Abstract:

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 this 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, flos