Safety Assessment of Autonomous Mobile Systems: Are We Ready?

Prof. Antoine B. Rauzy

Norwegian University of Science and Technology
Trondheim, Norway

Agenda

- Challenges for Safety Analyses of Autonomous Mobile Systems
- Hard Scientific and Technical Constraints
- The S2ML+X Family of Languages
- Model Synchronization
- Wrap-Up

Specificities of Autonomous Mobile Systems

- Mechanical but software intensive
- Cyber-physical (connected)
- Multi-phase
- Operate in evolving environments
- Safety critical
- Embed sensors
- Operate in fleet

Challenges for Safety Assessment

- Which safety standards to apply?
- How to take into account embedded software?
- How to take into account the multiple modes of operations?
- How to take into account cyber threats?
- How to take into account unconstrained and evolving environments?
- How to take into account fleets of autonomous mobile systems?
- How to collect reliability data (feedback experience)?
- How to integrate safety analysis and performance assessment?
- How to ensure the consistence of safety models with other types of systems engineering models?
- …

(R)evolution in Reliability Engineering

Yesterday:

Mechanical systems

Recording of failures

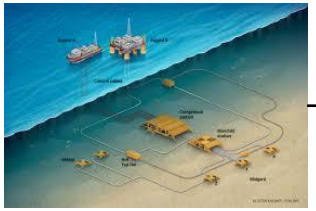
Local reliability databases

λ = 1.23e-6

Parametric distributions

Ad-hoc models, e.g. fault trees

Tomorrow:

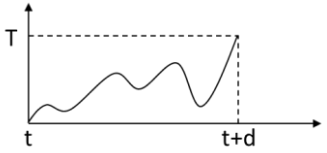


Cyber-physical systems

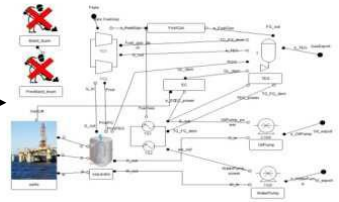
Health monitoring

Sensors

Distributed health condition databases



General distributions



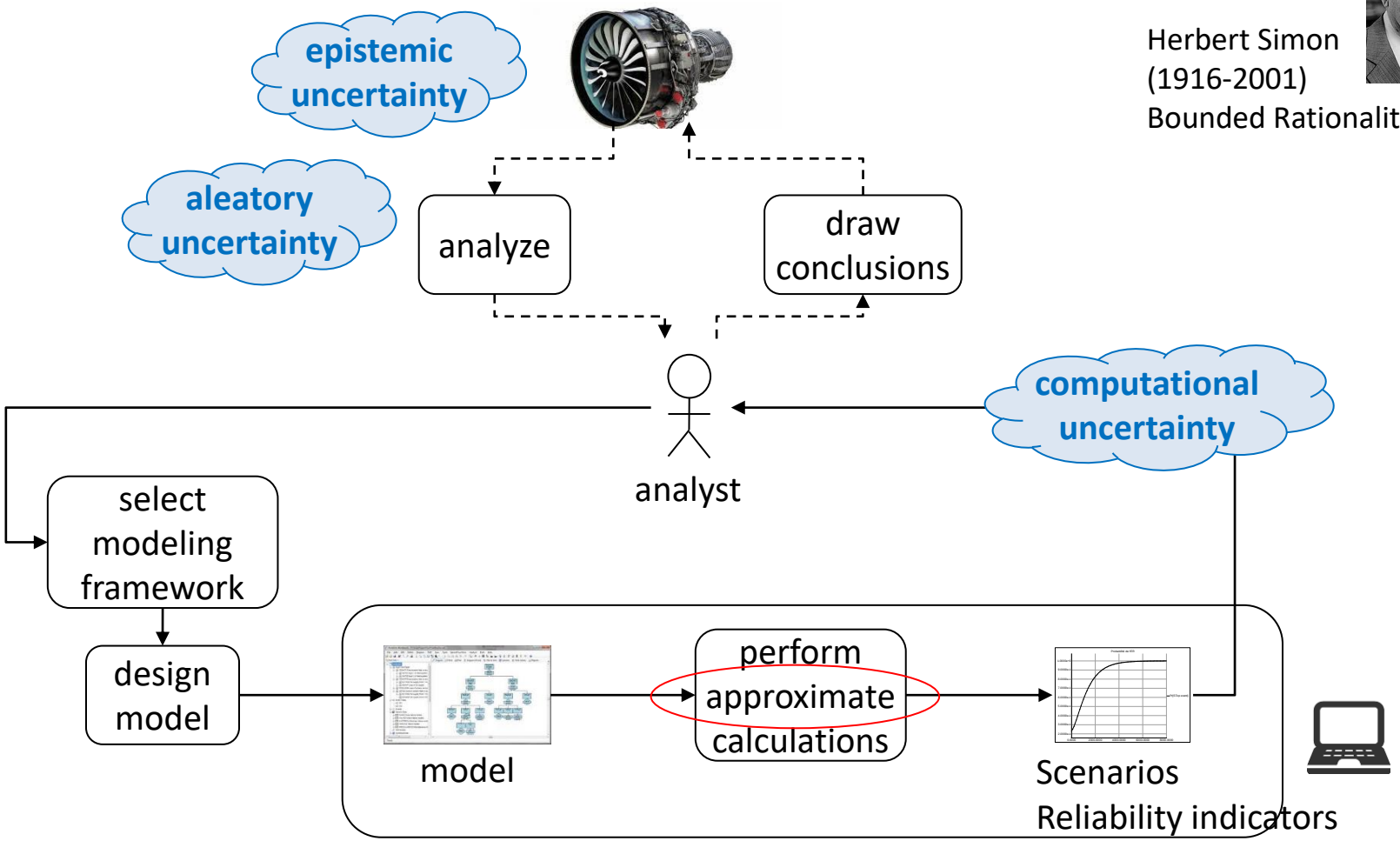
Behavioral models

Agenda

- Challenges for Safety Analyses of Autonomous Mobile Systems
- Hard Scientific and Technical Constraints
- The S2ML+X Family of Languages
- Model Synchronization
- Wrap-Up

Uncertainties in the Safety Assessment Process

Herbert Simon
(1916-2001)
Bounded Rationality



Classes of Modeling Languages

Combinatorial Formalisms
- Fault Trees
- Event Trees
- Reliability Block Diagrams
- Finite Degradation Structures

States Automata
- Markov chains
- Dynamic Fault Trees
- Stochastic Petri Nets
- …

Process Algebras
- Agent-based models
- Process algebras
- Python/Java/C++
- …

Expressive power

States | States + transitions | Deformable systems

Complexity of assessments

#P-hard but reasonable polynomial approximation | PSPACE-hard | Undecidable

Difficulty to design, to validate and to maintain models

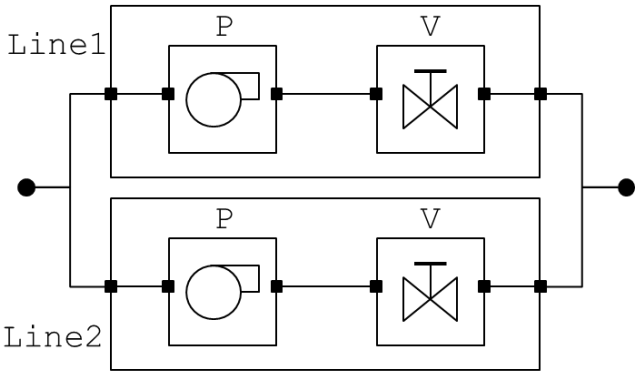
Agenda

- Challenges for Safety Analyses of Autonomous Mobile Systems
- Hard Scientific and Technical Constraints
- The S2ML+X Family of Languages
- Model Synchronization
- Wrap-Up

Characteristics of Behavioral Models

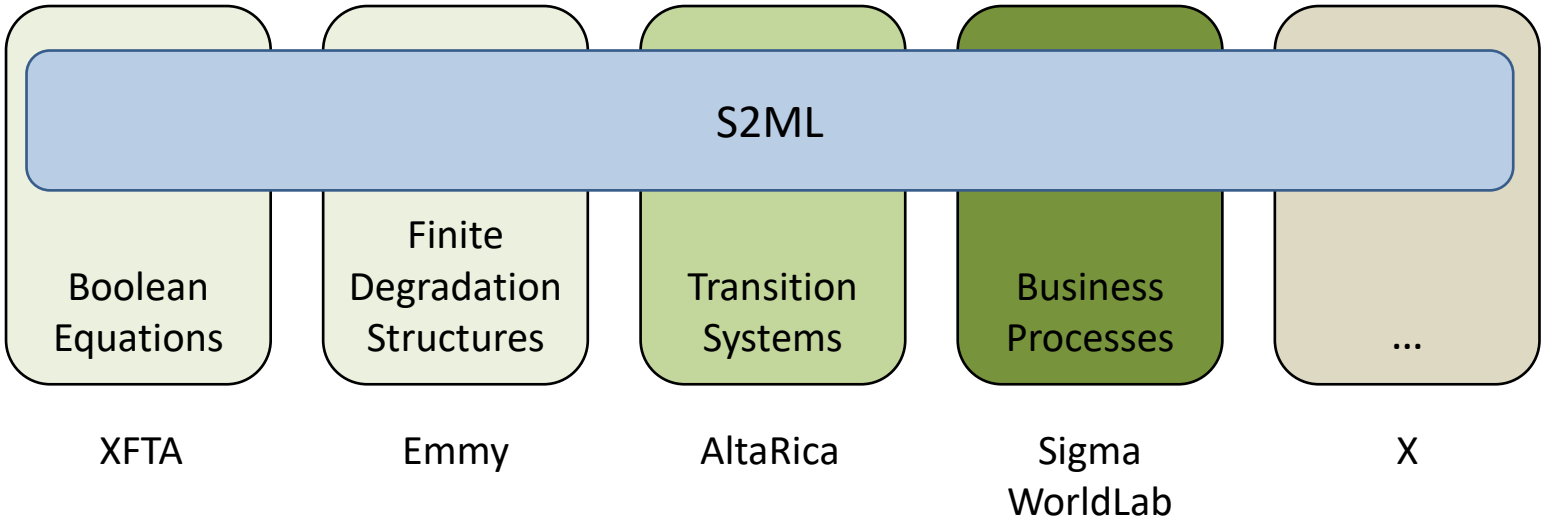
Behavior + Architecture = Model

- Any modeling language is the combination of a **mathematical framework** to describe the behavior and a **structuring paradigm** to organize the model.
- The choice of the **suitable mathematical framework** depends on which aspect of the system we want to study
- **Structuring paradigms** are to a very large extent **independent** of the chosen mathematical framework.



The S2ML+X Promise

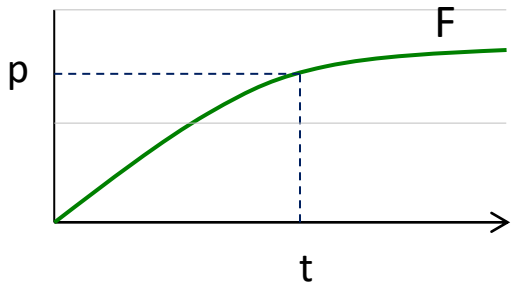
S2ML (System Structure Modeling Language): a coherent and versatile set of **structuring constructs** for any behavioral modeling language.



- The **structure of models** reflects the **structure of the system**, even though to a **limited extent.**
- **Structuring** helps to design, to debug, to share, to maintain and to align heterogeneous models.

Reliability Data

Probabilistic risk and safety assessments require **probability distributions** to be associated with **events** that change the state of the system under study.



F(t) = probability that the component is failed at time t

$F^{-1}(z)$ = (random) delay before the failure of the component

As of today, mostly **parametric probability distributions** (exponential, Weibull…)

From now on, more general calculation procedures:

- **Empirical distributions**
- **Learned distributions** (machine learning)

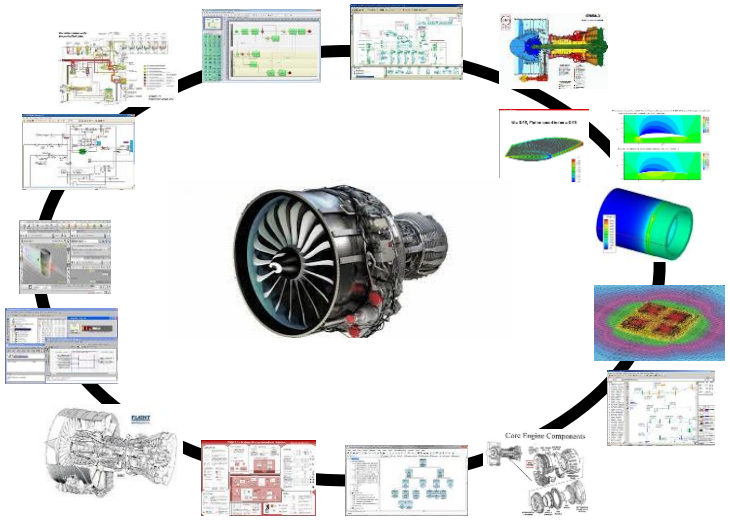
- A lot of data does not mean good data (rare events)
- Scenarios versus individual events

Agenda

- Challenges for Safety Analyses of Autonomous Mobile Systems
- Hard Scientific and Technical Constraints
- The S2ML+X Family of Languages
- Model Synchronization
- Wrap-Up

Model Diversity

Models are designed by **different teams** in **different languages** at **different levels of abstraction**, for **different purposes**, making **different approximations**. They have also **different maturities**.

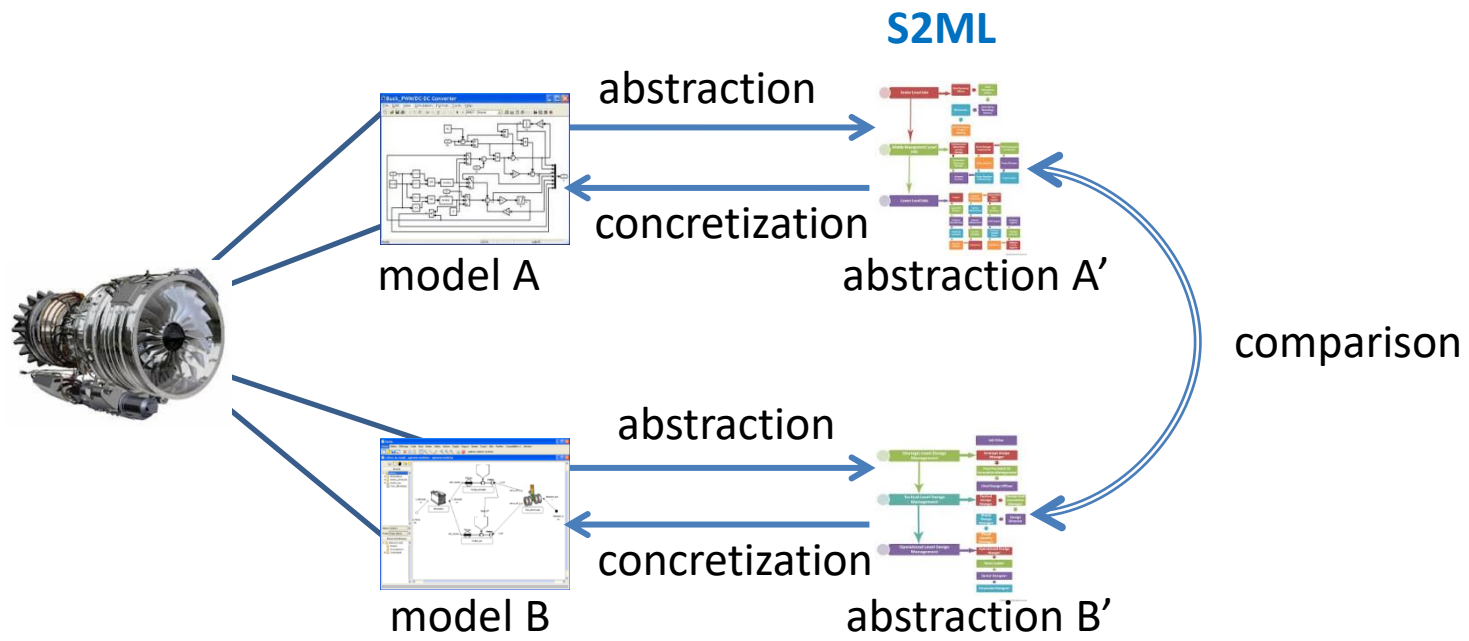


complexity → simplexity

1. The **diversity** of models is **irreducible.**
2. The **systemic digital twin** is a collection of **heterogeneous models**

Model Synchronization

Abstraction + Comparison = Synchronization



How to agree on disagreements?

Agenda

- Challenges for Safety Analyses of Autonomous Mobile Systems
- Hard Scientific and Technical Constraints
- The S2ML+X Family of Languages
- Model Synchronization
- Wrap-Up

Wrap-Up & Conclusion

- "Traditional" modeling approaches in reliability engineering are **no longer sufficient**:
  - Because the **systems** we are dealing with are **more complex**.
  - Because **new information technologies** open **new opportunities**.
  - Because **reliability models** should be **integrated** with models from other engineering disciplines, i.e. as a part of the **systemic digital twin**.

- **Huge benefits** can be expected from a full-scale deployment of model-based systems engineering. However, this requires:
  - To set up solid **scientific foundations** for **models engineering**.
  - To **bring to maturity** some **key technologies**.

- The **biggest challenge** is to **train new generation of engineers**:
  - With skills and competences in **discrete mathematics** and **computer science**, and
  - With skills and competences in **system thinking**, and
  - With skills and competences in **specific application domains**.