Introduction
- CPS include complex computing and networking architectures that must tolerate soft and hard errors.
- Our project is developing a unified modeling formalism that includes both discrete and continuous signals updated both synchronously and asynchronously.
- Must verify functional and timing correctness in the face of the inherently stochastic nature of CPS.
- Abstraction, partial order reduction, and compositional reasoning are key to achieve the scalability required to reason about such complicated systems.

Motivating Example
- Note 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 feasible allowing for sharing of processing power and enabling fault tolerance by having spare units.
- Prof. Yonezawa (NI/Tokyo) and his colleagues are designing such an NoC of ECUs.

LEMA Verification Tool
- CPS systems such as this NoC router design are complex, and various aspects must be verified.
- Traced procedures 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.

Unified Modeling Formalism
- In order to reason about CPS, a unified modeling formalism is necessary that integrates both discrete and continuous signals that have synchronous and asynchronous as well as stochastic behavior.
- 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.

Verifying Stochastic Properties
- Developing both statistical and stochastic model checking approaches.
- Statistical model checking employs stochastic simulation.
- Model the links as having a fault probability and attempt to find the probability that a packet is able to be routed.

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.aync.ece.utah.edu/CPG-Project/