Breakout Session: Challenges for Formal System Design and Analysis using Hybrid Automata Tools

Chair: Stanley Bak AFRL/RITA

This session will focus on existing challenges for system design (including synthesis) and analysis using hybrid automata and associated tools. Initial questions to begin the discussion include:

- Have you used reachability or other hybrid systems tools? What was your experience? What was stopped you from going further? Was anything lacking in these tools?

- What types of systems require reasoning about both software and hardware aspects? What are some example properties you would be interested in proving about these systems (how expressive of a specification language is necessary)?

- Are there remaining challenges with low-dimensional problems? Clearly, large models require tools that scale to a large number of variables. Are there also interesting problems for models with 1-4 variables? What are these challenges?

- Which features are fundamental to problems faced by reachability, such that they should have first-class support inside the tool? For example, time-triggered dynamics, pure discrete variables, urgent transitions, differential inclusions, more complex (discrete) data structures, networked automata support, others?

- What are the strengths and weaknesses of tools based on SMT solving (dReach, HySat) versus flow-pipe construction methods (SpaceEx, Flow*, HyCreate)?

- Is there a fair way to compare different reachability tools and methods? What would such a comparison look like?

- Is the hard part of reachability computation the continuous successors, or the discrete successors? What are the challenges in each?

- If you have used some of the tools, what was your process of parameter tuning? Could this process be automated, and what would automation require to be programmatically available?

- Have you used falsification tools (tools which try to find counter-example traces)? What are the most-pressing challenges with these methods?