

SMT-based Probabilistic Analysis of Timing Constraints in Cyber-Physical Systems

Li Huang¹ and Eun-Young Kang¹²,

¹School of Data & Computer Science, Sun Yat-sen University, China
huangl223@mail2.sysu.edu.cn

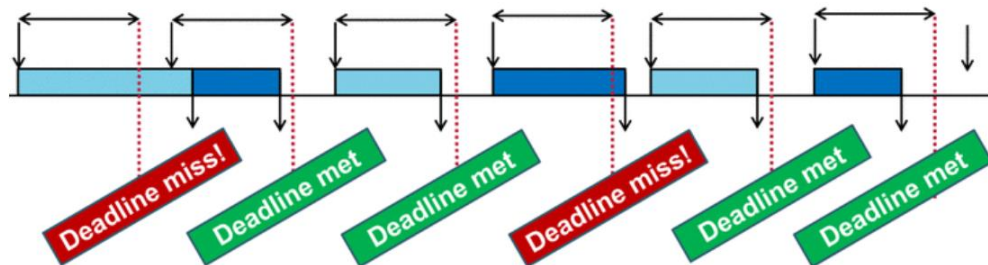
²PreCISE Research Centre, University of Namur, Belgium
eykang@fundp.ac.be

Background & Motivation

- Cyber Physical Systems (CPS), e.g., automotive systems, are **real-time** embedded systems.
- CPS contain **continuous dynamic** behaviors and **stochastic behaviors**.
- **Timing constraints** should be satisfied.



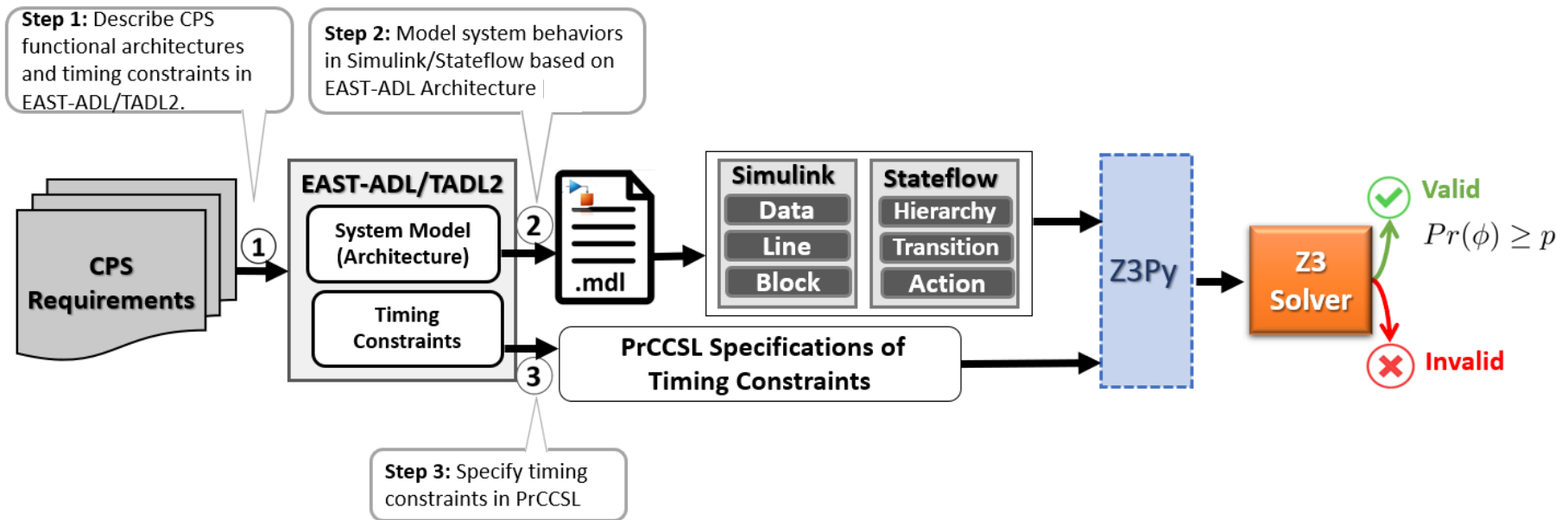
- Most of CPS are weakly-hard real-time systems, i.e., timing constraints **violations** can be **tolerated** if their **frequencies** are bounded.



Research Question

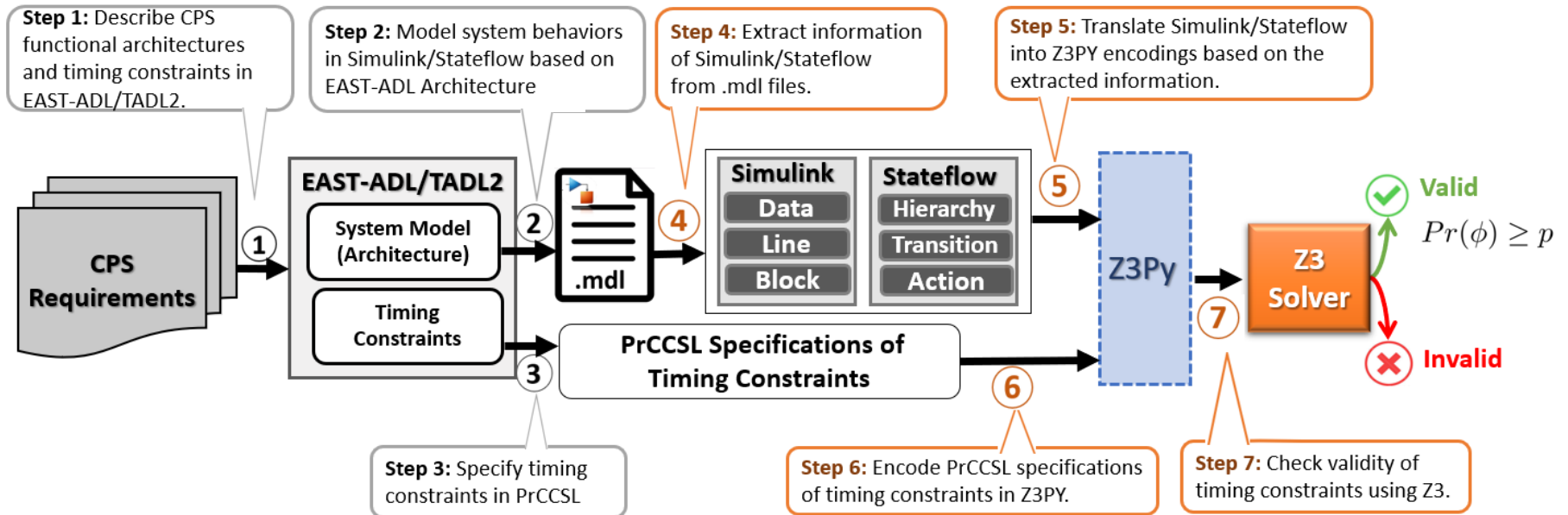
How to formally specify and verify timing constraints of
weakly-hard CPS with **stochastic** behaviors?

Approach



- [1] Eun-Young Kang and Li Huang. "Probabilistic Analysis of Timing Constraints in Autonomous Automotive Systems using Simulink Design Verifier." In *International Symposium on Dependable Software Engineering Theories, Tools and Applications (SETTA)*, pp. 170-186, Springer, 2018.
- [2] Eun-Young Kang, Dongrui Mu, and Li Huang. "Probabilistic Verification of Timing Constraints in Automotive Systems using UPPAAL-SMC." In *International Conference on Integrated Formal Methods (IFM)*, pp. 236-254, Springer, 2018.
- [3] Eun-Young Kang, Li Huang, and Dongrui Mu. "Formal Verification of Energy and Timed Requirements for a Cooperative Automotive System." In *Symposium On Applied Computing in Software Engineering (SAC)*, pp. 1492-1499, ACM, 2018.
- [4] Eun-Young Kang, Dongrui Mu, Li Huang, and Qianqing Lan. "Verification and Validation of a Cyber-Physical System in the Automotive Domain." In *International Conference on Software Quality, Reliability and Security (QRS)*, pp. 326-333, IEEE, 2017.

Approach



Experiments: Verification of Timing Constraints using Z3 Solver

Case studies: Cooperative Automotive System (CAS) and Autonomous Vehicle (AV)

Probability Threshold: 95%

Simulation Bound: 6000 Steps

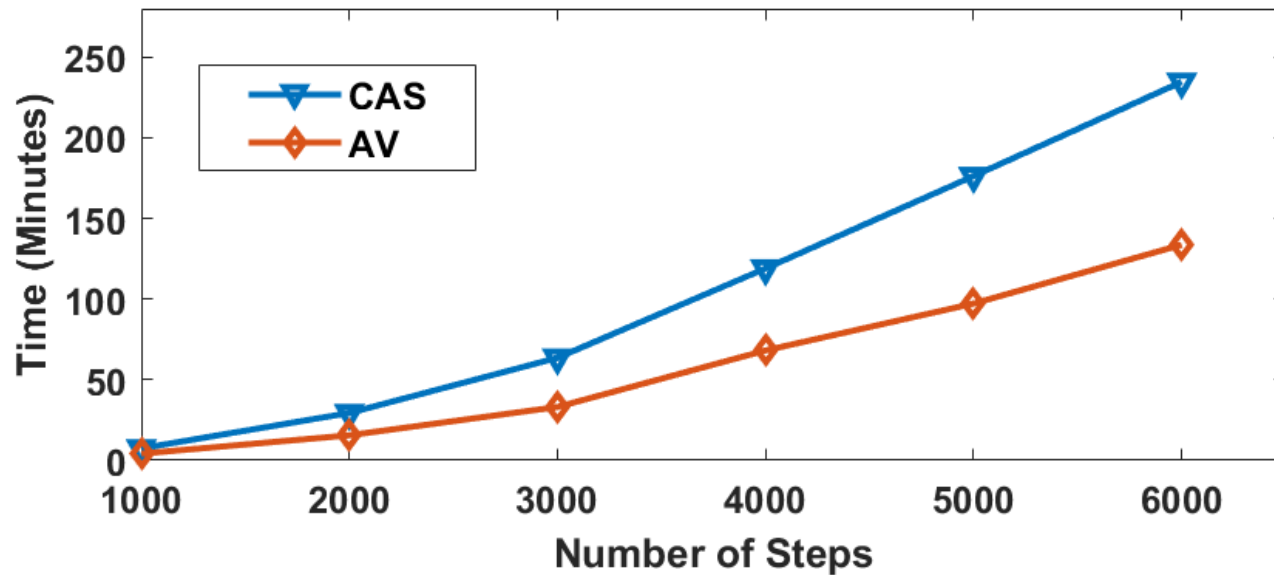


Fig. 1. Average analysis time for verifying ETC in Z3. The simulation bound (number of steps) ranges from 1000 to 6000 with increment as 1000.

On-going & Future work

- **Translation** of Simulink/Stateflow model of physical plant: **continuous dynamic** behaviors, **stochastic** behaviors.
- **Integration** of Z3PY encodings of **continuous** physical plant and **discrete** controller.
- **Development** of a fully automatic verification tool chain.

Thank You