

User-Interfaces for Hybrid Systems: Analysis and Design Through Hybrid Reachability

Meeko Oishi

Hybrid Systems Lab, Stanford University, Stanford, CA

`moishi@stanford.edu`

Hybrid systems combine discrete mode dynamics, which model mode-logic, and continuous state dynamics, which model the physical processes themselves. Human interaction with hybrid systems involves the user, the automation’s discrete mode-logic, and the underlying continuous dynamics of the physical system. A human interacting with a hybrid system is often presented, through information displays, with a simplified representation of the underlying system. This user-interface should not overwhelm the user with unnecessary information, and thus usually contains only a subset of information about the true system model. Yet if the interface is properly designed, it represents an abstraction of the true system which the human is able to use to safely interact with the system.

In safety-critical systems, correct and succinct interfaces are paramount: interfaces must provide adequate information and must not confuse the user. Such interfaces will have properties of “immediate observability”, in which the current state can be reconstructed from the information displayed as well as the last occurring event. We present an abstraction method which generates a discrete event system that can be used to analyze, verify, or design user-interfaces for hybrid human-automation systems.

The basis for the abstraction method is the computation of the hybrid reachable set – this is the largest region of the state-space in which we can guarantee that the system will always remain. We denote this the “safe region of operation”, and guarantee its invariance by implementing a specific controller, computed using the reachable set, on its boundary. Using the computed invariant regions as discrete modes, we create a discrete event system which is unambiguous with respect to the safety properties of the hybrid system. This abstraction, along with the formulation of an interface model as a discrete event system, allows the use of discrete techniques for interface analysis, including existing interface verification and design methods.

The methodology is applied to a system for which safety is paramount: the autopilot of a large civil jet aircraft during an automatic landing/go-around maneuver.