

MoDeVVa'17

Model Driven Engineering, Verification and Validation
Integrating Verification and Validation in MDE

Ernesto Posse[◦], Daniel Ratiu⁺, Gehan M. K. Selim[•], Faiez Zalila^{*}

[◦]Zeligsoft, Canada eposse@zeligsoft.com

⁺Siemens, Germany daniel.ratiu@siemens.com

[•]McMaster University, Canada seling@mcmaster.ca

^{*}Inria, France faiez.zalila@inria.fr

Abstract—Models are purposeful abstractions of systems and their environments. They can be used to understand, simulate, and validate complex systems at different abstraction levels. Thus, the use of models is of increasing importance for industrial applications. Model-Driven Engineering (MDE) is a development methodology that is based on models, metamodels, and model transformations. The shift from code-centric software development to model-centric software development in MDE opens up promising opportunities for the verification and validation (V&V) of software. On the other hand, the growing complexity of models and model transformations requires efficient V&V techniques in the context of MDE.

The workshop on Model Driven Engineering, Verification and Validation (MoDeVVa) offers a forum for researchers and practitioners who are working on V&V and MDE. The main goals of the workshop are to identify, investigate, and discuss mutual impacts of MDE and V&V.

For the 2017 edition of the MoDeVVa workshop, we put an emphasis on combining heterogeneous (possibly incomplete) V&V techniques of MDE artifacts, and using their combined verification results to increase the confidence in the V&V process. We have compared the used techniques with respect to different criteria (e.g., time efficiency, memory usage, soundness, completeness, user-friendliness).

Keywords: Model-Driven Engineering (MDE), models, meta-models, model transformations, verification and validation (V&V).

I. INTRODUCTION

The fourteenth Workshop on Model Driven Engineering, Verification and Validation (MoDeVVa) co-located with the twentieth International Conference on Model Driven Engineering Languages and Systems (MODELS) was held in Austin, TX, USA, in September 2017. The objective of MoDeVVa is to offer a forum for researchers and practitioners who are working on verification and validation (V&V) and/or Model-Driven Engineering (MDE).

Each year, MoDeVVa invites outstanding researchers from both MDE and V&V to present their work. For MoDeVVa'2017 edition, two keynote speakers were invited. Prof. Marc Pantel from the University of Toulouse, France, gave a talk entitled "Property driven approaches to formal verification for domain specific modeling languages". Also Dr. Kirstie L. Bellman, from Topcy House Consulting gave a talk entitled

"Building Self-aware Systems for Continual Self-Testing and Development".

The call for papers of MoDeVVa'2017 attracted 9 submissions covering both MDE and V&V activities. These papers range on a wide spectrum covering fundamental contributions, applications and tool development and improvements. Each paper was reviewed by at least three reviewers and the program committee accepted 6 papers. We congratulate the authors of these 6 papers and thank all authors who submitted articles to MoDeVVa'2017. The research papers presented at MoDeVVa'2017 covered research topics in the areas of:

- The integration of V&V approaches into MDE.
- The definition of V&V approaches that rely on MDE.
- Modeling the rules for combining sub-models in order to improve compositionality.
- Modeling conformance relations for checking the refinement of models.
- Modeling transformations between models used for design and models used for V&V.
- Incremental V&V (reuse as many V&V results as possible after a change in a model).
- The application of the above topics to MDE itself (V&V of meta-models, models and model transformations).
- Continuous V&V of models.
- V&V of models and modeling tools (e.g. generators) for safety critical systems using models to increase practicality of formal verification.
- Experience reports.

II. WORKSHOP CONTENTS

The MoDeVVa'2017 featured two keynotes and six papers as briefly described in the following.

A. Keynotes

a) *Keynote 1:* The first keynote of MoDeVVa'17, *Building Self-aware Systems for Continual Self-Testing and Development*, was given by Dr. Kristie Bellman. During the talk, Dr. Bellman presented the challenges to continual testing and verification of self-aware systems. Dr. Bellman discussed the roles of models in such self-aware systems and how a self-aware system can perform continual monitoring and testing

of its models and other components. As an example, she described the CARS robotic cars testbed that was used to study the development of self-aware systems that can partly develop and correct their own models.

b) *Keynote 2*: The second keynote of MoDeVva'17, *Property Driven Approaches to Formal Verification for Domain Specific Modeling Languages*, was given by Prof. Marc Pantel from the University of Toulouse. During this keynote Prof. Pantel advocated the use of languages or tools dedicated to specific kind of properties in order to translate automatically design models to verification models whose automated verification scales better than the one of generic approaches.

B. Technical Papers

The first paper, entitled "Modular transformation from AF3 to nuXmv" [1] presents an approach to modularize and reuse bi-directional model-to-model transformations between AF3 models and the input language of the nuXmv model checker. Parts of the forward transformations are reused when the counterexamples provided by nuXmv are lifted into AF3.

The second paper, entitled "Supporting Model Refinement with Equivalence Checking in the Context of Model-Driven Engineering with UML-RT" [3] proposes a framework to provide a formal approach to check the refinement relation between two models expressed with UML-RT. The checking was performed via a translation of the UML-RT models into the LNT formal language and then checking the equivalence by using the CADP formal verification tool.

The third paper, entitled "Modeling Frames" [4] is focused on the contexts for modeling activities. Modeling frames capture the implicit knowledge and assumptions made during the modeling process, which help assessing the quality of the result of a modeling activity. It also provides information about the context in which a modeling artifact is valid and can be reused.

The fourth paper is entitled "Architecture-Driven Reduction of Specification Overhead for Verifying Confidentiality in Component-Based Software Systems" [6]. It presents a model-driven approach that facilitates the creation and maintenance of confidentiality specifications for the verification of component-based software.

The fifth paper is entitled "Adding Random Operations to OCL" [5]. This paper presents an extension of OCL to allow modellers to deal with random numbers and probability distributions in their OCL specifications. It shows its implementation in the tool USE and discusses some advantages of this new feature for the validation and verification of models.

The sixth paper is entitled "Hierarchical Model Exploration for Exposing Off-Nominal Behaviors" [2]. It presents a model-driven requirements analysis approach that reduces state and rule explosion problems using a hierarchical model exploration strategy, and its empirical results with the pacemaker requirements.

REFERENCES

- [1] KANAV, S., AND ARAVANTINOS, V. Modular transformation from AF3 to nuxmv. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).
- [2] KAUSHIK MADALA, H. D., AND ACEITUNA, D. Hierarchical model exploration for exposing off-nominal behaviors. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).
- [3] OLIVEIRA, R., AND DINGEL, J. Supporting model refinement with equivalence checking in the context of model-driven engineering with UML-RT. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).
- [4] STEFAN KLIKOVITS, JOACHIM DENIL, A. M., AND SALAY, R. Modeling frames. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).
- [5] VALLECILLO, A., AND GOGOLLA, M. Adding random operations to ocl. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).
- [6] YURCHENKO, K., BEHR, M., KLARE, H., KRAMER, M., AND REUSSNER, R. Architecture-driven reduction of specification overhead for verifying confidentiality in component-based software systems. In *Proceedings of the 14th Workshop on Model-Driven Engineering, Verification and Validation co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, Texas, USA, September, 2017.* (2017).