Hybrid Systems—And Everything Else*

John Rushby

Computer Science Laboratory,
SRI International,
333 Ravenswood Avenue,
Menlo Park, CA 94025, USA

Abstract. Hybrid systems are at the core of most embedded and many other kinds of systems; formal methods for analysis of hybrid systems have made remarkable progress in the last decade and thus provide a strong foundation for assurance in the system core.

But there are many systems issues that interact with the hybrid systems core and complicate the overall system design and its assurance case. These include real time and fault tolerance, interaction with human operators, and the relationship between verification and certification.

For example, fault tolerance demands multiple redundant sensors, which are themselves prone to faults and inaccuracy, and whose precision degrades as real time progresses from the moment when the sample was taken to that when it is used. Fault tolerance generally also requires multiple independent channels of computation and this raises issues of their synchronization and coordination.

There are two broad classes of methods for dealing with these combined issues: one uses architectural means to separate them, so we can reason separately about hybrid control and fault tolerance, for example; the other integrates them, so that a single method is used to reason, for example, about real time and fault tolerance. I describe some of these methods and sketch some topics for further research.

In the larger systems context, the embedded core may be managed by a planning and execution system that uses AI techniques, and/or by a human operator. Both of these may have an imperfect model of the system and incomplete knowledge of its internal state. I outline these topics and some of the interesting research opportunities therein.

Finally, many of the systems we consider have the potential to do harm, and thus raise concern for informal or regulated certification. I outline recent developments in this area and their connection to verification.

The rich relationship between hybrid systems and everything else suggests a need to reason cooperatively across multiple domains. I sketch a proposal for “an evidential tool bus” to facilitate this.

* This work was supported by SRI International.