High-Level Modeling and Analysis of an Air-Traffic Management System*

Nancy Lynch

MIT Laboratory for Computer Science, Cambridge, MA 02139, USA
lynch@theory.lcs.mit.edu

Abstract. This talk describes progress in a current project on modeling and analyzing the TCAS II aircraft collision-avoidance system.
The state of the art in formal methods applied to air traffic management systems involves specifying software behavior in detail, using formalisms such as Statecharts. Although such methods are precise, they do not help much in understanding the systems intuitively; nor do they enable analysis of high-level global requirements, such as "Under condition A, the planes will not crash."
To aid people in understanding such systems, and to enable such analysis, we advocate defining high-level mathematical models for the system, including not only the control software, but also the airplanes, sensors, and pilots—that is, high-level hybrid system models.
In a current demonstration project at MIT and Berkeley, we have defined abstract models for the key system components of the new TCAS II (version 7) system. These are based formally on the Hybrid I/O Automaton (HIOA) model [1]. We are using these models to formulate and prove theorems about the behavior of the system under particular assumptions. Our results are intended only as illustrations—the models provide a foundation for study of a wide range of properties of the system's behavior. We hope that this project will help to produce improved validation methods for air-traffic management systems.

References

1. N.A. Lynch, R. Segala, F.W. Vaandrager, and H.B. Weinberg. Hybrid I/O automata. In R. Alur, T.A. Henzinger, and E.D. Sontag, editors, *Hybrid Systems III*, volume 1066 of *Lecture Notes in Computer Science*, pages 496–510. Springer-Verlag, 1996.

* Based on joint work with Carl Livadas and John Lygeros.

F.W. Vaandrager and J.H. van Schuppen (Eds.): HSCC'99, LNCS 1569, pp. 3–3, 1999.