

Thesis Proposal

Behavioral Robustness of Software System Designs



Changjian Zhang

Thesis Committee:

Dr. Eunsuk Kang (Co-chair)

Dr. David Garlan (Co-chair)

Dr. Jonathan Aldrich

Dr. Sebastian Uchitel

Abstract:

Software systems are designed and implemented with assumptions about the environment. However, once a system is deployed, the actual environment may deviate from its expected behavior, potentially leading to violations of desired properties. Ideally, a system should be robust to continue establishing its most critical requirements even in the presence of possible deviations in the environment. To enable systematic design of robust systems against environmental deviations, this work proposes a rigorous behavioral notion of robustness for software systems. Then, it presents a technique called behavioral robustification, which involves two tactics to systematically and rigorously improve the robustness of a system design against potential deviations.

Specifically, the robustness of a system is defined as the largest set of deviating environmental behavior under which the system is capable of guaranteeing a desired property. Then, we present an approach to compute robustness based on this definition. On the other hand, the system is not robust against an environment when the environment exhibits deviations causing a violation of the desired property. The robustification method finds a re-design that is capable of satisfying the property under such a deviated environment. In particular, two tactics, namely wrapper and specification weakening, are introduced. We show that how the robustification problem can be formulated as a multi-objective optimization problem with the goal of guaranteeing the desired property, while maximizing the amount of existing functionality and minimizing the cost of changes to the original design.

The proposed robustness computation and robustification methods are implemented in a tool, named Fortis. The applicability and efficiency of these approaches are evaluated through experimental results across five case studies, including a radiation therapy machine, an electronic voting machine, network protocols, a transportation fare system, and an infusion pump machine.

Date: April 10th, 2024

Time: 1:00 – 3:00 pm

Location: TCS 360