Formal Methods for Critical Systems

Steven P. Miller

Rockwell Collins, USA

Abstract. Formal methods have traditionally been reserved for systems with requirements for extremely high assurance. However, the growing popularity of model-based development, in which models of system behavior are created early in the development process and used to autogenerate code, are making precise, mathematical specifications much more common in industry. At the same time, formal verification tools such as model checkers continue to grow more powerful. The convergence of these two trends opens the door for the practical application of formal verification techniques early in the life cycle for many systems. This talk will describe how Rockwell Collins has applied both theorem proving and model checking to commercial avionics and security systems to reduce costs and improve quality.

D. Cofer and A. Fantechi (Eds.): FMICS 2008, LNCS 5596, p. 1, 2009.