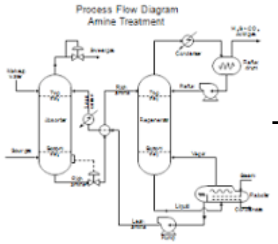
New Challenges and Opportunities for Model-Based Risk/Safety Assessment

Prof. Antoine B. Rauzy

Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology
Trondheim, Norway
&
Chair Blériot-Fabre
CentraleSupélec
Paris, France

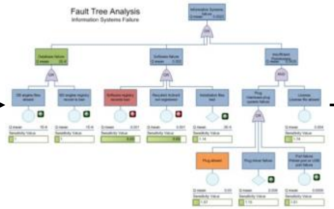
Probabilistic Risk/Safety Assessment

Systems Specifications

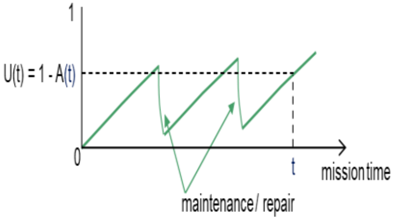


Reliability Data Bases

Models

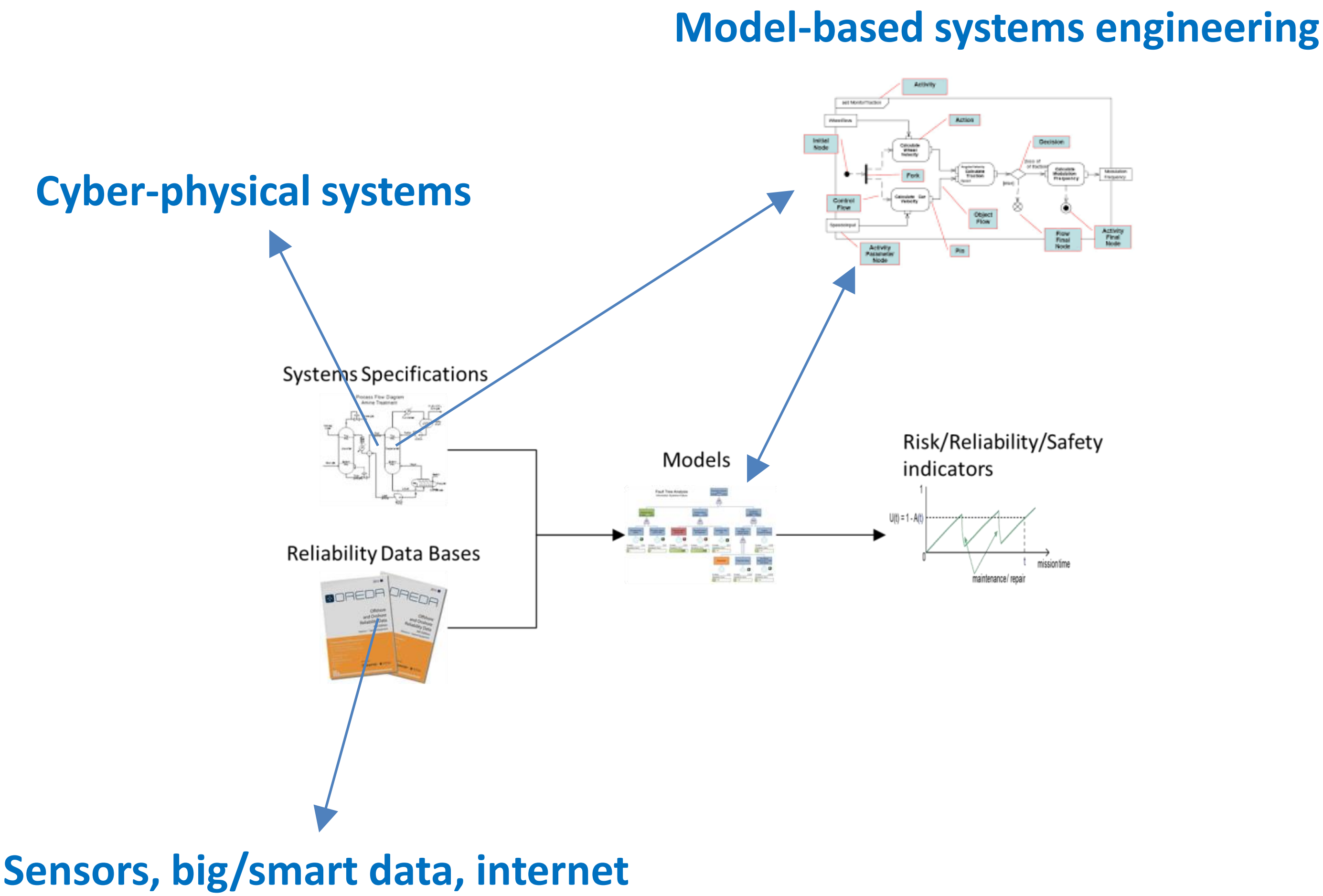


Risk/Reliability/Safety indicators



- Mechanical systems
- Knowledge in books
- Dedicated low level models (fault trees, block diagrams…)

Games Changers



Model-based systems engineering

Cyber-physical systems

Systems Specifications

Reliability Data Bases

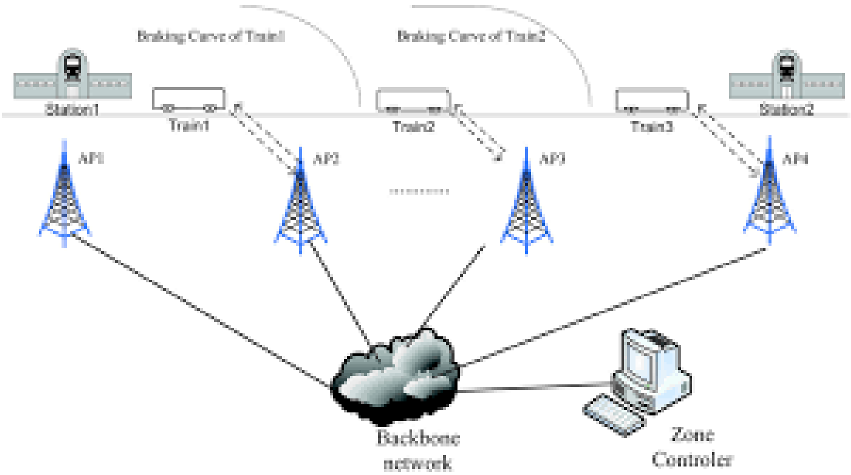
Models

Risk/Reliability/Safety indicators

Sensors, big/smart data, internet

From Mechanical to Cyber-Physical Systems

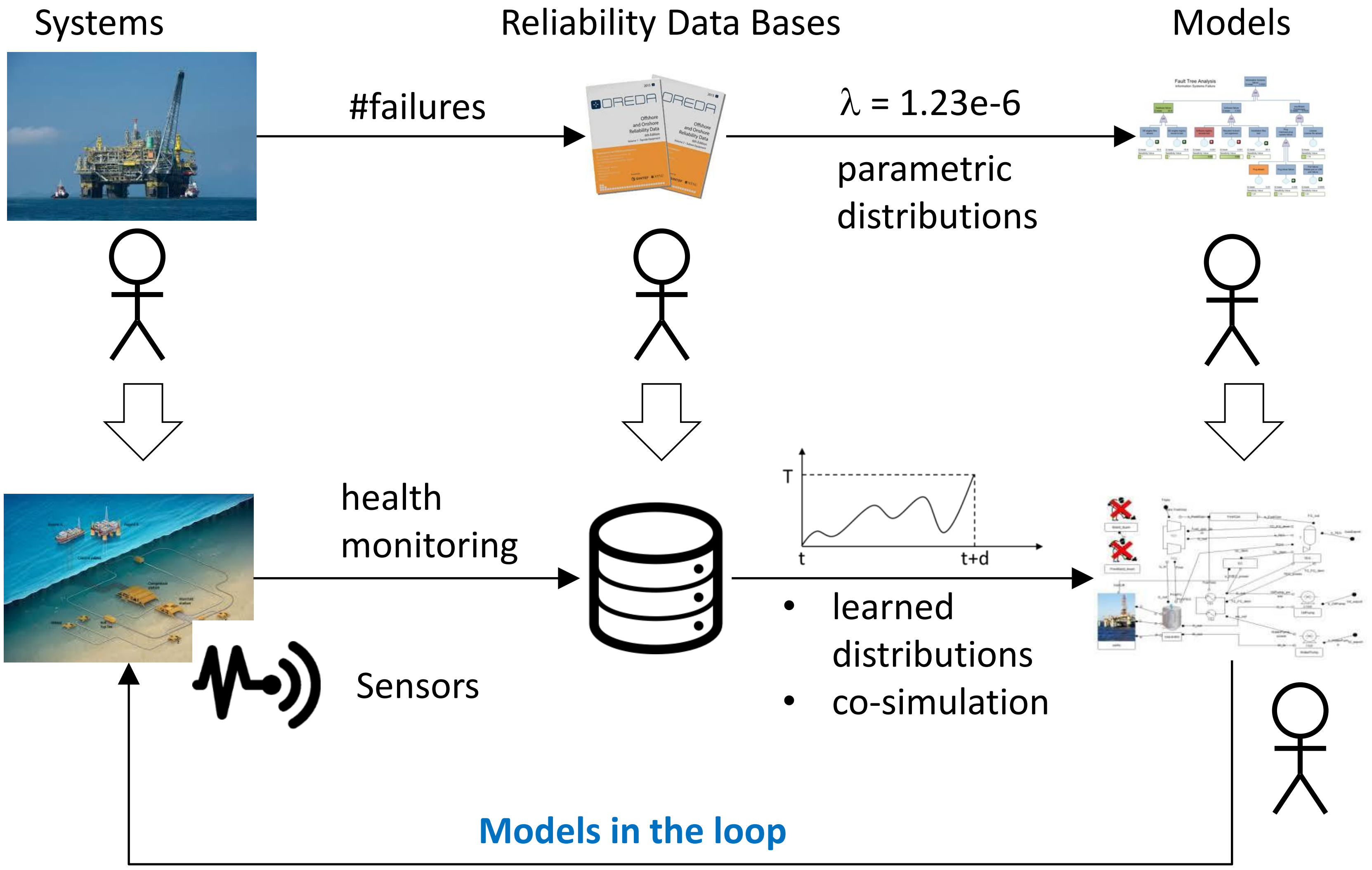
- Software intensive systems: how to model **control mechanisms**?
- Communicating systems: how to integrate **safety** and **security**?



New generations of systems are:

- **Opaque**: their states can be observed only by indirect means.
- **Reflective**: they embed models of their own behavior and environment.
- **Deformable**: their architecture changes throughout their mission.

Management of Reliability Data & Co-Simulation



Systems

Reliability Data Bases

Models

#failures

λ = 1.23e-6

parametric distributions

health monitoring

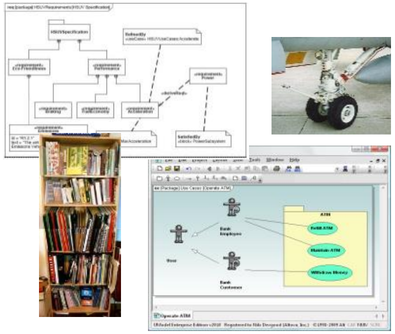
Sensors

- learned distributions
- co-simulation

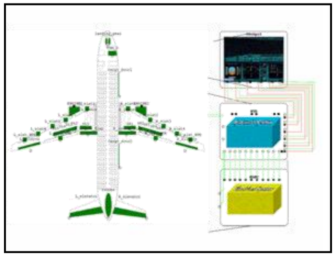
Models in the loop

The Promise of Model-Based Risk/Safety Assessment

Modeling systems at **higher level** so to reduce the distance between systems specifications and models (without increasing the complexity of calculations).



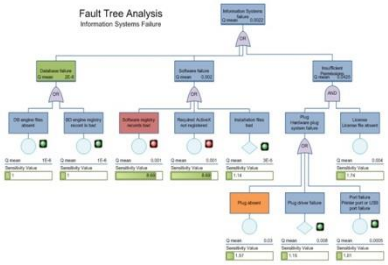
Systems Specifications



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

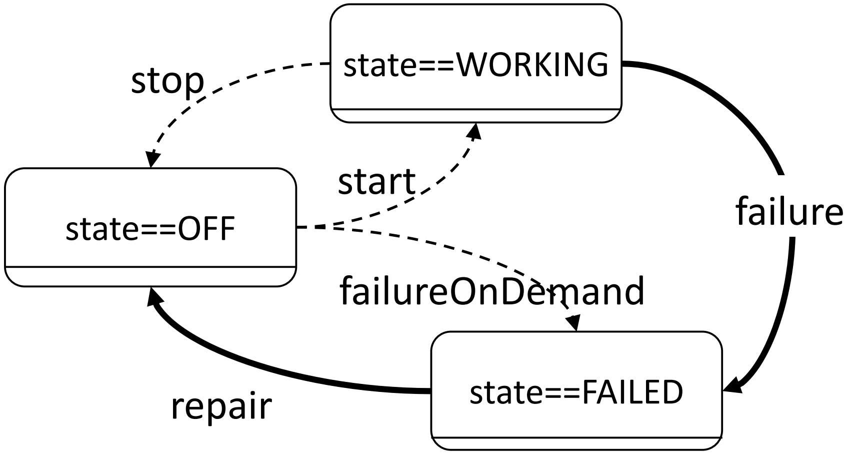
AltaRica 3.0

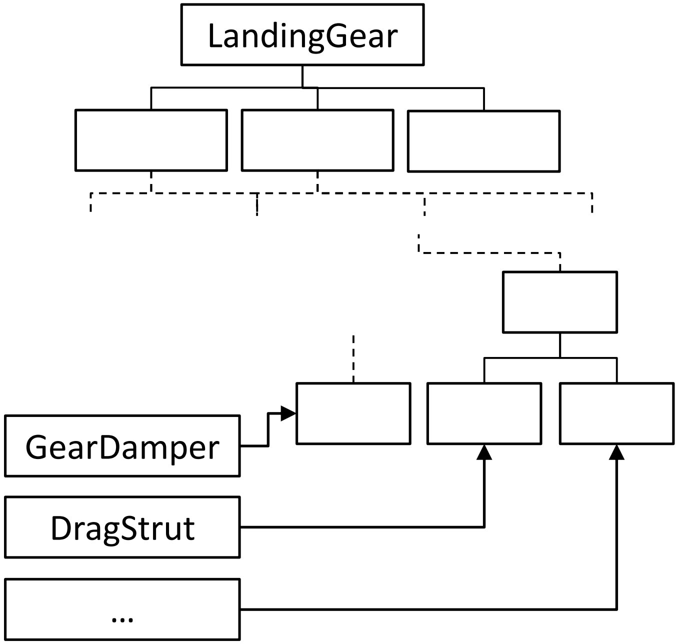
Models



AltaRica 3.0

Guarded Transitions Systems + System Structure Modeling Language





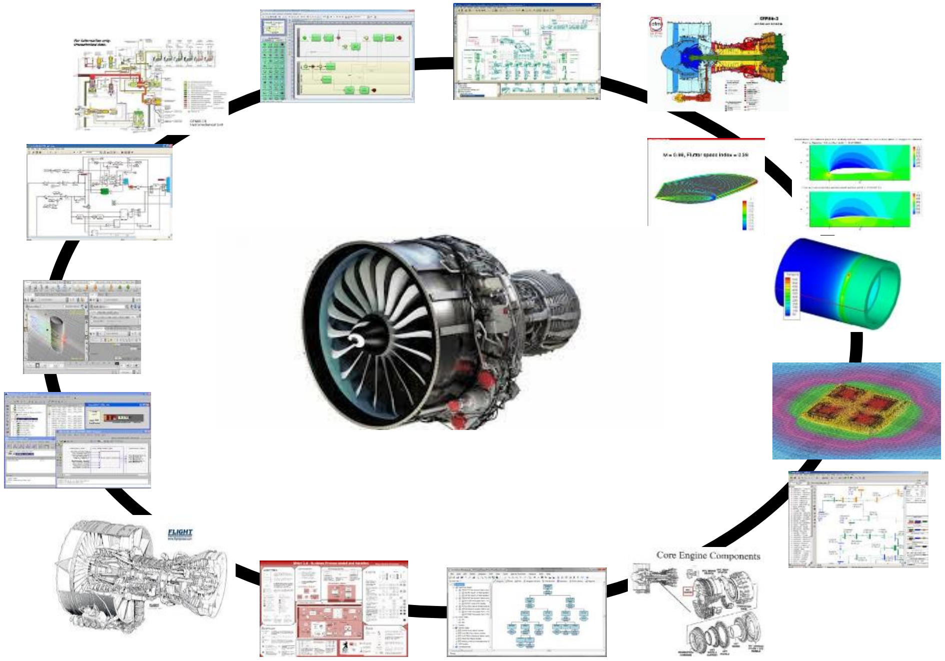
Generalization of usual modeling formalisms (fault trees, block diagrams, Markov chain, stochastic Petri nets…) at no algorithmic cost.

Object-oriented model structuring for a better re-use.
Modeling patterns.

Model-Based Systems Engineering

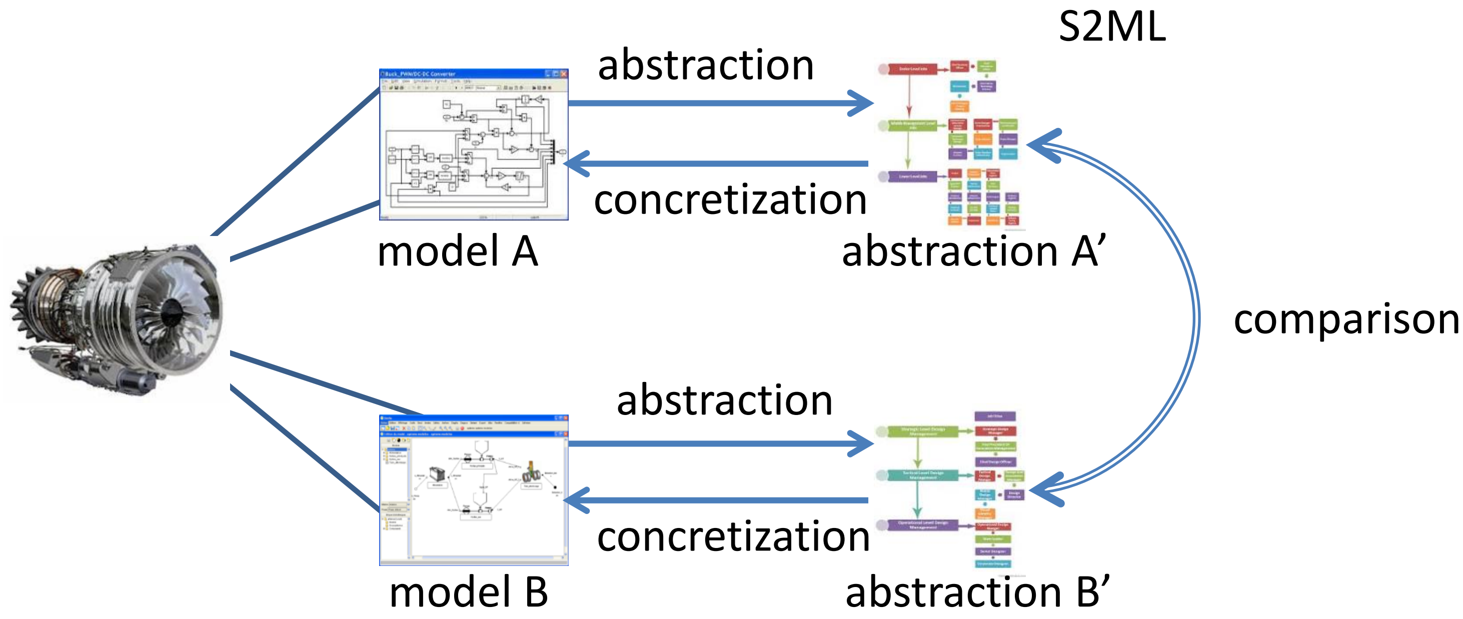
Key issues:

- How to manage models through the life cycle of systems?
- How to ensure that models are “speaking” about the same system?



Model Synchronization

Abstraction + Comparison = Synchronization



S2ML

abstraction

concretization

model A

abstraction A’

comparison

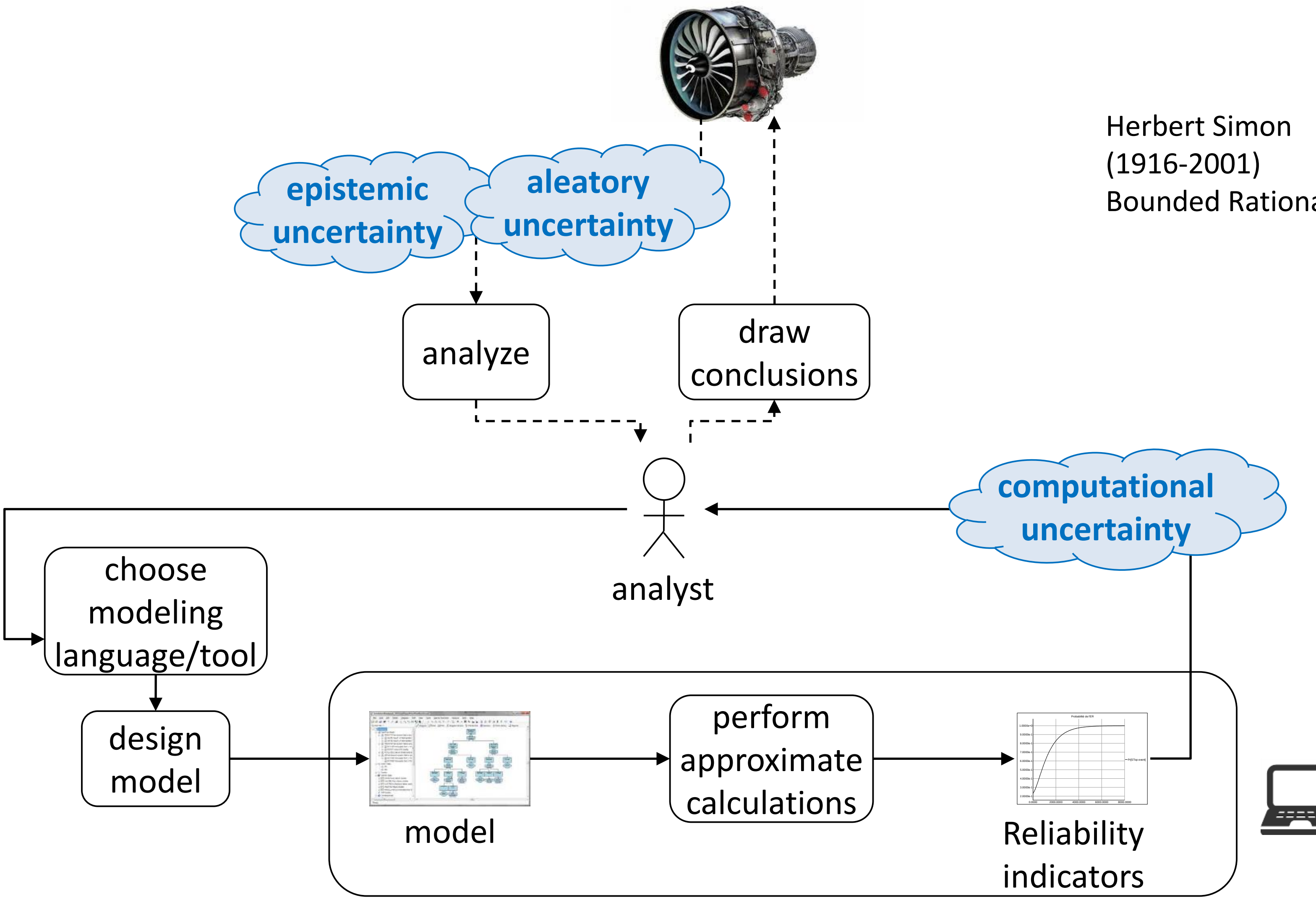
abstraction

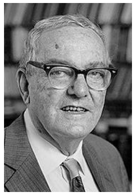
concretization

model B

abstraction B’

The Computational Complexity Barrier





Herbert Simon
(1916-2001)
Bounded Rationality

Challenges

- Tune **artificial intelligence techniques** to manage reliability data
  - Machine learning

- Design a new generation of modeling languages and assessment tools
  - Modeling languages
  - Algorithms & heuristics to push the limit of tractable models
  - Suitable abstractions of software parts of complex technical systems
  - Libraries of modeling patterns
  - **Model validation techniques**

- Integration of reliability engineering with other engineering disciplines
  - Co-simulation
  - **Model synchronization**