Politecnico di Milano
Dipartimento di Elettronica e Informazione
Piazza Leonardo da Vinci, 32
20133 Milano, Italia

Prof. Carlo Ghezzi

tel. (+39) 02-2399-3529, fax (+39) 02-2399-3411
e-mail ghezzi@elet.polimi.it

Frantisek Plasil, Ph.D.
Professor and Chair
Department of Software Engineering
Charles University
Malostranske nam.25
11800 Prague 1, Czech Republic

7 August 2010

RE: Ondrej Sery's Doctoral Thesis

Dear Professor Frantisek:

In response to your request of 29 June 2010, I'm herewith providing an evaluation report on Ondrej Sery's Doctoral Thesis. I apologize for the late submission of my report.

The doctoral thesis focuses on automated software verification via model checking. It consists of four conference papers and a comprehensive commentary that provides an overall context and conceptual links across the contributions described in the papers. The candidate has also co-authored six other scientific publications, only tenuously related to the main topic of the dissertation. I understand that a doctoral thesis in your university may be in the form of a commented collection of published papers, and therefore I agree that the material supplied for assessment complies with the requirements. Regarding the value of the work, I would argue that it fully qualifies the candidate for receiving the doctoral degree. I will hereafter provide comments to substantiate my recommendation.

The topic of the thesis is important and timely. The initial commentary (of about 70 pages) provides a rather extensive and accurate overview of the state-of-the-art approaches and tools supporting code model checking. Sery's work focuses on the application of such techniques in practice. Indeed, most of the existing tools are unfortunately quite hard to assess, understand, and compare in their offered features. Their practical application is difficult. The main body of contribution of Sery's work consists of providing some answers to theses problems.

In his first paper, he proposed a behavior specification extension to the BLAST model checker that facilitates property specification, thereby making the tool more easily usable in practice. In the second, co-authored paper he provides an industrial case study in which he shows how the practical usage of BLAST was made difficult by BLAST's limitations. In the third, co-authored paper, he proposes a methodology to combine model checking (with JPF) and unit testing (with Junit). In the last co-authored paper, he discusses the experience gained in two master courses on formal methods (and program verification).

Although my evaluation of Sery's work is largely positive, I have some critical remarks also.

1. The title of the thesis is too broad and ambitious. The thesis actually tries to put the current model checking technology into practice. It shows a number of obstacles to its acceptance and proposes some mitigation. This should have been made clearer in the title.
2. I found the paper on teaching formal methods rather disconnected from the main body of contribution. I would have listed it along with the other (mildly related) publications.
3. Although the thesis cannot cover the entire world of model checking, I was wondering which criteria were chosen to select certain tools and leave out others. I was for example wondering why Bogor is not reviewed.
4. I would have stressed more the role and usage of counterexamples as a practically relevant issue arising in the use of model checkers. The experience reported by many users is that the main benefit one gets from the model checker is not when the program is proved correct, but rather when a failure is found and a counter-example is given.
5. I found the treatment of "Other techniques" (Section 2.4) rather cursory (in particular, see the treatment of symbolic execution).

As I already mentioned, these remarks do not affect my positive evaluation of the doctoral thesis. My final recommendation is therefore that Ondrej Sery's doctoral thesis qualifies him for the doctoral degree at Charles University in Prague.

I hope you will find this assessment useful in your process to award the doctoral degree to Ondrej Sery. If you need further inputs, please do not hesitate to ask me.

Sincerely yours,

Carlo Ghezzi
Professor