults that can be tolerated before the loss of the safety function

- i.e. HFT = N means that N + 1 faults will cause a loss of the function

- Isograph selects HFT by calculating SFF and cross referencing it against the SIL target for the gate (tables 2 and 3 from IEC 61508-2)
IEC 61508 - PFH/PFD Calculation

- Calculation in the Fault Tree module or RBD module in Isograph
- Probability of dangerous Failure per Hour PFH (continuous or high demand mode)
  → Frequency $\omega$ in Isograph
- Probability of dangerous Failure on Demand PFD (low demand mode)
  → Unavailability Q in Isograph
Important Settings in Isograph

- Set IEC 61508 requirement by either defining
  - Required SIL or
  - Required risk reduction factor
Important Settings in Isograph

- Dormant failure model \(\rightarrow\) IEC 61508

- Logic for average: 1. Product of the function (Fault Tree Logic)  
  2. Average of the result
Important Settings in Isograph

- Default setting: calculation of PFD/PFH with dangerous failure rate $\lambda_{DU}$
- “Only model spurious trip failure”: calculation of PFH/PFD with $\lambda_S$
- “Only model spurious trip failure” and “Include DD failures for spurious trip”: calculation of PFH/PFD with $\lambda_S$ and $\lambda_{DD}$
Important Settings in Isograph

• For continuous or high demand functions (PFH): “Exclude DD failures in frequency”

→ Calculation of the frequency (PFH) with only dangerous undetectable failures $\lambda_{DU}$ according to IEC 61508 standard
Important Settings in Isograph

- Model type: IEC 61508
Common Cause Failures

• β Factor Model (used in IEC 61508)
  
  \[ Q_1 = (1 - \beta) \cdot Q_T; \quad Q_{CCF} = \beta \cdot Q_T \]

  \( Q_1 \): Q due to independant failure, \( Q_T \): Total Q, \( Q_{CCF} \): Q due to common cause failure

• β-factor can be determined by “Apply IEC model” with a questionnaire which is implemented in Isograph