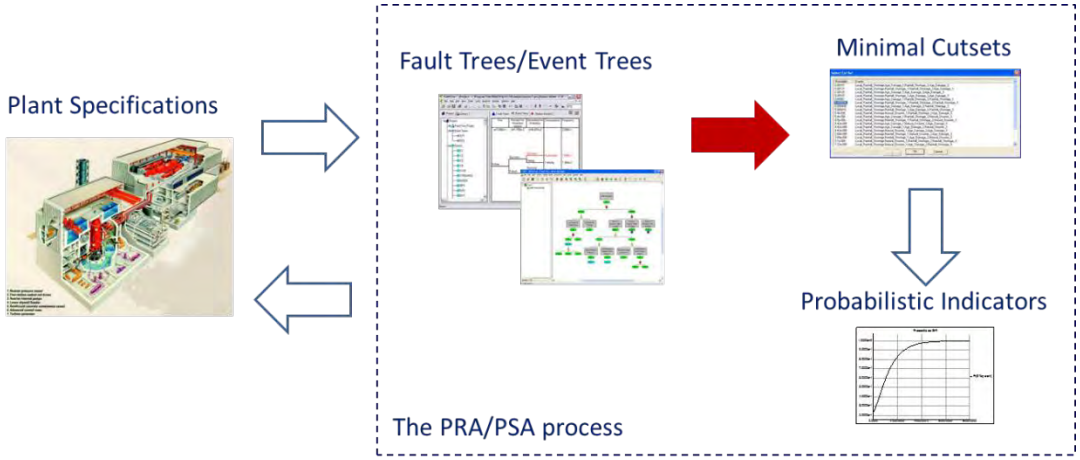
CentraleSupélec

New Logic Modeling Paradigms for Complex System Reliability and Risk Analysis

Antoine Rauzy
Chair Blériot-Fabre* - Ecole Centrale de Paris
Ecole Polytechnique
FRANCE
Antoine.Rauzy@ecp.fr
http://www.lgi.ecp.fr/pmwiki.php/PagesPerso/ARauzy

*Sponsored by SAFRAN group

Probabilistic Risk Assessment …

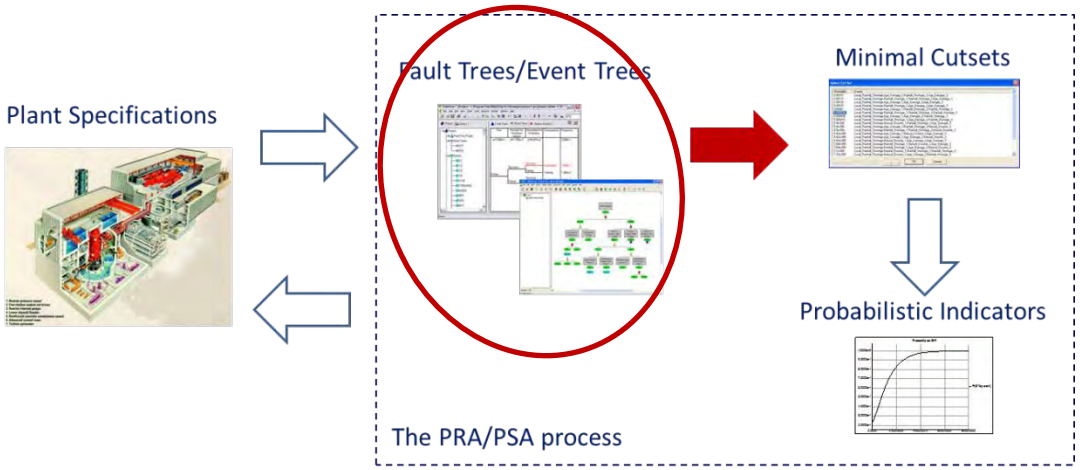


… is now established on a solid scientific ground
… is a mature technology
… is a great tool for decision making

So, what's next?

- More openness
- Higher level modeling languages
- Wider spectrum of applications

Standard Representation Formats



Issues

- **Models are tool-dependent**
- Calculations are provably difficult so **calculation engines perform unwarranted approximations**

Challenge/research direction:

Define **standard representation formats**, with all the necessary constructs, with a clear and sound semantics

Version 3 of the Open-PSA standard under redaction

- Simplifications
- Block Diagrams
- Multi-phase Markov Chains with Rewards

The **Open-PSA Standard Representation Format** for Fault Trees and Event Trees

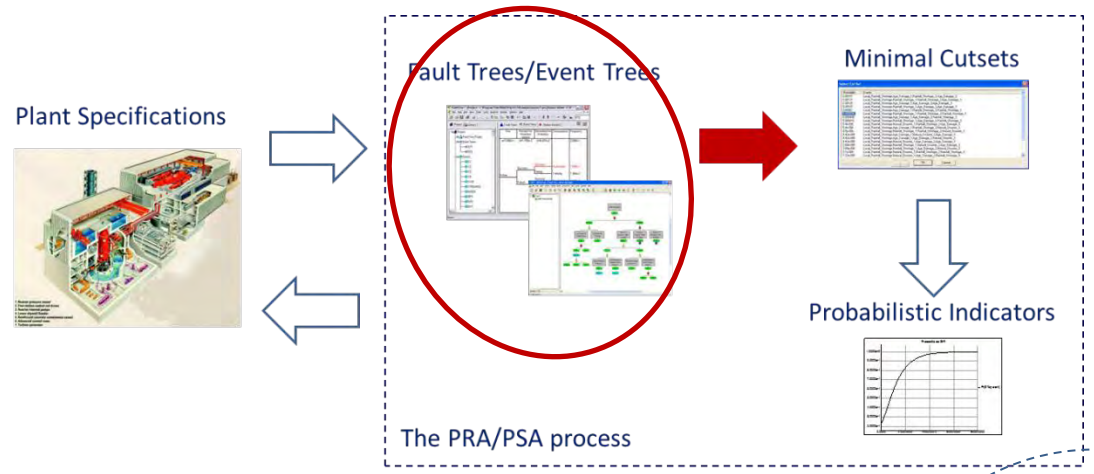

Open PSA Work Package

Project P08-4: «Validation of Open-PSA Model Exchange Format for Probabilistic Safety Analyses»

Project Specifications

```
<define-fault-tree name="FT1" >
  <define-gate name="top" >
    <or>
      <gate name="G" />
      <basic-event name="C" />
    </or>
  </define-gate>
  <define-gate name="G" >
    <and>
      <basic-event name="A" />
      <basic-event name="B" />
    </and>
  </define-gate>
</define-fault-tree>
```

New Algorithms for Model Assessment



Issues:

- Finding the **right level of abstraction** is difficult to achieve

Design **Filtering Algorithms** that to build simpler models that are **equivalent w.r.t. to observation means**

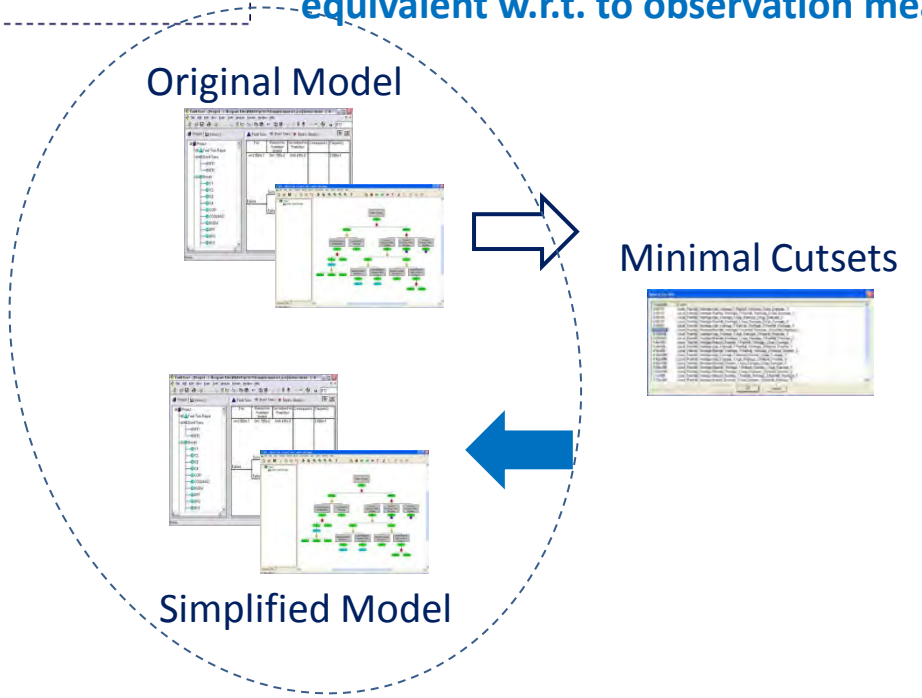
Typical example (US plant):

- ~2 500 Basic Events PSA model

What has been calculated:

- ~100 000 Minimal Cutsets
- 95% of the Core Damage Frequency with less than 5% of the Basic Events, 100% with 25%

In a word, 75% of the model is “useless”!



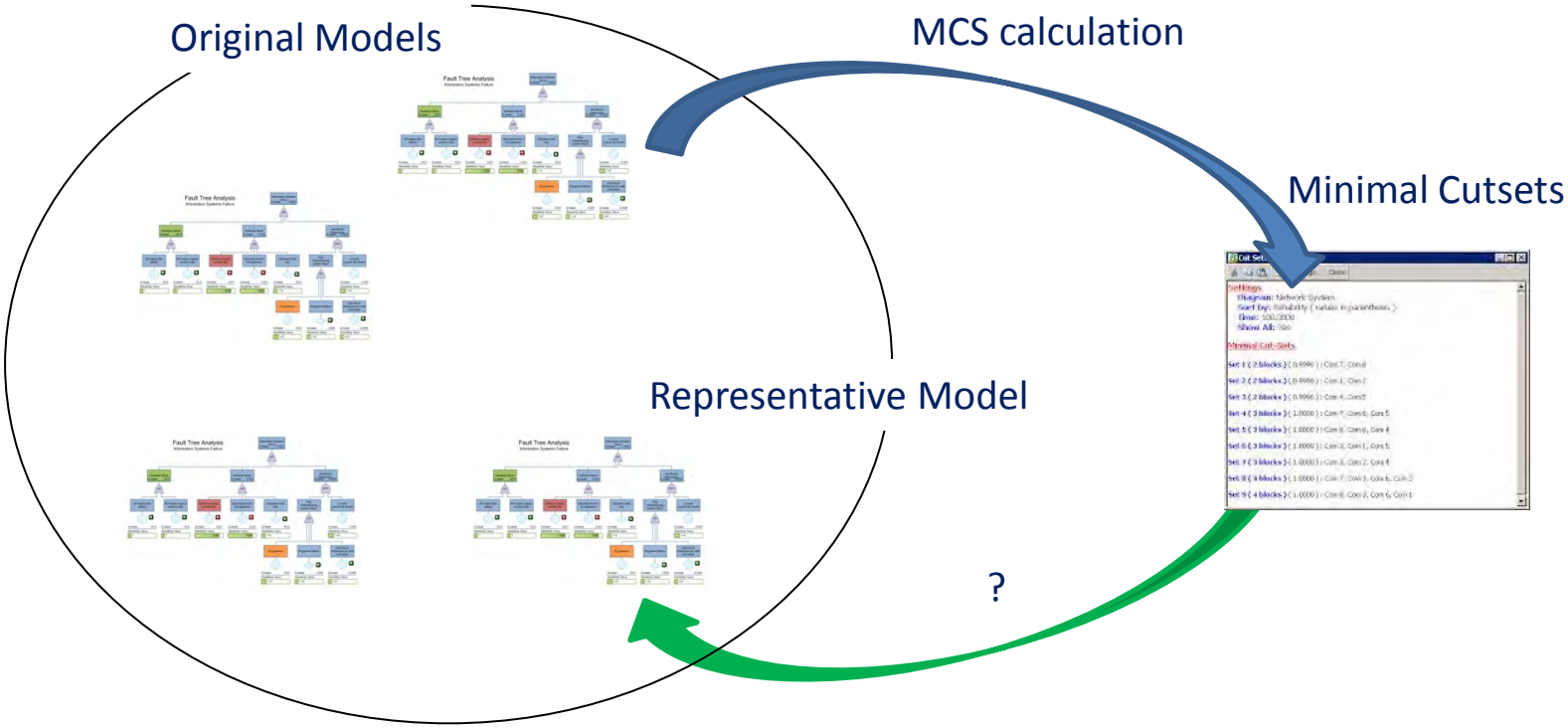
Categories of Models

Challenge/research direction:

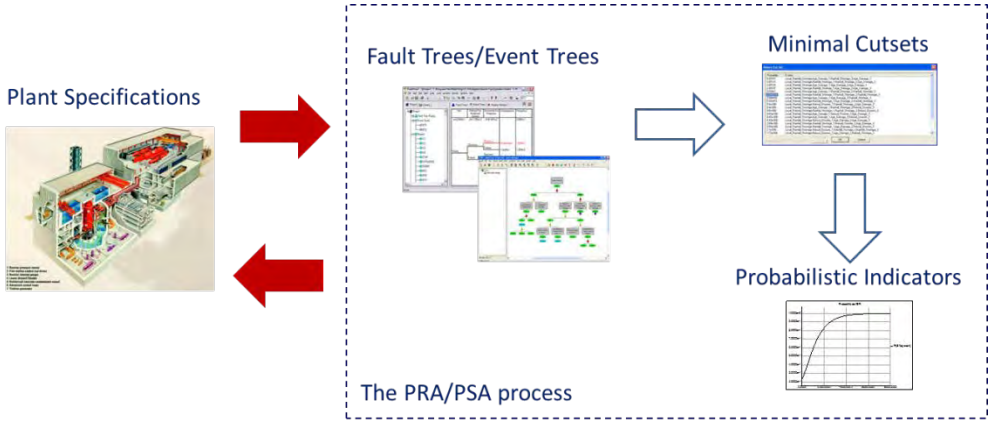
Many possibly very different models are **undistinguishable** by **observation means**, i.e. results of virtual experiments (typically, calculation of failure scenarios). They are **equivalent** in the **Turing test** sense.

Equivalent models form a **category**.

Design mathematical concepts, algorithms and tools to determine the **most representative** (simplest?) model of a category.



High Level Modeling Languages

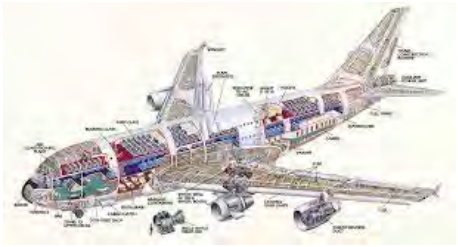


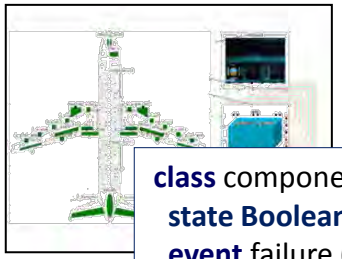
Issues:

- **Completeness** of specifications with respect to safety concerns
- **Distance** between system specifications and safety models
- **Integration** with other system engineering disciplines

AltaRica

System Specification





Automated Generation

Fault Trees

```
class component
  state Boolean working (init = true);
  event failure (delay = exponential(lambda));
 transition
    failure: working -> working := false;
end
```

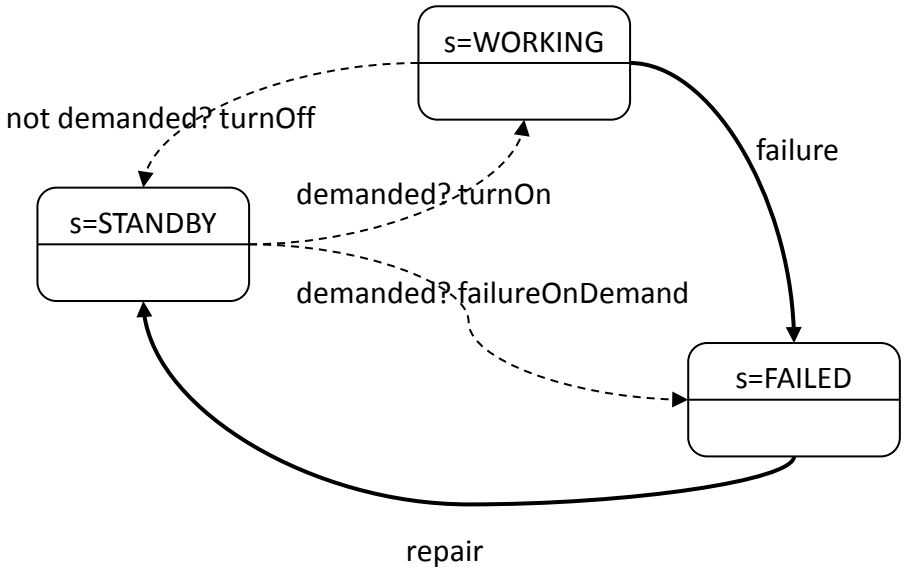
Calculations

AltaRica features

- Formal
- Event-Based
- Textual & graphical
- Multiple assessment tools

AltaRica Mathematical Framework

Guarded Transition Systems:




```
domain componentState { STANDBY, WORKING, FAILED}

class spareComponent
  componentState s (init = WORKING);
  Boolean demanded (reset = false);
  event turnOn (delay = 0, expectaction = 0.98),
        failureOnDemand (delay = 0, expectation = 0.02),
        turnOff (delay = 0),
        failure (delay = exponential(0.001)),
        repair (delay = exponential(0.1));
  transition
    turnOn: s==STANDBY and demanded  -> s := WORKING;
    failureOnDemand: s==STANDBY and demanded -> s := FAILED;
    turnOff: s==WORKING and not demanded -> s := STANDBY ;
    failure:  s==WORKING -> s := FAILED;
    repair:  s==FAILED -> s := STANDBY;
  end
```

Well founded generalization of:

- Fault Trees, Blocks Diagrams
- Markov chains, Stochastic Petri Nets

The AltaRica 3.0 Project

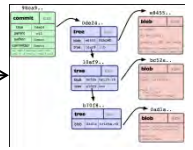
CentraleSupélec

Reliability Data

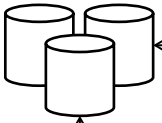
MIL-HDBK

GUI for modeling
GUI for simulation

Version & Configuration Management System



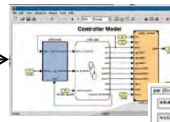
Libraries patterns



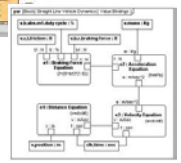
AltaRica 3.0

```
class Pump
...
end
```

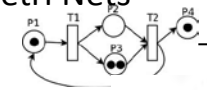
AADL



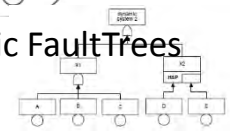
SysML



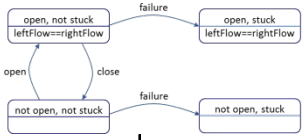
Petri Nets



Dynamic FaultTrees



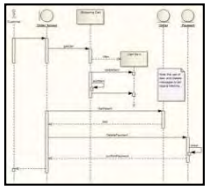
Guarded Transition Systems



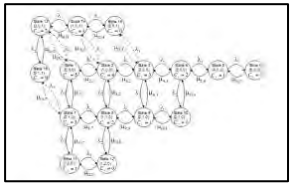
FMEA

compilation to Fault Trees

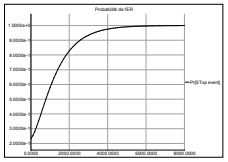
generation of sequences



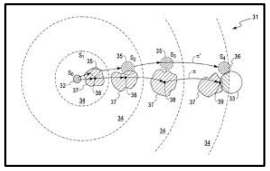
compilation to Markov Chains



stochastic simulation



model checking



reliability allocation

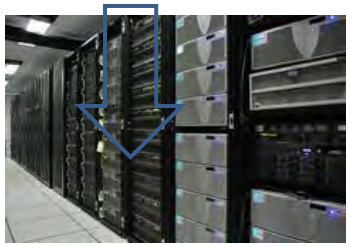
$$C_i(R_i) = e^{(1-f)\cdot\frac{R_i - R_{\min,i}}{R_{\max,i} - R_i}},$$

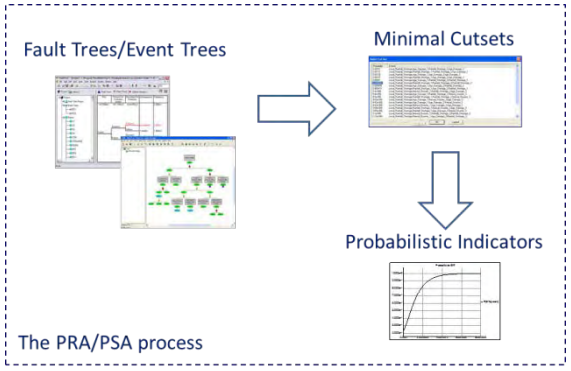
Performances Assessment

Issues:

- The **business model** of industry is moving from **selling products** to **selling capacities**
- Companies have to take **commitments** and to do so to **assess performances** of systems in presence of hazards.





=

PRA languages and tools are well suited to **assess capacities** (it mainly suffices to assess mathematical expectations rather than probabilities)