Preservation of Extra-Functional Properties in Embedded Systems Development

Mehrdad Saadatmand
Preservation of Extra-Functional Properties in Embedded Systems Development

Mehrdad Saadatmand

Abstract

The interaction of embedded systems with their environments and their resource limitations make it important to take into account properties such as timing, security, and resource consumption in designing such systems. These so-called Extra-Functional Properties (EFPs) capture and describe the quality and characteristics of a system, and they need to be taken into account from early phases of development and throughout the system’s lifecycle. An important challenge in this context is to ensure that the EFPs that are defined at early design phases are actually preserved throughout design phases as well as during the execution of the system on its platform.

In this thesis, we provide solutions to help with the preservation of EFPs: targeting both system design phases and system execution on the platform. Starting from requirements, we form the constraints of EFPs, we propose an approach for modeling Non-Functional Requirements (NFRs) and evaluating different requirements against respect to the satisfaction of the NFRs. Considering the relationship and trade-off among EFPs, an approach for balancing timing versus security properties is introduced. Our approach enables balancing in two ways: in a static way resulting in a fixed set of components in the design model, and in a dynamic way during the execution of the system through runtime adaptation. Considering the role of the platform in preservation of EFPs and mitigating possible violations of them, an approach is suggested to enrich the platform with necessary mechanisms to enable monitoring and enforcement of timing properties. In the thesis, we also identify and demonstrate the issues related to accuracy in monitoring EFPs, how accuracy can affect the decisions that are made based on the collected information, and propose a technique to tackle this problem.

As another contribution, we also show how runtime monitoring information collected about EFPs can be used to fine-tune design models until a desired set of EFPs are achieved. We have also developed a testing framework which enables automatic generation of test cases in order verify the actual behavior of a system against its desired behavior.

On a high level, the contributions of the thesis are thus twofold: proposing methods and techniques to improve maintenance of EFPs within their correct range of values during system design, and identifying and mitigating possible violations of EFPs at runtime.

List of Publications

Publications Included in the Thesis

- **Model-Based Trade-off Analysis of Non-Functional Requirements**: An Automated UML-Based Approach. Mehrdad Saadatmand, Antonio Cicchetti, Mikael Sjödin. The Sixth International Conference on Software Engineering Advances (ICSEA), Barcelona, Spain, October, 2011.

Other Relevant Publications

Licentiate Thesis


Conferences & Workshops

- **Mapping of State Machines to Code: Potentials and Challenges**: Mehrdad Saadatmand. The Ninth International Conference on Software Engineering Advances (ICSEA), Nice, France, October, 2014.
- **Runtime Verification of State Machines and Defect Localization Applying Model-Based Testing**: Mehrdad Saadatmand, Detlef Scholle, Cheuk Wing Leung, Sebastian Ulbrich, Joanna Fredriksson Larson. First Workshop on Software Architecture Erosion and Architectural Consistency (SAEroCon) (ACM) (Co-located with WICSA 2014), Sydney, Australia, April, 2014.
- **Runtime Verification of State Machines and Defect Localization Applying Model-Based Testing**: Mehrdad Saadatmand, Detlef Scholle, Cheuk Weng Leung, Sebastian Ulbrich, Joanna Fredriksson Larson. First Workshop on Software Architecture Erosion and Architectural Consistency (SAEroCon) (ACM) (Co-located with WICSA 2014), Sydney, Australia, April, 2014.

Advisors

- Model-Based Engineering of Embedded Systems

The Model-Based Engineering of Embedded Systems research group led by Prof. Mikael Sjödin focuses on development of methods and tools for model-based engineering of embedded systems; including topics such as new methods for architectural and behavioral design of systems, and system requirements, techniques for analyzing and transforming models, and runtime architectures for resource-efficient predictable embedded systems.
The ITS-EASY post graduate school for Embedded Software and Systems

ITS-EASY is an industrial research school in Embedded Software and Systems, affiliated with the School of Innovation, Design and Engineering (IDT) at Mälardalen University (MDH) as an integrated part of the MDH strategic research area Embedded Systems (ES).

ITS-EASY is funded by the Knowledge Foundation (KKS), and the eleven participating companies. ITS-EASY started October 1st 2011, and will continue until September 30th 2020. During that period the PhD students will complete their studies and obtain the doctoral degree in Computer Science.

ITS-EASY is a large organization: it counts 22 PhD students, 14 main advisors from IDT, 18 co-advisors from IDT and the partner companies, and more than 25 associated members; senior researchers and industrial specialists. The board, led by Helena Malmqvist, ABB, has six members, and the industrial committee where all participating companies are represented, has 11 members. The management team of the research school consists of four members. All in all, about 85 persons are directly engaged in ITS-EASY.

www.mrtc.mdh.se/projects/itseasy

Board
Helena Malmqvist, Chair of the board and Head of the External Research Collaboration, ABB AB Corporate Research
Antonia Bertolino, Leader of the Software Engineering Research Laboratory at ISTI, Istituto di Scienza e Tecnologie dell’Informazione
Hans Hansson, Professor of Real-Time Systems, Mälardalen University
Kristina Forsberg, Technical specialist at Electronic Defence Systems at SAAB AB
Rikard Mäki, Director Technology Planning and Public Funding, Volvo Construction Equipment
Claes Wohlin, Professor of software engineering, Blekinge Institute of Technology

Industrial Committee
ABB: Peter Löfgren
Addiva: Dag Lindahl
Alten: Detlef Scholle
Bombardier: Christer Persson
Effective Change: Stig Larsson
Ericsson: Sigrid Eldh
Etteplan: Johan Sundell
Hök Instrument: Bertil Hök
MotionControl: Christer Gerdtman
SICS: Markus Bohlin
VOLVO CE: Peter Wallin

Management Team
Director: Prof. Kristina Lundqvist
Communications manager: Malin Rosqvist
Finance manager: Gunnar Widforss
School coordinator: Radu Dobrin