Name der/ des Kandidatin/ Kandidaten: Juan Martin, Perez Cerrolaza (0627534)

Name der Prüfer/innen:

O.Univ.Prof. Dr.phil. Dr.h.c. Hermann Kopetz

Prof. Eugenio Villar

Titel des Dissertation: “Executable Time-Triggered Model (E-TTM) for the development of safety-critical embedded systems”

Länge (ca. 250 Wörter):

This thesis addresses the complexity management problem in the development of safety-critical embedded systems, defining an executable PIM (Platform Independent Model) modeling approach for the design of TTA (Time-Triggered Architecture) based safety critical systems. This approach supports the following properties/features: time and value domain determinism, period-phase conserving simulation and strategies to tackle the complexity challenge.

The Executable Time-Triggered Model (E-TTM) approach is based on the time-triggered Model-Of-Computation (MoC) and can be used from the early stages of a development process, in order to develop time-triggered executable specifications and PIM models. The E-TTM meta-model has been implemented as a C++ library that extends SystemC, and enables the codesign and execution of models in SystemC.

Distributed models can be defined and connected using physical communication channels such as Ethernet and Time-Triggered Ethernet (TTE). In the simulation of periodic control applications, simulation time period and phase relationships are kept constant but independently configurable, enabling the simulation of models to be executed faster, slower or at the same pace as the physical time (in a similar way as a video-recorder might be played faster) but always producing the same results at the same simulation time instants.

The E-TTM modeling approach is assessed in the modeling of two case study systems: an example industrial real-time control system and a safety-critical railway odometry system. In both cases, executable models enable early dependability assessments where the distributed execution of models can be used to reduce the overall simulation time and as reference models for the design and verification of subsystems. The E-TTM modeling approach can also be combined with Software Fault Injection (SFI).