Algorithmic stability verification of cyber physical systems

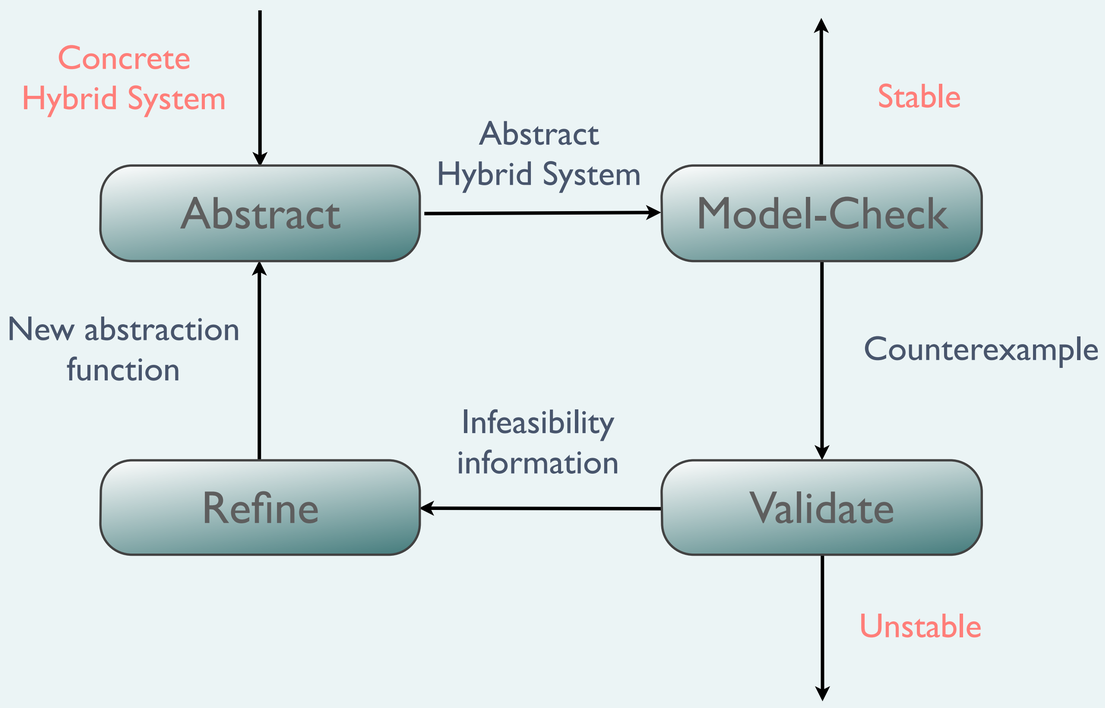
Miriam García Soto and Pavithra Prabhakar
IMDEA Software Institute, Madrid, Spain

Motivation

- **Cyber Physical Systems (CPS):** systems which combine control, communication and computation.
- **Applications:** aeronautics, automotive, manufacturing processes, robotics, medical devices and consumer appliances.
- **Challenge:** design methodology for building high-confidence systems.
- **Unique feature:** mixed discrete-continuous behaviour.
- **Formal verification:** a promising approach based on strong mathematical foundations.

An algorithmic framework

Algorithmic	Fully automated verification by an exhaustive state-space exploration.
Deductive	verification by reduction to a theorem proving task, often requires substantial user input.

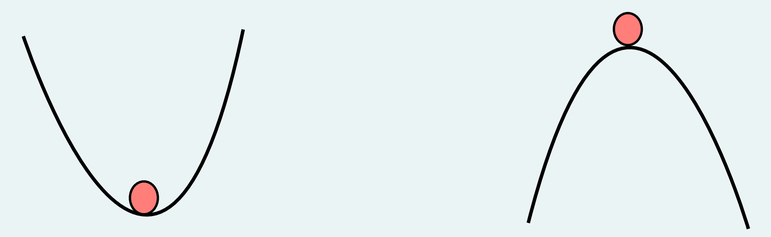


- **Abstraction:** construct a simpler system; a modified predicate abstraction resulting in a finite weighted graph.
- **Model-checking:** state-space exploration; check for the existence of cycles indicating instability.
- **Validation:** check if counter-example corresponds to a bug; check if the cycle corresponds to a diverging infinite path (not a bounded model-checking problem).
- **Refinement:** construct a more precise system; add more predicates.

Stability verification problem

Given a hybrid automaton, is it stable?

- **Hybrid Automaton:** model capturing the mixed discrete-continuous behaviour.
- **Stability:** small perturbations in the initial state/input of a system induce only small variations in the eventual behaviour of the system.



A stable system *An unstable system*

Tool Architecture

AVERIST: Algorithmic VERIfier for STability