Methods and Tools for Verification of Cyber-Physical Systems

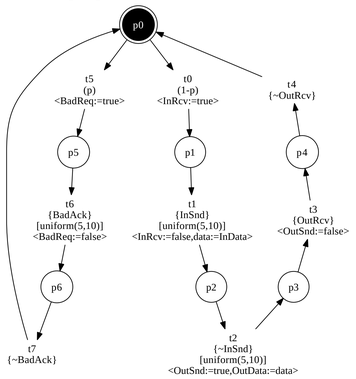
Chris Myers[1], Jian Wu[1], Zhen Zhang[1]
Hao Zheng[2], Yingying Zhang[2], Ping Hou[2]
[1]University of Utah
[2]University of South Florida

Introduction

- *Cyber-Physical Systems* (CPS) are deployed in a wide variety of safety critical applications from avionics, medical, and automotive domains.
- For these applications, it is essential to create a precise specification and formally verify that the implementation behaves as specified.
- The formal verification of these systems presents a wide variety of challenges.
- Models of these systems must represent the physical world, analog sensors and actuators, computer hardware and software, networks, and feedback control.
- These models must deal with the fact that correctness may depend on timing, concurrency, system dynamics, and stochastic behavior.

Unified Modeling Formalism

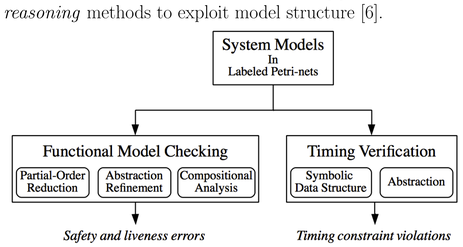
- Our research project has developed a general unified hybrid system modeling formalism that is capable of representing continuous and discrete dynamics, timing, and stochastic behavior [2].
- These models must unify elements normally described in a variety of formalisms such as:
  - Hardware description languages such as VHDL/VHDL-AMS/SystemVerilog used for hardware.
  - Continuous modeling languages such as SPICE and Simulink used for analog circuits and the physical environment.
  - Programming languages such as C for software.
  - System level modeling languages such as SystemC for complete systems.
- To achieve these goals, the *labeled Petri net* (LPN) model has been developed as well as techniques to generate them from various languages and simulation data.



LPN model for a faulty buffer.

Improving Verification Capacity

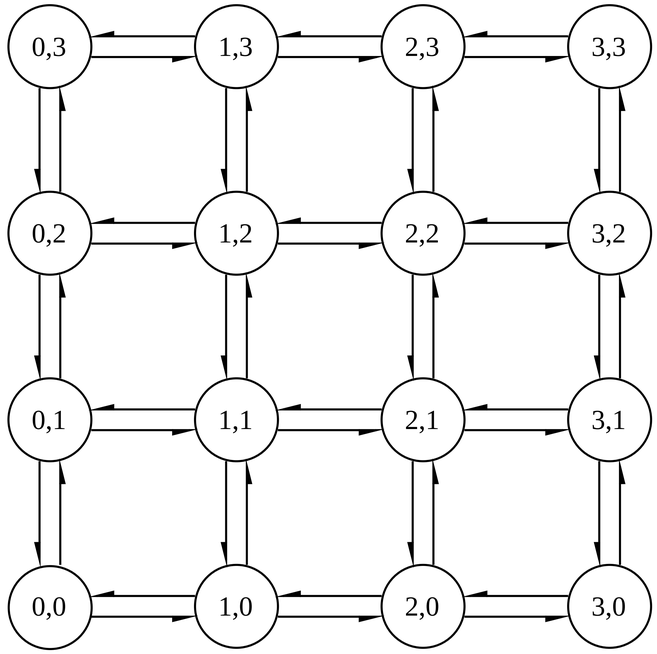
- The complexity of CPS models makes the formal verification of them extremely difficult.
- To address this, it is essential to develop more scalable verification methods.
- In particular, we have developed:
  - Automated model *abstraction* methods to reduce model complexity [1, 3].
  - *Partial order reduction* methods to address model concurrency [4].
  - *Symbolic methods* to utilize efficient data representations [5].
  - *Compositional reasoning* methods to exploit model structure [6].



Details for our verification methodology.

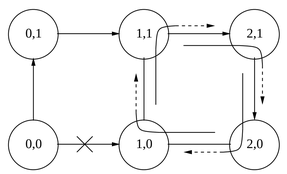
Motivating Example

- Now possible to integrate multiple cores on a single chip forming a *network-on-chip* (NoC).
- In automotive electronic systems, there are often more than 50 *electronic control units* (ECUs) to operate everything from the entertainment system to the anti-lock breaks.
- Each ECU is statically tied to specific sensors and actuators so processing power cannot be shared, and an ECU failure causes a malfunction in the corresponding sensor/actuator.
- An NoC approach makes mapping between ECUs and sensors/actuators flexible allowing for sharing of processing power and enabling fault tolerance by having spare units.
- Prof. Yoneda (NII/Tokyo) and his colleagues are designing such an NoC of ECUs.

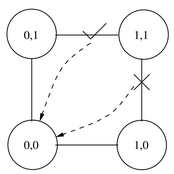


A 4x4 NoC routing mesh of automotive ECUs.

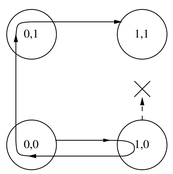
- An NoC routing protocol must be carefully designed to avoid deadlock and be fault-tolerant while still achieving latency and throughput goals.
- Glass/Ni propose restricting the allowed "turns" in order to guarantee absence of deadlock and that a packet can always be routed around a single failed router.
- If faults occur on the links, the Glass/Ni protocol can experience deadlock and a single link failure can cause a packet to not be routable.



Deadlock problem



Fault forwarding

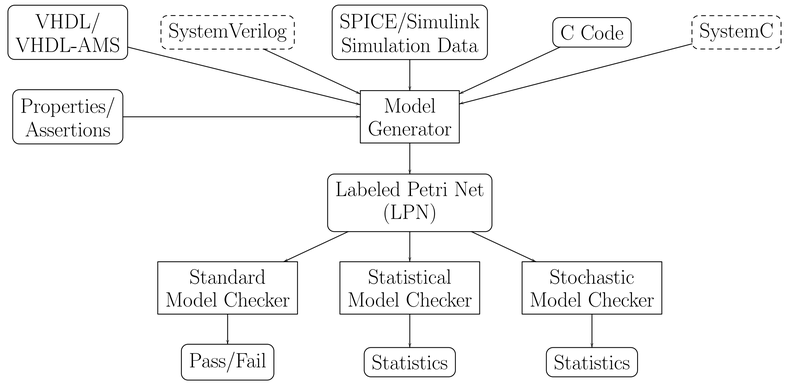


Our new protocol

- Yoneda et al. proposed a modified version of the protocol which forwards fault information, but this method still cannot consider link failures on the south and west edges of the grid.
- Our new routing protocol allows illegal "turns" without blocking on them, resulting in both deadlock freedom and a guarantee to avoid any single link failure without extra fault forwarding hardware.

LEMA Verification Tool

- CPS systems such as this NoC router design are complex, and various aspects must be verified.
- Complicated by the need to reason about concurrent, timing, and stochastic behavior.
- Developing `LEMA`, a verification tool for CPS.
- This tool must be able to verify numerous things including:
  - Functional properties such as the protocol does not deadlock, and the circuit implementation is free of hazards.
  - Timing properties such as meeting a required response time.
  - Stochastic properties such as the probability of a packet being lost.
- A prototype version of `LEMA` for Windows, Linux, and MacOS is available from our website.



LEMA tool flow.

Conclusion

- The verification methods proposed will enable the design and implementation of cyber-physical systems with higher reliability and fault tolerance.
- Since such systems are becoming ubiquitous, these improvements should have tremendous impact.
- The abstraction and hierarchical approaches will allow large systems to be analyzed and verified in a unified framework efficiently, thus improving confidence in the final products.
- Should allow design margins to be reduced, improving performance and reducing cost.
- Please see: `http://www.async.ece.utah.edu/CPS-Project/`

References

[1] R. Thacker, K. Jones, C. Myers, and H. Zheng. Automatic abstraction for verification of cyber-physical systems. In *The 1st ACM/IEEE International Conference on Cyber-Physical Systems*, April 2010.

[2] R. Thacker, C. Myers, K. Jones, and S. Little. A new verification method for embedded systems. In *The 27th IEEE International Conference on Computer Design*, October 2009.

[3] H. Yao, H. Zheng, and C. Myers. State space reductions for scalable verification of asynchronous designs. In *2010 IEEE Int. High Level Design Validation and Test Workshop*, November 2010.

[4] Y. Zhang, E. Rodriguez, H. Zheng, and C. Myers. An improvement in partial order reduction using behavioral analysis. In *IEEE Computer Society Annual Symp. on VLSI*, August 2012.

[5] H. Zheng, A. Price, and C. Myers. Using decision diagrams to compactly represent state space for explicit model checking. In *2012 IEEE Int. High Level Design Validation and Test Workshop*, November 2012.

[6] H. Zheng, E. Rodriguez, Y. Zhang, and C. Myers. A compositional minimization approach for large asynchronous design verification. In *19th Int. SPIN Workshop on Model Checking of Software*, July 2012.