Industrial Use of Formal Methods

Final report

Ulf Nilsson
20th Dec 2003

Summary of project results

The project results are divided into the following three subprojects:

Fault isolation in object-oriented control systems: This project, which is still on-going, is carried out in cooperation with the Division of automatic control, LiU, and ABB Robotics AB. The starting point is a large, configurable robot control software marketed by ABB Robotics. System failures result in propagating error messages, which are hard to analyze for operators without knowledge about the internal structure of the software. We have proposed model based techniques to alleviate this problem; in [13,14,18] we proposed a structural approach to pinpoint the real source of the failure based on the error reporting from the system and a UML model of the software (mainly relying on class diagrams). In subsequent work [1,2,3,5,9,10] we extended our approach to take into account also behavioral information expressed by means of UML state diagrams. The main contribution of the work is an abstraction technique which in many cases seems to circumvent the state space explosion which otherwise prohibits analysis of such systems.

Tool support for design inspection: This project proposes a novel approach to tool-based inspection focusing on the functional correctness of early designs expressed in a subset of UML [15,16]. The approach is based on conventional inspection in the style of Fagan, but extended with elements of formal verification in the style of Hoare; an early design is annotated with assertions expressing conditions on the state of the modeled system. In contrast to formal verification, we allow an incomplete axiomatization of the assertions beyond the point where a formal correctness proof may no longer be possible. Our hypothesis is, that relaxing the requirements on formal rigor makes it easier for the average developer to express and reason about early designs while still permitting the automatic generation of relevant, focused questions that help in finding defects. The questions are addressed in the inspection, thus filling the somewhat loosely defined steps of conventional inspection with a very concrete content [6,7,12]. As a side-effect our approach facilitates a novel, systematic and asynchronous inspection process based on collecting and assessing the answers to the questions. To demonstrate the feasibility of our approach, we developed a prototype for the

inspection of early designs expressed in a subset of UML. The project was carried out in cooperation with Ericsson SoftLab AB.

Constraint based modeling and verification: We also investigated the use of constraint technology for the purpose of describing and reasoning about discrete systems:

- In [19] we evaluated and showed the feasibility of an existing method for design synthesis applied to a real-time avionics application (commissioned by SAAB Dynamics). The method was implemented in a logic programming language with constraints.
- In [11,17,20] we developed a new algorithm for local and symbolic model checking of temporal properties expressed in the specification language CTL, based on execution principles from logic and constraint programming. Based on the preliminary results from a prototype implementation the new algorithm seems to outperform the conventional global and symbolic algorithms in many cases. The project is still ongoing and further results are expected.
- In cooperation with Laurent Fribourg, Ecole Normale Superieure de Cachan/CNRS, we developed a method for semi-automatic verification of so-called self-stabilizing distributed systems, i.e. systems that automatically recover from transient faults even though no single process has complete knowledge about the global system state.
- In cooperation with P. Dell'Acqua (ITN) and L.M. Pereira (Univ. Lissabon) we developed a model, based on logic programming, for asynchronous updatable multi-agent systems with the ability to communicate, update themselves and others, synthesize hypotheses and explain observations which, in turn, facilitates rational and proactive behavior [4].

Degrees resulting from the project

The project has resulted in one Ph.D. thesis

- T. Heyer. *Semantic Inspection of Software Artifacts: From Theory to Practice,* Linköping Studies in Science and Technology, PhD Dissertation no 725, 2001.

Additionally there has been one licentiate thesis

- D. Lawesson. *Towards Behavioral Model Fault Isolation for Object Oriented Control Systems*. Licentiate thesis no 863, 2000.

Dan Lawesson is expected to complete his Ph.D. thesis in 2004.

Ulf Nilsson was promoted to full professor in 2003.

M.Sc. projects

The following M.Sc. projects are direct consequences of the present CENIIT project:

- Hampus Weddig. A Prototype Implementation of a Tabled Constraint Logic Language with Constructive Negation. LiTH-IDA-Ex-03/20. 2003.

- Jens Rydholm. Tool Supported Design Inspection: Question Generation. LiTH-IDA-Ex-03/44. 2003.
- Johan Kjellberg. Application of OO-concepts for Real-time. LiTH-IDA-Ex-00/32. 2003.
- Anders Lindahl, Mattias Svensson. Complementation of Büchi Automata (tentative title). To be presented January 2004.

Staff

The project has funded the research and supervision of Ulf Nilsson, and a new Ph.D. student admitted in 2003; Vladislavs Jahundovics. In addition the following staff has participated in the project but has been funded from elsewhere

- Dan Lawesson (ISIS)
- Tim Heyer (Vinnova)
- John Lübcke (TFR)

Industrial contacts and cooperation

Several industrial contacts were pursued in the projects:

- The on-going project on fault isolation is carried out in cooperation with ABB Robotics AB. Some of the early results on structural fault isolation of the project will be incorporated in the next generation of the robot control software. There was also cooperation with another CENIIT project: Diagnosis for industrial processes.
- The project reported in [19] was done on commission from SAAB Missiles AB. How, or if, the results were later used is unknown to us.
- The project on design inspection was carried out in cooperation with Ericsson SoftLab AB. The cooperation aimed primarily at knowledge transfer and the project results were not intended for commercialization.

Publications

1. D. Lawesson and U. Nilsson and I. Klein. Fault Isolation in Discrete Event Systems by Observational Abstraction. In *Proc of 42nd IEEE Conf on Decision and Control (CDC), Maui Hawaii*. 2003.
2. D. Lawesson and U. Nilsson and I. Klein. Fault Isolation Using Automatic Abstraction To Avoid State Space Explosion. In *Workshop on Model Checking and Artificial Intelligence, Acapulco*. 2003.
3. D. Lawesson and U. Nilsson and I. Klein. Model Checking Based Fault Isolation Using Automatic Abstraction. In *Proc. of the 14th Intl Workshop of Principles of Diagnosis, Washington DC*. 2003.
4. P. Dell'Acqua, U. Nilsson, L.M. Pereira. *A Logic Based Asynchronous Multi-Agent System*. Electronic Notes in Theoretical Computer Science, 70(5), 2002.
5. D. Lawesson and U. Nilsson and I. Klein. *Fault Isolation using Process Algebra Models*. In 13th Intl Workshop on Principles of Diagnosis, DX02. 2002.
6. T. Heyer. *Semantic Inspection of Software Artifacts: From Theory to Practice*, Linköping Studies in Science and Technology, PhD Dissertation no 725, 2001.

7. T. Heyer. *Semantic Inspection of UML Designs,* Proc. Workshop on Inspection in Software Engineering (WISE'01). M. Lawford and D.L. Parnas (editors), pp. 58-67, Paris, 2001
8. M. Duflot, L. Fribourg, U. Nilsson. *Unavoidable Configurations of Parameterized Rings of Processes*. Proc. of Concurrency Theory (CONCUR'01), Ålborg, Lecture Notes in Computer Science 2154, Springer-Verlag, Aug 2001.
9. D. Lawesson, U. Nilsson, I. Klein. *Model-Checking Based Fault Isolation in UML*. In Proc. 12th Intl Workshop on Principles of Diagnosis, DX01, San Sicario, Italy. 2001.
10. D. Lawesson. Towards Behavioral Model Fault Isolation for Object Oriented Control Systems. Licentiate thesis no 863, 2000.
11. U. Nilsson, J. Lübcke. *Constraint Logic Programming for Local and Symbolic Model-checking*. Proc of Int'l Conf. on Computational Logic CL2000, London, Lecture Notes in Artificial Intelligence 1861, Springer-Verlag, 2000.
12. T. Heyer, *Tool Support for Design Inspection: Automatic Generation of Questions*. Internrapport, 2000.
13. M. Larsson and I. Klein and D. Lawesson and U. Nilsson. *Fault Isolation in Object Oriented Control Systems*. In IFAC SAFEPROCESS 2000, Budapest. June 2000.
14. M. Larsson, I. Klein, D. Lawesson, U. Nilsson. *Model Based Fault Isolation for Object-Oriented Control Systems* . Teknisk rapport LiTH-ISY-R-2205, Nov 1999.
15. T. Heyer, *Tool Support for Design Inspection: A Specification Notation*. Internrapport, 1999.
16. T. Heyer, *Tool Support for Design Inspection: A Design Notation*. Internrapport, 1999.
17. J. Lübcke, U. Nilsson, *On-the-Fly Model Checking of CTL Formulas using Constraint Logic Programming*. Intl Workshop on Constraint Programming for Time Critical Applications, Lisbon, 1999.
18. M. Larsson, I. Klein, D. Lawesson, U. Nilsson. *The Need for Fault Isolation in Object-Oriented Control Systems*. Technical report LiTH-ISY-R-2098, Feb 1999.
19. U. Nilsson, S. Streifert, A. Törne, *Detailed Design of Avionics Control Software*. IEEE Intl Symposium on Real-time Systems, Madrid, 1998.
20. J. Lübcke, U. Nilsson, *CTL Model Checking using Tabled Logic Programs*. Workshop on Constraint Programming for Time Critical Applications, Nice, 1998.