Statistical Approach for Timed Reachability in AADL Models

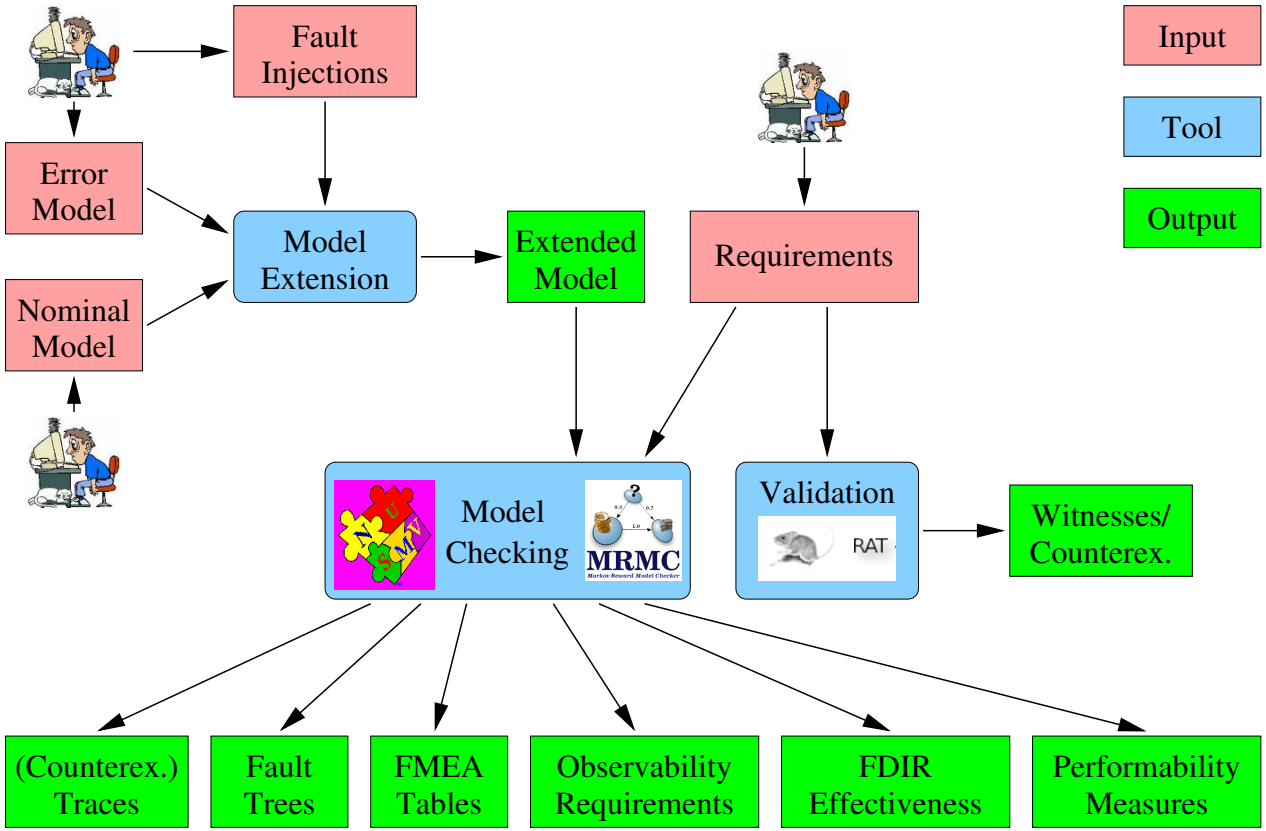
Software Modeling and Verification Chair
RWTH AACHEN UNIVERSITY

COMPASS

Main objective

Develop a model-based approach to system-software co-engineering while focusing on a coherent set of modeling and analysis techniques for evaluating system-level correctness, safety, dependability, and performance of on-board computer-based aerospace systems.

Methodology



COMPASS

Project goal: extend our capabilities to analyze timed and probabilistic systems, avoiding hard- and software failures and improve overall confidence.

Otherwise, prevent bad things from happening:

Insert any picture of rather expensive equipment unintentionally exploding here.

COMPASS

Problem: Currently 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

SLIM

SLIM is a modeling language based on AADL

Example nominal:

```
device gpsDevice
    features
        measurement : out data port bool default false;
end gpsDevice;

device implementation gpsDevice.i
    flows
        measurement := true  in modes (active);
    modes
        acquisition : activation mode urgent in 20 sec;
        active      : mode;
    transitions
        acquisition -[ within 10 sec to 20 sec ]-> active;
end gpsDevice.i;
```

SLIM

SLIM is a modeling language based on AADL

Example error:

```
error model gpsError
    features
        nok : out error propagation;
end gpsError;

error model implementation gpsError.i
    events
        transient_fault   : error event occurrence poisson 0.001 per hour;
        hot_fault         : error event occurrence poisson 0.001 per day;
    states
        ok                : initial state;
        transient_failure_prop : error state;
        transient_failure : error state urgent in 400 msec;
        hot_failure_prop  : error state;
        hot_failure       : error state;
    transitions
        ok                -[ transient_fault                ]-> transient_failure_prop;
        transient_failure -[ nok within 200 msec to 400 msec ]-> ok;
        ok                -[ hot_fault                      ]-> hot_failure_prop;
        hot_failure       -[ @activation                    ]-> ok;
        transient_failure -[ @activation                    ]-> ok;
end gpsError.i;
```

Preliminaries

SLIM

A fully formalized language derived from AADL, with support for:

- Timed behavior (clocks, guard and invariants)
- Data flows
- Synchronizing events
- Nonblocking events
- Probabilistic error events
- Component reconfiguration (@activation)

Statistical model checking for COMPASS/HASDEL

Ever growing demand for probabilistic/dependability analysis.

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

COMPASS:

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

Monte Carlo simulation

A brief intro

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

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

Strategies

Path generation

Generate steps until property can be determined true or false. For CSL, simple to check for basic state formulae:

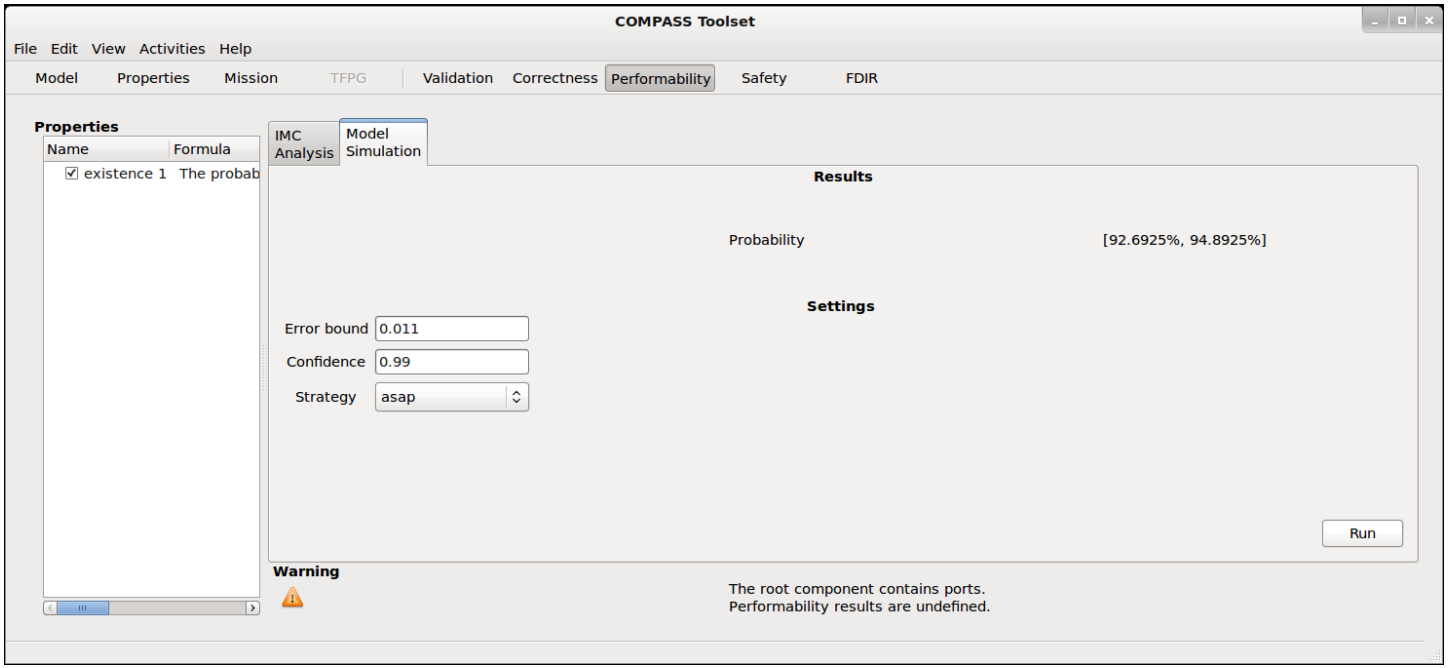
- $M \models a \Leftrightarrow a$ holds true in the current state
- $M \models \psi \wedge \phi \Leftrightarrow M \models \psi \wedge M \models \phi$
- etc...

For path based formulae (i.e. $\psi \mathbf{U}^{[l,u]} \phi$), a tri-state approach is used (true, false, ``not yet known'').

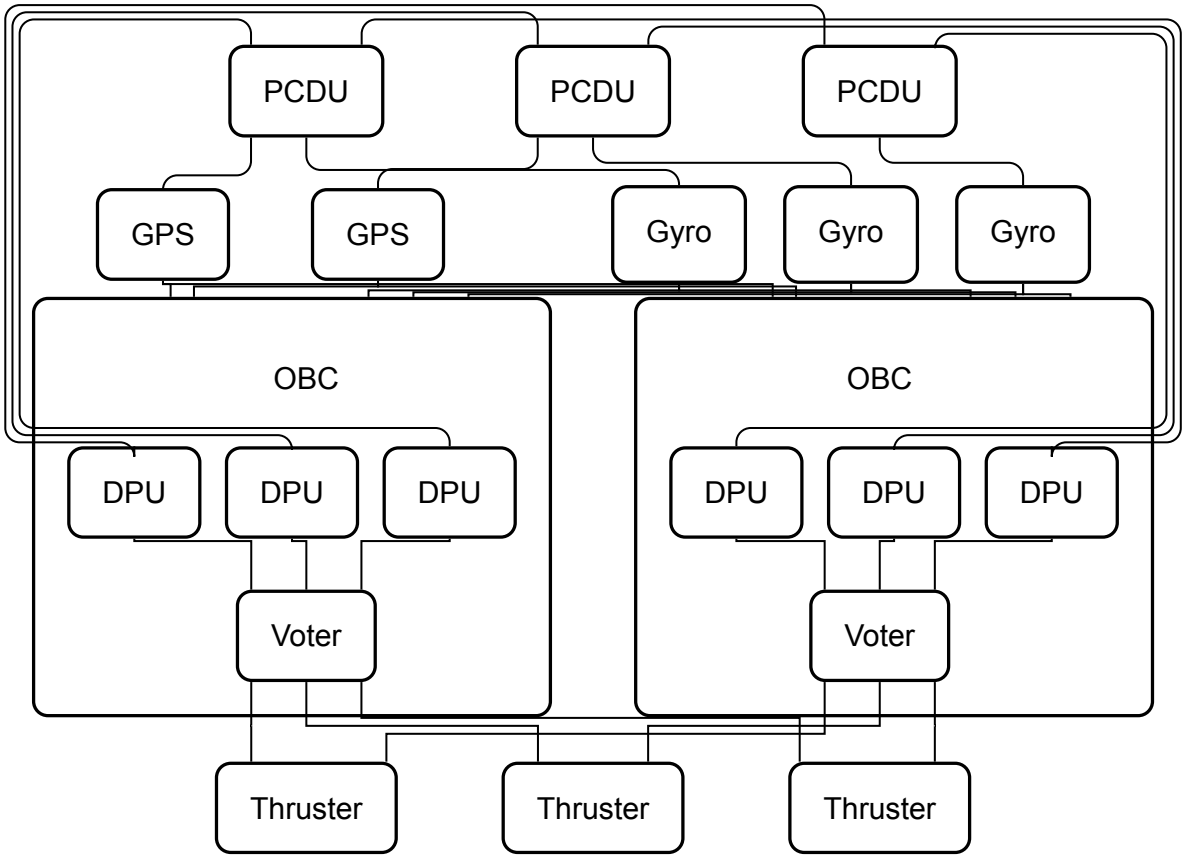
For the operator $Pr_{\bowtie c}(\psi)$, (recursive) simulation is used. Note: `slimsim` currently does not support nesting.

Special cases: Zeno behavior and deadlocks

Toolset integration



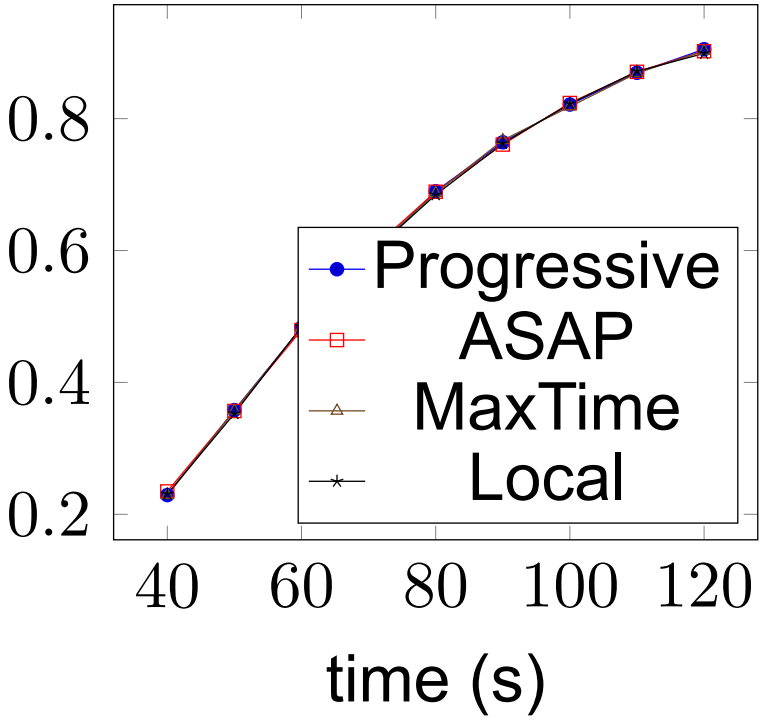
Avionics case study

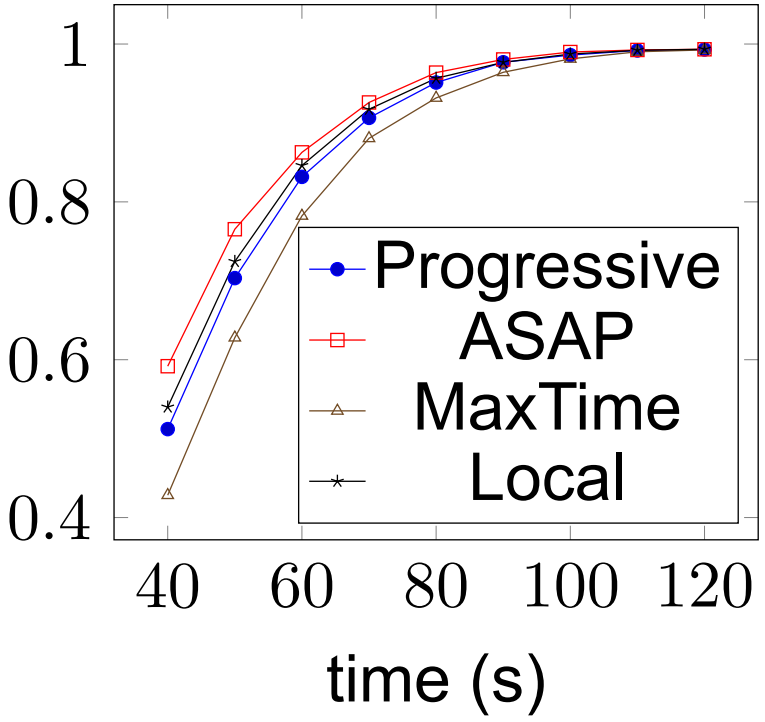


The architecture of the industrial case study. The connections between the GPS, Gyro and DPU units have been hidden for clarity. Rounded connections are for power, the others for signals.

Experimental results

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





Conclusion

- COMPASS/HASDEL project
- Real-time extensions: Monte-Carlo approach
- Investigate different strategies
- Implement and performed case study w/ Astrium/ADAS

Conclusion

Project websites

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

Thank you for your attention

Any questions?