NSF National Workshop on Transportation CPS
Session IV: Model-Based Design, Verification and Validation
Breakout 3: Formal Methods
Moderator: Dan Work (UIUC) dbwork@illinois.edu
Scribe: Tom Fuhrman (GM) thomas.e.fuhrman@gm.com

Challenges

- What formalisms / semantics are appropriate for both cyber (discrete) and physical (continuous) systems and their interactions?
  - Hybrid automata, linear and non-linear
  - Protocols vs. data processing
- What degree of fidelity is needed in formal models (which are abstractions of reality) to proof properties of interest?
- How to conquer the state explosion problem (scalability to problems of industrial complexity)?
- How do we define requirements / specifications against which we are verifying? How do we know that they are themselves correct and complete? What are the assumptions?
- Inclusion of time
- "Robustify" formal methods with respect to uncertainties (physical system, human / social behaviors, environment)
- How to handle partial visibility of a system, incomplete measurements

Potential Research Strategies / Solutions

- Mix simulation and formal methods
  - Simulation-guided formal methods
  - Formal-directed simulation
  - Monte Carlo simulation
  - Simulate some components / layers, formally verify others
- **Probabilistic or statistical / stochastic methods, or based on empirical data, data analytics**
- Abstraction techniques – solve a simpler problem
  - Bring formal methods earlier in the process
- Synchronization within time bounds
- **Compositional reasoning: Decompose based on structure of the system**
  - Layering, guarantee services of one layer at a time
  - Integration of individually-verified components
  - Assume – guarantee reasoning
  - Use different methods / tools for each component / layer of the system
- Taxonomy of classes of systems and appropriate verification approaches for each – and their composition
- Formal methods for security, malicious attacks
- Benchmarks for CPS, challenge problems
- Restrict engineering implementations to what we can model
- Guarantee or formally verify the formal tools themselves

Impacts if Research is Successful

-

Other Related Research Questions

-