Attachment No. 11:

Habilitation thesis reviewer's report

Masaryk University Faculty	Faculty of Informatics
Field of study	Informatics
Applicant	Ing. RNDr. Barbora Bühnová, PhD
Unit	Department of Computer Systems and Communications
Habilitation thesis (title)	*Quality-Driven Architecture Design of Software Systems*
Reviewer	Univ.-Prof. Dr. Uwe Zdun
Unit	Universität Wien Research Group Software Architecture

Reviewer's report (extent of text up to the reviewer)

Software systems today are part of many aspects of our daily and business lives, including many critical and important processes. Software quality plays an ever increasing role, as more and more aspects of our daily and business lives are automated in and dependent on software. Software quality addresses how well the software conforms to a given design, based on functional requirements or specifications, and also meets its non-functional requirements. The sheer size and complexity of software systems today renders many traditional quality assessment techniques difficult to apply or makes them non-applicable. More recent approaches tackle the problem through divide-and-conquer strategies, focusing on specific quality aspects, for instance based on the software architecture, business processes, design models, or other system abstractions.

The thesis presented focuses on architecture-based quality modelling and assessment during the system development process. In the context of the system design, the thesis focuses on three different perspectives of quality-driven design of a software system: functional correctness and two major quality attributes: reliability and performance. Approaches for modelling and assessing the quality of a system design are provided, along with architecture-based design decision support and architecture design optimization.

The thesis consists of:
- a summary document, which explains contributions in 3 main areas: Software architecture models (with sub-areas: functionality, reliability, and performance), architecture quality assessment (with sub-areas: functionality, reliability, and performance), and design process (with sub-areas: design decision making and architecture optimization);
- a collection of articles: 6 journal articles, 1 book chapter, and 13 articles in conferences and workshop proceedings.

In the area of software architecture models, major contributions include the study of the applicability of the Component-Interaction automata notation, introduced in doctoral thesis of Dr. Bühnová, in the context of business and industrial systems. Basically, these contributions focus on modelling realistic component based systems using a labelled transition system notation. Particularly interesting are the critical assessment of modelling issues in this context,

studies of asynchronous communication, component instance handling, and modelling of exception handling of the internal persistent state of a component and the relation to the global shared state within the system.

A number of the contributions in the software architecture modelling area relate to software reliability analysis. A major contribution is considering the execution environment and usage profile modelling in software reliability analysis, and the subsequent reliability modelling and assessment for large-scale software systems. The Palladio Component Model, originally designed for performance modelling and prediction, was extended with such models, and tool support is provided for an automated transformation of the software system models into Markov chains. Space-effective evaluation of these chains is implemented using Eclipse/the Palladio tools. In addition, the approach was extended to support various commonly used fault-tolerance mechanisms at different abstraction levels, as well as reasoning support about the effect of various fault-tolerance mechanisms on the reliability. Because of certain specifics of embedded systems, Dr. Bühnová and her colleagues have further developed reliability models for embedded systems.

Other contributions in software architecture modelling relate to performance modelling for early performance assessment. Among others, the author studied the dependence of performance on a configuration, context, or history related state of the system. So called performance completions, introducing models of quality-relevant details into the system model using model transformations, were studied for possible conflicts among them. Further, a specific performance model for embedded systems (automotive systems) was studied.

Based on the modelling support, the second major contribution field of the thesis is quality assessment, i.e. to quantify the quality of a design alternative in comparison with alternative designs. With regard to the functionality, various correctness properties have been studied based on an extended version of action-based linear time logic LTL, called CI-LTL. Model checking tools have been used for verification purposes and reduction techniques have been devised, as a large portion of the model checking complexity can be abstracted away during verification. The complexity induced by a high number of component instances has been addressed by verification techniques for checking LTL-like interaction properties on the specific type of systems with a certain component occurring in many instances.

Again, for reliability assessment, the execution environment and usage profile have been considered. A reliability solver based on the Palladio tools has been devised. Sensitivity analysis has been introduced to study the software components that are strongly affecting system reliability. Techniques for user-defined reliability, such as that no critical and at most one non-critical fault occurs during system execution, have been proposed. Finally, reliability assessment techniques for embedded system contexts have been introduced.

Regarding performance, an extension to the Palladio approach, which enabled the author to experimentally evaluate the increase in performance prediction accuracy and model size costs associated with including state information in performance models, has been developed. The completion approach, mentioned above, contains a method that optimises the completion order, based on its validity and performance-relevant impact.

The final area of major contributions is design process support. Here, architecture decisions are of vital importance and can hence be supported using design decision making support. In this context, a number of rather specific contributions have been made. The reliability and

performance works mentioned above enabled the author to identify quality-critical model parameters and detect the parameters whose uncertainty needs to be reduced by further investigation to prevent the distortion of quality assessment results. Methods to detect model accuracy (as explained above) and model completions to make the models more precise have been studied. Model uncertainties can be revealed by the sensitivity analysis mentioned above and methods to model uncertainties are part of the contributions.

Finally, approaches for optimizing the solutions have been devised. As architects might face a huge number of design alternatives when searching for an optimal architecture design with respect to defined quality attributes and constraints, targeted optimization approaches can help. In particular, reliability optimization via deployment changes, performance/reliability/cost optimization via redundancy allocation changes, and reliability/energy consumption optimization via redundancy allocation changes are the main contributions in this area. Tool support in the ArcheOpterix framework has been developed.

In the thesis Dr. Bühnová has presented major research contributions in the area of quality-driven architecture design of software systems. The works significantly extend the state of the art in the area. The summary text provides the bigger picture, setting the individual research contributions into a larger context and research plan. A strength of this thesis is that all concepts have been fully developed with great care for detail. The presentation is clear and the thesis is well structured.

A substantial number of different research methods have been used, including formal methods, prototype development, case studies, and experimentation. The work has been applied to various different fields, including large enterprise systems, cloud-based applications, and automotive embedded systems. This breadth in the work and application fields is very important in my point of view.

Dr. Bühnová shows significant expertise in her research areas. She has the ability to bring across ideas from multiple sub-disciplines of software engineering in order to foster innovations and solve complex problems. She can transform theoretical ideas and concepts into realistic settings and realize and experiment with them in realistic settings. I like particularly the attempts to transforming foundational concepts into concepts applicable in real life/industry settings.

Regarding the creativity and originality of the research work I see a high level of creativity and originality, with a clear focus on possible practical applicability of the research results. That is, the major creative and original contribution is in finding scientific problems that are of real interest and applying novel ideas to address these problems, as well as showing the feasibility of these ideas.

Dr. Bühnová has achieved a significant number of publications in excellent academic conferences and journals, including a number of highly cited articles in IEEE Transactions on Software Engineering, ACM SIGSOFT Software Engineering Notes, Journal of Systems and Software, and QoSA to name but a few. I judge her academic output both in terms of quantity and quality as very good. I am fully convinced that she will continue to produce excellent outputs and accepting her habilitation would be a perfect next step. I think that she is ready and fully capable to develop his own research agenda.

Overall Dr. Bühnová's work gives me the impression of an active and successful researcher, who has already established a very good standing in the scientific communities in her area of research. I expect her to continue making excellent contributions in her field of research.

Reviewer's questions for the habilitation thesis defence (number of questions up to the reviewer):

- Arguably the three different perspectives of quality-driven design of a software system chosen in the thesis (functional correctness and the two major quality attributes: reliability and performance) are among the most easy to measure qualities of the system. A lot of often contradicting qualities, such as usability, interoperability, security, maintainability, reusability, and testability, to name but a few, are harder to assess.
  - What are the implications of the thesis results in relation to those other qualities?
  - How could they be integrated in the framework provided by the thesis?
- Architectural decision modelling is today a major approach for architectural knowledge management and relates to the thesis contributions on design decision making support.
  - How do the thesis contributions map in to current architectural decision modelling approaches?
  - How can the optimization approaches support architecture decision modelling approaches?
  - How are the relations of the thesis contributions to tactics, patterns, styles and other forms of reusable knowledge often used in architectural decision modelling?

Conclusion

The habilitation thesis submitted by Ing. RNDr. Barbora Bühnová, PhD entitled *Quality-Driven Architecture Design of Software Systems* **meets** the requirements applicable to habilitation theses in the field of Informatics.

In Vienna on 16 February 2017