Tutorial 5

Architecting Dependable Systems: Preventing and Tolerating Faults

Rogerio de Lemos
University of Kent, UK

Cristina Gacek
Newcastle University, UK

The aim of this tutorial is to provide an insight on how the structuring of software systems at the architectural level is fundamental for the development of dependable systems. Taking as a basis the different dependability means, the intention is to show how dependability should be considered at the architectural level, and the impact this should have when developing dependable systems. The main objectives of this tutorial are the following:

- to establish the major principles associated with software architectures and dependability that are relevant when reasoning about faults at the architectural level;
- to introduce and discuss existing approaches for architecting dependable systems, particularly, in the context of fault prevention and tolerance;
- to identify the main challenges that lie ahead when considering the structuring of dependable systems at the architectural level.

At the end of the tutorial, the participants should have a better appreciation of the challenges, problems and solutions that are currently associated with the structuring of dependable systems at the architectural level. These should include methods, techniques, and tools that are relevant in the context of dependability means, mainly, rigorous design, and fault tolerance. The material of the tutorial will be presented in the context of several case studies, including, embedded and service oriented systems, and we will be using UML2.0, ACME, and AADL description languages to support our examples.

About the speakers

Rogerio de Lemos is a Lecturer in Computing Science at the University of Kent (UK). Before joining the Computing Laboratory at the University of Kent he was a Senior Research Associate at the Centre for Software Reliability (CSR) at the University of Newcastle upon Tyne (UK). He has participated in several conference PCs, including HASE 2001 and HASE 2002; FMRTFT 2002; EDCC-4, EDCC-6 and EDCC-7; ISADS 2003; WICSA 2005, WICSA 2007, and WICSA 2008; LADC 2005; ICSE 2006 Emerging Results Track; SRDS 2006; and ICDCS 2006; and the PC co-chair of LADC

2003. Until recently, he was a member of the Steering Committee of LADC, and he is on the editorial board of the Journal of Hybrid Systems. He gave a tutorial at SCTF 1997 on safety analysis of critical software, and tutorials at LADC 2005 and ICSE 2006, DSN 2007, LADC 2007 on software architectures for dependable systems. He has co-edited four books and a journal special issue on Architecting Dependable Systems.

Cristina Gacek is a Lecturer at the School of Computing Science of the Newcastle University (UK). She has extensive work experience both as a researcher and as a practitioner. She received a Ph.D. in Computer Science from the University of Southern California (USC - USA), where she worked as a research assistant. Dr. Cristina Gacek was the leader of the Software Architectures group at the Fraunhofer Institute for Experimental Software Engineering (IESE), and worked both for TRW (USA) and IBM Brasil. She has participated in several conference program committees, was the program committee chair for ICSR-7, and has co-organized many workshops, including several on Architecting Dependable Systems. She has given a tutorial on software architectures for product lines at ICSR-6 and on software architectures for dependable systems at DSN 2007. Cristina is an IEEE and ACM member and has several scientific publications. She is a co-editor of four books and a journal special issue on Architecting Dependable Systems.