Abstraction and Verification of Properties of a Real-Time Java

Martin Strecker

IRIT-ACADIE, Paul Sabatier University, Toulouse, France
martin.strecker@irit.fr
http://www.irit.fr/~Martin.Strecker/

Abstract: The talk will give an overview of ongoing work on verification of concurrent real-time Java programs. Uncontrolled access to shared objects by concurrently executing threads may lead to data incoherencies. We propose to annotate program sections of Java threads with temporal information indicating their activation times. We map this information to Timed Automata (TA) and can then verify by model checking whether the considered program may display resource access conflicts. In our talk, we will describe this approach and present first steps towards a formal verification of the soundness of this abstraction, by modeling the semantics of the formalisms (Java and TA) in a proof assistant.

Keywords. Formal verification, concurrent Java program, data incoherence, Timed Automata, resource access conflict, semantics, proof assistant.

Key Terms. FormalMethod, VerificationProcess, MathematicalModel, Methodology.