RQIC-7

AFRL CALL FOR RESEARCH

1. **Research Title:** Counter-Example Generation for Cyber-Physical Systems Verification
2. **Individual Sponsor:**

Dr. Stanley Bak
AFRL/RQQA Bldg 146, Room 300
2210 Eighth Street
WPAFB, OH 45433-7542
stanley.bak.1@us.af.mil

3. **Academic Area/Field and Education Level:** Computer Science, Electrical Engineering, Computer Engineering, Control Theory, Formal Methods, Applied Mathematics. MS or Ph.D Level

4. **Objectives:** Develop a counter-example generation framework for cyber-physical systems (CPS), where computer systems interact with the physical world. The counter-example generation problem, also called falsification, attempts to generate concrete counterexamples which violate formal specifications.

5. **Description:** Develop a counter-example generation framework for cyber-physical systems (CPS), where computer systems interact with the physical world. The counter-example generation problem, also called falsification, attempts to generate concrete counterexamples which violate formal specifications. The hybrid automaton formalism will be used to specify models of CPS, where system behavior is described as a combination of a finite state machine and discrete updates (software), along with differential equations (physical world interactions). Formal properties are given as invariants over the state variables, and the initial set of states is a set of states. Simulations can be used to explore specific behaviors of a hybrid automaton. Monte-Carlo simulation, thus, is one possible falsification method.

However, due to the large state space and various sources of non-determinism, exhaustive simulation is not possible. Thus, falsification methods try to guide simulations towards regions where violations are more likely to occur. Such strategies can be coupled with state-space exploration (reachability) techniques which reason over sets of states, and construct guarantees over approximations of the (possibly infinite) set of possible simulations.

The framework will be integrated into the existing Hyst tool, which can parse and interpret models of hybrid automata specified in the SpaceEx (a tool for hybrid systems reachability) input format. A comparison can be done versus plain Monte-Carlo simulation, as well as other falsification tools like S-TaLiRo, or recent results using branch and bound search strategies. Metrics (how close is the current state to a violation) can be developed and analyzed for guiding the search for counter-examples. Finally, exploring parallelization inside falsification frameworks could be investigated to provide further speedups.

6. **Research Classification/Restrictions:** This research falls under the 6.1 basic research classification and as such has no restrictions. No citizenship restrictions.

7. Eligible Research Institutions:

■ **DAGSI** (Wright State University, AFIT, Ohio State University, University of Dayton, Miami University, Ohio University, University of Cincinnati). Note: Public Release Pending

■ **AFIT** (only)

■ **USAFA** (only)

If you are submitting a topic for the USAFA, indicate if you are also interested in sponsoring a USAF Cadet in summer 2015 (Average cost for USAF Cadet for 33 days is $5000)

■ Yes ☐ No

Public Release Pending