Abstract

Cyber-physical systems have penetrated almost every application domain in the modern world - from kitchen appliances to automotive as well as avionics control. Due to their safety-critical nature, the reliability guarantee offered by such systems is of utmost importance. This thesis explores the application of formal methods as an alternative to traditional reliability analysis via rigorous testing in the context of the cyber-physical systems. The primary contributions of this thesis can be summarised as follows.

- This thesis proposes a C-like specification framework which can capture the behavioral description of an embedded application and formally analyze its overall reliability based on the reliability of the underlying components. Given multiple reliability options for underlying components, this thesis has also proposed suitable design space exploration methods for reliable system synthesis.

- This thesis examines the problem of lifetime reliability estimation of cyber-physical systems from a high-level behavioral model point of view based on their component usage while factoring in active and passive reliability decay rates. Further, this thesis also proposes reliability-aware online scheduling strategies for sporadic task-sets to mitigate the effect of transient faults in heterogeneous distributed embedded systems.

- This thesis proposes tools and frameworks for formally verifying the reliability guarantee offered by control software implementations in the face of transient sensor errors caused by environmental disturbances. The methodologies developed has also been suitably adapted for verification of performance guarantee provided by fault tolerant controllers designed to mitigate intermittent faults affecting the underlying hardware platform.

- Given reliability and security targets, this thesis proposes suitable design space exploration methods leveraging standard fault mitigation techniques and existing security hardening techniques to aid in reliable and secure cyber-physical system design on heterogeneous multicore platforms. This thesis has also explored reliability, security trade-offs in the design of secure cyber-physical systems to propose lightweight security alternatives against stealthy false data injection attacks.

We believe that the approaches outlined in this thesis would be helpful in the context of next-generation synthesis and verification tool development for embedded and cyber-physical systems.
Keywords:*Reliability, Formal Verification, Cyber-physical Systems*