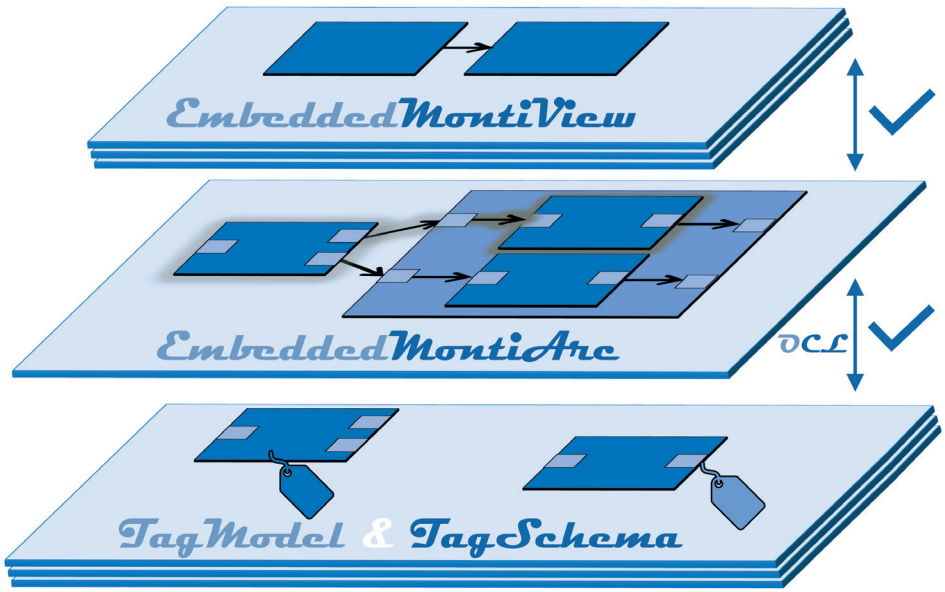
SE | RWTH AACHEN UNIVERSITY

Michael von Wenckstern

Verification of Structural and Extra-Functional Properties in Component and Connector Models for Embedded and Cyber-Physical Systems



Aachener Informatik-Berichte,
Software Engineering

Band 44

Hrsg: Prof. Dr. rer. nat. Bernhard Rumpe

Verification of Structural and Extra-Functional Properties in Component and Connector Models for Embedded and Cyber-Physical Systems

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Dipl.-Math. Michael von Wenckstern
aus Karl-Marx-Stadt

Berichter: Universitätsprofessor Dr. rer. nat. Bernhard Rumpe
University Professor Shahar Maoz, PhD

Tag der mündlichen Prüfung: 31.10.2019

Aachener Informatik-Berichte, Software Engineering

herausgegeben von
Prof. Dr. rer. nat. Bernhard Rumpe
Software Engineering
RWTH Aachen University

Band 44

Michael von Wenckstern
RWTH Aachen University

Verification of Structural and Extra-Functional Properties in Component and Connector Models for Embedded and Cyber-Physical Systems

Shaker Verlag
Düren 2020

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: D 82 (Diss. RWTH Aachen University, 2019)

Printed in Germany.

ISBN 978-3-8440-7239-6
ISSN 1869-9170

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

The industry area of embedded and cyber-physical systems is one of the largest and it influences our daily life. The global embedded systems marked was valued at about 160 billion US dollar in 2015 and it is getting up to 225 billion US dollar by end of 2021 [Zio17]. Example domains of embedded and cyber-physical systems are: automotive [DHJ+08], avionics [FLV03], robotics [WICE03], railway [DNCH10], production industry [EWSG94], telecommunication [ZSM11], healthcare [ERA09], defense [BNP+04], and consumer electronics [VOVDLKM00].

Model-based engineering, esp. component and connector (C&C) models to describe logical architectures, are one common approach to handle the large complexity of embedded and cyber-physical systems [FR07, MBNJ09, OMG15, EJL+03]. Components encapsulate software features; the hierarchical decomposition of components enables formulating logical architectures in a top-down approach. Connectors in C&C models describe the information exchange via typed ports; they model black-box communication between software features.

The current development of complex C&C-based embedded systems in industry mostly involves the following steps [BMR+17a, DGH+19]: (1) formulating functional and extra-functional requirements as text in *IBM Rational DOORS*; (2) creating a design model of the software architecture including its environment interactions in *SysML*; (3) developing a complete functional/logical model to simulate the embedded system in *Simulink*; and (4) system implementation based on available hardware in C/C++ satisfying all extra-functional properties.

This current development process has the following disadvantages [KBFS12, HKK+18, BMR+17a]: (a) *SysML* models do not follow a formalized approach; i.e., engineers may interpret these models differently due to missing semantics; (b) the check between the informal *SysML* architecture design against the *Simulink* model is done manually, and thus, error-prone and very time-consuming; (c) refactoring of *Simulink* models (e.g., dividing a subsystem) needs manual effort in updating the design model, and therefore, due to timing constraints this step is often skipped resulting in inconsistencies; and (d) most tools do not support a generic approach for different extra-functional property kinds, and thus, extra-functional properties are mostly modeled as comments or stereotypes and consistencies between these properties are checked manually.

This thesis aims to improve the software development process of large and complex C&C models for embedded and cyber-physical systems by providing model-based methodologies to develop, understand, validate and maintain these C&C models. Concrete, this thesis presents concepts to support the embedded software engineer with: (i) automatic consistency checks of C&C models; (ii) automatic verification of logical C&C models against their design decisions; (iii) automatic addition of traceability links between design and implementation models; (iv) finding structural inconsistencies during model evolution; (v) providing a flexible framework to define different extra-functional property types; (vi) presenting an *OCL* framework to specify (company-specific) constraints about structural or extra-functional properties for C&C models; and (vii) generation of positive or negative witnesses to explain why a C&C model satisfies or violates its extra-functional or structural constraints or its design decisions.

Prototype implementations of above mentioned concepts and an industrial case study in cooperation with Daimler AG show promising results in improving the model-based development process of embedded and cyber-physical systems in industry.

Acknowledgments

Special thanks goes to my doctor father Prof. Dr. Bernhard Rumpe for giving me the opportunity to research in the area of model-driven software engineering and for providing many connections to other research groups and industrial partners; participating in several research and automotive industry projects gave me access to many different views on this research topic. Furthermore, I want to express great laud to Prof. Dr. Bernhard Rumpe for the fruitful discussions, ideas and feedback rounds - especially during the 3-day long research workshops - on this thesis.

I would like to thank Prof. Shahar Maoz for being the second reporter of this thesis. Additionally, I want to express gratitude to Prof. Shahar Maoz, Dr. Jan Oliver Ringert, and Prof. Dr. Bernhard Rumpe for the successful teamwork on the GIF research project I-1235-407.6/2014, for the published papers together, and for the time together in Tel Aviv and in Aachen. I also want to thank the Deutsche Forschungsgemeinschaft (DFG) for funding this research and thus supporting this thesis.

Moreover, I would like to thank Prof. Dr. Stefan Kowalewski for heading my PhD exam committee, and Prof. Dr. Erika Ábrahám for being part of this committee.

In addition, my thank goes to Prof. Dr. Manfred Nagl for many interesting discussions about computer science, GI, and architecture.

“If everyone is moving forward together, then success takes care of itself.” - Henry Ford about teamwork. Therefore, special thanks goes to Evgeny Kusmenko; together we developed the EmbeddedMontiArc modeling family and had good times on several conferences and workshops presenting our papers. Moreover, I want to thank Dr. Pedram Mir Seyed Nazari for the interesting discussions about language engineering and digitalization; for the first level MontiCore support thanks goes to Pedram, Marita Breuer, and Galina Volkova. Additionally, I want to thank Dr. Alexander Roth, Dr. Christoph Schulz, and Vincent Bertram for the many papers we wrote together. I want to thank Deni Raco for organizing all the extra activities such as poker, or soccer events on our chair.

I also would like to thank the students whose bachelor or master theses supported my research significantly; without them the large evaluation part would not be possible. Thanks goes to “Web(Assembly) expert” Jean-Marc Ronck, “OCL specialist” Ferdinand Mehlan, “C++ generator enthusiast” Sascha Schneiders, and “tooling and gaming fan” Malte Heithoff for supporting me more than two years.

I want to extend my thanks to the other students: Luca Tabone, Stefan Brunecker, Alexander Kogaj, Nicolai Strodthoff, Severin Tolksdorf, Vladimir Parashin, David Ernst, Christian Bajana, Igor Shumeiko, Dinh-An Ho, Fabian Kahlert, Manuel Schrick, Ievgen Strepkov, Ahmet Tayfun Özen, and all seminar and lab students.

Special thanks for reviewing this PhD thesis goes to Sebastian von Wenckstern, Pedram Mir Seyed Nazari, Evgeny Kusmenko, Kai Adam, Simon Varga, and Oliver Kautz.

Furthermore, I would like to thank all colleges of the Software Engineering chair for the nice time together: Lennart Bucher, Arvid Butting, Manuela Dalibor, Anabel Derlam, Florian Donath, Imke Drave, Robert Eikermann, Dr. Timo Greifenberg, Sylvia Gunder, Dr. Arne Haber, Dr. Lars Hermerschmidt, Dr. Christoph Herrmann, Gabriele Heuschen, Steffen Hillemacher, Dr. Katrin Hölldobler, Carsten Kolassa, Thomas Kurpick, Achim Lindt, Dr. Markus Look, Matthias

Markthaler, Dr. Judith Michael, Dr. Klaus Müller, Sonja Müßigbrodt, Lukas Netz, Jerome Pfeiffer, Nina Pichler, Dimitri Plotnikov, Manuel Putzer, Dr. Dirk Reiß, David Schmalzing, Stephanie Schrader, Brian Sinkovec, Max Voß, Louis Wachtmeister, and Dr. Andreas Wortmann.

My largest thanks goes to my family - Bettina, Bodo, and Sebastian von Wenckstern - who supported me all these years; and their belief that education is the best investment for my future.

Aschaffenburg, 13.12.2019
Michael von Wenckstern

Contents