Verification of Complex Cyber-Physical Systems

A Collaborative Proposal by

Carnegie Mellon University, Smart Information Flow Technology, and Newcastle University

Objective:

This project will combine and extend our statistical model checking and hybrid systems decision procedures to enable verification of complex, realistic cyber-physical systems.

Approach:

We will develop a general *concolic* (combined concrete and symbolic) verification framework for cyber-physical systems, by bringing together simulation-based techniques (statistical model checking) and efficient symbolic decision procedures. As our recent work has shown, statistical model checking (SMC) is an effective and scalable verification technique. However, SMC is incomplete when it is used on hybrid systems, because of the undecidability of reasoning involving real numbers. In separate research on numerical methods for complex hybrid systems, we have shown that solving an appropriate relaxation of the (undecidable) verification problem for nonlinear systems enables us to reason about hybrid systems featuring realistic nonlinear dynamics. The main disadvantage of this technique is its high complexity. A concolic testing framework would combine, complement, and extend the strengths of the statistical and numerical techniques, leading to new approaches for verifying cyber-physical systems. Our new methods will be implemented in the SILVER tool, supporting testing, evaluation, and application to verification of real-world systems.

Outcome/Impact:

The proposed research lies at the forefront of verification technologies for cyber-physical systems. Currently, it is impossible to verify behaviors of complex hybrid (discrete-continuous) systems, involving non-linear continuous dynamics. Our new system, SILVER, will provide a game-changer technique, enabling a quantum leap in our verification capabilities. Cyber-physical systems, involving digital control of systems with continuous dynamics (such as warships, aircraft, cars, reactors, etc.), pervade the modern environment. Assuring correct behavior of such systems is a critical requirement for their development, certification, fielding, and maintenance.