INTO-CPS
Practical Verification for Cyber-Physical Systems

Jim Woodcock
University of York

Linköping University

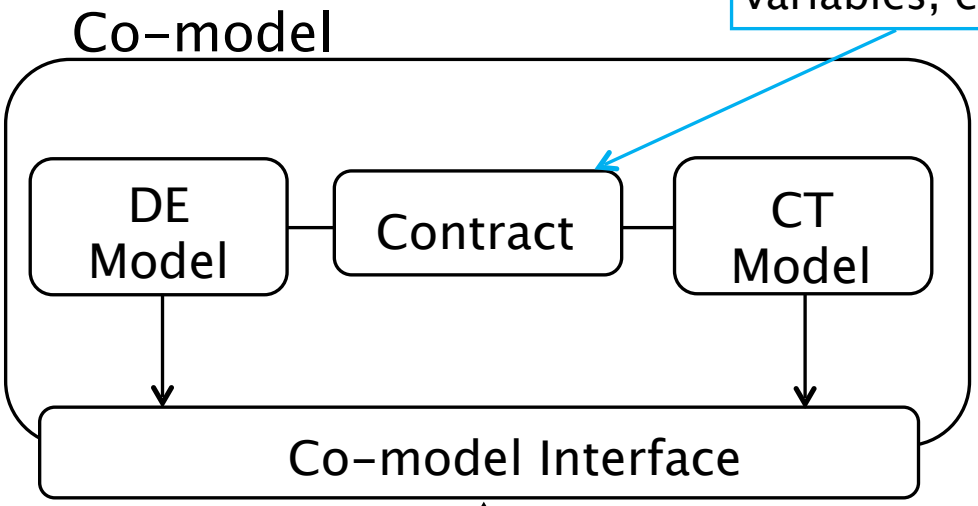
INTO-CPS

- Three-year Horizon 2020 project
- Integrated toolchain for cyber-physical systems
- Heterogeneous components
  - concurrent, discrete, continuous, stochastic,…
- Verification
  - co-simulation with diverse tools
  - verification, model checking with diverse semantics
- Three most important ideas in the project:
  - automation
  - automation
  - automation

Heterogeneous Semantics

- Single meta-language for heterogeneous semantics
  - Unifying Theories of Programming
  - discrete and hybrid relational calculi
- Implementation in Isabelle/HOL theorem prover
- Support for verification activities
  - test-case/scenario generation, test/simulation oracles
  - structural verification:
    - model consistency, deadlock, livelock, determinism
  - property verification: theorem provers/model checkers
  - refinement checking
  - design space exploration
  - engineering emergent properties

Collaborative (Co-) Modelling



Shared design parameters, variables, events

Design parameters fixed per run
Variables modified during run

Ideal, realistic, faulty behaviours
Fault modelling including error states & faulty functionality
Fault activation during simulation managed by the script

Settings & Script

Initialise variables
Set design parameters
Swap components
Simulate user input
Inject faults

Co-model Outputs