CHARLES UNIVERSITY PRAGUE

faculty of mathematics and physics

The Board of Doctoral Studies
Faculty of Mathematics and Physics
Charles University Prague
Ke Karlovu 3
12116 Prague 2

Prague, August 14th, 2014

Re: Jaroslav Keznikl, Doctoral Thesis – Advisor‘s Reference

The submitted PhD thesis concentrates on the task of engineering dynamic software architectures for Resilient Distributed Systems (RDS for short), i.e., large-scale distributed systems, often closely bound to the real world, that provide dependability despite operating in dynamic, open-ended, and unpredictable environments. The main challenge of this task stems from the fact that the properties of RDS (i.e., distribution on a large scale and open-endedness in particular) and their environments (i.e., recurrent dynamism and unpredictability) make the development of software architectures using the contemporary architecture models and abstractions problematic.

In this context, the thesis targets the following goals: (1) to propose architecture abstractions that are specifically tailored for building dynamic software architectures of RDS, (2) to complement these architecture abstractions with adequate design models and processes in order to support software architectures of RDS at design time, and (3) to elaborate the semantics of these architecture abstractions in a way that enables efficient implementation, execution, and analysis, including also an execution environment prototype.

With respect to the above goals, the major scientific contributions of the thesis lie in:

- The *DEECo component model* (Dependable Emergent Ensembles of Components), which brings novel architecture abstractions that are centered on the concept of component ensembles – dynamic, self-organizing groups of autonomous components. The architecture abstractions of DEECo are particularly tailored for building dynamic software architectures of RDS. The thesis also presents a rigorous computational model of DEECo.
- The *jDEECo execution environment prototype*, which maps the DEECo abstractions, their semantics, and the computational model to the Java programming language.
- The *Invariant Refinement Method* (IRM), which is a design method inspired by goal-oriented requirements elaboration that supports the DEECo abstractions at design time by governing a traceability between system requirements and DEECo-based architectures. Being formally grounded, IRM also enables design analysis and validation.

- The *ARCAS method* (Automated Resolution of Connector Architectures using Constraint Solving), which targets open-ended design and automated synthesis of dependable software connectors for heterogeneous and dynamic component deployments with emergent component bindings, as is the case of DEECo. ARCAS is based on structuring the connectors as hierarchical composites of reusable connector elements and their automated composition via constraint solving.
- A formalization of the DEECo operational semantics and an evaluation of the potential for formal verification of DEECo-based systems via model checking.
- An evaluation of the architecture abstractions of DEECo in terms of a DEECo-based architecture of a RDS that targets adaptive application deployment in ad-hoc cloud systems. The thesis further refers to case studies under a non-disclosure agreement that are centered on cooperative vehicle navigation (proposed by Volkswagen AG). The evaluation has sown that the DEECo architecture abstractions, accompanied by the related techniques for architecture design and analysis, effectively address the challenges of building large-scale, open-ended, and highly dynamic architectures for RDS.

As to the contents, the thesis starts with an overview with identification of goals and challenges (Chapter 1) and an extensive discussion of the state-of-the-art approaches in the areas of software architecture abstractions, software architecture dynamism, and application of formal methods for specification and analysis of software architectures (Chapter 2). Then, the above contributions are presented in terms of a commented collection of co-authored publications (Chapter 3), which includes 6 publications (all of them published in at top-notch peer reviewed conferences and a journal with IF). The thesis is concluded with the author's vision of the promising research directions and open challenges stemming from the results of the thesis (Chapter 4).

During his PhD work, Jaroslav Keznikl has co-authored 16 peer-reviewed papers published at international conferences and workshops, as well as in a journal with impact factor. These include the Software and Systems Modeling journal (IF: 1.250), WICSA 2014 and 2012 (core A, proceedings by IEEE CS), ECSA 2014 (proceedings by Springer), CBSE 2013 (core A, proceedings by ACM), FACS 2013 (proceedings by Springer), ICPE 2013 and 2012 (proceedings by ACM). The thesis is based on 6 of these papers. The intermediate results of the thesis were applied in a number of research projects, most importantly the EU FP7 project ASCENS, several bilateral research projects of the department with Volkswagen AG, and the department research project DEECo.

In my view, Jaroslav Keznikl has proved the ability to make substantial, high-quality research contributions in the field of software engineering, especially in the area of distributed software architectures. The research was done systematically and according to sound scientific principles. With respect to all these facts, I strongly recommend to accept the thesis for defense and to grant a PhD degree to Jaroslav Keznikl.

Doc. RNDr. Tomáš Bureš, Ph.D.
Advisor