Model checking safety-critical systems specified as X- machines

George Eleftherakis and Petros Kefalas

Computer Science Department, City Liberal Studies.
Affiliated College of the University of Sheffield
13 Tsiraiski Str., 54624 Thessaloniki, Greece
{ eleftherakis, kefalas }@ city.academic.gr

Abstract

Misleading user requirements, inappropriate specification and errors in the implementation of a system, are the usual reasons responsible for the creation of non-safe systems. The use of formal methods in the development of safety critical systems is demonstrated in the past. In this paper a formal technique is proposed in order to assist software engineers to find mistakes in the specification of the system, thus providing the ability to prove that certain desired properties exist in the final product. It is argued that the X-machine as a specification tool combined with the proposed model checking verification technique, gives the ability to the software engineer to formally and intuitively specify a system and then automatically check if this model has all the desired properties. Since complete testing of X-Machine specifications has been demonstrated elsewhere, integration of these techniques built around X-Machine theory leads towards an integrated framework for system development, ranging from validity of model properties to implementation correctness. The proposed ideas in this paper are illustrated through an example describing the specification of a medical safety-critical system.