Verification and Validation for Industrial Control Systems

Xiaoqing Jin

Toyota Technical Center: James Kapinski, Jyotirmoy Deshmukh, Hisahiro Ito, Ken Butts

External Collaborators: Sriram Sankaranarayanan, Aditya Zutshi, Nikos Aréchiga, Thao Dang, Tommaso Dreossi, Alexandre Donzé, Sanjit Seshia, Georgios Fainekos

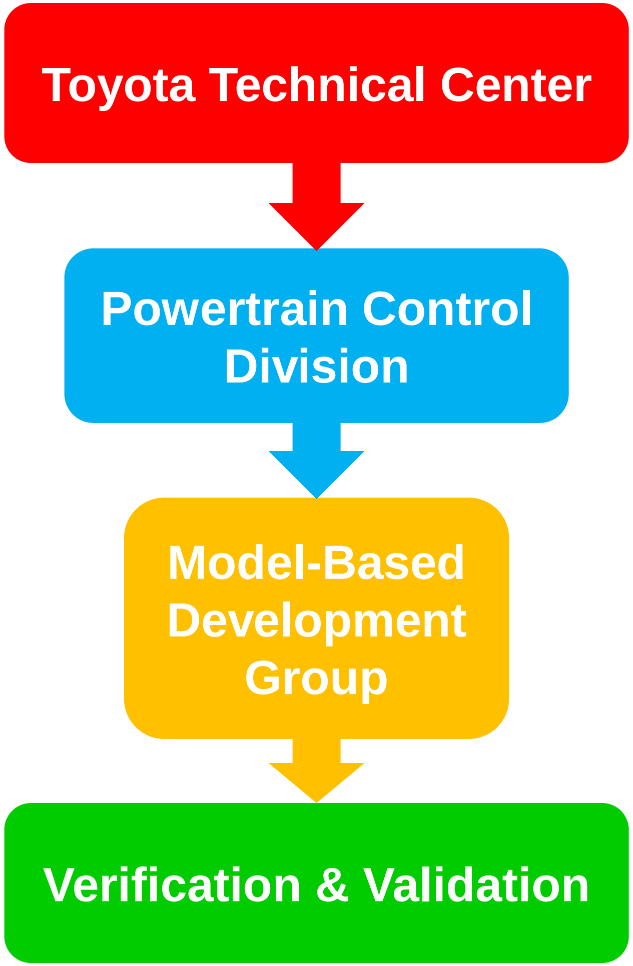
September 19, 2014

Dr. Clarke’s Influence on V&V in Our Research Group

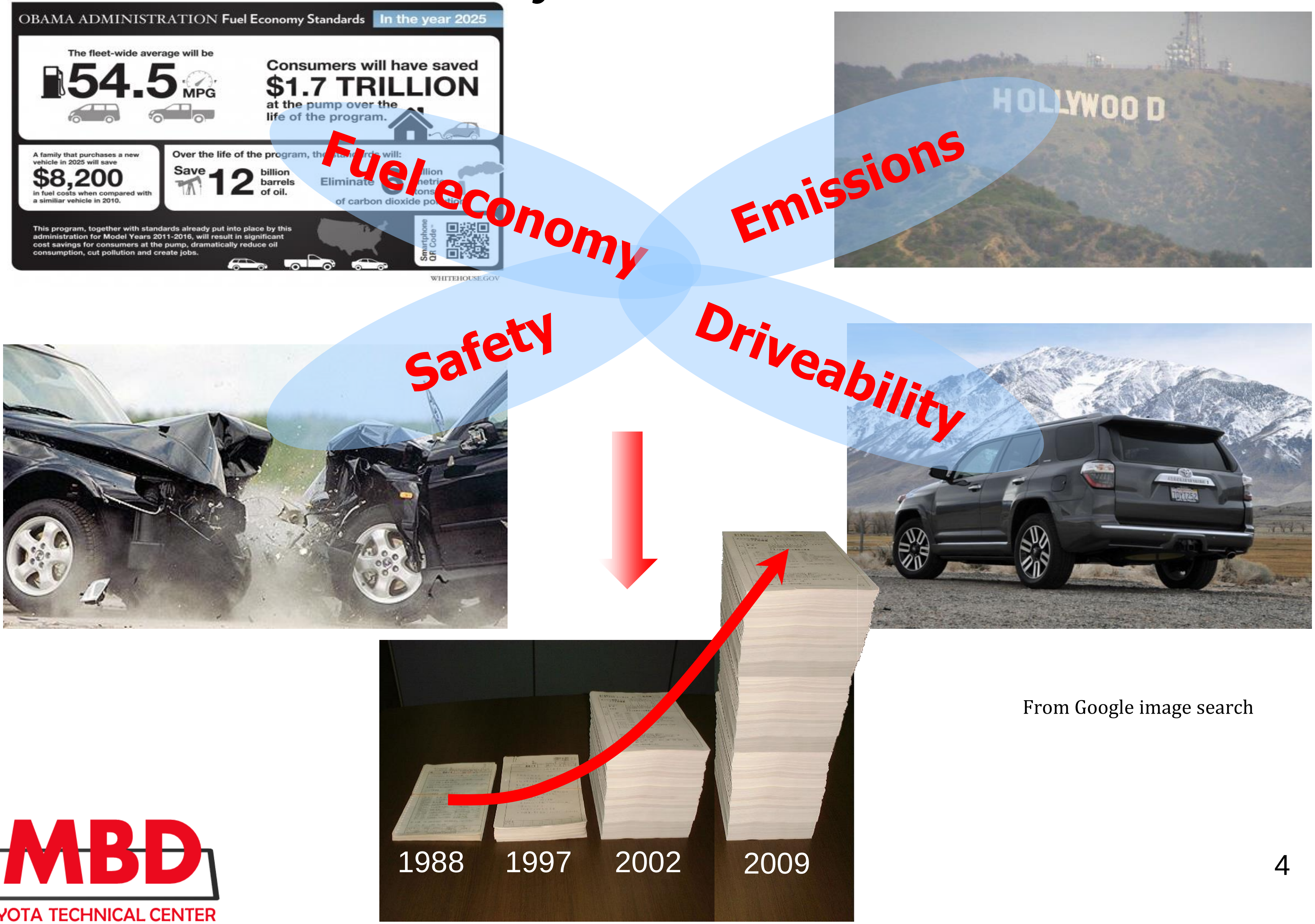
- Model checking
  - Tool of interest: CBMC
- Falsification of hybrid systems
  - Technology of interest: CEGAR
- Stability analysis of hybrid systems
  - Tool of interest: dReal (Nonlinear SMT solver)

Toyota MBD Group

- **Our group focus**
  - Advanced research in V&V for powertrain controller designs
- **Our group background**
  - Cyber-physical systems (hybrid systems)
  - Formal verification methods
- **Our perspective**
  - Focus is on techniques for application-level real-time controller development


Toyota Technical Center
Powertrain Control Division
Model-Based Development Group
Verification & Validation

Why V&V?



OBAMA ADMINISTRATION Fuel Economy Standards In the year 2025

The fleet-wide average will be 54.5 MPG

Consumers will have saved $1.7 TRILLION at the pump over the life of the program.

A family that purchases a new vehicle in 2025 will save $8,200 in fuel costs when compared with a similiar vehicle in 2010.

Over the life of the program, the standards will:

Save 12 billion barrels of oil.

Eliminate 6 billion metric tons of carbon dioxide pollution.

This program, together with standards already put into place by this administration for Model Years 2011-2016, will result in significant cost savings for consumers at the pump, dramatically reduce oil consumption, cut pollution and create jobs.

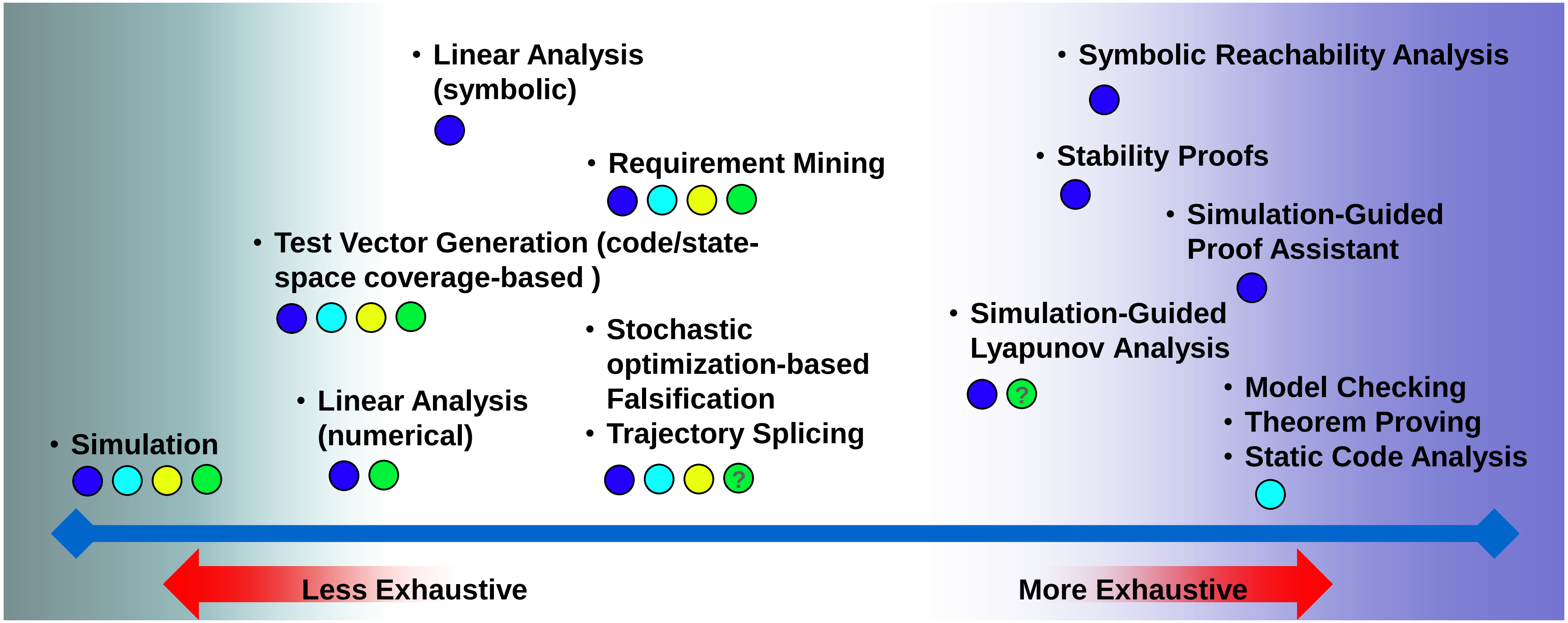
Smartphone QR Code™

WHITEHOUSE.GOV

From Google image search

Spectrum of Analysis Techniques

● Simplified closed-loop controller design models (small scale, abstract)
● Open-loop controller component models (small scale, detailed)
● Open-loop complete controller models (large scale, detailed)
● Closed-loop system models (large scale, detailed)



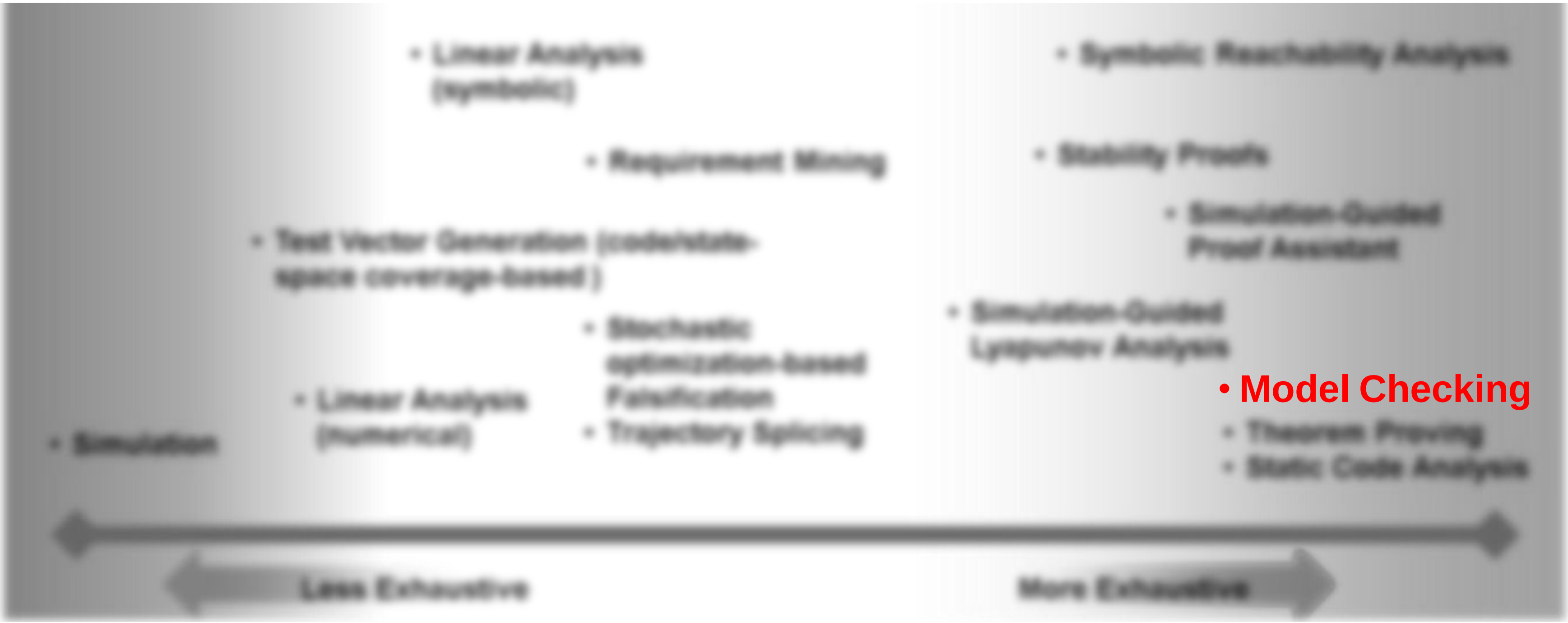
- Linear Analysis (symbolic)
- Requirement Mining
- Test Vector Generation (code/state-space coverage-based)
- Stochastic optimization-based Falsification
- Trajectory Splicing
- Linear Analysis (numerical)
- Simulation
- Symbolic Reachability Analysis
- Stability Proofs
- Simulation-Guided Proof Assistant
- Simulation-Guided Lyapunov Analysis
- Model Checking
- Theorem Proving
- Static Code Analysis

Less Exhaustive

More Exhaustive

Spectrum of Analysis Techniques

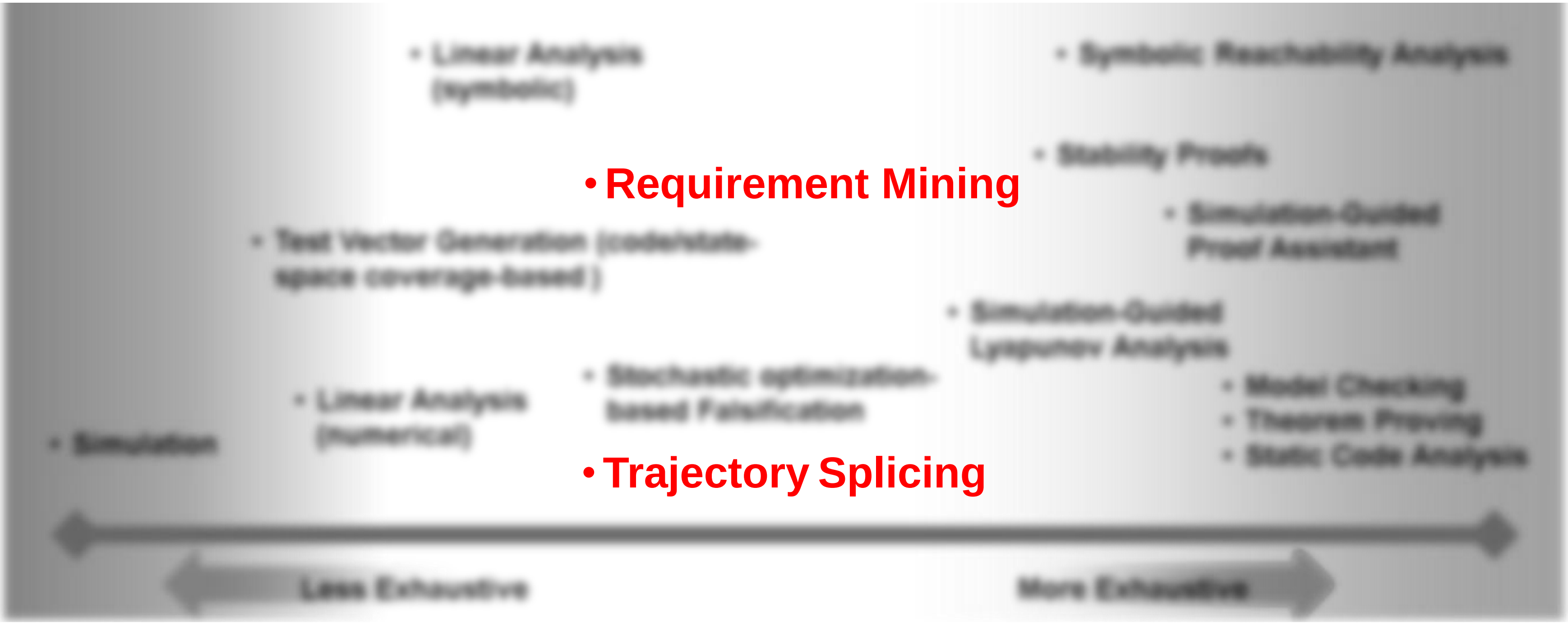
[Clarke, Emerson**]** *Design and Synthesis of Synchronization Skeletons Using Branching-Time Temporal Logic*, **1982.**
[Clarke, Kroening, Yorav**]** *Behavioral consistency of C and Verilog programs using bounded model checking* **DAC, 2003**.


• Linear Analysis (symbolic)
• Symbolic Reachability Analysis
• Requirement Mining
• Stability Proofs
• Simulation-Guided Proof Assistant
• Test Vector Generation (code/state-space coverage-based)
• Simulation-Guided Lyapunov Analysis
• Stochastic optimization-based Falsification
• Model Checking
• Linear Analysis (numerical)
• Trajectory Splicing
• Theorem Proving
• Static Code Analysis
• Simulation
Less Exhaustive
More Exhaustive

Spectrum of Analysis Techniques

[Clarke, Grumberg, Jha, Lu, Veith**]** *Counterexample-guided abstraction refinement* **CAV, 2000.**

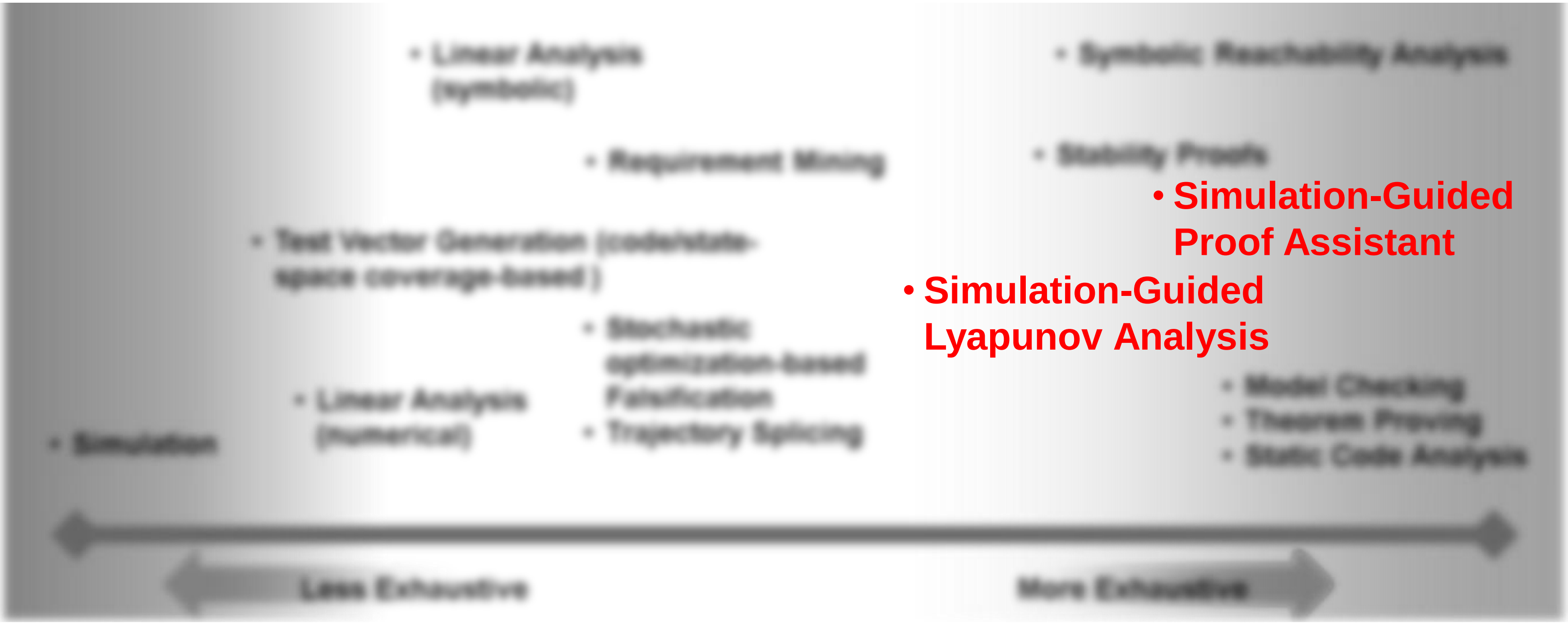
[Fehnker**, Clarke**, Jha, Krogh**]** *Refining abstractions of hybrid systems using counterexample fragments* **HSCC, 2005**.


• Linear Analysis (symbolic)
• Symbolic Reachability Analysis
• Stability Proofs
• Simulation-Guided Proof Assistant
• Test Vector Generation (code/state-space coverage-based)
• Simulation-Guided Lyapunov Analysis
• Stochastic optimization-based Falsification
• Linear Analysis (numerical)
• Simulation
• Model Checking
• Theorem Proving
• Static Code Analysis
Less Exhaustive
More Exhaustive

- **Requirement Mining**
- **Trajectory Splicing**

Spectrum of Analysis Techniques

[Gao, Kong, **Clarke**] *dReal: An SMT solver for nonlinear theories over the reals* **CADE, 2013.**



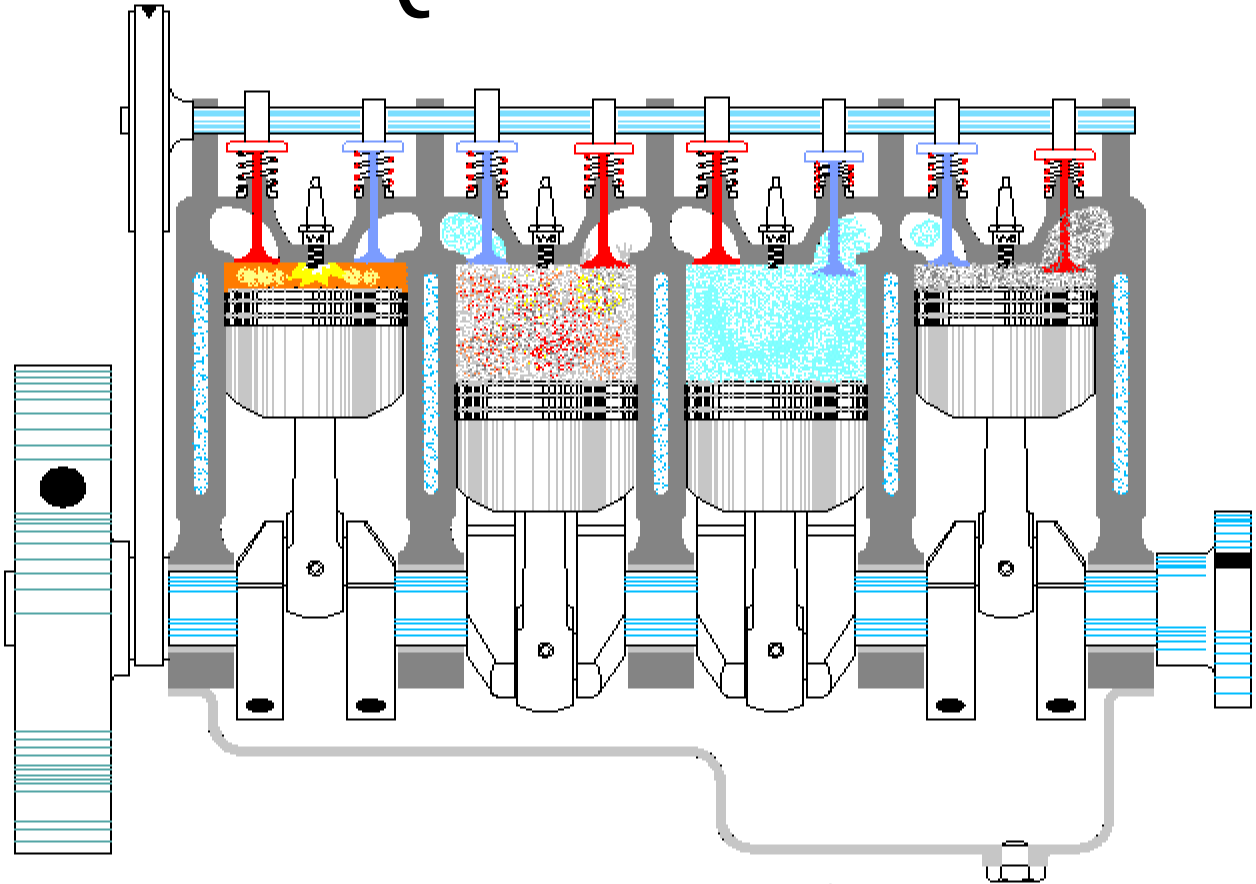
- Linear Analysis (symbolic)
- Symbolic Reachability Analysis
- Requirement Mining
- Stability Proofs
- **Simulation-Guided Proof Assistant**
- Test Vector Generation (code/state-space coverage-based)
- **Simulation-Guided Lyapunov Analysis**
- Stochastic optimization-based Falsification
- Model Checking
- Theorem Proving
- Linear Analysis (numerical)
- Trajectory Splicing
- Static Code Analysis
- Simulation

Less Exhaustive

More Exhaustive

Thank you for your attention.

Questions?



From: http://xorl.wordpress.com/2011/03/05/the-basics-of-4-stroke-internal-combustion-engines/