Formal Modeling of Safety Requirements in the Model-Driven Development of Safety Critical Embedded Systems

Safety requirements are a very important artifact in the development of safety critical embedded systems. They are usually identified during safety analyses and are used by experts as a basis for the correct selection and implementation of safety mechanisms. Various safety analysis research groups have worked on formal modeling of safety requirements with the goal of determining if a system can meet these requirements. In this abstract, we propose the application of formal models of safety requirements throughout all development phases of a model-driven development process. The safety requirements identified during safety analysis can be used to automatically generate appropriate mechanisms in the code generation phase and to verify the suitability of these mechanisms in the verification phase. By establishing safety requirements as a formal basis of all process phases, a consistent development process can be achieved.

Stichworte:
- embedded, ftos

Kongress-/Buchtitel:
- Proceedings of the Eighth European Dependable Computing Conference (EDCC 2010)

Jahr:
- 2010

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Informatik > Lehrstühle der Informatik > Informatik 6 - Lehrstuhl für Echtzeitsysteme und Robotik (Prof. Knoll) > 2010