ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow:	**Dr. Shashidhar Kodamballi**
Visited Location:	**Fraunhofer IESE, Kaiserslautern, Germany.**
Duration of Visit:	**1st October 2009 to 30th September, 2010**

I - Scientific activity

During the fellowship period my main focus has been on ***model-based safety analysis***. Model-based safety analysis of systems is an emerging trend in systems engineering. It comes on the heels of adoption of model-based approaches by industry for system development with considerable success. The distinguishing feature of this trend is the use of high-level models to capture aspects of system design in order to enable automated analysis for safety assessment. Several approaches have been proposed in the recent literature to shape this trend. They differ in the types of models used, the analyses supported and their rigor. One interesting development here is the renewed interest in the application of formal methods to provide a precise semantics to the models in play and analyze them with guarantees of soundness.

My research has been to direct the attention of application of formal methods to more *expressive* systems, which is currently less investigated. Examples for such systems are *timed* and *hybrid* sytems. In the context of timed systems, so far, timing information related to the occurrences of faults has only been analyzed *qualitatively*. We have developed a novel *quantitative analysis* method to capture exact time-stamps and time-intervals for occurrence of faults that can lead to hazards in a popular safety artefact called fault-trees. The novelty lies in encoding of the fault-tree synthesis problem in game-theoretic terms and using a games solver to compute a *strategy* for hazard reachability. The method is currently being implemented and requires experimental validation before it can become part of a methodology for model-based safety analysis for timed systems.

Apart from the model-based safety analysis, which was the major focus, the scientific contact, Dr. Mario Trapp, provided me ample freedom and opportunity to actively collaborate with researchers at Fraunhofer IESE on a number of related topics, which are part of ongoing and planned research at the institute. The topics included a wide range and the opportunity helped broaden my research perspective in model-driven engineering. In particular, I've obtained an exposure to the following research areas:

- *Model-based hazard identification,*
- *Model-based testing for safety and security,*
- *Formal methods for integration of safety and product-line engineering,*
- *Hazard and risk analysis, and*
- *(Safety) requirements refinement.*

II- Publication(s) during your fellowship

1. **Title:** *Integrating Software Safety and Product Line Engineering using Formal Methods: Challenges and Opportunities.*
   Authors: Martin Becker, Soeren Kemmann and K. C. Shashidhar.

   Forum: 1st International Workshop on Formal Methods in Software Product Line Engineering (FMSPLE'10). Held in conjunction with 14th International Software Product Line Conference (SPLC'10), Jeju Island, South Korea, September 2010.

   Abstract: Product line engineering and safety engineering for software have both become mainstays to address the current challenges in developing software-intensive, safety-critical embedded systems. They address orthogonal concerns and the concepts and methods used by them have naturally evolved independently. A holistic, streamlined approach toward system engineering, however, obviously needs to identify and exploit the opportunities for a beneficial interplay between the two. We believe that appropriate formal models and methods can provide a suitable backbone in realizing such an approach. In this article, we present the challenges that arise while addressing safety in the software product line engineering context; and discuss where opportunities exist for leveraging formal methods and how they can provide the necessary techniques to address them.

2. **Title:** *CoGenTe: A Tool for Code Generator Testing.*
   Authors: A. C. Rajeev, P. Sampath, K. C. Shashidhar and S. Ramesh.

   Forum: 25th IEEE/ACM International Conference on Automated Software Engineering (ASE'10), Antwerp, Belgium, September 2010.

   Abstract: We present the CoGenTe tool for automated black-box testing of code generators. A code generator is a program that takes a model in a high-level modeling language as input, and outputs a program that captures the behaviour of the model. Thus, a code generator's input and output are complex objects having not just syntactic structure but execution semantics, too. Hence, traditional test generation methods that take only syntax into account are not effective in testing code generators. CoGenTe amends this by incorporating various coverage criteria over semantics. This enables it to generate test-cases with a higher potential of revealing subtle semantic errors in code generators. CoGenTe has uncovered such issues in widely used real-life code generators: (i) lexical analyzer generators Flex and JFlex, and (ii) The MathWorks' simulator/code generator for Stateflow.

III -Attended Seminars, Workshops, and Conferences

- 2nd to 5th March, 2010: *Quantitative Model Checking*, Copenhagen, Denmark.
- 6th to 10th September, 2010: *Advanced Applications of Model Checking Techniques*, Pisa, Italy.
- 22nd to 24th September, 2010: 25th IEEE/ACM International Conference on Automated Software Engineering (ASE'10), Antwerp, Belgium, September 2010.

IV – Research Exchange Programme (12 month scheme)

First visit:

Scientific Contacts: Professor Kim Guldstrand Larsen and Professor Anders P Ravn
Email addresses: kgl§cs.aau.dk; apr§cs.aau.dk
Institute: DANAIM, Denmark
Member Organization: Department of Computer Science, Aalborg University, Aalborg.
Group: Distributed and Embedded Systems & Center for Embedded Software Systems
Start Date: 1st March, 2010
End Date: 31st March, 2010
Outcome:

- The research discussions during the visit were focused on how the UPPAAL tool suite could be used for synthesizing safety artefacts for timed systems. The idea of using TiGa, a timed games solver provided by the UPPAAL tool-suite, for synthesis originated during the visit. The visit helped gain some proficieny in using the tool-suite and also clarify many of the subtleties of its internal engines.
- I attended a PhD School on *Quantitative Model Checking* held in Copenhagen during 2-5 March 2010. The lectures at the school covered the state-of-the-art in *real-time*, *probabilistic*, and *hybrid model checking* techniques.

Second visit:

Scientific Contacts: Professor Alessandro Fantechi and Dr. Stefania Gnesi
Email addresses: fantechi§dsi.unifi.it; stefania.gnesi§isti.cnr.it
Institute: National Research Council of Italy (CNR)
Member Organization: Istituto di Scienza e Tecnologie dell'Informazione (ISTI)
Group: Formal Methods and Tools (FM&&T)
Start Date: 6th September, 2010
End Date: 10th September, 2010
Outcome:

- The research discussions with Professor Alessandro Fantechi and Dr. Stefania Gnesi, as well as their colleagues, were focused on the topics that were currently underway at University of Florence and at FM&&T on application of formal methods in model-driven engineering of safety critical systems. The discussions provided feedback on my research activity and also new pointers to related work.
- I attended a PhD School on *Advanced Applications of Model Checking Techniques* held in Pisa during 6-10 September 2010. The lectures at the school covered a whole range of application domains where model checking techniques is being fruitfully leveraged, viz., *safety-critical systems*, *security*, *systems biology*, *human-computer interaction* and *web-service orchestration*.