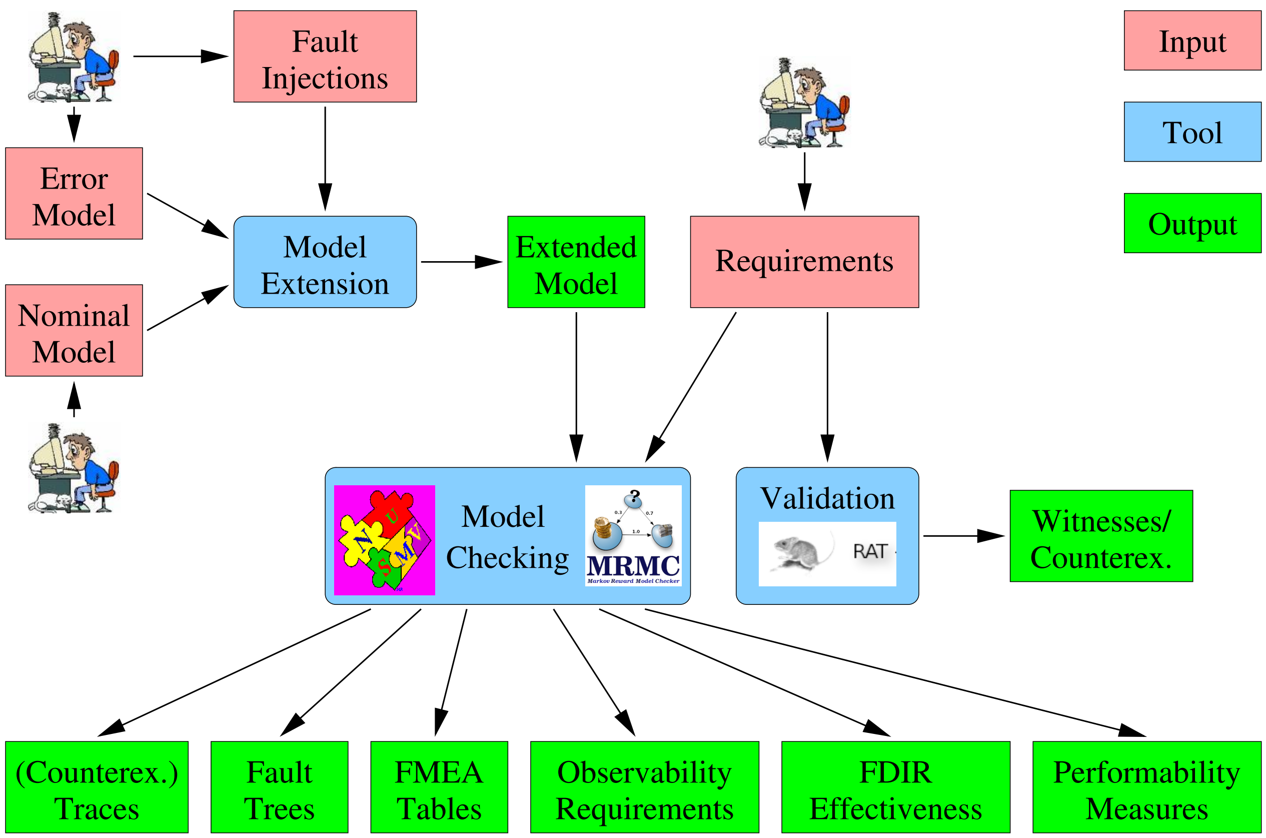
Statistical Approach for Timed Reachability in AADL Models

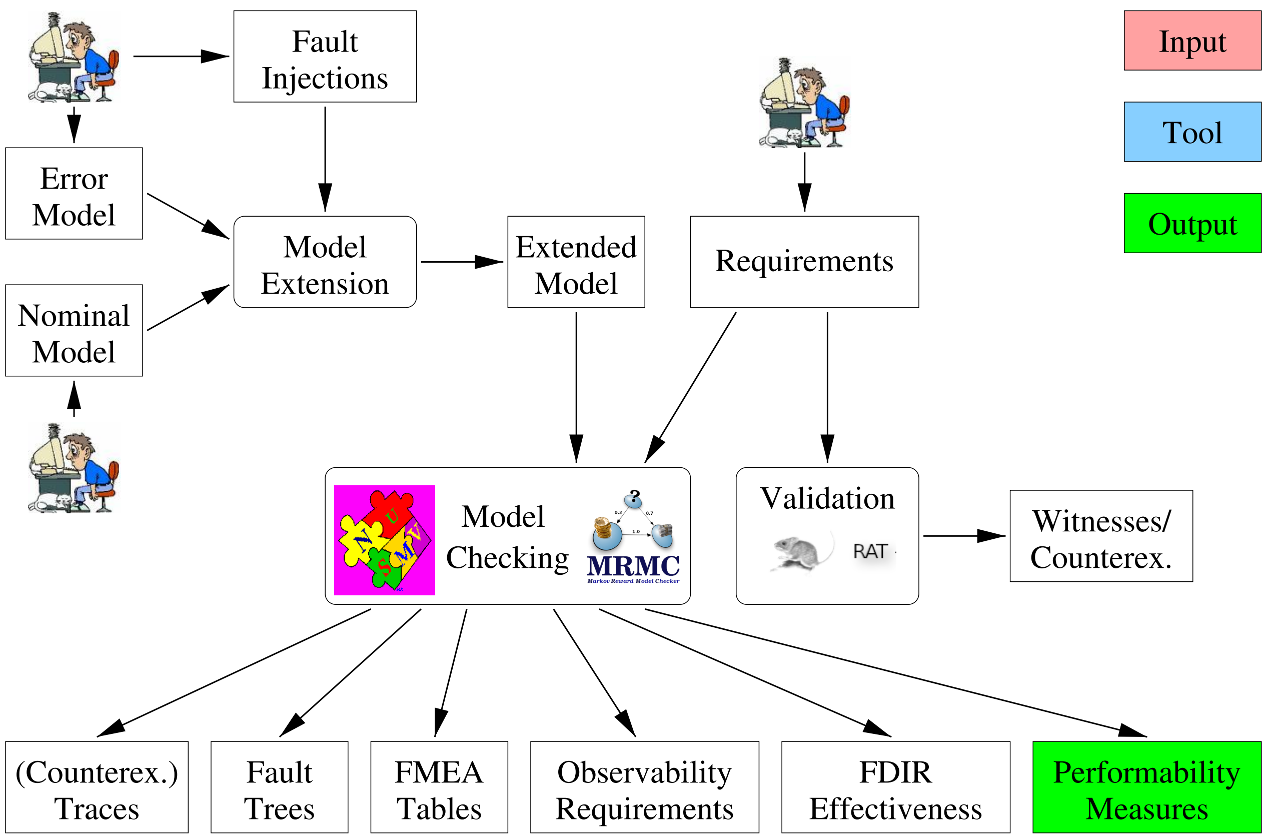
Harold Bruintjes, Joost-Pieter Katoen, David Lesens

Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

Methodology



Methodology



Introduction

Ever growing demand for probabilistic/dependability analysis.

HASDEL: Analysis of hybrid and probabilistic systems, used for space launchers and vehicles.

Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

Introduction

Ever growing demand for probabilistic/dependability analysis.

HASDEL: Analysis of hybrid and probabilistic systems, used for space launchers and vehicles.

What is in COMPASS:

- Analysis of timed/hybrid systems;
- Analysis of probabilistic systems;

Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

Introduction

Ever growing demand for probabilistic/dependability analysis.

HASDEL: Analysis of hybrid and probabilistic systems, used for space launchers and vehicles.

What is in COMPASS:

- Analysis of timed/hybrid systems;
- Analysis of probabilistic systems;
- **No** analysis of timed and probabilistic systems.

Introduction

Ever growing demand for probabilistic/dependability analysis.

HASDEL: Analysis of hybrid and probabilistic systems, used for space launchers and vehicles.

What is in COMPASS:

- Analysis of timed/hybrid systems;
- Analysis of probabilistic systems;
- **No** analysis of timed and probabilistic systems.

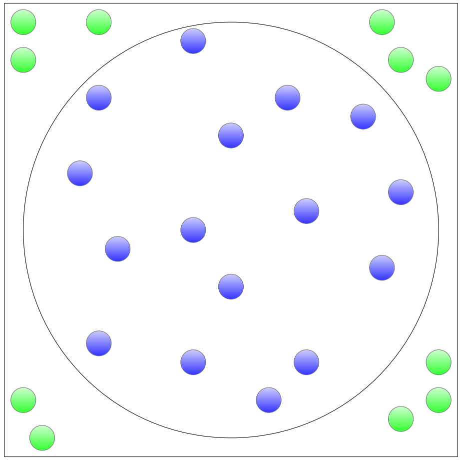
Problem: No tools (or algorithms) that support probabilistic analysis of the systems that can be described in the toolset.

Our approach: Use (Monte Carlo) simulation to approximate the system behavior

Statistical model checking for COMPASS/HASDEL

Monte Carlo simulation

Generate samples for a process generating random events. When enough samples are generated, with a certain probability the likelihood of the events can be determined.

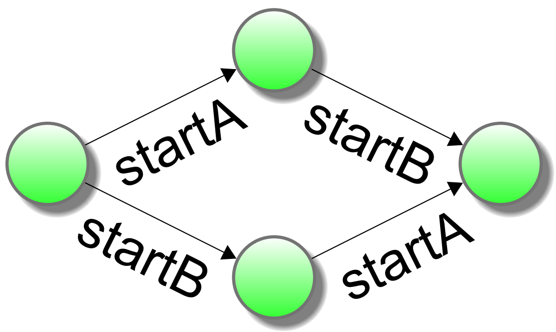


In our case: Event = Property true/false. Generating event = Generating path

Statistical model checking for COMPASS/HASDEL

Non-determinism

Non-determinism: Underspecification in the model, to model e.g. freedom of implementation, or parallelism.



As Monte-Carlo simulation is purely stochastic, this needs to be dealt with. Simulation cannot execute all choices at the same time.

Statistical model checking for COMPASS/HASDEL

Strategies

Non-determinism of choice is resolved by uniform distribution: Each possibility is equally likely to occur.

Four strategies have been implemented to resolving non-determinism of time:

- ASAP: Execute a step as soon as possible;
- Progressive: Randomly select a time delay where any transition is possible;
- Local: Randomly select any valid time delay;
- MaxTime: Delay as much as possible.

Statistical model checking for COMPASS/HASDEL

Strategies

Non-determinism of choice is resolved by uniform distribution: Each possibility is equally likely to occur.

Four strategies have been implemented to resolving non-determinism of time:

- ASAP: Execute a step as soon as possible;
- Progressive: Randomly select a time delay where any transition is possible;
- Local: Randomly select any valid time delay;
- MaxTime: Delay as much as possible.

(For testing there is also the option of manually inputting the next step)

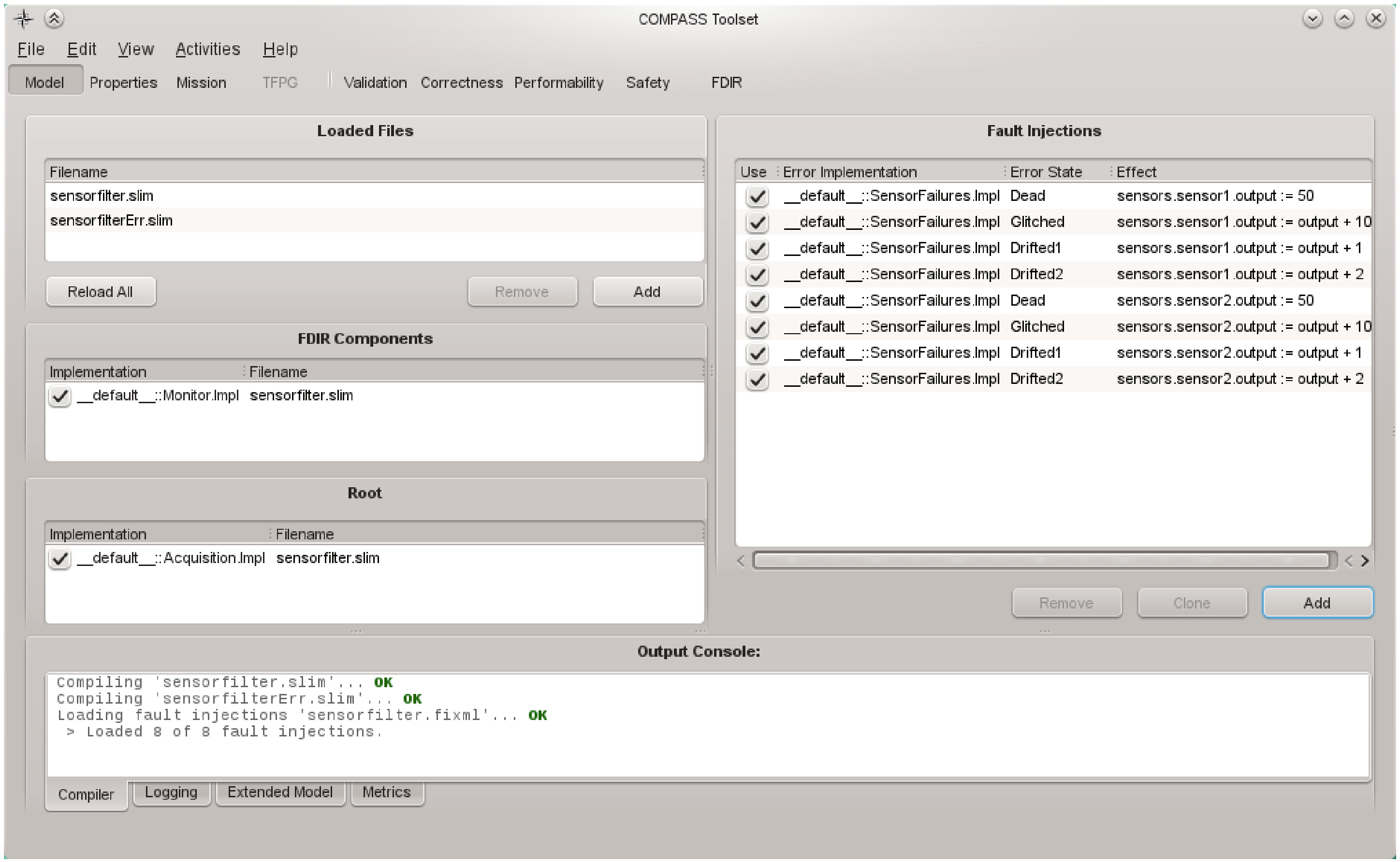
Monte-Carlo simulator for COMPASS implemented in `slimsim`

Inputs:

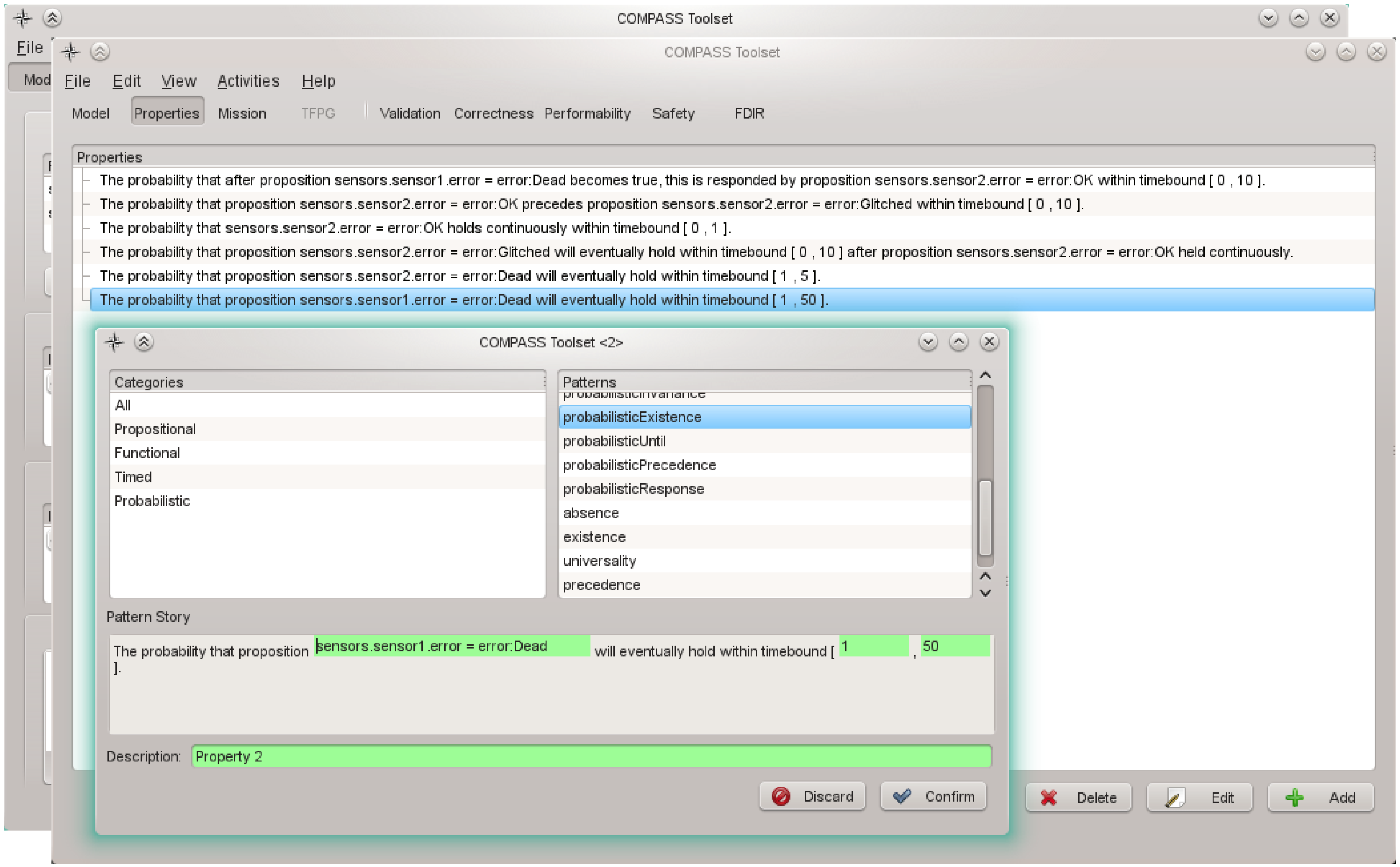
- SLIM models: nominal and error;
- Fault injections;
- Property;
- Strategy;
- *Error bound*: Width of resulting probability range;
- *Confidence*: Probability of *actual* value being within returned range.

Output: Probability range that the property holds true in the given model.

Toolset integration



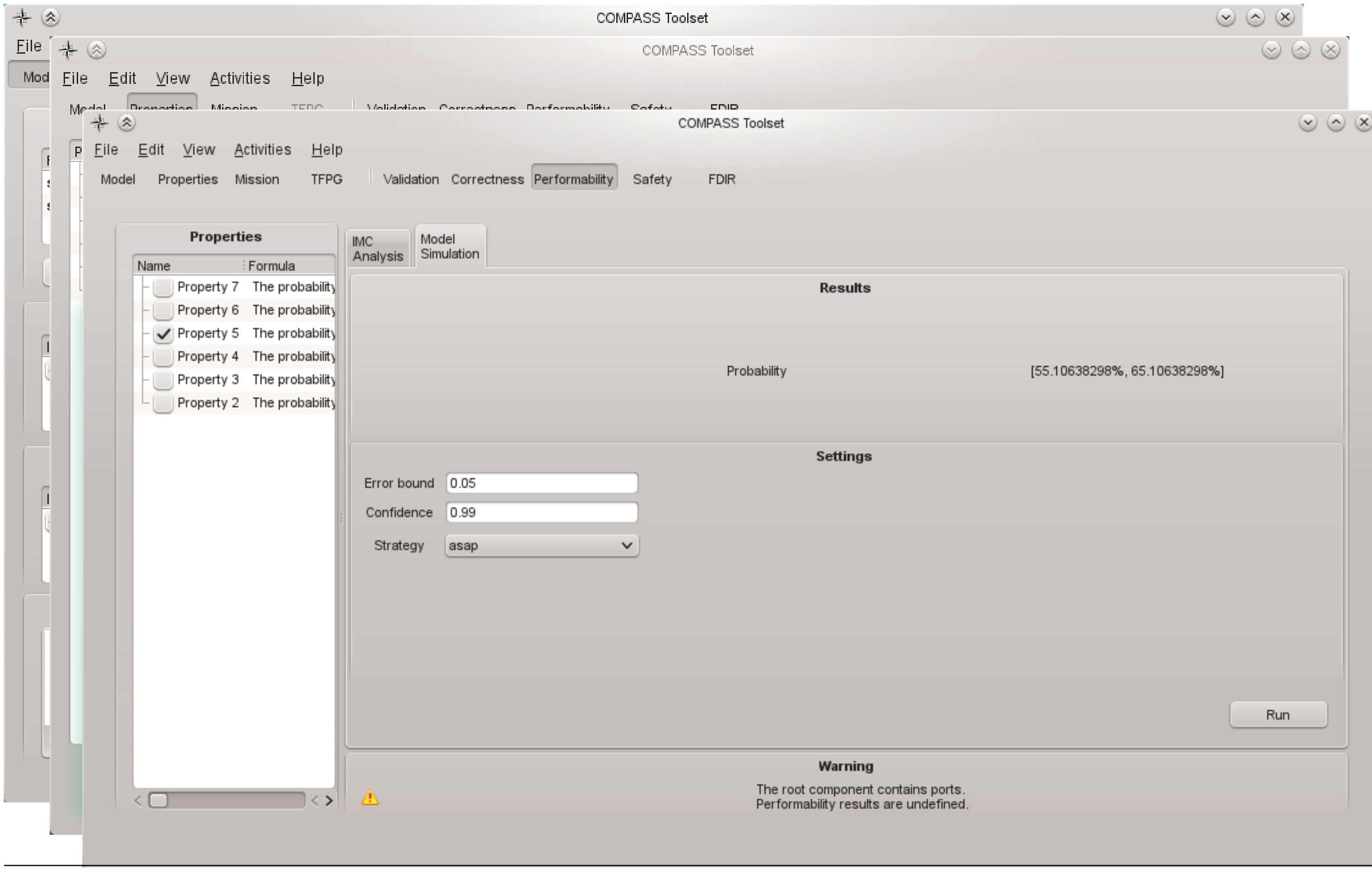
Toolset integration



Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

Toolset integration



Software Modeling and Verification Chair

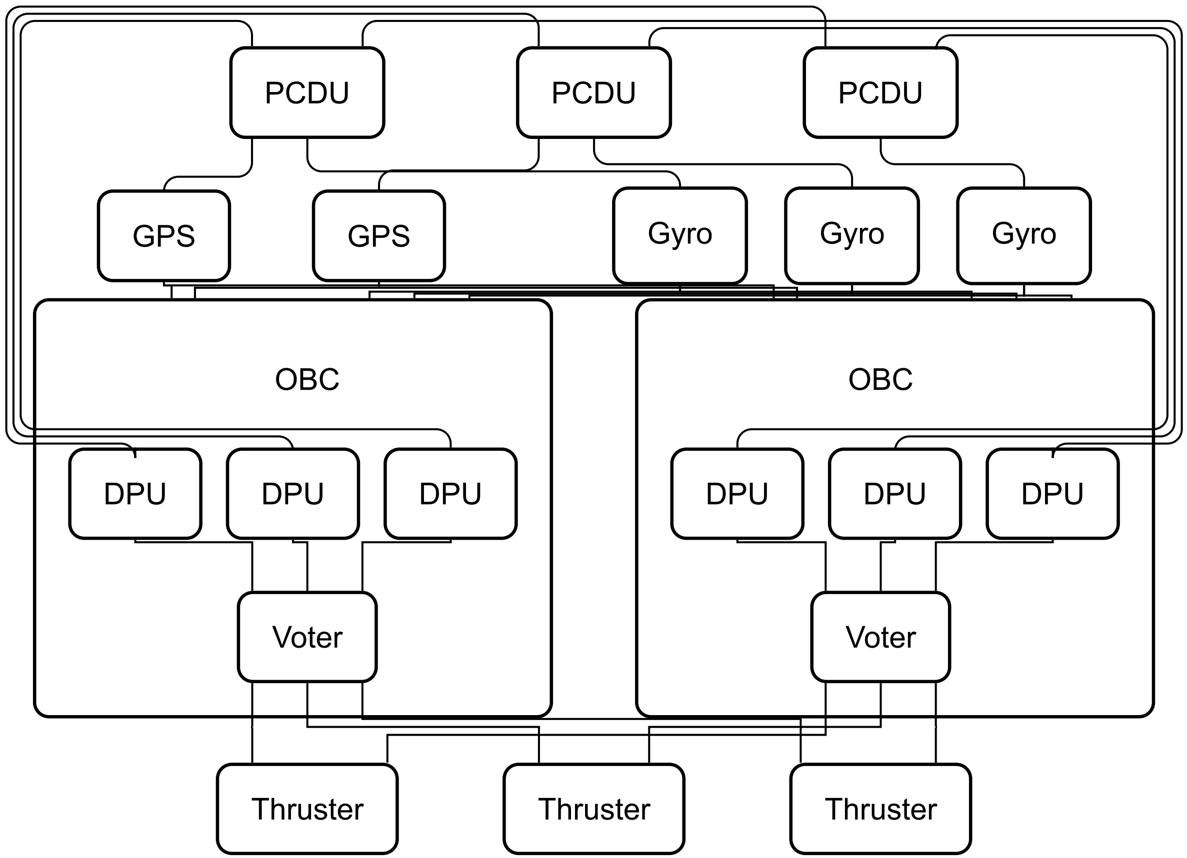
RWTH AACHEN UNIVERSITY

Avionics case study

As part of the evaluation of the HASDEL toolset, together with Airbus Defense and Space a case study has been performed. It defines some systems for a hypothetical launcher:

- Triple redundant Power Conditioning and Distribution Units (PCDU)
- Two redundant GPS devices
- Triple redundant Gyroscopes (Gyro)
- Two redundant On-Board Computers (OBC), consisting of:
  - Triple redundant Data Processing Units (DPU)
  - A Voter for the DPU outputs
- Three thrusters

Avionics case study



The architecture of the industrial case study. The connections between the GPS, Gyro and DPU units have been hidden for clarity. Rounded connections are for power, the others for signals.

Avionics case study

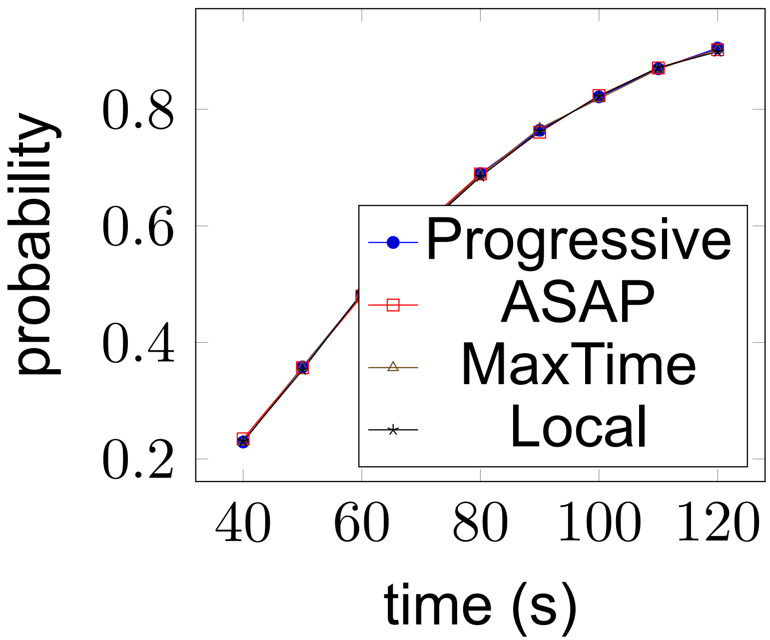
For each component, an error model is associated, defining transient, hot and permanent faults.

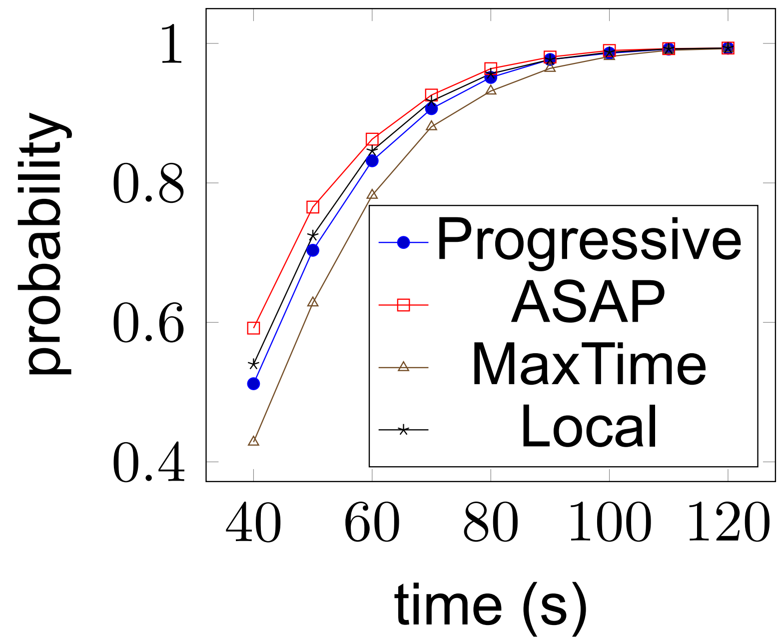
- 20 nominal and error component definitions
- 37 component instances
- 20 fault injections

Failure analysis was performed using Monte-Carlo simulation. System failure defined as both OBCs having failed.

Experimental results

Probabilities of system failure containing DPUs without (left) and with (right) repair





Conclusion

Project websites

`http://compass.informatik.rwth-aachen.de`
`https://es-static.fbk.eu/projects/hasdel`

Software Modeling and Verification Chair | RWTH AACHEN UNIVERSITY