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 ongoing, 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

Additionally there has been one licentiate thesis

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:

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