Foreword

Hybrid Systems are notoriously hard to analyze and verify. So far, techniques based on either explicit or implicit state reachability have failed to scale with the size of such systems. Statistical Model Checking may prove useful, but sacrifices absolute certainty about the correctness of the answer obtained. In both cases, numerical error may change the truth-value of the result from False to True or vice versa. An alternative is to use a combination of decision procedures for real arithmetic and interactive theorem proving. Andre Platzer's Ph.D. thesis explores this alternative approach in great depth. He proposes a logic called Differential Dynamic Logic for specifying properties of Hybrid Systems, investigates the meta-theory of the logic, and gives inference rules for it. He has developed an extremely impressive graphical interface for the resulting tool KeYmaera, which is based on the KeY Prover for verifying Java programs, developed at the University of Karlsruhe, Chalmers, and Koblenz. Particularly noteworthy are the use of Differential Invariants for reasoning about complex Hybrid Systems and the examples that he is able to do: "The European Train Control System" and a curved flight roundabout maneuver for aircraft collision avoidance. Both examples are beyond the scope of current Hybrid System Model Checking tools. I believe that his verification tool is unique – there is no other one like it. I heartily recommend his book and theorem prover for those who need to verify complex cyber-physical systems.

Pittsburgh, February 2010 *Edmund M. Clarke*