SAFETY ARCHITECT©

ALL4TEC

A FMEA tool compatible with System Engineering concepts and tools

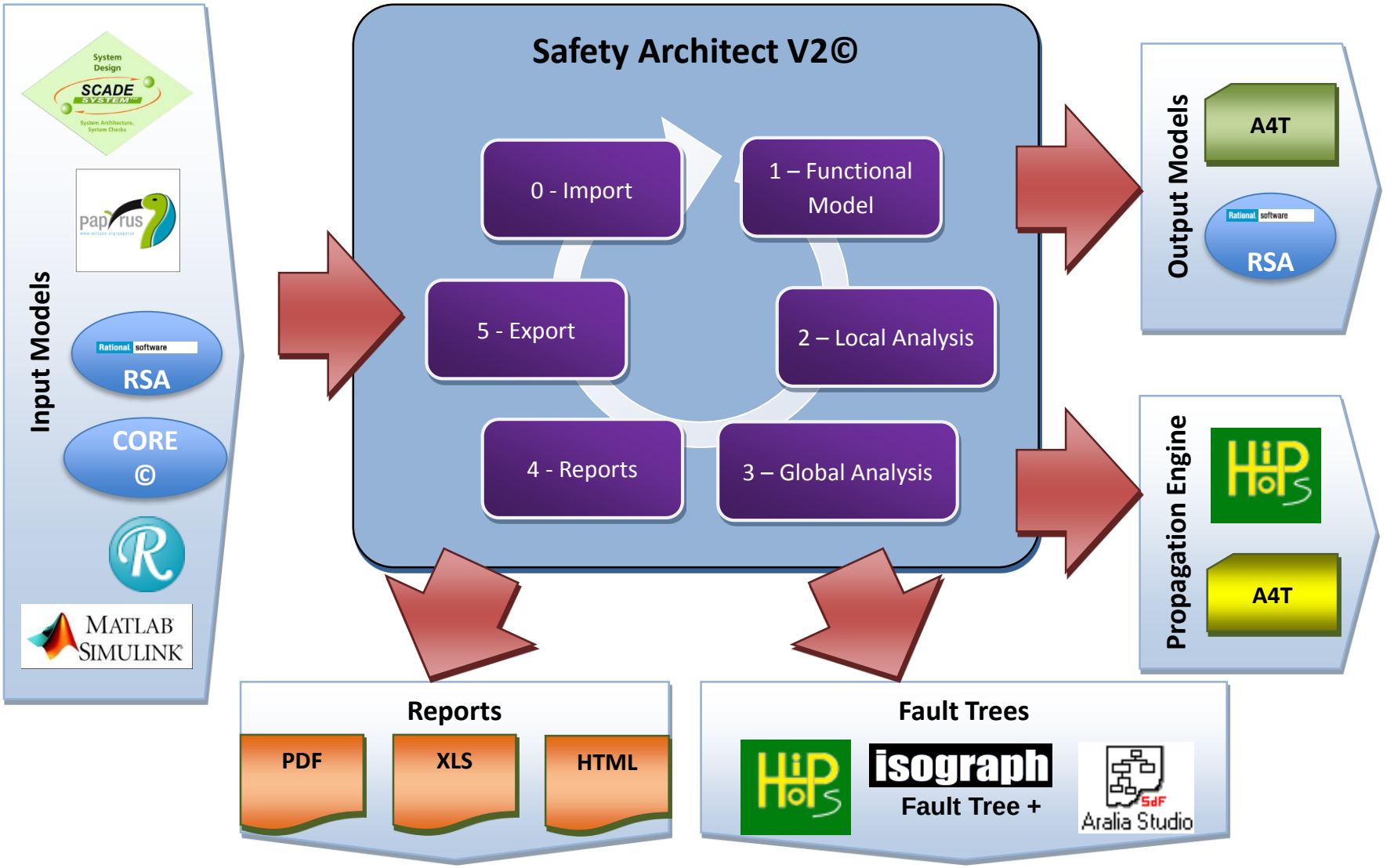
- System Engineering
- Safety - dependability
- Reliability
- FMEA
- Fault Tree Analysis

Safety Architect is supported by European Community FEDER-2007-2013

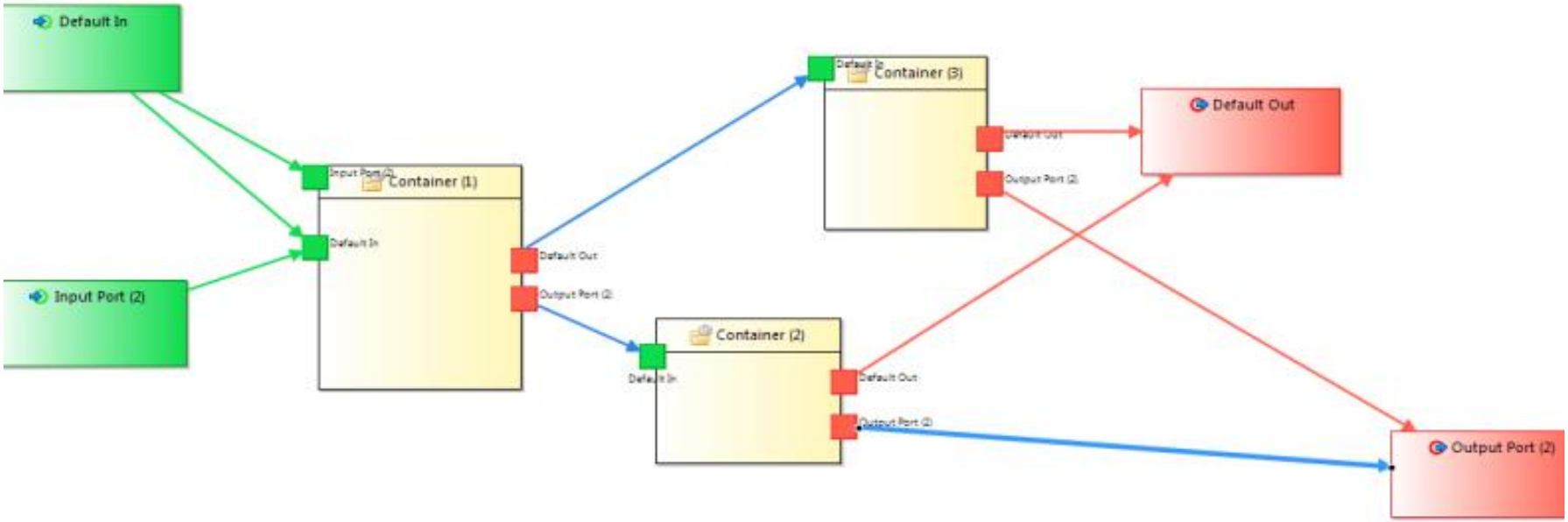
3 – The Safety Architect tool

- Interfacing Safety Architect
- Safety Architect functionalities
- Modeler
- Safety Architect methodology
- Safety Architect features

Overview of Safety Architect IOs



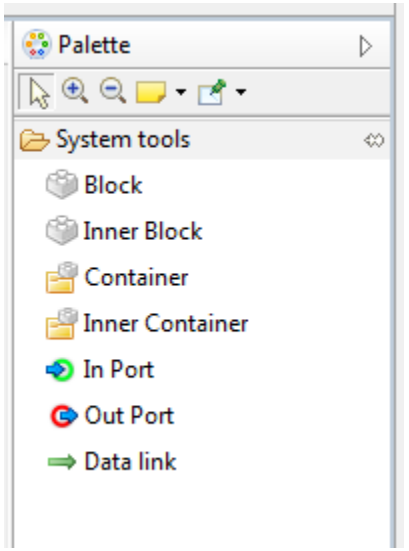
3 – The Safety Architect tool - Modeler



Sample of a view model created with Obéo

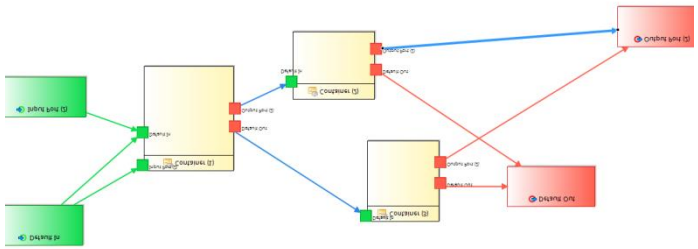
3 – The Safety Architect tool - Methodology

System modeling



- Define your System
  - Drag & drop the container from the right-side palette
  - Resize your Container in order to fill it then
  - Add the In and Out ports by dragging & dropping from the palette into the container
  - Go down your container with right click on the container => “Navigate” => Open [Container(1)] Functional Subsystem1

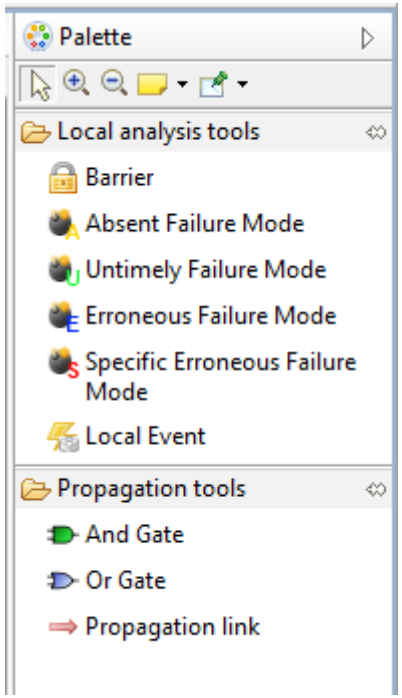
- Define your Sub-Systems
  - Dag & drop containers or blocks, depends on the system model
  - Add ports according to your needs
  - Link the required ports together, and then build your system representation

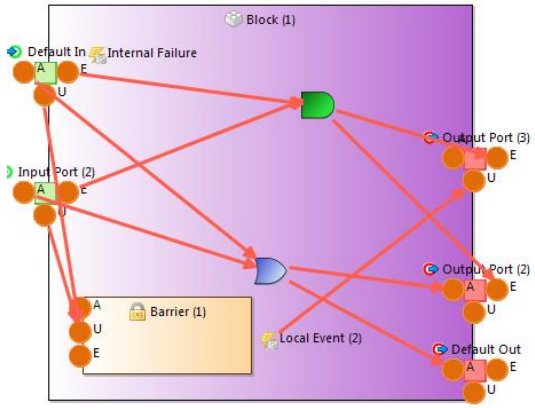


3 – The Safety Architect tool - Methodology

Local analysis

- Create the local analysis
  - Under the Safety category, open the Dysfunctional System representation by double-clicking on it
  - On your System container, right-click => “navigate” => “new detail1” => Dysfunctional Sub-System. A dysfunctional Subsystem point of view is created
  - Under the view Dysfunctional Sub-System, right click on a bloc you want to analyze => “Navigate” => “New Detail: local Analysis”, then you can give a name to this local analysis
  - In your block, fill local equations (local analysis) in the blocks by linking the Failure modes for each port.
  - Add logical doors (AND or OR) for effects of failure
  - Add Barriers of local Event in the block local analysis
  - Define feared events on the output ports
  - Perform this local Analysis for all blocks in the model

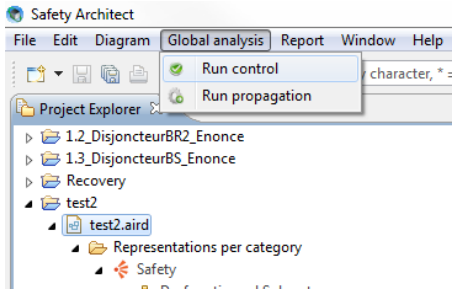


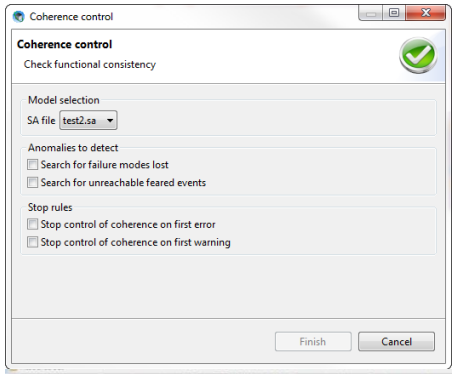


3 – The Safety Architect tool - Methodology

Global Analysis

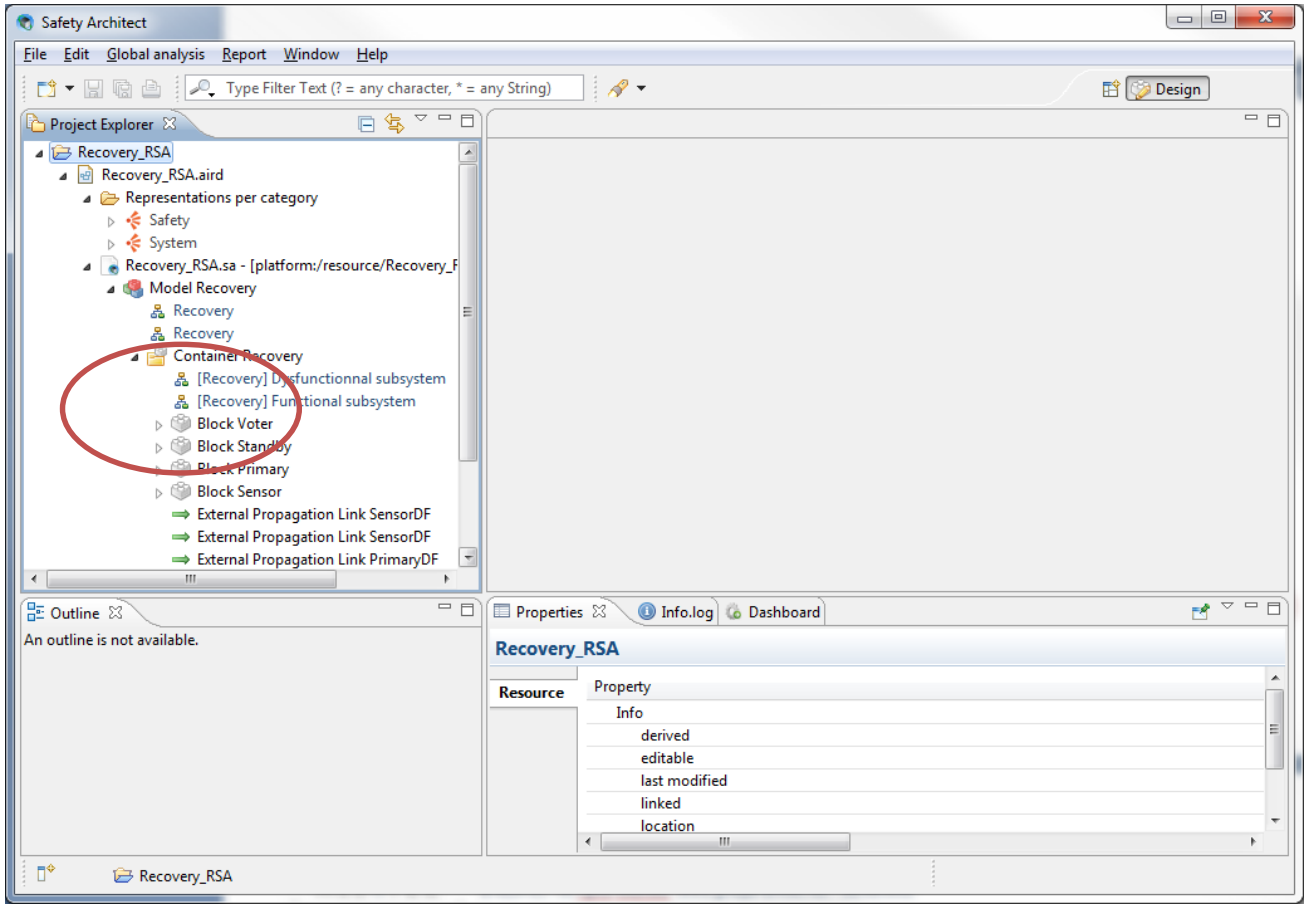
- You can first check the model consistancy, by clicking on the .aird in the model structure, then click on “Global Analysis” => “run control”, select the criteria you need, and start the model checker
- You can propagate the local equations, by clicking on the .aird, then click on “Global Analysis” => “Run Propagation”
- Then you can choose between the 2 propagation tools: A4T or Hip-Hops
- Then you can choose which feared event you want to propagate





3 – The Safety Architect tool – Features

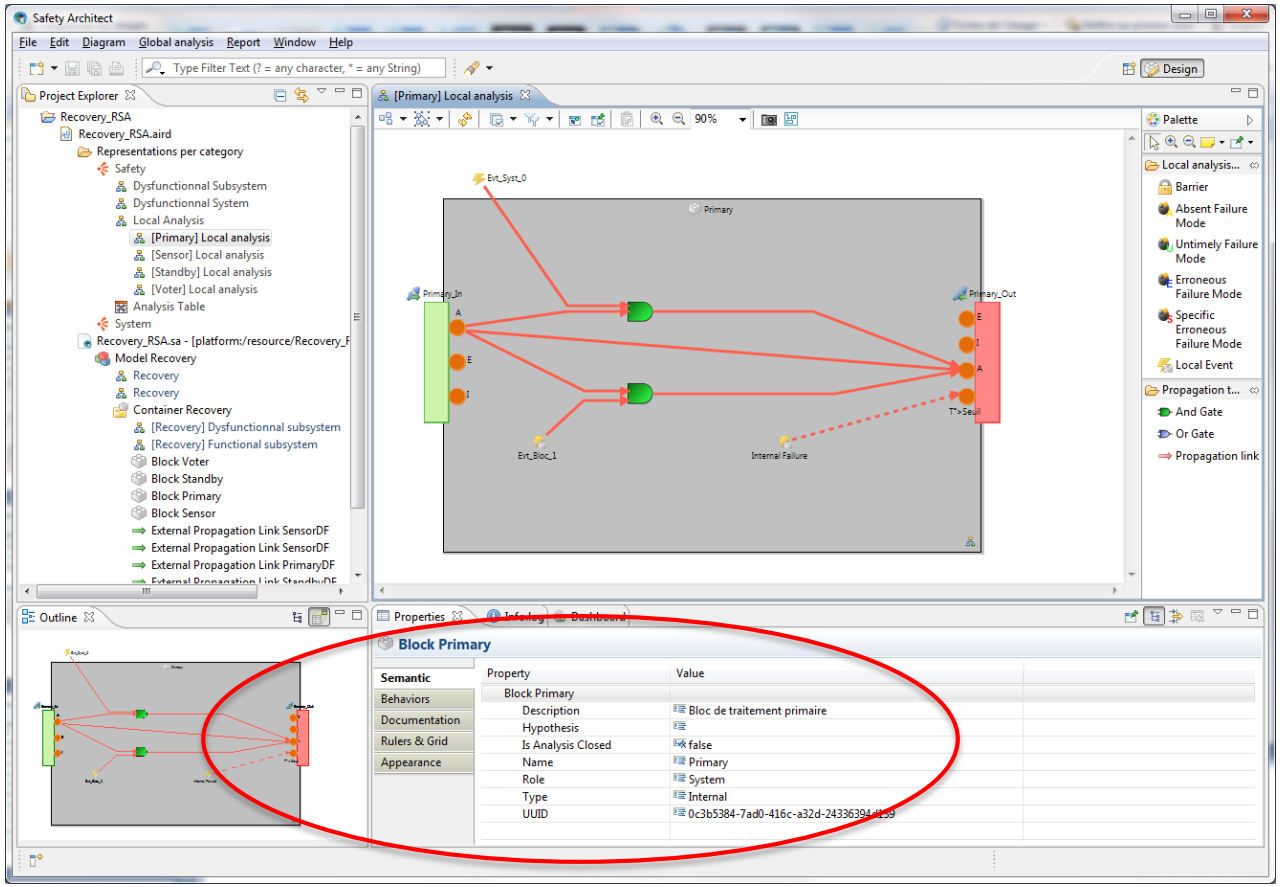
Model breakdown



UML model structure decomposition

3 – The Safety Architect tool - Features

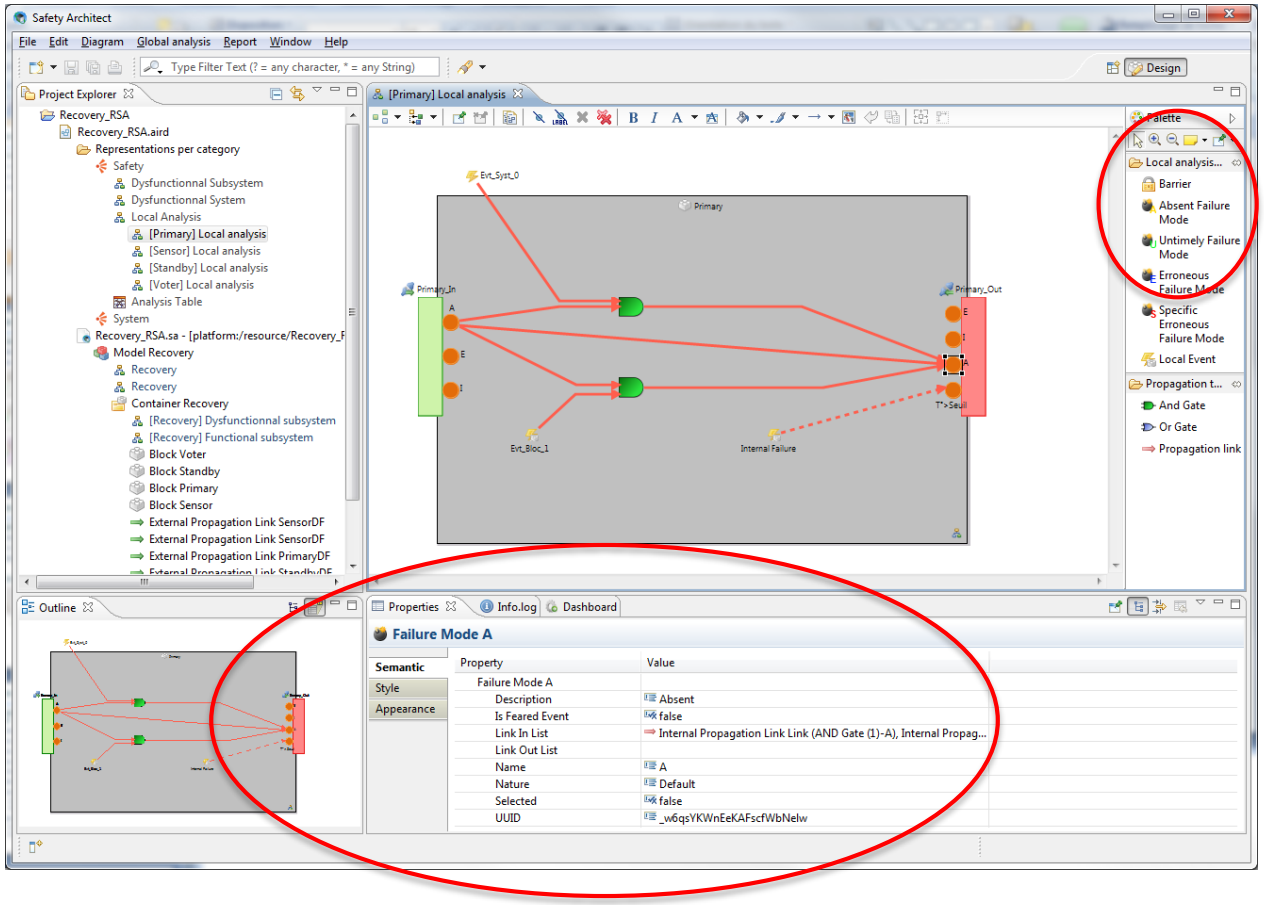
Properties



Container, block, link, port and failure mode properties view

3 – The Safety Architect tool –

Failure Modes



Failure modes from palette – customization possible

3 – The Safety Architect tool – Features

Reports

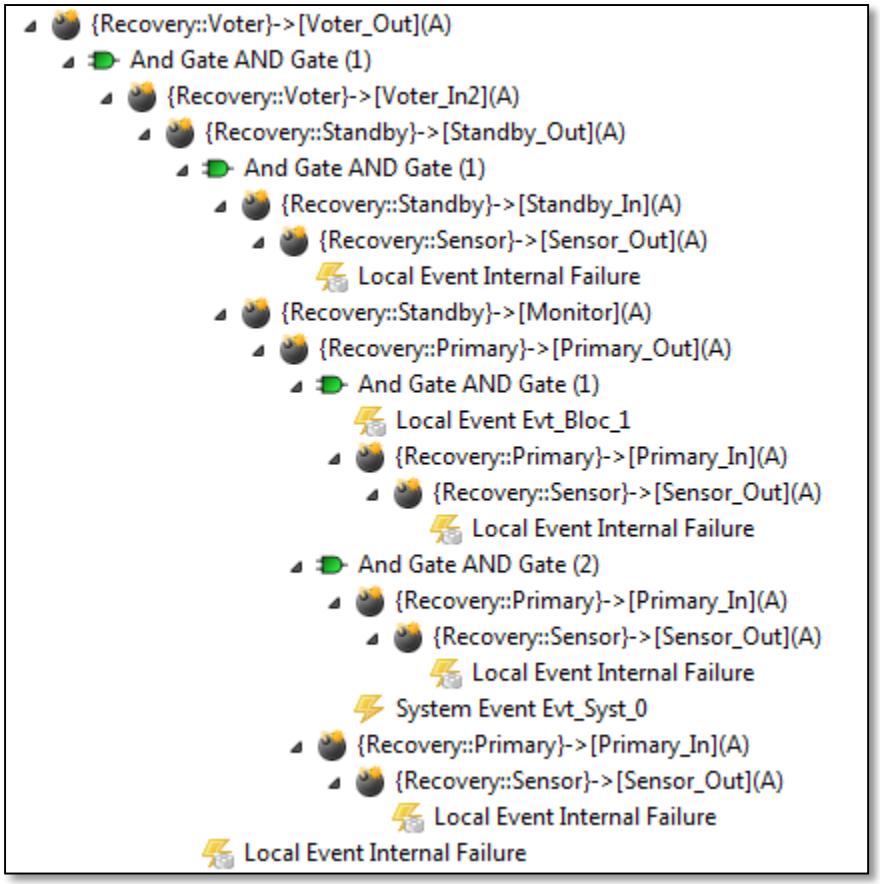
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	CC	Flux	MD	Flux	MD	Flux	MD	Flux	MD	Flux	MD	Flux	MD	Flux
93	CC [91]	E25	Errone	F132	Absent	F14	Absent	F322	Absent	F42	Absent			
94	CC [92]	E332	Errone	F322	Absent	F42	Absent							
95	CC [93]	E3	Absent	F522	Absent	F322	Absent	F42	Absent					
96	CC [94]	E21	Absent	F11	Absent	F132	Absent	F14	Absent	F33	Absent	F42	Absent	
97	CC [95]	E25	Errone	F132	Absent	F14	Absent	F33	Absent	F42	Absent			
98	CC [96]	E21	Intempestif	F11	Intempestif	F132	Intempestif	F33	Absent	F42	Absent			
99	CC [97]	E25	Errone	F132	Intempestif	F33	Absent	F42	Absent					
100	CC [98]	E21	Absent	F11	Absent	F132	Absent	F14	Absent	F34	Absent	F42	Absent	
101	CC [99]	E25	Errone	F132	Absent	F14	Absent	F34	Absent	F42	Absent			
102	CC [100]	E21	Intempestif	F11	Intempestif	F131	Intempestif	F34	Absent	F42	Absent			
103	CC [101]	E24	Errone	F131	Intempestif	F34	Absent	F42	Absent					
104	CC [102]	E21	Intempestif	F11	Intempestif	F132	Intempestif	F14	Intempestif	F311	Intempestif	F42	Intempestif_en_inhibition	
105	CC [103]	E25	Errone	F132	Intempestif	F14	Intempestif	F311	Intempestif	F42	Intempestif_en_inhibition			
106	CC [104]	E231	Errone	F311	Intempestif	F42	Intempestif_en_inhibition							
107	CC [105]	E26	Absent	F42	Intempestif_en_inhibition									
108	CC [106]	E21	Intempestif	F11	Intempestif	F132	Intempestif	F14	Intempestif	F312	Intempestif	F42	Intempestif_en_inhibition	
109	CC [107]	E25	Errone	F132	Intempestif	F14	Intempestif	F312	Intempestif	F42	Intempestif_en_inhibition			
110	CC [108]	E231	Errone	F312	Intempestif	F42	Intempestif_en_inhibition							
111	CC [109]	E3	Intempestif	F521	Intempestif	F312	Intempestif	F42	Intempestif_en_inhibition					
112	CC [110]	E26	Absent	F42	Intempestif_en_inhibition									
113	CC [111]	E21	Intempestif	F11	Intempestif	F132	Intempestif	F14	Intempestif	F321	Intempestif	F42	Intempestif_en_inhibition	
114	CC [112]	E25	Errone	F132	Intempestif	F14	Intempestif	F321	Intempestif	F42	Intempestif_en_inhibition			
115	CC [113]	E332	Errone	F321	Intempestif	F42	Intempestif_en_inhibition							
116	CC [114]	E26	Absent	F42	Intempestif_en_inhibition									
117	CC [115]	E21	Intempestif	F11	Intempestif	F132	Intempestif	F14	Intempestif	F322	Intempestif	F42	Intempestif_en_inhibition	
118	CC [116]	E25	Errone	F132	Intempestif	F14	Intempestif	F322	Intempestif	F42	Intempestif_en_inhibition			
119	CC [117]	E332	Errone	F322	Intempestif	F42	Intempestif_en_inhibition							
120	CC [118]	E3	Intempestif	F522	Intempestif	F322	Intempestif	F42	Intempestif_en_inhibition					

Propagation results are summarized into report which can be exported into an Excel or Pdf file

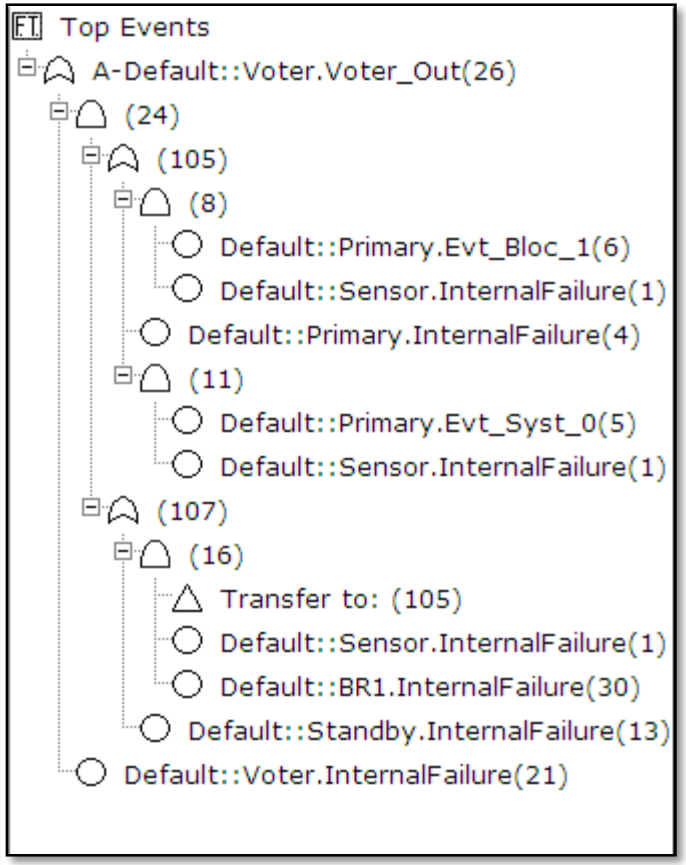
3 – The Safety Architect tool – Features

Fault Trees

Safety Architect format



Hip Hops© format



Propagation results are shown in a minimal fault tree