Probabilistic Risk Assessment: Some Challenges

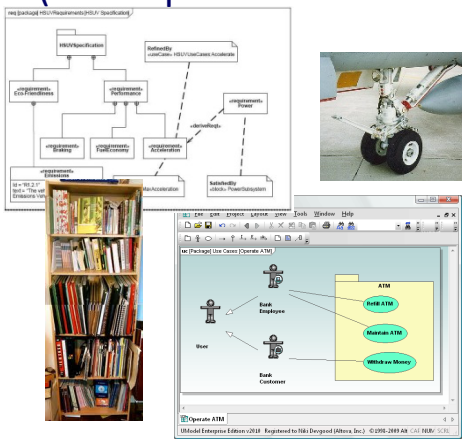
Antoine Rauzy
LIX – École Polytechnique
FRANCE

Context

- Increasing complexity of systems (systems of systems)
- Evolution of the market: from products to capabilities
- Ubiquity of software
- Integration of engineering disciplines
- Model Based Design

Probabilistic Risk Assessment

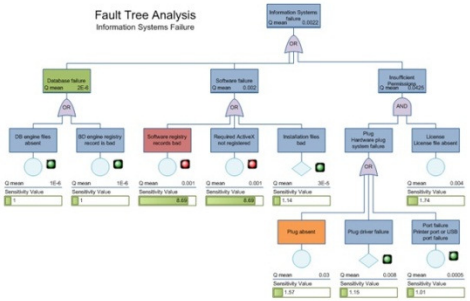
System Specifications
(and experience feedback)



Modeling

Improvements
Certification

Models



Fault Trees, Event Trees, Markov Chains, Stochastic Petri Nets…

Virtual Experiments

- Failure Scenarii
- Reliability Indicators

Issues:

- **Completeness** of specifications with respect to safety concerns
- **Distance** between system specifications and safety models
- **Size** of the models
- **Complexity** of virtual experiments

Filtering

A model is designed to capture/study one aspect of the system.
It should be at the **right level of abstraction**.

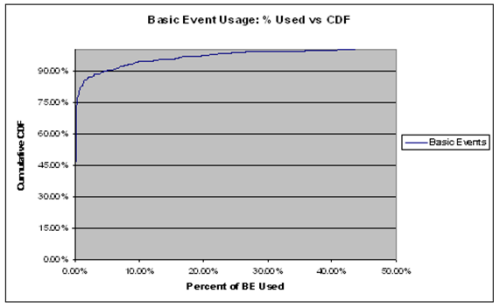
Easy to say, but difficult to achieve

The designed model:

- ~2500 basic events PSA

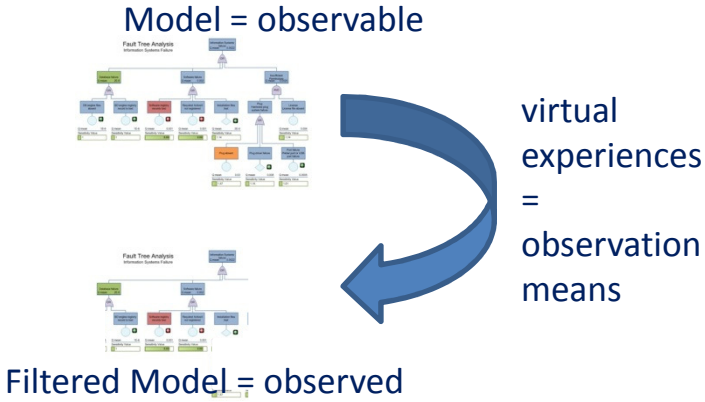
The calculated model:

- ~100000 cutsets
- 95% of the CDF with less than 5% of BE, 100% with 25%



Challenge/research direction:

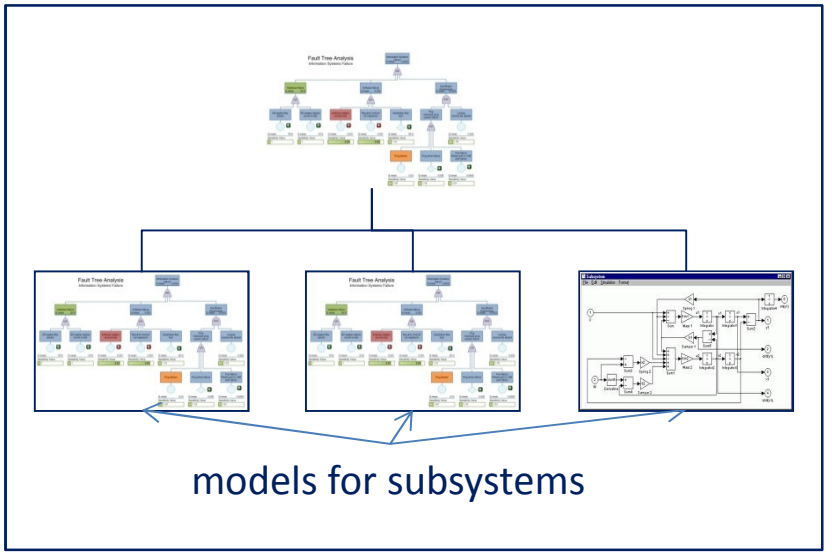
Design mathematical concepts, algorithms and tools to **filter** models w.r.t. to results of virtual experiments (typically, calculation of failure scenarios)



Abstraction/Concretization

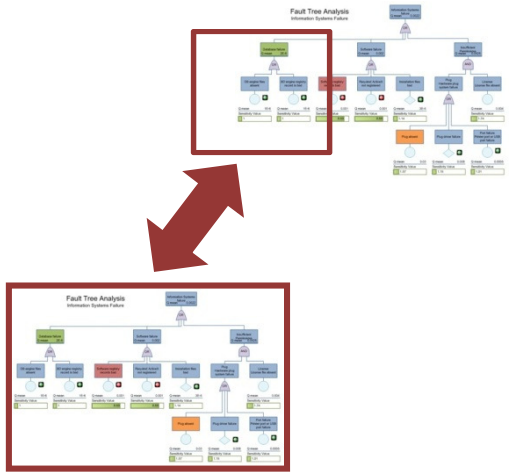
Complex systems need to be described by **multi-scale models**

- The composition of models of subsystems is often too big to be handled
- Models of subsystems are often heterogeneous… and designed by suppliers



Challenge/research direction:

Design mathematical concepts, algorithms and tools to **abstract** the model of subsystems into the model of the system and vice-versa



Standard Representation Formats

Two major trends:

- Models are more and more used as a contractual basis
- A high quality assurance is demanded on models

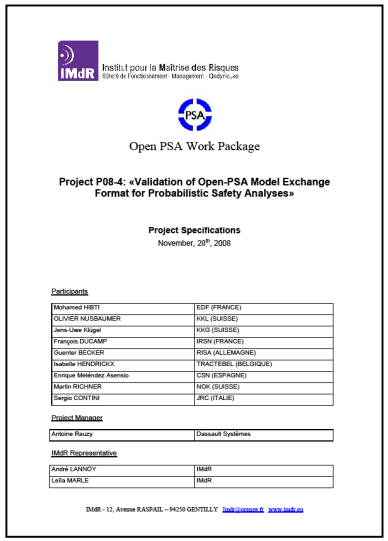
As a consequence, models must be:

- Peer-reviewed
- **Tool independent**

Challenge/research direction:

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

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



IMdR Institut pour la Maîtrise des Risques

Open PSA Work Package

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

Project Specifications
November, 28th, 2008

Participants

Mohamed HIBTI	EDF (FRANCE)
OLIVIER NUSBAUMER	KKL(SUISSE)
Jens-Uwe Klügel	KKG (SUISSE)
François DUCAMP	IRSN (FRANCE)
Guenter BECKER	RISA (ALLEMAGNE)
Isabelle HENDRICKX	TRACTEBEL (BELGIQUE)
Enrique Meléndez Asensio	CSN (ESPAGNE)
Martin RICHNER	NOK (SUISSE)
Sergio CONTINI	JRC (ITALIE)

Project Manager

Antoine Rauzy	Dassault Systèmes

IMdR Representative

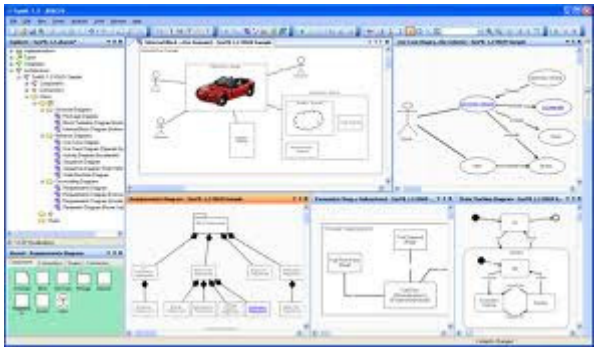
André LANNOY	IMdR
Leila MARLE	IMdR

IMdR - 12, Avenue RASPAIL – 94250 GENTILLY Imdr@cemsen.fr www.imdr.eu

```
<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>
```

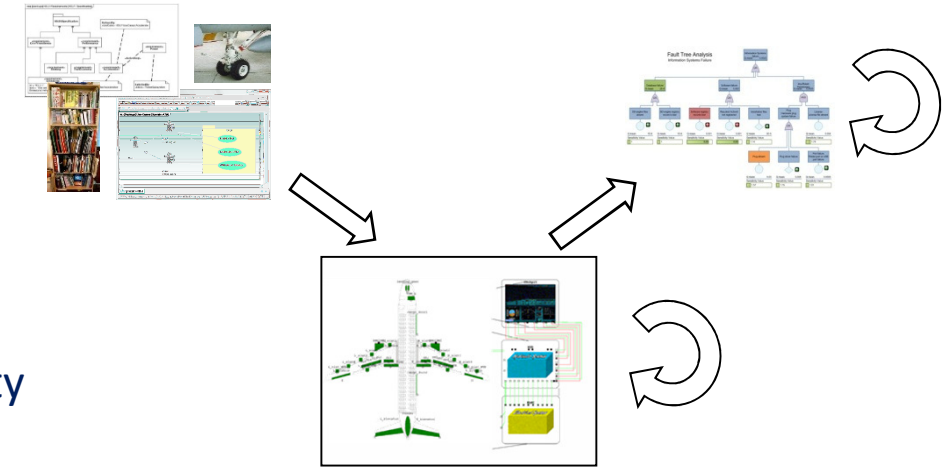
Model Based Design

SysML: an emerging standard of system architecture



Challenge/research direction:

- Better integration of Safety Analyses with System Architecture
- Engineering of models of engineering
- High Level Modeling Languages
- Modeling process as a cognitive activity



AltaRica