Travel Report from “Architectural Paradigms for Dependable Embedded Systems” Summer School in Baden/Vienna

Viacheslav Izosimov
Linköpings universitet, IDA
viaiz@ida.liu.se
25th October 2005

Vienna University of Technology in a framework of the DECOS project hosted a summer school on “*Architectural Paradigms for Dependable Embedded Systems*” from 12th to 16th September. The summer school was organized in Baden, a satellite town of Vienna. The head of the summer school, Prof. *Hermann Kopetz* from Vienna University of Technology, invited many interesting speakers from industry and academia. The school was supposed to facilitate contacts among participants, especially between academia and industry that are historically separated in Europe. More than 100 participants across the Europe, U.S., and Japan clubbed together.

The school started with the speech by *Hermann Kopetz*, who presented challenges in designing dependable embedded systems and emphasized importance of a systematic approach, implemented, for example, in the Time-Triggered Architecture (TTA). Hermann’s talk was followed by *Hans-Georg Frischkorn*, Senior Vice President System Architecture and Integration at BMW, who introduced modern automotive design principles and concepts. *Peter Bishop*, Chief Scientist at Adelard, UK, pointed out on human factors in designing dependable systems and warned that ignoring such problems as “drunk driver” due to one or another reason results in unacceptably low levels of safety. Among other very good presentations, I want to especially distinguish the talks by *William H. Sanders* (Professor at University of Illinois at Urbana Champaign), *David Powell* (Directeur de Recherche CNRS at LAAS, France), *Pascal Traverse* (Head of Safety & Reliability Development at Airbus, France), and *Kevin Driscoll* (Fellow at Honeywell, USA).

David Powell’s presentation was especially interesting for me and many participants. Usually embedded systems are designed to achieve levels of reliability not more than 10^{-9}. However, if designers should design systems with the level of 10^{-14} such as railway systems, then interesting problems arise. Designers have to overcome their consciousness, which is usually between 10^{-4} and 10^{-6}, and start asking “what if?” for everything. Pascal’s and Kevin’s presentations were a sort of contradicting and, at the same time, complementing each other. Pascal presented Airbus A380 architecture and how certification requirements by Airworthiness Authorities were considered during its design. Kevin discussed design of airborne applications from designers’ point of view. It is essential to do as much as you can, think thoroughly before doing anything when designing such safety-critical applications. William H. Sanders presented probability analysis based on Markov chains, programs for analyzing complex systems such as satellites, airplanes, how to use various distributions to describe fault behavior.

Vienna and Baden were excellent places to host the summer school. Cultural activities were the most interesting for me. I went to a classic music concert in Baden and to the Wiener Staatsopera.