Title: Markov Model Guided Online Testing for Mission Critical Applications.

Abstract:
Mission Critical Systems (MCS) are systems whose failure might cause catastrophic consequences - someone dying, damage to property, financial losses. Typically, the examples of MCS are in avionics, medical life support systems, autonomous vehicles, etc. There are famous examples of MCS failures such as TheracTwentyFive (radiation therapy machine) malfunctioning resulted in fatal overdoses, Patriot missile failure led to over 100 casualties, Mars Climate Orbiter crash costed 327.6 million USD. Such failures, when evolving in their early phases often expose just as insignificant deviations of MCS characteristics that are difficult to observe and detect. Timely detection and compensation of failure causes could avoid their further progression to catastrophic ones. Since the system degradation process can emerge possibly under rare circumstances and pass several phases, their detection needs not only passive monitoring but active interaction that drives the system into an observable error state. On the other hand, any test interaction with MCS during its operation must not interfere the mission accomplishment. Such requirements pose strict constraints to tests' durations as well as their timing. This talk is about a novel approach to online model-based testing of MCS applications with the goal to identify system reliability mode under strict timing constraints. The test hypothesis are selected based on the Markov model of the MCS reliability modes. For each mode behavior a test pattern is formally specified as a test case against which the system behavior is checked. Finally, the test cases serialization strategy that satisfies given timing and priority constraints is synthesized. The theoretical results are illustrated with a system-on-chip routing system use case.