Project VerSyKo

Verifikation von Systemen synchroner Software-Komponenten

Verification of Systems With Synchronous Components

Summary. The goal of VerSyKo is the development of a general and universal approach to modeling and verification of the software of distributed safety critical embedded systems; an approach that is innovative for the industrial practice and addresses the scalability problem. Such safety-critical systems must adhere to very high quality requirements concerning safety, reliability and availability. Hence, a very high effort has to be put into verification, validation and certification. The project focuses on the model based development and analysis of asynchronously communicating embedded control systems that are composed from components that operate synchronously. This system paradigm is known as GALS (*globally asynchronous - locally synchronous*) architecture. For synchronous controllers the model based development approach of SCADE is an attractive solution, which provides code generation, (formal) verification and test automation. Also for asynchronous systems there are several different modeling formalisms with good tool support (e.g. PROMELA / SPIN, UPPAAL, or UML2/Enterprise Architect). In VerSyKo we close the methodological gap between synchronous component systems and asynchronous system of systems through domain specific modeling formalisms. The main emphasis is upon modeling and specification (with and without explicit consideration of real time and stochastic aspects pertaining random component failures), verification, validation and test. To evaluate all methods, languages and tools that we develop we use case studies from the railway, avionics and automotive domain provided by the industrial partners. The project results show that our methods of model based testing and formal verification using bounded model checking are very well applicable to industry relevant GALS systems. Consequently, the developed tools and methods are now used by the industrial partners in their productive customer projects.