CAREER: Towards Reliability Assurance for Cyber-Physical Systems Via Fair Model Repair for Multi-tolerance

Overview. Cyber-Physical Systems (CPS) deployed in safety- and security-critical application domains such as transportation, manufacturing, and smart health must satisfy strict requirements on reliability. Recent studies explore formal methods to provide rigorous assurance of reliability requirements to CPS. Unfortunately, existing methods only focus on assuring a particular class of property for individual CPS components at one time. In contrast, heterogeneous cyber and physical components in a CPS may impose a divergent or even contradicting set of constraints and goals, such as assuring consistent functionality of physical actuators while guaranteeing fail-stop of software controller in the presence of faults and attacks. This CAREER project proposes a holistic approach to investigating formal assurance to repair CPS design models to meet multi-class reliability properties **simultaneously**, named FARMER, Formal Repair for Assuring Multiple Reliability in Cyber-Physical System Designs. The project's impacts are in (1) exploring new theoretical insights and developing new technologies to enforce the reliability of CPS under diverse and dynamic environment and (2) strengthening STEM education, workforce readiness and encouraging minority participation for CPS engineering in the Michigan region and nationally.

Keywords— Formal Methods, Model Repair, Reliability, Adversarial Environment, Multi-tolerance

Intellectual Merit. The intellectual merit of this project lies in investigating the multi-class reliability of complex CPS via theoretical analysis, algorithm design, and the development of practical tools and framework. In particular, the key research proposed in this project is three-fold.

(1) This project will investigate the computational complexity of automated addition of multi-class reliability assurance (referred to as the **MRA** problem in this proposal) to CPS designs. CPS faults of heterogeneous software and hardware components will be modeled based on a unified representation of *transition* systems in cyber and physical space. Then, PI will employ temporal logics such as *hyperproperties* to model the specification of the MRA problem. The fault models will be further integrated with the MRA specification, enabling theoretical complexity analysis using formal language and problem reduction. (2) This project will investigate efficient algorithms and heuristics for analysing and assuring different class of the MRA problem of CPS designs respectively. First, this project will develop model checking heuristics to analyze the feasibility of the MRA problem for given CPS. The PI will integrate efficient partition of formal CPS model with algorithms that transform deterministic and probabilistic verification problems, enabling scalable analysis of complex CPS in the presence of state explosion. Second, This project will develop sound and complete algorithms for automatic assurance of the MRA requirements to CPS models that are in P. For certain MRA problems that are harder, such as NP-complete, polynomial-time heuristics will be developed. This project will also investigate tradeoff of assuring such MRA problems to account for potentially diverging or contradicting reliability requirements of different CPS components. (3) *FARMER* will integrate the above formal models and algorithms into a unified framework to simplify the design, synthesis and analyzing of Cyber-Physical Systems (CPS) for developers and operators. The applicability of *FARMER* will be evaluated through applications provided by collaborators from Boston General Hospital and Yale Medical School.

Broader Impacts (1)The results will advance the understanding and assurance of reliability properties in CPS design and support researchers to revisit existing reliable patterns for CPS design to adapt the future environment. (2) The developed research platform and artifacts will close the gap between advanced research and education in CPS. As a female faculty advisor of both Women in Computing club at OU and Michigan Aspiration in Computing committee, the PI will make this project appealing to youth in Michigan who self-identify as women, genderqueer or non-binary.