ASTEC

Advanced Software Technology

Report for Phase 2
1999-2000

UPPSALA
UNIVERSITY

ASTEC

Advanced Software Technology

This document is the

Final report for Phase 2

The years 1999 and 2000.

Uppsala April 6, 2001

Professor Bengt Jonsson

Director

Up-to-date information about current activities can be found on the
WWW page http://www.astec.uu.se/

Summary

The main results of ASTEC during Phase 2.

- The volume of work carried out has continued to increase with 40% per year.
- ASTEC has developed a critical mass with a clear profile and competence on highest international level in key strategic areas. This is reflected by the increased publication rate and decreased cost per publication to 50% of initial value.
- Impressive and recognized research results have been produced and published in totally 97 publications (58 during phase 2), of both theoretical and practical nature.
- Results from ASTEC work have been transferred and are nowadays used in industry.
- The industrial participation in and contribution to ASTEC has been steadily increasing.
- The production of Ph.D., Lic., and M.Sc. graduates has acquired momentum with 13 degrees in 2000.
- The centre contributes courses to national and local graduate and undergraduate education.
- Network activities such as seminars and meetings has increased from almost absent to several per month.
- ASTEC collaborates with other national research initiatives, and has strong international collaboration links, including several European Community research projects.

Sammanfattning

De viktigaste resultaten av ASTEC under etapp 2.

- Mängden arbete som utförs har fortsatt öka med 40% per år.
- ASTEC har uppnått en kritisk massa med en tydlig profil och inom strategiska områden på högsta internationella nivå. Detta visas av den ökade publikationstakten och minskade kostnade per publikation till 50% av kostnaden 1996.
- Impornerande och erkända forskningsresultat har producerats och publicerats i totalt 97 publikationer (58 under etapp 2) inom både teoretiska och praktiska områden.
- Resultat från forskningen har överförts och utnyttjas nu inom industrin.
- Industrins medverkan och instaser har fortsatt öka.
- Doktors, Licenciat och magisters examina har ökat kraftigt till 13 examina år 2000.
- Kompetenscentrumet bidrar med kurser nationellt och lokalt till både doktorandutbildning och grundutbildning.
- Nätverkaktiviteter som seminarier och möten har ökat till flera per månad.
- ASTEC samarbetar med andra svenska forkningscentra och har starka internationella kontakter inklusive flera EU-projekt.

Contents

Introduction

ASTEC (Advanced Software Technology) is a competence centre which focuses on Advanced Tools and Techniques for Software Development. Development of software accounts for a significant part of the costs in the construction of a number of important products, such as communication systems, transportation and process control systems, of Swedish industry. It is thus a vital interest to be able to produce better software at lower cost. One of the means to achieve this is to improve the tools and techniques used for software development. ASTECs vision is that, wherever possible, software should be developed using high-level specification and programming languages, supported by powerful automated tools that assist in specification,

analysis, validation, simulation, and compilation. The purpose of ASTEC is to conduct pre-competitive and industrially applicable research that contributes to this vision, to build up and offer a concentrated research environment in the software technology area, and to be a forum for contacts and exchange of ideas between academia and industry.

ASTEC has been formed as a consortium of academic partners with strong research programs in different areas of software technologies, and of companies which either have a substantial software production or produce tools for software development. During the first two years, the focus of ASTEC was to connect academia with industry by conducting projects where techniques from academia were applied to problems in industry. This phase created a network of contacts between academia and industry. After the initial phase, a strategic perspective for the long-term development of ASTEC was added, which has led to a focus and build-up of effort in key strategic areas.

Currently, ASTEC has developed into a focussed and distinct research unit, having a broad contact area with a number of companies. It is a natural forum for collaboration, discussions, and new contacts in the software technology area.

Basic Facts

ASTEC has been formed as a consortium of the following academic and industrial partners during phase 2.

- Research groups at *Uppsala University*, the *Royal Institute of Technology*, the *Swedish Institute of Computer Science* (SICS), and *Mälardalen University*, working mainly on formal methods, functional, logic and constraint programming, compilation, and on embedded, distributed, and real-time systems, together with

- companies with a substantial software production and thus a large interest in software development. These include companies: *ABB Automation Products AB*, *Ericsson Utvecklings AB*, *Mecel AB*, *Telia Validation AB*, and *Volvo Technological Development Corporation*, and

- companies that produce tools for software development: *IAR Systems AB*, *Prover Technology AB*, *Telelogic AB*, *UPAAL AB*, and *Volcano Communication Technologies AB*.

Further details can be found in appendices 1-3.

Appendix 1. ASTEC business ratios.
　　Give figures for the development of contributions to ASTEC, man power, publications, degrees and management.

Appendix 2. Partners and persons
　　ASTEC partners, Board, Scientific evaluators and Staff.

Appendix 3. Economic report for phase 2.

A. Performance and Development as a Competence Centre

A.1. Long-Term Goals and Progress of the Centre

Background

Industrial and academic collaboration should be particularly relevant for research on software systems: many advances in software technology occur in universities but on the other hand the major part of software production occurs in industry. Such a collaboration thus offers the opportunity for industry to exploit recent advances in software technology and for researchers in academia to evaluate the effectiveness of new techniques in a "real-world" environment.

Though this observation is probably universal, it is particularly applicable to a country like Sweden. Several major products of Swedish industry, e.g., data communication and process control systems, are to a significant extent based on software. Swedish academia has a strong tradition of research in some areas which have potential applications to software development. The indirect impact of this research on industrial practice, through mobility of individuals and ideas, has been noticeable: functional programming and formal methods have influenced software development in the Swedish telecommunications industry, as witnessed, e.g., by the creation of high-level languages such as Erlang, SDL, and TTCN. ASTEC is intended to build on this tradition, and strengthen direct contacts between academic research and industrial practice, so that advances in academic research can indeed benefit industrial software development, which in its turn can guide the agenda for academic research.

Goals and Strategies

ASTECs vision is that, wherever possible, software should be developed using high-level specification and programming languages, supported by powerful automated tools that assist in specification, analysis, validation, simulation, and compilation. ASTECs goals are to contribute to this vision by

1. carrying out industrially relevant pre-competitive research at the highest international research level which can be both published in leading scientific conferences and journals and exploited by the industrial parties,

2. building up and maintain a critical-mass concentrated research environment for research, graduate education, collaboration, problem solving, and long-term competence development, and

3. being a forum for contact between industrial and academic software researchers.

The strategies chosen by ASTEC to meet these goals are based on the following principles.

1. Academic-industrial collaboration and technology transfer require that both parties take an active interest. Therefore, ASTEC work should be conducted with active participation by both industry and academia. Collaboration and technology transfer will thus be built in from the beginning. This strategy has been successful in building strong links between researchers in academia and in industry.

2. Longer-term project planning and the build-up of a concentrated research environment is guided by a *strategic research plan*. The plan structures the challenges addressed by ASTEC into program areas, more precisely described in Section B.

3. ASTEC runs and supports seminars and workshops for contact between industrial and academic researchers.

History and Evaluations

During phase 1, i.e., the first two years, the focus of ASTEC was to establish collaboration links academia with industry by conducting projects where techniques from academia were applied to problems in industry. This phase created a network of contacts between academia and industry. Projects conducted in phase one have developed into major research directions of ASTEC; this is the case for development of software in automotive industry, and calculation of execution time analysis. In phase two, a strategic perspective for the long-term development of ASTEC was added. A *Strategic Research Plan* was developed, which structures longer-term challenges addressed by ASTEC (this was also recommended in the First Evaluation). The plan is described in more detail in Section B. The strategic research plan formulates longer-term research goals which require basic research and address important industrial problems. Based on the plan, research competence has been recruited and strengthened to build up key areas, and long-term Ph.D. thesis projects have been formulated. As example, the area of compilation was included within ASTEC, where competence has been recruited and strengthened.

Also in phase two, an international Scientific Advisory Board was appointed, consisting of profs. Alan Burns (York), Neil Jones (Copenhagen), and Bernhard Steffen (Dortmund), later also prof. Neeraj Suri (Gothenburgh). The board has conducted two self-imposed internal reviews (April - 98 and March -00). Follow-up and administrative work has been taken on by a Research Coordinator (Roland Grönroos, 40%), and was made accessible and transparent by building a WWW structure containing all documents produced within ASTEC.

The First NUTEK Evaluation was not fully satisfied with ASTECs functioning. Its recommendations have been addressed by working out the strategic plan, including new competence areas, appointing the Advisory Board, and strengthening the administrative support. Industrial seminars have been conducted with a largely industrial audience, ASTEC work has been presented at industrial conferences, and ASTEC has developed courses for graduate education.

A follow-up review, conducted by NUTEK in September 1998, showed satisfaction with the measures taken since the first review, and added some recommendations, most of which have now been implemented. The reviews of the Scientific Advisors have pointed out strengths and weaknesses in the technical work, and resulted in some shifts of projects. As an example, the work on requirements, started in Phase 1, has been phased out in favour of work on testing.

Phase 2

During phase 2, ASTEC has developed into a focussed research unit with a critical mass within its key areas. ASTEC performs research on the highest international level. Impressive recognized research results have been produced, of both theoretical and practical nature, and are published in leading conferences. ASTEC collaborates with other national research initiatives, and has strong international collaboration links, including several European Community research projects.

ASTEC is recognized and supported by Uppsala University as an important long-term strategic research unit. In written and oral presentations of research in IT at its hosting institutions, ASTEC is referred to as a strong pillar of research in Computer Science, and as a good example of successful collaboration with industry. The basis of academic partners is expanding, and now includes Mälardalen University.

The industrial participation in and contribution to ASTEC has been steadily increasing. The number of companies has grown from 6 to 10 during phase 2. The contributions from companies are now exceed 7 MSEK per year, and cash contributions have grown from virtually nothing to 1.6 MSEK per year. Results from ASTEC work have been transferred and are nowadays used in industry. The centre employs 3 industrial Ph.D. students. Senior researchers at companies are making substantial contributions to ASTEC work. ASTEC researchers and graduates have moved to the industrial partners of ASTEC, and senior ASTEC researchers have part-time appointments with companies.

The production of graduates (Ph.D., Lic. and M.Sc.) has now acquired momentum (5 in 1999, 13 in 2000). During ASTECs operation, three key researchers (Parosh Abdulla, Hans Hansson and Wang Yi) have been promoted to full professor rank, and one to docent (Konstantinos Sagonas), partly in recognition of work carried out in ASTEC. The centre has developed and conducted graduate courses in its area of competence, and is involved in industrially oriented undergraduate education.

A.2. International and National Collaboration

The competence profile of the centre's academic research groups covers the areas of semantics, formal specification and verification, functional, logic and constraint programming, compilation, real-time systems, embedded systems computer architecture, which are important for the strategic research directions of the centre.

The companies also contribute to the centre's research profile. Several companies are world-leading suppliers of technology for software development, and are thus also on the frontier of international research in the areas of relevance. As examples, Prover Technology AB owns one of the the world's most powerful solver for satisfiability problems, and Telelogic AB is a leader in development of standards for testing of communication and embedded systems.

ASTEC researchers are firmly established in the international research community. Senior researchers are members of program committees in key conferences of the areas of the strategic research plan. For 1999-2000, these include

- CAV (Conference on Automated Verification, where also a 3-hour invited tutorial was given in 2000 by Parosh Abdulla and Bengt Jonsson),
- CONCUR (Conference on Concurrency Theory),
- LCTES (Workshop on Languages, Compilers, and Tools for Embedded Systems),
- RTCSA'2000 (Int. Conference on Real-Time Computing Systems and Applications) there Prof. Hans Hansson was also Program co-chair in 2000.
- RTSS (IEEE Real Time Systems Symposium),
- TACAS (Tools and Algorithms for the Construction and Analysis of Systems). Wang Yi will be Program Chairman in 2001.

Research of ASTEC has received numerous signs of recognition. Two notable examples are that an ASTEC paper received the best paper award of EAPLS -- the European Association for Programming Languages and Systems, at the ETAPS conferences in 2000, and that an international evaluation of Swedish Computer Science research supported by TFR (The Research Council for Engineering Sciences) conducted by prof. Ruzena Bajcsy (NSF), president Gilles Kahn (INRIA), and prof. Jeff Ullman (Stanford) in Nov. 1999 commended ASTEC groups by *"over all this is a success story. It has the right combination of theory and practice"*.

ASTEC has a strong network of international contacts. As examples, the UPPAAL project has been collaborating very closely with Aalborg University in Denmark since 1995. ASTEC groups

have has long been an active collaboration with Seoul National University (SNU) (Professor Sang Min from SNU was appointed as a senior lecturer during 1998-99, and Andreas Ermedahl (ASTEC Ph.D. student) has visited SNU for 6 months 2001), and with. C-Lab in Paderborn, Germany (including a longer visit by Dr. Peter Altenbernd visited ASTEC during 1997). Other international collaborations involving longer mutual visits include Rice University, Bell Laboratories, Paris Univ. 7, and Dortmund Univ.

In addition to visits within the collaboration just mentioned, ASTEC attracts both long- and short-term visitors. As an example, Dr. Thomas Noll was on a one-year visit to the Department of Teleinformatics at Royal Institute of Technology (KTH) from the Department of Computer Science at RWTH Aachen. During this visit he was actively participating in the ASTEC work on verification of Erlang code.

Through its partners, ASTEC participates in several European Community research projects. The WOODDES (Workbench for Object Oriented Design and Development of Embedded Systems) project is devoted to development technology for embedded systems in automotive and telecommunication industry within the framework of UML. The project has 6 industrial partners (Peugeot-Cit"oet, Verilog, Greek Telecom/INTRACOM, I-logix, Commissariat `a l'Energie Atomique and Mecel AB) representing European automotive industry, telecommunication and tools developers and 2 academic partners: Oldenburg University, Germany and Uppsala University. The European VERIFICARD project will study security aspects of the JavaCard programming platform for Smartcards, by means of software verification techniques. A contribution will be to adapt work on compositional proof techniques developed within ASTEC. The ADVANCE project "Advanced Validation for Telecommunication Protocols", will develop tools that extend the power of formal analysis. Its partners include Uppsala and Ericsson. Our participation in all these projects builds directly on ASTEC work.

The national research programme ARTES which supports research and promotes graduate education, hosted at Uppsala University and funded by SSF (The Swedish Foundation for Strategic Research) with a budget of 88MSEK during 1998-2002, was initiated in 1998 with the support and involvement of several ASTEC researchers. Currently, Prof. Hans Hansson is program director, and he and Parosh Abdulla and Wang Yi conduct projects funded by ARTES. There is a close coordination between ASTEC and ARTES work: the two bodies share Roland Grönroos as research coordinator, and several ASTEC projects are closely related to ARTES projects.

ASTEC has co-organized several international workshops and conferences, including **NWPT '99,** the 11th Nordic Workshop on Programming Theory, in Uppsala, October 1999, and **FTRTFT '96,** the *Fourth International School and Symposium on Formal Techniques in Real Time and Fault Tolerant Systems* in Uppsala, Sept. 1996. A collection of scientific papers, which represent ASTEC work, has been jointly submitted to the Springer Verlag journal STTT (Software Tools for Technology Transfer), together with a cover paper which presents the ASTEC framework, with the goal of presenting ASTEC to a wider scientific community.

ASTEC conducts technical seminars, and seminars directed to an industrial audience. Industrial one-day seminars have been conducted on the topics of Automotive software development (Gothenburgh 1999) and on Software development for the Telecom industry (Stockholm 1999). Topical seminars include regular one-day seminars on Verification Tools, on Programming Languages and Implementation. In addition, one-day seminars have been organized on topics like Security, and on Design Patterns.

A.3. Linkages and Collaboration within the Centre.

ASTEC Organisation and Meetings.

ASTEC is organised around the agreement between NUTEK, Uppsala University and the 10 industries (see appendix 2). The work has been regulated by a number of contacts with the main aim to provide research results to the participating industries. Within Uppsala University, ASTEC is a separate financial unit, hosted by the Department of Information Technology. All personnel involved in ASTEC are employed by the participating institutions and companies.

Management

The board (see appendix 2) has been formed by persons from the participating companies and universities. All funding decisions are taken by the board. The board follows activities through project reports every 6 months, and contributes to ensuring the industrial relevance of ASTEC work. The board also take part in the long term development and strategic planing of ASTEC.

The director (Bengt Jonsson, Uppsala University) carries out the daily and long term management and the decision taken by the board, initiate meetings, and keep contact with the scientific advisors.

The Scientific advisory board (see appendix 2) comments on long-term project planning and on project proposals and has also conducted 2 internal reviews the years 1998 and 2000.

The research coordinator (Roland Grönroos, Uppsala University) take care of daily administrative matters, prepare reports in cooperation with the director, arrange seminars and meetings, collect and prepare board meeting material.

Project leaders (see appendix 2), Proposes new projects and project areas, lead and carry out the day to day research in cooperation with industrial and academic staff.

Meetings

ASTEC-seminar series (see http:// www.astec.uu.se/Seminars) consist of scientific or industrial presentations in the area of software technology. The volume has increased from a few seminars per year to 10 and 28 for 1999 and 2000 respectively. There is now about one seminar each week during the semesters.

Project leader meetings (project leaders ca 7-8 persons) are held about once a month for information, planning and generation of new ideas.

Board meetings there have been 10 board meetings during 1999-2000.

Workshops, ASTEC has arranged 3 workshop meetings for the entire ASTEC during phase 2. The aim has been to increase contacts between industry and academia, plan projects and present results within the center.

Public seminars with substantial ASTEC involvement
- **ASTEC Telecom software seminar** May 20 1999 at Ericsson, Älvsjö, Sweden.
- **Workshop on Security, Middleware, and Languages**, Stockholm, June 15-16, 2000
- **Sixth International Erlang/OTP User Conference**, Tuesday October 3, 2000. Ericsson, Älvsjö, Sweden.
- **Competence center day 2000** (see www.astec.uu.se/cc-day2000/), ASTEC was one of the hosts at the NUTEK competence center day last year.

The scientific work in ASTEC is carried out in cooperation between the participating research groups, both in industry and academia. Beside the flora of formal meetings mentioned above there are many informal links, discussions, and technical links between projects within ASTEC.

An example of close coordination between different activities in ASTEC is the synergy between the Whole-Program Optimization (WPO) and Worst-Case Execution Time analysis (WCET) projects are collaborating around a common tool and algorithm base. They have common needs in that both projects need to have information about a an entire program, and not just individual source files. A research compiler based on a commercial product of IAR Systems AB has been used by both groups, and Jakob Engblom of the WCET project has been actively involved in developing an industrial proof of concept implementation of a WPO compiler at IAR. Also, the compiler infrastructure of the WPO project is used in the WCET project to research program flow analysis, and as a basis for the necessary gathering of information about an entire program.

The links between industry and academia are strengthened by the fact that several key researchers are appointed jointly by academia and industry. For instance, Parosh Abdulla is part-time employed by Prover Technology, thus bridging the development of techniques which occurs within the company with the development in academia. ASTEC currently employs 3 industrial Ph.D. students, which are part-time employed by companies to carry out research in ASTEC projects.

The contacts within ASTEC have inspired new contacts and collaborations between companies. Joint M.Sc. projects have been defined. The testing project involves 3 companies, and has also indirectly inspired technical contacts with other companies in ASTEC.

A.4. The Centre and the Host University

During the last several years Uppsala University has taken several measures in order to increase the visibility and operational efficiency of its educational and research programs in the information technology field. In 1998 the various small departments dealing with different aspects of IT were joined to two large departments, one in the Faculty of Science and Technology, the other one in the Faculty of Social Sciences. In order to help coordinate the work in these two departments and to increase the collaboration between the IT field and other fields at the university the "virtual IT faculty" was created. The head of the IT-faculty was appointed vice-rektor/rektorsråd i.e. senior advisor to the rector of the university, thus putting information technology on the same level as undergraduate education, graduate education and external relations in terms of the central university organisation. Several new chairs in the information technology field have been created and the already very extensive educational programs have been expanded both in terms of number of programs and courses and number of student positions.

ASTEC has been part of this development both in the sense that the program has had advantages from it and that the activities within ASTEC have been seen as part of the focus on IT at Uppsala University. The head of the IT-faculty, Ewert Bengtsson has also served on the ASTEC board thus linking the program directly to the central university organisation.

The merger of the two departments which had most of ASTEC activities at Uppsala University into the new IT department has facilitated many administrative routines. ASTEC is formally a separate administrative unit within Uppsala University. The administration is hosted in the IT department but the accounting is separated from that of the department.

ASTEC is together with a few other strategic research programs always presented as an important part of the research strategy of the university. It can for example be reached through only two obvious mouse clicks from the central web-page of Uppsala University, in contrast to most activities at the university which usually require many more or less obvious linking steps.

ASTEC is (almost) always mentioned in accounts of the research program in Computer Science at Uppsala University. Examples include STUNS report, and presentation of Research in IT to representatives of the leadership of research at SUN and ABB.

Several of the new faculty chairs that have been created in the last years at Uppsala University (and also Mälardalens Högskola) are in areas that support ASTEC work, including real-time systems, computer architecture, computer communications, and computing science. ASTEC has indirectly catalyzed the creation of some of these chairs.

ASTEC researchers are involved in graduate and undergraduate teaching, and development of courses within its area. More details can be found in Section B.5.

A.5. Future Plans and Strategies

The future plans and strategies follow the goals outlined in the introduction and ASTEC's long-term goals described in Section A.1. They also include direct input from the industrial and academic partners, and from the recommendations given by ASTEC's International Scientific Advisory Board.

ASTEC projects that are state-of-the-art and have reached a sufficient level of maturity (e.g., HiPE, SMC) will strive towards achieving a complete technology transfer and become (or be integrated into) a commercial product. Similarly, projects that are successful in their prototype phase (e.g., ErlVer, WCET) will aim towards becoming more usable or integrated into an existing tool. In both cases, additional efforts (e.g., in the form of case studies) and closer collaboration between the academic and industrial partners will be required to evaluate and tune the performance/effectiveness of the resulting system in its actual industrial uses. The time investment, although substantial, is expected to have a substantial impact to industrial partners and achieve ASTEC's long-term goals.

Projects that are somehow related or whose research/application areas partly overlap should interact further and achieve greater cooperation between them. Also, as pointed out by the Scientific Advisory Board, greater interaction between other researchers in Sweden working on similar topics or projects is strongly desirable. ASTEC will encourage these activities more in the form of theme workshops or seminars.

On the educational side, ASTEC will continue its successful upper-level undergraduate courses (on verification, real-time systems and compiler technology) at Uppsala University, and will try to enrich them with new courses of current interest (e.g., a course on security of programming languages for the internet). Efforts will be made to also attract in them students from geographically close universities and encourage the participation from members of the industrial partners of ASTEC in its regular seminar series.

Last but not least, although it is expected that the research areas and application fields of ASTEC (see Section A.4) will remain as currently, ASTEC's competence and expertise should be also be applied in new research areas of active interest. Examples of new research activities currently under consideration include application areas related to the internet, and verification of safety and security properties of code for distributed applications. Also, it will be investigated to what extent experiences gained from working on an existing ASTEC project can be applied to a similar project of related nature: e.g., how techniques developed within the context of verification project can be applied to debugging, simulation, and other forms of validation of multi-threaded applications.

B. Technical Results and Scientific Outputs

B.1. Research Programme

The research activities of ASTEC are structured into *program areas*, which focus the efforts from several projects and are responsible for a wider dissemination of the conclusions, conducting seminars or specialised courses as deemed necessary. The areas are interrelated in that progress in one area is dependent on the state of the art in the others.

Each program area is either an *application* area, which provides problems to drive the research, or a *technical* program area, which serve to develop techniques, tools, and methods. A particular project can very well span over several of these areas, typically at least one technical area and one application area.

The application areas are

- **Software for Automotive and Vehicle Applications**, including embedded and safety-critical software, often deployed on a distributed network, and
- **Data- and telecommunication systems**, with requirements on mobility, high distribution, massive concurrency, and code replacement without disruption of the continuous operation of the system.

The technical areas are

- **Validation and verification** is concerned with high-level notations for expressing requirements and design specifications, together with tools and (formal) methods for analysis of specifications for the purposes of verification, validation, test generation, and tracing of requirements.
- **Programming language implementation and compilation** is concerned with the implementation and use of high-level (concurrent) programming languages, together with the development of compilation technology for (time- or space-) efficient program execution and code generation for different architectures.
- **Real-time, embedded, and distributed systems** is concerned with features specific to software development for real-time, embedded, or distributed systems, such as predictability, timeliness, scheduling, and distribution.

Projects within ASTEC can be classified using a 2*3 matrix (Table 1).

ASTEC Projects per Research Area	Validation and Verification Technology	Programming Languages and Implementation Technology	Technology for Real-Time Distributed Systems
Datacom and Telecom Applications	ErlVer Testing BUS SMC SA	SA HiPE	HiPE BUS
Automotive and Vehicle Applications	Auto BUS SMC Testing	WCET WPO	Auto WCET

Table 1. ASTEC projects per programme area 1999-2000.

The projects acronyms stands for:

Auto: A design methodology for embedded real-time systems
BUS: Modeling and analysis of a industrial bus protocol
ErlVer: A Verification Method for Erlang
HiPE: High Performance Erlang
SA: Analysis of types and process topology for static debugging
SMC: Symbolic Model Checking
Testing: Automated Testing
WCET: Calculation of Worst-Case Execution Times
WPO: Whole-Program Optimization in Compilers for Embedded Systems

A notable feature of projects carried out under the aegis of ASTEC is that state-of-the-art academic research can have access to production-size industrial-quality software, given as source code, which can be used to conduct experiments. This has given the research on compilation, execution-time analysis, and on formal verification, a unique opportunity to evaluate the applicability and effectiveness of new techniques in realistic settings rather than on toy benchmarks.

B.2. Technical and Scientific Achievements

The presentation of the achievements are structured according to area.

Software for Automotive and Vehicle Applications

Typically, vehicle software is deployed in the nodes of a distributed network. Requirements on resource consumption are often very stringent, and systems are assembled from parts delivered by subcontractors. A lot of effort is currently devoted to developing and formalizing a complete methodology for building software in embedded systems, for instance within the automotive industry. Such a methodology should cover the entire chain from requirements to running code on a specific target platform. Challenging research problems include development of notations for requirements, techniques for system modeling and for analyzing whether a component or a collection of components conform to requirements, techniques for mapping a design onto a distributed target architecture, for generating code which satisfies often stringent requirements on memory, power and timing consumption. These challenges generate problems in different technical areas.

Within ASTEC, several case studies using UPPAAL have been carried out aiming at evaluating the industrial applicability and usefulness of the existing techniques and tools, some of which are developed in the Validation and Verification area. The UPPAAL tool implements techniques for modeling systems and their components on a high level of abstraction, and for analyzing whether a collection of components actually cooperate to meet system requirements. It has been successfully applied to the analysis of timing-dependent bus protocols. The Ph.D. thesis of Paul Pettersson contains a sequence of case studies which analyze the behaviour of systems of components, using the UPPAAL tool. Several case studies are taken from automotive applications. A conference paper presenting a case study on a gearbox controller, conducted in collaboration with Mecel AB, was invited for publication to the Springer Verlag journal STTT (Software Tools for Technology Transfer). Mecel AB and Uppsala also collaborated on the analysis of a car locking system at SAAB.

A result of the work on case studies within ASTEC, is the development of BUTLER by Mecel AB. BUTLER is a tool set for structuring requirements and design models for automotive systems. Recently a start-up company based on BUTLER has been established by the main developers of BUTLER.

Embedded systems often contain an interaction between discrete control and continuous behaviour, which must be modeled by a combination of discrete automata and differential questions, resulting in so-called hybrid systems. A tool for animating a hybrid system based on a mathematical definition of its behaviour has been developed and evaluated in case studies. The animator is being integrated with UPPAAL.

In recent years, there has been an increasing industrial interests in using UML as a standard modeling language, for the development of embedded systems. Most software tools for UML support only editing, modeling and simulation, and no analysis. Gunnar Övergaards Ph.D. thesis (to appear) lays a foundation for such tools by providing a formal semantics for a significant portion of UML. Future plans include the development of UPPAAL as a plug-in module in commercial UML tools to support automated analysis of UML models integrated with timing information.

Software for Data- and Telecommunication Systems

ASTEC's vision is that development of communications software should be conducted, not by large organisations with heavy software development processes, but by small, well-qualified teams working with powerful development tools to turn an innovative idea into a product. This means that the tools should preferably embody solutions to typical requirements for these systems, including reliability, massive concurrency, ability to update systems with new functionality while in operation etc. In this respect, ASTEC has been actively involved in the development of the Erlang programming language, both at the level of their efficient execution (*cf.* the HiPE system) and at the verification of applications written in Erlang (*cf.* the EVT tool described below).

An another important aspect of work that falls under this application area is the development of compilation techniques for embedded systems software, in which the code size of the programs is a very important consideration. Smaller code size means that the hardware can be made cheaper and have decreased power consumption. Minimizing code size by compression techniques at the level of source code and by employing manually clever tricks at the level of memory layout is a tedious and error-prone process for embedded software engineers. The ASTEC WPO project is working on powerful techniques for automatically shrinking the compiled code of such programs.

Validation and Verification Technology

The area considers methods and tools for specifying and analysing the correctness of systems and system components. Emphasis is on formal approaches to requirement and design specification, and on methods and tools for establishing adherence of systems to their specifications.

Software for telecommunication systems often possess certain characteristics, such as massive and dynamic concurrency and on-line updating of software, that prohibit the use of fully automatic verification techniques. To permit verification of such software programmed in Erlang a major effort has been undertaken: an operational semantics for Erlang has been developed, with a property specification language and a novel proof system for compositional and inductive reasoning. To support verification a proof assistant with a state-of-the-art graphical user interface and considerable support for proof automation is available: the Erlang Verification Tool - EVT. The feasibility of the method has been illustrated in case studies such as, e.g., the verification of a core part of the Mnesia distributed database system which is part of the standard Erlang distribution. As a side effect of the Erlang verification effort, two patent applications at Ericsson's Computer Science Laboratory were indirectly stimulated.

ASTECs effort to develop new and more efficient symbolic verification techniques for finite-state systems have generated very interesting results. The FixIt tool which adapts standard algorithms for symbolic reachability analysis to work with SAT-solvers, such as Stålmarck's algorithm, instead of the classical technique based on Boolean Decision Diagrams (BDDs). Although BDDs have been the dominating tool in symbolic model checking for the last 15 years, the FixIt technique scales up better on several classes of applications. Furthermore, we have recently extended SAT-based techniques to deal with systems with infinite-state spaces, which are beyond the capabilities of BDDs.

The project on modeling and analysis of an industrial bus protocol was a very interesting case study, embodying one of the few full-scale applications of automated verification to a communication protocol used in process control industry. At ABB, several abstract models of a working Bus Protocol have been developed and analyzed using the UPPAAL tool. To our knowledge, this is the largest case study where the UPPAAL tool has been applied, involving 150 pages of protocol specification, and about 2000 lines of Modula-2 code. Various imperfections in the protocol logic and its implementation have been found, and respective improvements have been suggested.

An interesting example of how practical problems can inspire advances in fundamental research is the development of the *regular model checking* paradigm, presented in Marcus Nilsson's Lic. Thesis. The original inspiration was to improve the techniques for formally verifying systems of unbounded size, e.g., a bus protocol designed for an arbitrary number of nodes or processes, which are considered in the case study project at ABB, or in the effort to verify Erlang code. Through a sequence of papers, the approach was distilled and generalized, so that it is now formulated in basic automata-theoretic terms. It extends the techniques of basic automata theory by a powerful technique for computing, e.g., the set of configurations that may occur in a run of a Turing machine. The new general formulation is able to handle not only systems with an arbitrary number of components, but also several unbounded data structures, such as arrays, queues, and stacks.

We are applying techniques, developed within the formal verification, to improve techniques for testing of software. Techniques have been developed for translating formal specifications into so-called test oracles, i.e., programs that observe the specified system during testing and report when requirements are violated. Such translations exist in automated verification tools, such as UPPAAL, but they are also finding other applications. Among our contributions is to consider new types of constructs in formal specifications, which are relevant for embedded systems, for communication software, and for WWW-based internet services. Such a translation can potentially save much effort in writing test programs or test scripts, and they link requirements to the actual system behaviour in a direct way.

Programming Language Implementation and Compilation

The area is concerned with the implementation and use of high-level (concurrent) programming languages, together with the development of system software tools such as compilers for (time- or space-) efficient execution of programs written in these languages and code generation for different computer architectures.

The biggest effort in this area has been centered around the Erlang language. Erlang is a concurrent, strict, functional programming language designed to ease the development of large-scale distributed control applications. So far, it has been used quite successfully in the telecommunication industry, both within Ericsson Telecom, where it was designed and developed, and by other companies (both within Sweden and internationally). This has happened despite the fact that Erlang implementations are based on emulators of virtual machines and their performance is slow, even compared to implementations of other functional languages.

The work aimed to improve the performance characteristics of Erlang implementations has concentrated on the development of the **HiPE (High Performance Erlang)** system. HiPE is an efficient just-in-time native code compiler for Erlang programs incorporating many compiler optimizations which have been proven successful in the context of similar programming languages. In addition, many other compiler techniques have been adjusted and sometimes developed taking the characteristics of Erlang into account. These include support for concurrency, communication, distribution, fault-tolerance, on-the-fly code reloading, automatic memory management, and preservation of tail-recursion in the context of a mixed mode (i.e., emulated and native code) execution. The HiPE system, based on Open Source Erlang (OSE), has been publicly released as open-source in March 2000. It is currently the fastest Erlang system and is competitive in performance with implementations of other functional programming languages such as Concurrent ML.

During the last year, the "HiPE group" has also initiated stronger contacts with the Erlang/OTP development teams which are responsible for the Open Source Erlang implementation. This cooperation has already resulted in important technology transfer from academia to industry: a new data representation which removes the address limitations of OSE has been incorporated in Ericsson's current development version released in September 2000 (see also www.erlang.se). Other efforts are currently underway to transfer more technology and successful compilation techniques from HiPE to OSE. The eventual goal is to merge the two systems.

The WPO (whole program optimization) project has focused on the development of compiler optimization techniques for embedded systems. In embedded systems, memory is an expensive and sometimes limited resource, and thus it is desirable to find techniques that lower the hardware costs by reducing memory usage of programs for embedded system through efficient memory allocation techniques and code compression. In the context of this effort, algorithms for code compaction through a technique called procedural abstraction have been investigated. In procedural abstraction, the program control flow graph is scanned for semantically equivalent graph fragments, which are then factored out into a new procedure. The project has investigated the effectiveness and advantages of applying procedural abstraction at the level of intermediate code. It was found that doing so provides opportunities for more powerful code compaction by e.g., not interfering or be negatively influenced by the effects of register allocation or of other compiler optimization steps.

In order to correctly evaluate the effectiveness of the new compilation techniques developed, ASTEC projects have collected source code from industry sources and used them to evaluate tools and drive research in directions relevant for industry. The work has also generated two publications regarding how to benchmark tools for embedded systems.

Real-Time Distributed Systems

This area considers the particular challenges that arise when building embedded real-time and distributed systems. The emphasis is on the needs of software that operates under tight timing constraints and with high requirements for correctness. Analyzing and verifying the timing aspects of a system is the least understood and thus the most difficult part of developing embedded real-time systems. Reliable estimates of computation times are necessary for scheduling and resource allocation, and for analyzing whether a program will meet all deadlines.

ASTEC has produced a sequence of results related to the problem of calculating the worst-case execution time (WCET) of a code module. The main industrial partner is IAR systems, and the ultimate goal is to integrate WCET analysis into a commercial tool for development of embedded systems.

The WCET research in ASTEC has proposed an architectural framework for how to integrate the WCET calculation into a development tool used for real-world programs, and used this architecture as driver to generate research problems and to integrate research results. Part of the framework consists of target- and method-independent data representations which help making WCET tools retargetable and flexible. The initial steps in the framework were formulated in the M.Sc. thesis of Jakob Engblom (at ASTEC), which received the SNART award for best real-time M.Sc. thesis in Sweden in 1998.

On the software side, the execution time of a program depends primarily on the program flow and the timing aspects of the hardware used to run it. In Jan Gustafsson's Ph.D. thesis, it is demonstrated how techniques used for flow analysis in compiler research, such as abstract interpretation, can be employed to automatically extract flow information of a program, which is an important step towards an automatic WCET analysis tool.

On the hardware side, in order to yield reasonable and safe execution time estimates for a code module, the timing effect of processor pipelines must be addressed. A conceptually simple but powerful technique for analysing the effect of pipelines has been developed. The technique makes it easy to integrate the results of high-level program flow analysis and analysis of cache memories. Since the technique only depends on having a cycle-accurate simulator for the CPU available, it can easily be ported to new target architecture, which is very important in the highly fragmented embedded systems market.

Novel tool technology like WCET also needs appropriate packaging as a product in order to become mainstream. To better understand the needs of engineers in the field and guide research in relevant directions, a questionnaire and interview survey was conducted in 1997. We investigated the current methods for timing analysis in industry and the requirements on a static WCET tool.

Given information about the timing of each program part, analyzing the interaction between different nodes in a real-time distributed system is a very difficult problem. Here, the UPPAAL tool has been used in several case studies, reported in earlier sections, to show how such problems can be tackled analytically instead of using extensive testing (which is inherently unsafe and thus unsatisfactory for safety-critical systems).

Some Selected Highlights.

A few of the most interesting achievements in fundamental research are

- The result on the use of SAT-solvers for symbolic verification techniques for finite-state systems. The paper on the tool FixIT received the best paper award of EAPLS -- the European Association for Programming Languages and Systems, at the ETAPS conferences in 2000. The ETAPS conferences receive a total of several hundred submissions.
- Flexible techniques for calculation of pipelines on execution times of programs
- The development of the regular model checking paradigm,

The following achievements in building tools for the Erlang language should be put forward.

- The HiPE compiler, which has been publicly released, and
- the Erlang Verification Tool.

Very interesting case studies have also been carried out. We want to put forward

- the modeling and verification of a large bus protocol at ABB, which is in industrial use,
- compilation and benchmarking of the AXD/301 ATM Switch, and
- formal verification of a core part of the Mnesia distributed database in Erlang.

Short data for each project can be found in Appendix 4.

The ASTEC publications can be found in Appendix 5 .
In ASTEC business ratios (Appendix 1) is a summary of publications and degrees over the years shown**.**

B.4. Degrees

A list of degrees is included at the end of the publication list in Appendix 5. In ASTEC business ratios (Appendix 1) is a summary of degrees over the years shown.

B.5. Education and Training Activities

ASTEC has contributed to the development and execution of courses within its area.

- Upper-level undergraduate and graduate courses have been developed and given on Testing and Verification, Real-Time Systems, Compiler Technology, and Theory of Distributed Systems, by senior researchers in ASTEC.
- A national graduate course on *modeling and analysis of Real-Time Systems* has been developed and conducted (in collaboration with ARTES)
- In collaboration with ASTEC companies, one-semester project courses, with 20 participating students, have been conducted. It will most likely be given regularly in the future.
- ASTEC Companies are providing many guest lecturers for undergraduate courses given at Uppsala University and KTH, which helps to bring industrial aspects into university education and providing students with some impression of the realities of software development practice. For example, senior scientists at Prover Technology AB give lectures at the courses on Programming Theory and Software Engineering, and IAR Systems gives lectures in Compiler- and Real-Time courses.

C. Industrial Relevance, Benefits and Effects

C.1. Industrial Involvement and Interaction

The industrial involvement in ASTEC has increased during the last 3 years when measured as *in natura* and cash contributions (see figure). The number of companies has grown from 6 initially to 10. The industrial involvement is particularly strong on the level of individuals: many companies have reorganised and changed names during the period, but the involved personal contacts has been increasingly strong and expanding.

A company UPAAL AB was started in 1999, to a large extent because of experiences from previous projects and to take on new tasks. It is to provide consulting service in the area of modeling and verification of timed systems. The long-term goal

Industrial contributions to ASTEC
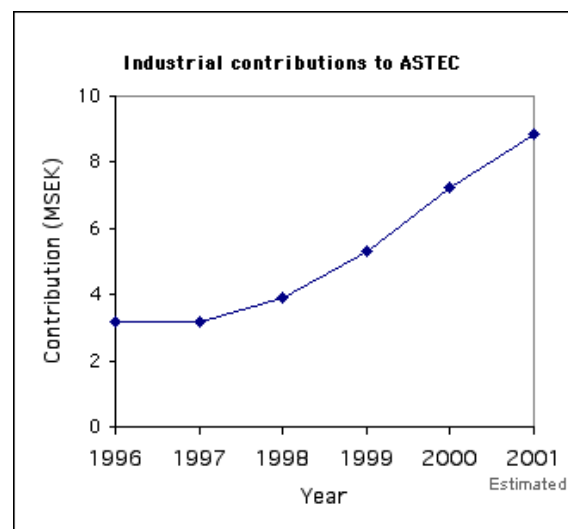
is to develop and commercialize UPPAAL as a plug-in tool for verification and debugging of real time embedded systems.

Two companies has left the centre after the first phase. Rational Software Scandinavia AB (initially Objectory AB) moved research and development from Sweden to the US, and consequently withdrew from ASTEC. Ericsson Radio AB was initially involved in a case study, one of whose conclusion was that the technique applied in ASTEC performed well on one case study but would probably not perform as well on other important future applications.

Mobility between academia an industry is examplified by the following.

- Currently, the centre employs 3 industrial Ph.D. students (Jakob Engblom, Johan Runesson, Jan Sjödin). The students are employed half-time by a company in order to carry out their Ph.D. work in collaboration with the company. A 4th position has been announced and is being filled.

- Senior researchers at companies are making substantial contributions to projects.

- Senior academic researchers have moved to industrial partners. Examples are Thomas Lindgren and Ken Tindell, who are now valuable connections and discussion partners in industry

- A number of M.Sc. graduates have moved to ASTEC industrial partners.

C.2. Industrial Partners' Expectations

From the companies own statements (Appendix 6), it is clear that the main expectations were

- to get in contact with state of the art research and techniques
- to benefit from these contacts
- to solve complex problems in simple ways, for specific info see Appendix 6
- to find new ways to solve problems

The fulfilment of the expectations is presented in sections C.3. and C.4.

C.3. Commercialisation and Technology Transfer Activities

Preparations for achieving a more full-scale technology transfer are in progress for several ASTEC projects. In spring 2000, Jan Sjödin and Jakob Engblom have developed a technology demonstrator which integrates research results into a commercial compiler at IAR Systems. The purpose is to demonstrate the potential of the technology and provide input for concrete product plans that exploit the results of the WPO and the WCET projects. An analogous development is foreseen for the HiPE system.

An industrial success story is the development of BUTLER by Mecel, partly performed within the *Auto* project of ASTEC. BUTLER is a tool set for structuring requirements and design models for automotive systems. Recently a start-up company, named *Systemite*, based on BUTLER has been established by the main developers of BUTLER.

C.4. Industrial Benefits

The benefits to companies are of many different forms. ASTEC has allowed companies to gain knowledge about new technology and its potential applications. As an example, Ulf Hammar, ABB Automation Products AB, states "Very soon we found errors in the protocol even though the model was small and implemented in a few hours. We plan to introduce the use of UPPAAL in our organisation" in appreciation of the working of a new technology. Thomas Arts, Ericsson writes "ASTEC brought, above all, much knowledge into Ericsson... The area of Software

Verification is a rather new one and Ericsson has to stay upto date w.r.t. the developments in this field. The ASTEC cooperation is a perfect way for that". An unexpected benefit from the collaboration was that the project contributed in obtaining a patent for a software solution: "The cooperation also pointed out an application area for software verification, viz. software patents, which had not yet been in the picture before."

ASTEC work has also provided concrete solutions to company problems, "HiPE has been highly beneficial to us at Ericsson Utvecklings AB where we develop the Erlang/OTP product. During the six months of year 2000 we have achieved very concrete results in a short time thanks to assistance from HiPE." writes Kenneth Lundin, Ericsson Utvecklings AB.

Discussions conducted within ASTEC have generated contacts and ideas that resulted in industrially successful projects. An example is an M.Sc. project in collaboration between Volcano Communication Technologies and Mälardalen University, which developed new algorithms for scheduling analysis that are now incorporated into Volcano products.

An appreciated benefit is the potential for contacts with the international scientific community. As examples, six researchers in ASTEC's network of contacts from Korea, USA, Germany, and the UK have held research seminars at IAR Systems in conjunction with visits to Uppsala. Some presentations have concerned direct commercial collaboration.

One of the major advantages of ASTEC is its building of stable and long-term contacts between industry and academia. As Olle Landström, IAR System AB, writes: "The best results come from the projects not originally planned for but emerging in the creative environment where researchers meet the industry based developers."

Appendix 6 collects some statements from companies within ASTEC.

Appendices

1. ASTEC business ratios
2. Partners and persons Phase 2
3. Financial report phase 2
4. Project descriptions
5. Publications
6. Industrial partners statements at mid-term evaluation.

Appendix 1

Business ratios for ASTEC 1995 - 2000

ASTEC business ratios are calulated from the costs and activities each year. There is no profit within ASTEC. The research results are transferred to the participating companies that may profit from them and according to the contracts share the profit with the researchers.

 The following tables and figures i summarized here.

The contributions to ASTEC has increased for the first 5 years (1a, b). The last two years increase is partly due to increased contributions by NUTEK. Their contribution will level out at 6 MSEK per year during phase 3.

Management costs has increased in absolute values but declined relative to total costs since 1997 (1a). Extraordinary management costs of 250 KSEK for evaluation and Competence center day year 2000 are not included. Management includes all expences exept direct research.

The cost for each man-year decreased to 55% of its inital value in 1998 and has since then been rather contant (1a).

The amount of work carried out (man years) has increased with about 40% per year during the 5 years (2a). During year 2000 there were large increases in the categories Professors, Industry researchers, Industry PhD students and Master of Science students (2b). Technical/administrative staff has decreased each year (2b).

The publication rate has increased and the cost per publication has gone down (1a, 3a,d). The major publication type in this field of research is conferences (with referee system), technical reports and workshops(3a,b). There were large increases in conference and degree publications year 2000 (3a,b). The time requirement per publication reflects the initiation of new projects at the start of phase 1 and 2 (3c).

ASTEC

1a) **ASTEC Business Ratios**. The contributions by ASTEC parts, Management, Man power and Publication form the basic data for; the cost per man year (KSEK/man year); the publication cost (KESK/publkication); the effort per publication (man years/publication); the relative management cost (Management/Total).

Contributions by	Year					Sum
	1995-96	1997	1998	1999	2000	
INDUSTRY	3568	2778	3520	5293	7219	22378
ACADEMY	2375	3450	2347	4557	4688	17417
NUTEK	2295	3395	3134	5202	6869	20896
Total (KSEK)	8238	9623	9001	15053	18777	60691
Management (KSEK)	380	818	721	1038	1066	4023
Man power(man years	6,0	9,1	12,5	17,5	25,0	70,1
Publications (no.)	8	19	12	22	36	97
						Mean
KSEK/man year	1371	1054	719	858	753	865
KSEK/Publication	1030	506	750	684	522	626
Man years/publication	0,75	0,48	1,04	0,80	0,69	0,72
Management/Total	5%	9%	8%	7%	6%	7%

1b) **The development of contributions to ASTEC by NUTEK, Academy and Industry.**

ASTEC contributions year 1-5
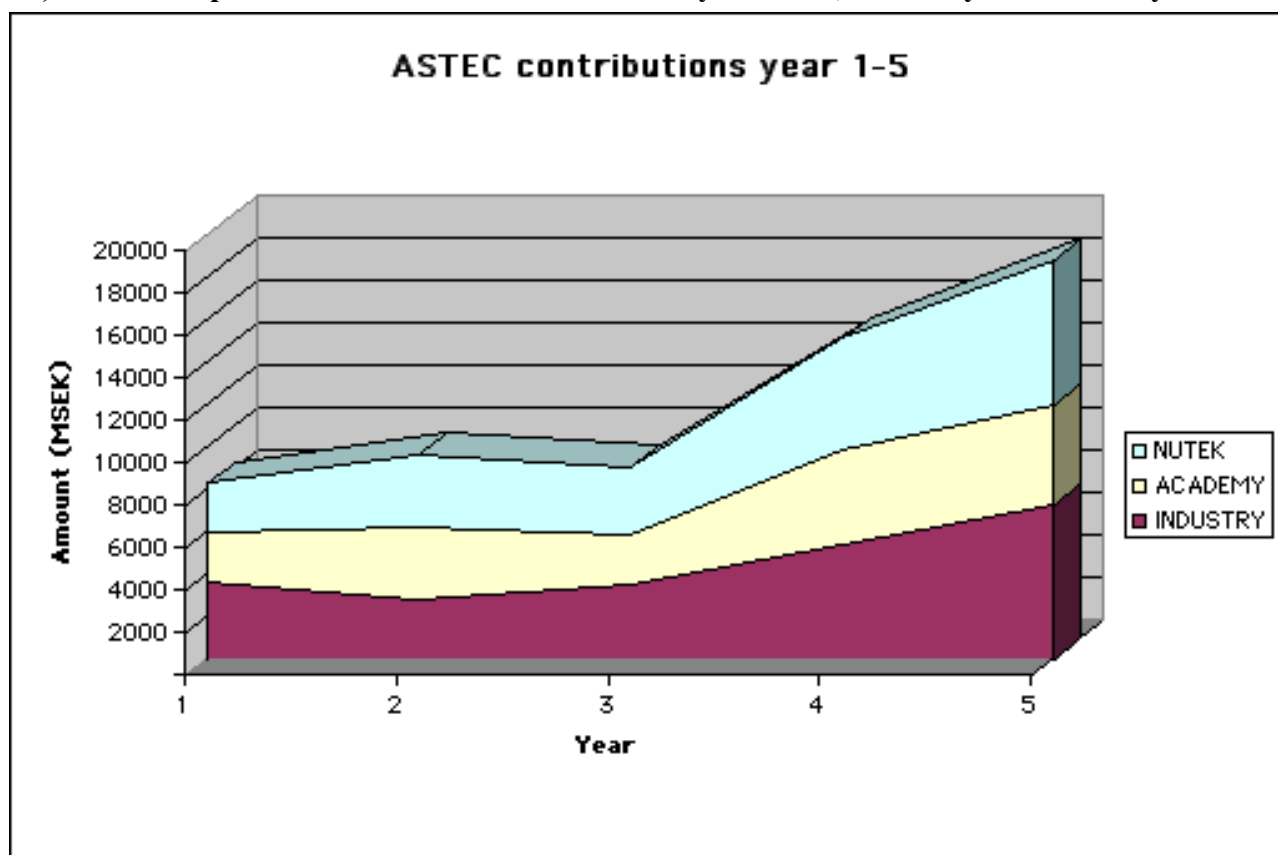
**2a) Development of ASTEC man years, note the rate increase.**
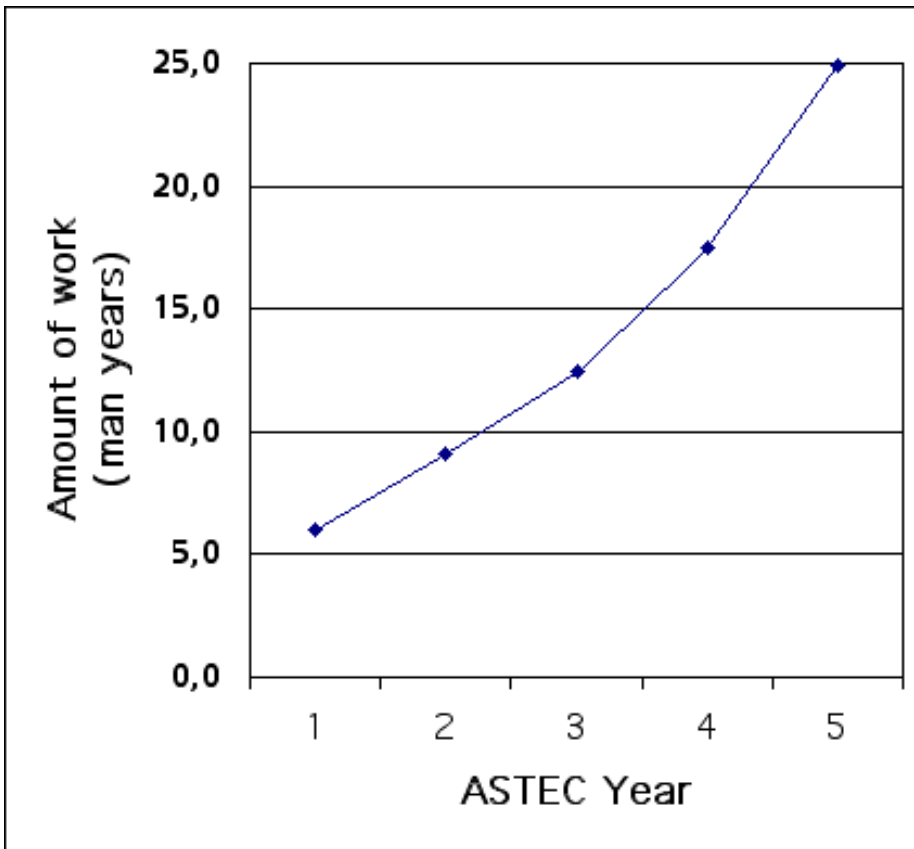
2b) Development of ASTEC staff categories, note the recent increase in Professors, Industry researcher and PhD-students and M.Sc. students.

Category	Amount each year (man years)				
	1995-1996	1997	1998	1999	2000
Professor	0,5	0,3	0,6	0,6	2,1
Senior researcher	1,2	2,1	2,5	4,1	2,8
PhD student	3,3	4,1	6,3	7,1	9,0
Industry researcher	1,0	1,7	2,2	2,1	3,8
Industry PhD students				2,0	3,0
Master of Science students				1,0	3,9
Technical/administrative		1,1	1,0	0,6	0,5
Total=	6,0	9,1	12,5	17,5	25,0
Increase each year (man years)	-	3,1	3,4	5,0	7,4
Increase each year (%)	-	52%	37%	40%	42%

Publications and exams

3a) Publication rate, note the increase and the shift from phase 1 to phase 2 1997-1998.

Development of ASTEC publication
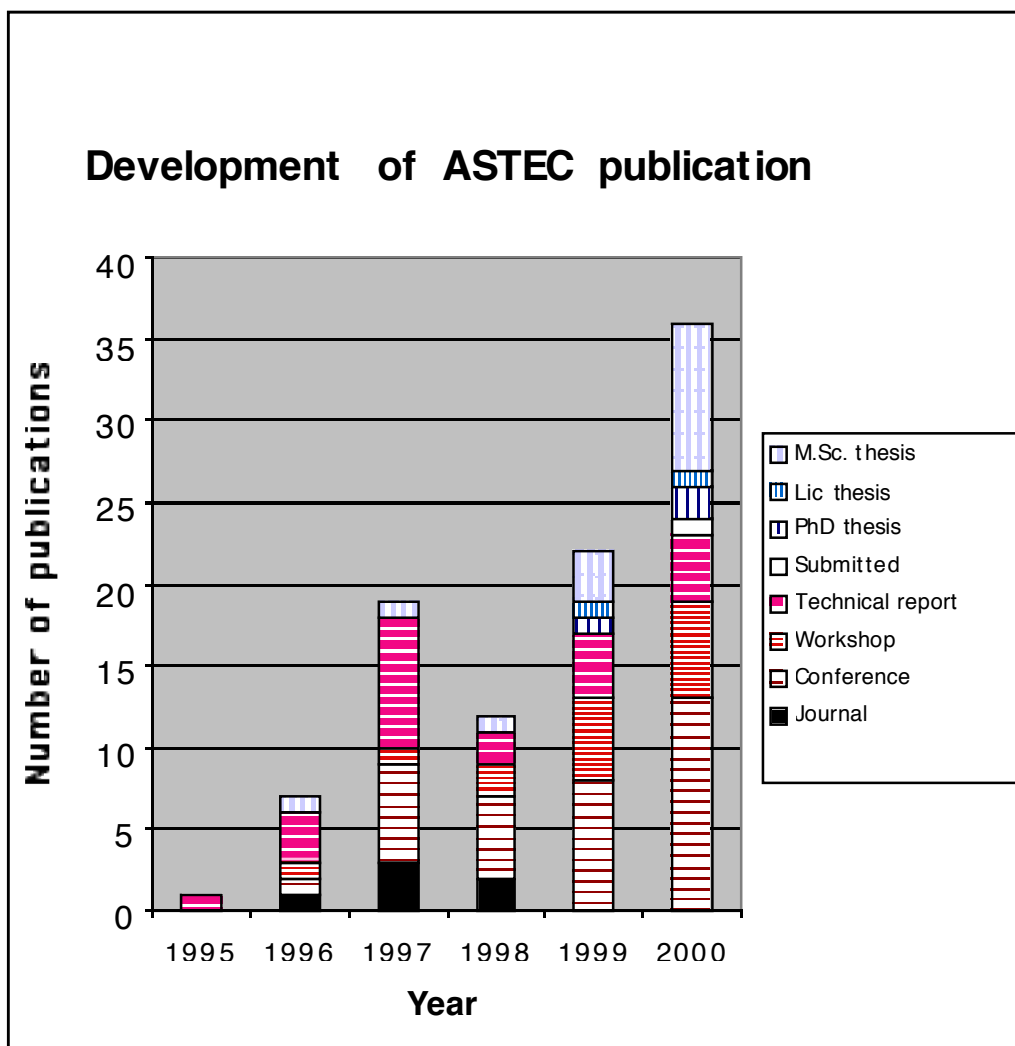
3b) Publication divided into differernt publication categories, note that conference, technical reports, workskop and theses are dominating.

Publications type	1995	1996	1997	1998	1999	2000	Sum
Journal	0	1	3	2	0	0	6
Conference	0	1	6	5	8	13	33
Workshop	0	1	1	2	5	6	15
Technical report	1	3	8	2	4	4	22
Submitted	0	0	0	0	0	1	1
PhD thesis	0	0	0	0	1	2	3
Lic thesis	0	0	0	0	1	1	2
M.Sc. thesis	0	1	1	1	3	9	15
Sum	1	7	19	12	22	36	97

3c) Time requirement and cost per ASTEC publication, note the decrese in time per publication as a new phase develops. Phase 1 started 1995 and phase 2 started 1998.
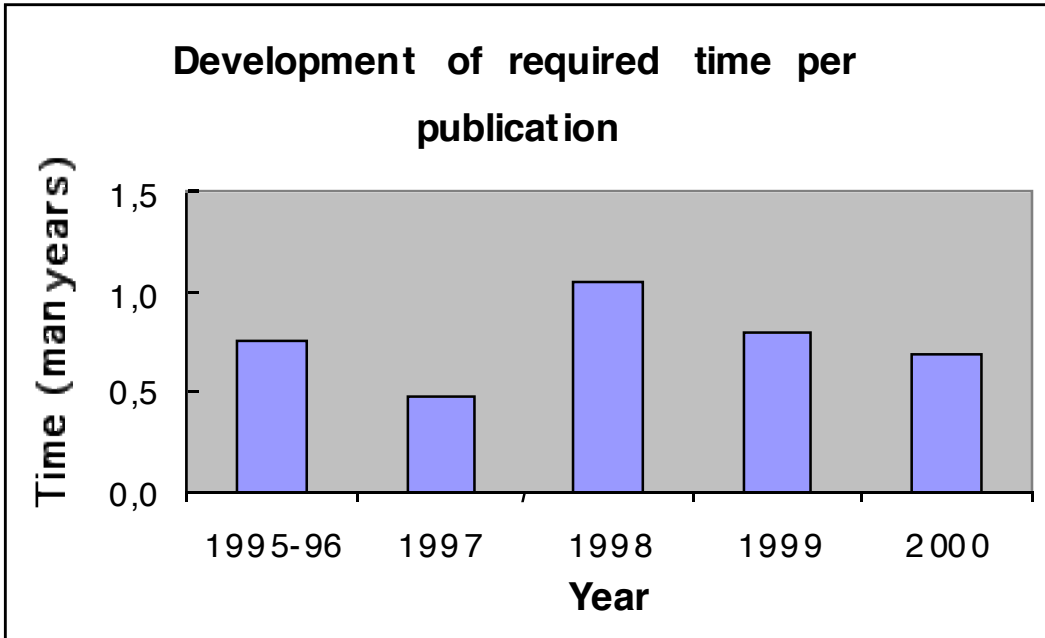
3c) The cost per ASTEC publication, note the decrease in cost per publication over time.
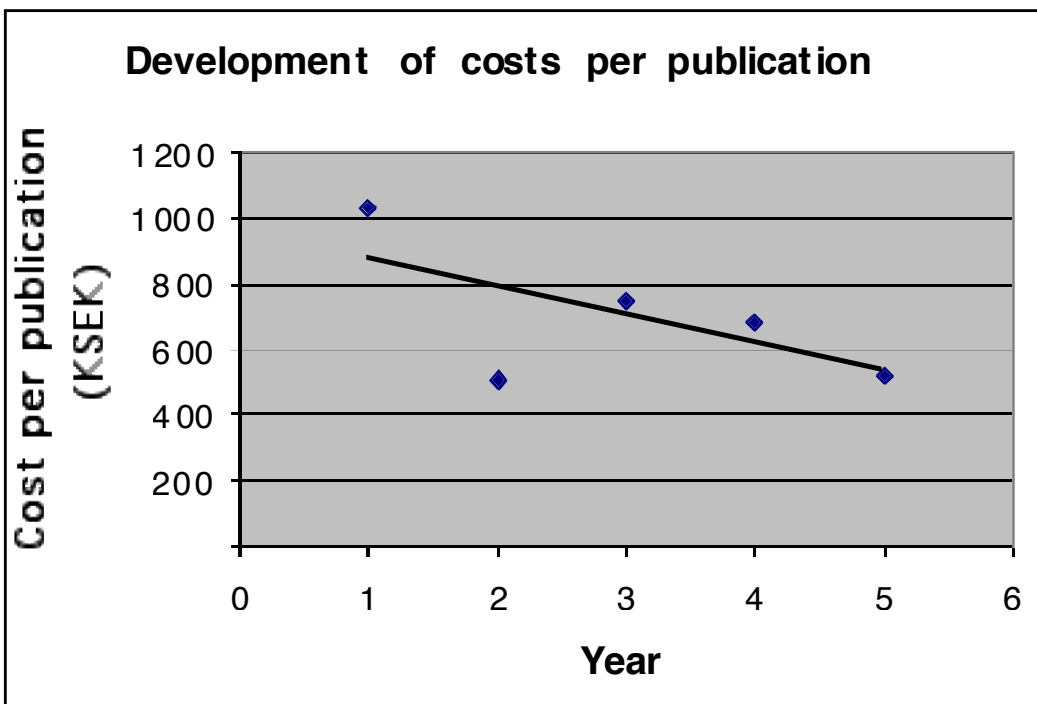
ASTEC Partners and Persons Phase 2

Academic research groups 1999-2000

1. Uppsala university   , Department of Information Technology
   The Hard Real-Time group
       Leader: Professor Hans Hansson
   The Formal Verification Group
       Leader: Professor Parosh Abdulla and Bengt Jonsson
   The UPPAAL group
       Leader: Professor Wang Yi
   The Programming Language and Implementation Group
       Leader: Dr. Kostis Sagonas
2. SICS (Swedish Institute of Computer Science)
   Code Verification Group
       Leader: Dr. Dilian Gurov
3. Mälardalen University   , Department of Computer Engineering
   The Computer Science Laboratory
       Leader: Professor Björn Lisper

ASTEC industry partners 1999-2000

Industry	Employees
ABB Automation Products AB	1400
Ericsson Utvecklings AB	1200
IAR Systems AB	111
Mecel AB	140
Prover Technology AB	50
Telia Validation AB	500
Telelogic AB	850
UPAAL Sweden AB	0
Volcano Communication Technologies AB	21
Volvo Teknisk Utveckling AB	400

Industry Interest per Research Area	Validation and Verification Technology	Programming Languages and Implementation Technology	Technology for Real-Time Distributed Systems
Datacom and Telecom Applications	ABB, Ericsson, Prover, Telelogic, Telia, Volvo	Ericsson	ABB, Prover, Telelogic, Telia, Volvo
Automotive and Vehicle Applications	Mecel, Prover, Telelogic, Telia, Volvo	IAR, Volcano Com. Tech.	IAR, Mecel, Prover, Telelogic, Telia, Volvo

The participating companies 1999 - 2000, interest per research area.

Persons involved in ASTEC during 1999-2000 (Phase 2)

The amount of work carried out has been increasing with about 40% each year for the last three years. During Phase 2 has 57 persons been directly involved in ASTEC including the board. Three new board members Martin Eriksson, Erik Hagersten and Björn Lisper were appointed 2000-01-01.
Comments : The amount of Professor involvement increased year 2000 partly due to changes at the Universities so that Professor competent researchers could also obtain the title; note the corresponding decrease in senior researchers. There were industrial PhD and MSc students before 1999 but they were not shown separately. However during year 2000 a substantial increase in both categories has been obtained.

ASTEC board

Name	Affiliation	Period
Ewert Bengtsson	Uppsala University	990101 to 991231
Bjarne Däcker	Ericsson Utvecklings AB	990101 to present
Martin Eriksson	Validation AB	000101 to present
Erik Hagersten	Uppsala University	000101 to present
Seif Haridi	SICS/KTH	990101 to 991231
Sten Hellström	Mecel AB	990101 to 001208
Olle Landström	IAR AB	990101 to present
Björn Lisper	Mälardalen University	000101 to present
Åke Sandberg	Telia Validation AB	990101 to 991231

ASTEC scientific advisory board

Prof. Neil Jones	University of Copenhagen
Prof. Bernhard Steffen	University of Dortmund
Prof. Neeraj Suri	Chalmers University of Technology

The number of persons each category involved in ASTEC during1999-2000.

(board not included).

Category	no.
Professor	5
Senior researcher	5
PhD student	11
Industry researcher	11
Industry PhD students	3
Master of Science students	11
Technical/administrative	3
Total=	49

Amount of work carried out within ASTEC.

Category	Amount each year (man years)				
	1	2	3	4	5
Professor	0,5	0,3	0,6	0,6	2,1
Senior researcher	1,2	2,1	2,5	4,1	2,8
PhD student	3,3	4,1	6,3	7,1	9,0
Industry researcher	1,0	1,7	2,2	2,1	3,8
Industry PhD students				2,0	3,0
Master of Science students				1,0	3,9
Technical/administrative		1,1	1,0	0,6	0,5
Total=	6,0	9,1	12,5	17,5	25,0
Increase each year	-	3,1	3,4	5,0	7,4
Increase each year (%)	-	52%	37%	40%	42%

- Uppsala University
  - Department of Information Technology
    - ASTEC

ASTEC Financial Report Phase 2

Costs compared to contract for Phase 2 (1999-2000).

The amount of contributions from the parts follow the planned proportions according to the ASTEC agreement for 1999-2000. The total amount for 1999 were 8% lower than calculated, this has been compensated for by increased activity 2000. Ericsson Utvecklings AB has contributed with 3200 kkr in cash; all other industry contribution were emoluments paid in kind. A special funding of 250 kkr was received from NUTEK for the Competence center day and evaluation during 2000, this has not been included in contract money but otherwise it is included below.

Part	Contract	%	Cost	%
Industry	12200000	36	12512295	37
Uppsala Universitet	9530000	28	9245489	27
NUTEK	12000000	36	12071660	36
Sum	33730000	100	33829443	100

Contributions by ASTEC industrial parties compared to the contract.

Industry	Contract (SEK)	Cost	Changes (%)
ABB Autom. Prod. AB	170000	327400	93
Ericsson Utvecklings AB	4100000	4910000	20
IAR Systems AB	3600000	4258763	18
Mecel AB	900000	824601	-8
Prover Technology AB	720000	515281	-28
UPAAL Sweden AB	300000	0	-100
Telelogic AB	780000	168750	-78
Telia Validation AB	1350000	1350000	0
Volcano Com. Tech. AB	100000	0	-100
Volvo Tech. Dev. AB	180000	157500	-13
Sum	12200000	12512295	3

Proportion of costs on ASTEC programme areas compared to budget.

ASTEC COSTS 1999-2000 per Research Area	Validation and Verification Technology	Programming Languages and Implementation Technology	Technology for Real-Time Distributed Systems	Sum
Datacom and Telecom Applications	26,8	17,4	4,9	49,1
Automotive and Vehicle Applications	9,1	21,6	20,2	50,9
Sum	35,9	39,0	25,1	100,0

ASTEC Budget 1999 per Research Area	Validation and Verification Technology	Programming Languages and Implementation Technology	Technology for Real-Time Distributed Systems	Sum
Datacom and Telecom Applications	28,2	15,2	6,4	49,9
Automotive and Vehicle Applications	11,5	17,5	21,2	50,1
Sum	39,6	32,8	27,6	100,0

Management, administration and network activity costs

The cost for mangement is not fully visible since there is no compensation for the part carried out by the board. The director´s time is mainly a part of Uppsala Universitys contribution. The cost for management and administration has been as budgeted for 1999 and slightly lower than planned during 2000 due to possibilities for coordination with other tasks at the University and reimbursement by NUTEK for costs at Competence center day 2000 and evaluation. The cost for 1999-2000 were 2362 kkr   including support to network activities such as conference NWPT 99, Competencecenter day 2000, evaluation of both ASTEC and SUMMIT, seminars, project leader meetings and visiting scientists.

Funds 2000-12-31 and the planned use of these

At the start of Phase 2 (1998-12-31) were 538 756 SEK available. At the end of the phase were 4 623 503 SEK available. However of these funds were 3 MSEK obtained during dec 2000 for phase 3, and 750 627 SEK are reserved for phase 2 costs. The remaining 872 876 SEK is planned to be used during phase 3. This has been discussed with NUTEK during the planing of Phase 3 and at board meetings.

Remaining funds 2000-12-31		Reserved funds	
Within ASTEC	3717096	For Phase 3	3000000
within projects	906407	For projekts	290000
Sum	4623503	Within projekts	436106
		Evaluation of SUMMIT	24521
		Advance from contributors 2000-12-31	872876
		SUM	4623503

- Uppsala University
  - Department of Information Technology
    - ASTEC

ASTEC Projects

- **Auto: A design methodology for embedded real-time systems**
  This project takes a broad view on the development of embedded real-time systems. The main focus is on
    - techniques for describing functional modules of a design and their relationships,
    - methods for mapping a network of connected functional modules onto a distributed target architecture. Important aspects are resource sharing, resource allocation and scheduling.

  A starting point is the software development method BASEMENT proposed in the VIA project, which includes an outline of a signal-flow based design language.
  Participating industries: Mecel AB.

- **SMC: Symbolic Model Checking Using Stålmarck's Method**
  The goal of the project is to extend the applicability and efficiency of model checking algorithms. The main approach is to consider an alternative approach for symbolic verification by using SAT-solvers such as Stålmarck's method, instead of BDDs as a search engine in model checking.
  The main issues are
    - to design methods that scale for large and complex system models, in particular for control systems, signalling systems, hardware circuits, etc.
    - to make analysis as complete and powerful as possible in the case that complete coverage of the system model is impossible.

  The work will be based on Stålmarck's method for proving large formulas in propositional logic and in restricted fragments of first-order logic.
  Participating industries: Prover Technology AB.

- **BUS: Modelling and analysis of a bus protocol**
  This project is primarily a case study. It aims at modeling and analyzing a bus protocol, developed and implemented by ABB Automation Products, using state-of-the-art model checking tools, primarily UPPAAL. The purpose is
    - to construct an abstract model of the protocol, and finding sources of potential execution problems.
    - using the experiences gained in the case study, to develop further the general methodology for modeling bus protocols, and the tool support for analysis.

  Participating industries: ABB Automation Products AB, UPAAL Sweden AB.

- **Automated Testing**
  This project aims at further development of techniques for automated testing of software systems. Issues to be addressed include:
    - Automated generation of test suites from requirements on software.
    - Selection and Assessment of test suites.
    - Investigation into the relationship between requirements and test suites.

  The project will make a number of studies on how testing can be automated in collaboration with different industrial partners.
  Participating industries: Telelogic AB, Telia Validation AB and Volvo Teknisk Utveckling AB.

- **ErlVer: A Verification Method for Erlang**
  This project develops a methodology which consists of the following.

- On the theoretical side, of an operational semantics, property specification language based on temporal logic, and a proof system for Erlang.
  - On the practical side, of a tool set that supports verification of properties by means of a proof assistant, extended with a graphical user inteface, and with considerable support for proof automation.
  - Evaluation of the approach using a range of case studies in telecommunications systems, kindly submitted by Erlang software developers.

  Participating industries: Ericsson Utvecklings AB.

- SA: Analysis of types and process topology for static debugging
  This project develops a method and an implementation for analysis of the Erlang programming language. The analysis is intended to give information similar to that of a static typing system, helping the programmer to validate and debug a program while it is being constructed. The approach is specifically aimed at handling features that are characteristic of Erlang and telecommunications programs, such as processes and communication. The analysis is also intended to provide information to an Erlang compiler, which can be used for compilation.
  Participating industries: Ericsson Utvecklings AB.

- HIPE: High Performance Erlang
  The project aims at developing techniques for efficient compilation of concurrent functional programming languages. The project focuses on the Erlang language. Within the project, the following issues are addressed.
  - Techniques for efficient compilation of programming language features and abstractions that are prominent in communication software, such as process communication, process creation and code replacement. Efforts should be guided by the characteristics of realistic industrial applications.
  - Methods for measuring usage characteristics and execution properties of software, which is useful for guiding optimization efforts
  - Evaluation on industrial-size programs found in telecommunications systems, such as ATM switches and WWW servers.

  The project is based on the current development of a compiler for Erlang, currently being developed at Uppsala University. This compiler is a platform for experimenting with optimizations, and for application to industrial-size programs, which exist today.
  Participating industries: Ericsson Utvecklings AB.

- WPO: Whole-Program Optimization in Compilers for Embedded Systems
  This project addresses
  - Methods for automated and efficient compilation of code to meet stringent constraints on memory, power, timing, and irregular hardware architectures.
  - The target applications are taken from small embedded programs.
  - The approach to solve this problem is to develop static analysis methods that consider the entire program. The entire application is analyzed and optimizations are performed based on the information obtained. In the embedded market, the normal applications are small enough for this approach.

  The goal should be "keyword-free programming", in which the compiler relieves the programmer from the burden to optimize for particular features of the platform. Techniques for automatically generating efficient optimized code for a variety of hardware platforms shall be developed.
  Participating industries: IAR Systems AB.

- WCET: Calculation of Worst-Case Execution Times
  The project addresses static analysis of programming languages and hardware in industrial use, in order to extract information about the execution time of code fragments. This information is of vital importance for the development of predictable embedded and real-time systems.
  This project addresses three main areas:
  - Static and automatic analysis of program flow, in order to determine the worst possible program executions without manual intervention.

Examples of problems that are attacked is recursion, loops, and inheritance in object-oriented languages.

○ Analysis of hardware features like pipelines, caches, and external memory, to provide timing estimates on the level of single clock cycles.

○ The combination of flow information and hardware information to calculate final execution time estimates, including how to account for compiler optimizations that makes the relation between source code and object code complex.

Participating industries: IAR Systems AB and Volcano Communications Technologies AB.

ASTEC publication list 2001-04-03   Appendix 5

Number of publications in different categories.

Journal publications	10
Conference publications	33
Workshop publications	16
Technical reports	23
Submitted publications	1
PhD theses	3
Lic thesis	2
M.Sc. theses	15
SUM	103

Publications in refereed scientific journals

Altenbernd, P. and Hansson, H. 1998. The Slack Method: A new method for static allocation of hard real-time tasks. Real-Time Journal, Kluwer, ASTEC Report 97/12 15(2) .

Arts, T., Chugunov, G., Dam, M., Fredlund, L., Gurov, D. and Noll, T. 2001. A Tool for Verifying Software Written in Erlang. International Journal on Software Tools for Technology Transfer, accepted .

Dam, M. 2001. Proof System for pi-calculus Logics. To appear. de Queiroz (ed.), "Logic for Concurrency and Synchronisation", Studies in Logic and Computation, Oxford

Univ Press. .

Engblom, J., Ermedahl, A., Sjödin, M., Gustafsson, J. and Hansson, H. 2001. Worst-Case Execution-Time Analysis for Embedded Real-Time Systems. International Journal on Software Tools for Technology Transfer, accepted .

Gustafsson, J. and Ermedahl, A. 1998. Automatic derivation of path and loop annotations in object-oriented real-time programs. Journal of Parallel and Distributed Computing Practices 1 (2) 61 - 74.

Hansson, H., Lawson, H., Bridal, O., Eriksson, C., Larsson, S., Lönn, H. and Strömberg, M. 1997. BASEMENT: An Architecture and Methodology for Distributed Automotive Real-Time Systems. IEEE TC 46(9) 1016-1027.

Hansson, H., Lawson, H., Strömberg, M. and Larsson, S. 1996. BASEMENT a distributed real-time architecture for vehicle applications. Real-Time Systems 11223-244.

Hansson, H., Sjödin, M. and van der Velde, H. 1997. CAN-based Real-Time Lab Environment. CAN Newsletter 3 48-49.

Johansson, E., Pettersson, M., Sagonas, K., and Lindgren, T. 2001. The Development of the HiPE System: Design and Experience Report. International Journal on Software Tools for Technology Transfer, accepted .

Lindahl, M., Pettersson, P., Yi, W. 1997. Formal Design and Analysis of a Gear-Box Controller: an Industrial Case Study using Uppaal. ASTEC Report 97/09, 4th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). Gulbenkian

Foundation, Lisbon, Portugal, 1998. and in LNCS vol 1384, and in International Journal on Software Tools for Technology Transfer (STTT), 1998 .

Publications in refereed scientific conferences

Abdulla, P. A., Bjesse, P. and Eén, N. 2000. Symbolic Reachability Analysis Based on SAT-Solvers. In Proc. International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS) .

Abdulla, P. A., Bouajjani, A., Jonsson, B. and Nilsson, M. 1999. Handling Global Conditions in Parameterized System Verification. In Proc. 11th Int. Conf. on Computer Aided Verification LNCS1633 134-145.

Abdulla, P. A., Iyer, P. and Nylén, A. 2000. Unfoldings of unbounded petri nets. In Proc. 12 Int. Conf. on Computer Aided Verification, Lecture Notes in Computer Science 1855 495-507.

Amnell, T., David, A. and Yi, W. 2000. A Real Time Animator for Hybrid Systems. In Proc. 6th ACM SIGPLAN LCTES'2000. To appear in LNCS. accepted .

Arts, T. and Dam, M. 1999. Verifying a Distributed Database Lookup Manager written in Erlang. ASTEC Report 99/01, In Proc. World Congress on Formal Methods (FM) LNCS 1708 682-700.

Arts, T., Dam, M., Fredlund, L. and Gurov, D. 1998. System Description: Verification of Distributed Erlang Programs. In Proc. 15th International Conference on Automated Deduction (CADE'98) LNCS 1421 38-41.

Bouajjani, A., Jonsson, B., Nilsson, M. and Touili, T. 2000. Regular Model Checking. In Proc. 12th Int. Conf. on Computer Aided Verification, LNCS .

Carlsson, M., Ottosson, G. and Carlson, B. 1997. An Open-Ended Finite Domain Constraint Solver. Proceedings of International Symposium on Programming Languages: Implementations, Logics, and Programming, LNCS, Springer-Verlag 1292 .

Carlsson, M., Ottosson, G. and Carlson, B. 1996. Towards an Open Finite Domain Solver. In Principles and Practice of Constraint Programming---CP96, Springer-Verlag LNCS 1118 531-532.

Dam, M. and Fredlund, L. 1998. On the verification of open distributed systems. In Proc. of the 1998 Symposium on Applied Computing (SAC'98) .

Dam, M. and Gurov, D. 1999. Compositional Verification of CCS Processes. In Proc. International Conference PERSPECTIVES OF SYSTEM INFORMATICS (PSI'99) LNCS 1755 247-256 .

Dam, M. and Gurov, D. 2000. μ-Calculus with Explicit Points and Approximations . Fixed Points in Computer Science (FICS 2000) .

Dam, M., Fredlund, L., and Gurov, D. 1998. Toward Parametric Verification of Open Distributed Systems . In Proc. Compositionality: the significant difference, H. Langmaack, A. Pnueli and W.-P. de Roever (eds.), Springer-Verlag LNCS 1536 150-185.

David, A. and Yi, W. 2000. Modelling and Analysis of a Commercial Field Bus Protocol. 12th Euromicro Conference On Real-Time Systems, Stockholm, Sweden,June 19th-21th .

Engblom, J. 1999. Static Properties of Commercial Embedded Real-Time Programs, and Their Implication for Worst-Case Execution Time Analysis. In Proc. Fifth IEEE Real-Time Technology and Applications Symposium (RTAS '99). IEEE Computer Society Press, Vancouver, Canada 46-55.

Engblom, J. 1999. Why SpecInt95 Should Not Be Used to Benchmark Embedded Systems Tools. Proc. ACM SIGPLAN 1999 Workshop on Languages, Compilers, and Tools for Embedded Systems (LCTES '99) 96-103.

Engblom, J. and Ermedahl, A. 1999. Pipeline Timing Analysis Using a Trace-Driven Simulator. In Proc. The 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99) .

Engblom, J. and Ermedahl, A. 2000. Modeling Complex Flows for Worst-Case Execution Time Analysis. Proc. 21st IEEE Real-Time systems Symposium (RTSS 2000), Orlando, Florida, December .

Engblom, J., Altenbernd, P. and Ermedahl, A. 1998. Facilitating Worst-Case Execution Time Analysis For Optimized Code. ASTEC Report 98/02, 10th Euromicro Workshop on Real-Time Systems, Berlin .

Ericsson, C., Wall, A. and Yi, W. 1999. Timed Automata as Task Models for Event-Driven Systems. In proc. The 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99), IEEE press .

Ermedahl, A. and Gustafsson, J. 1997. Deriving Annotations for Tight Calculation of Execution Time. ASTEC Report 97/04, Euro-Par '97, LNCS 1300 1298-1307.

Ermedahl, A., Hansson, H. and Sjödin, M. 1997. Responce-Time Guarantees in ATM Networks.. In Proc. 18th IEEE Real-Time Sytems Symposium (RTSS) 274-284.

Ermedahl, A., Hansson, H., Papatriantafilou, M. and Tsigas, P. 1998. Wait-free Snapshots in Real-Time Systems: Algorithms and Performance. ASTEC Report 98/04, Conference version of report 98/04, In Proc. of the 5th International Conference on Real-Time Computing Systems and Applications (RTCSA'98) .

Fredlund, L.-Å. and Gurov, D. 1999. A Framework for Formal Reasoning about Open Distributed Systems. In Proc. Asian Computing Science Conference (ASIAN'99) LNCS 1742 87-100.

Getoor, L., Ottosson, G., Fromherz, M. and Carlson, B. 1997. Effective Redundant Constraints for Online Scheduling. ASTEC Report 97/08, In Proceedings of the Fourteenth National Conference on Artificial Intelligence (AAAI '97). American Association for Artificial Intelligence, July .

Gurov, D. and Chugunov, G. 2000. Verification of Erlang Programs: Factoring out the Side-effect-free Fragment. In Proc. 5th International ERCIM Workshop on Formal Methods for Industrial Critical Systems (FMICS'2000) GMD Report 91 109-122 .

Gustafsson, J. 2000. Eliminating Annotations by Automatic Flow Analysis of Real-Time Programs. In Proc. Seventh International Conference on Real-Time Systems and Applications (RTCSA 2000), IEEE Computer Society Press accepted .

Johansson, E., Pettersson, M. and Sagonas, K. 2000. A High-Performance Erlang System. In Proceedings of ACM SIGPLAN. International Conference of Pinciples and Practices of Declarative Programming. .

Jonsson, B. and Nilsson, M. 2000. Transitive Closures of Regular Relations for Verifying Infinite-State Systems. In Proc. International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), LNCS .

Lindgren, M., Hansson, H. and Thane, H. 2000. Using Measurements to Derive the Worst-Case Execution Time. In Proceedings of RTCSA 2000 Cheju Island, South Korea. IEEE Computer Society .

Lönn, M. and Pettersson, P. 1997. Formal Verification of a TDMA Protocol Start-Up Mechanism. ASTEC Report 97/16, In Proceedings of the 1997 IEEE Pacific Rim International Symposium on Fault-Tolerant Systems 235-242.

Ottosson, G. and Sjödin, M. 1997. Worst-Case Execution Time Analysis for Modern Hardware Architectures. ASTEC Report 97/01, SIGPLAN 1997 Workshop on Languages, Compilers and Tools for Real-Time Systems .

Wall, A., Sandström, K., Mäki-Turja, J., Norström, C. and Yi, W. 2000. Verifying Temporal Constraints on Data in Multi-Rate Transactions Using Timed Automata. In Proc. Seventh International Conference on Real-Time Systems and Applications (RTCSA 2000), IEEE Computer Society Press accepted .

Publications in scientific workshops

Abdulla, P. A., Bouajjani, A., Jonsson, B. and Nilsson, M. 1999. Binary Communication in Parameterized System Verification. Nordic Workshop on Programming Theory, Uppsala, October 7, Technical report 1999-008, Department of Information Technology. 8 .

Arts, T. and Noll, T. 2000. Verifying Generic Erlang Client-Server Implementations. Proceedings of the 12th International Workshop on the Implementation

of Functional Languages, Lecture Notes in Computer Science,

Springer Verlag, Berlin LNCS .

Benac Earle, C. 2000. Symbolic Program Execution using the Erlang Verification Tool. International workshop on functional and logic programming, Benicassim, Spain .

Carlsson, M. and Ottosson, G. 1996. Anytime Frequency Allocation with Soft Constraints. In CP96 Pre-Conference Workshop on Applications .

Chugunov, G. and Fredlund, L.-Å. 1999. Verification of Sequential Erlang Programs. Nordic Workshop on Programming Theory, Uppsala, October 7 .

David, A., Hammar, U. and Yi, W. 1999. Modeling and Analysis of a Field Bus Protocol Using Uppaal. Nordic Workshop on Programming Theory, Uppsala, October 7 .

Engblom, J., Ermedahl, A. and Stappert, F. 2000. Structured Testing of Worst-Case Execution Time Analysis Methods. Work in Progress Session at 21st IEEE Real-Time systems Symposium (RTSS 2000), Orlando, Florida, December .

Fersman, E. and Jonsson, B. 2000. Abstraction of Communication Channels in Promela: a Case Study. In SPIN 2000: 7th Int. SPIN Workshop on Model Checking of Software, Stanford University, California, in Lecture Notes in Computer Science, Springer Verlag .

Fredlund, L.-Å. 1999. Towards a Semantics for Erlang. Workshop on Foundations of Mobile Computation, Chennai, December 16 .

Fredlund, L.-Å. , Gurov, D. and Noll, T. 2001. The Erlang Verification Tool. Proceedings of the ETAPS conference 01 (to be published) .

Gustafsson, J. and Ermedahl, A. 1997. Automatic derivation of path and loop annotations in object-oriented real-time programs. ASTEC Report 97/14, in Workshop for Parallel and Distributed Real-Time Systems (WPDRTS '97), Workshop on Object-Oriented Real-Time Systems (WOORTS'97) and 11th International Parallel Processing Symposium (IPPS'97) .

Håkansson, J., Jonsson, B. and Lundkvist, O. 1999. Automated Generation of Test Oracles from Temporal Logic SPecifications. Nordic Workshop on Programming Theory, Uppsala, October 7 .

Johansson, E., Nyström, S.-O. 2000. Profile-guided optimization across process boundaries. ACM SIGPLAN Workshop on Dynamic and Adaptive Compilation (Dynamo'00), January 18 .

Runeson, J., Nyström, S.-O. and Sjödin, J. 2000. Optimizing Code Size through Procedural Abstraction. In Proc. of Workshop on Languages, Compilers, and Tools for Embedded Systems (LCTES'2000) .

Övergaard, G. 1998. A Formal Approach to Relationships in the Unified Modeling Language. Workshop on Precise Semantics for Software Modeling Techniques, ISCE'98 in Kyoto, Japan, April .

Övergaard, G. and Palmkvist, K. 1998. A Formal Approach to Use cases and their Relationships. In Proc. of UML ´98: Beyond the notations 309-317.

Technical reports

Abdulla, P. A., Iyer, P. and Nylén, A. 2000. SAT-solving the coverability problem for unbounded Petri net. Technical report, Department of Information Technology, Uppsala University .

Altenbernd, P. 1997. Cross-Compiling Software Circuits to CHaRy. ASTEC Report (replaced by Altenbernd, P. and Hansson, H. 1998) 97/11 .

ARENA 1996. Applying and Evaluating the ARENA Methodology for Requirements Engineering. ASTEC Report 96/03 .

Auchter, D. 1997. From Requirements Engineering to Design: Combining the ARENA and SOMT Method. ASTEC Report 97/13 .

Auchter, D., Blom, J., Bol, R., Fredlund, L.-Å. and Grelsson, T. 1997. Requirements Engineering in a Telecommunication Environment. ASTEC Report, Replaces report 96/02 97/10 .

Börjesson, H. 1995. Incorporating Worst Case Execution Time in a Commercial C-compiler. ASTEC Report 95/01 .

Carlson, B., Carlsson, M. and Stålmarck, G. 1997. NP (FD) A Proof System for Finite Domain Formulas. ASTEC Report 97/15 .

Carlsson, R. 2000. Extending Erlang with structured module packages. Technical Report series from the Department of Information Technology, Uppsala University 2000-01 .

Carlsson, R., Gustavsson, B., Johansson, E., Lindgren, T., Nyström, S.-O., Pettersson M. and Virding R. 2000. Core Erlang 1.0 language specification. Technical reports from the Department of Information

Technology 30 28.

Engblom, J. 1998. Static Properties of Commercial Real-Time and Embedded Systems, Results from the MARE Project (Measurements of Actual Real-Time and Embedded Programs). ASTEC Report 98/05 .

Engblom, J., Ermedahl, A., Sjödin, M., Gustafsson, J. and Hansson, H. 1999. Towards Industry-Strength Worst-Case Execution Time Analysis. ASTEC Report 99/02 .

Ermedahl, A. and Gustafsson, J. 1996. Redovisning av Studiecirkel/Kurs i Exekveringstidsanalys. ASTEC Report 96/04 .

Ermedahl, A., Gustafsson, J. 1997. Realtidsindustrins syn på verktyg för exekveringstidsanalys. ASTEC Report 97/06 .

Johansson, E., Nyström, S.-O., Jonsson, C. and Lindgren, T. 1999. Evaluation of HiPE, an Erlang Native Code Compiler. ASTEC Report 99/03 .

Johansson, E., Nyström, S.-O., Pettersson, M. and Sagonas, K. 1999. HiPE: High-Performance Erlang. ASTEC Report 99/04 .

Larsson, J. 1996. ScheduLite, A Fixed Priority Scheduling Analysis Tool. ASTEC Report 96/01 .

Larsson, J. 1997. Information interface to the scheduling level of a hard real-time systems design model. ASTEC Report 97/02 .

Larsson, J. 1997. Fixed priority scheduling analysis of the powertrain management application example using the schedulite tool. ASTEC Report 97/03 .

Lindgren, T. 1998. Module merging: aggressive optimization and code replacement in highly available systems. Reports in Computing Science 154 .

Lindgren, T. and Jonsson, C. 1999. The Design and Implementation of a High-Performance Erlang Compiler. ASTEC Report 99/05 .

Nyström, S.-O., Runesson, J. and Sjödin, J. 2001. Code Compression Techniques for Embedded Systems. To appear: Technical reports from the Department of Information Technology .

Ottosson, G., Carlsson, M. 1997. Using Global Constraints for Frequency Allocation. ASTEC Report 97/07 .

Pettersson, M. 2000. A staged tag scheme for Erlang. Technical reports from the Department of Information Technology 29 19

Submitted

Håkansson, J., Jonsson, B. and Lundqvist, O. 2000. Generating On-Line Test Oracles from Temporal Logic Specifications. Submitted .

PhD Theses

Gustafsson, J. 2000. Analyzing Execution-Time of Object-Oriented Programs Using Abstract Interpretation. Ph.D. thesis, Uppsala University, DoCS report 00/115 and MRTC report 00/10 .

Pettersson, P. 1999. Modelling and Verification of Real-Time Systems Using Timed Automata: Theory and Practice. Ph.D. thesis, DoCS report 99/101, Uppsala University .

Övergaard, G. 2000. Formal Specification of Object Oriented Modeling Concepts. Ph.D. thesis, KTH nov .

Lic. Theses

Johansson, E. 1999. Performance Measurements and Process Optimization for Erlang. Ph.Lic. thesis, Uppsala University .

Nilsson, M. 2000. Regular Model Checking. Licentiate Theses from the Department of Information Technology 8 66

M. Sc. Theses

Andersson, M. 2000. Using SAT Solvers to Verify SMV programmes. M.Sc. thesis, Uppsala University .

Auchter, D. 1997. Tool Support for Requirements Engineering: Applying the ARENA Methodology. M.Sc. thesis, Uppsala University, ASTEC Report 97/05 .

Benac Earle, C. 2000. Symbolic Program Execution using the Erlang Verification Tool. M.Sc. thesis, Uppsala University .

Burlin, J. 2000. Optimizing Stack Layout For Embedded Systems. M.Sc. thesis, Uppsala University

Eén, N. 1999. Symbolic Reachability Analysis based on SAT-Solvers. M.Sc. thesis, Uppsala University .

Engblom, J. 1998. Worst-Case Execution Time Analysis for Optimized Code. M.Sc. thesis, ASTEC Report 98/01, Uppsala University .

Evestedt, D. and Kamensky, L. 2000. Symbolic Model Checking of SMV-programs using SAT-solvers. 2 M.Sc. theses, Uppsala University .

Håkansson, J. 2000. Automated Generation of Test Scripts from Temporal Logic Specifications. M.Sc. thesis, Uppsala University

Larsson, P. 1996. Ett effektivt bevissystem för S4. M.Sc. thesis, Institutionen för teoretisk filosofi, Stockholms Universitet .

Löf, D. 2000. Automated Testing of WWW Applications. M.Sc. thesis, Uppsala University .

Montan, S. 2000. Verification of the timing of a cycle-accurate simulator. M.Sc. thesis, Uppsala University .

Nilsson, M. 1999. Analyzing Parameterized Distributed Algorithms. M.Sc. thesis, Uppsala University

Padilla, G. 2000. An Execution Semantics for MSC2000. M.Sc. thesis, Uppsala University .

Runeson, J. 2000. Code compression through procedural abstraction before register allocation. M.Sc. thesis, Uppsala University .

Wiklander, C. 1999. Verification of Erlang Programs using Spin. M.Sc. thesis, KTH .

Ericsson Utvecklings AB

Results from coopration within ASTEC

The Erlang Verification Project

Date:22 Aug 2000
From: Thomas Arts, thomas@cslab.ericsson.se
Organization: Computer Science Lab, Ericsson Utvecklings AB

ASTEC experience w.r.t. the Erlang Verification Project.

During the last two years the collaboration with ASTEC (read SICS)
has been based upon a jointly development of a tool for the
verification of Erlang programs. The prototype of the tool had
been constructed at the time of starting the project.

The first phase of the project has mainly been used by Thomas to
learn to use the tool and to run a rather large case study,
proving a property part of the Mnesia database. This turned out to
be a challenging job, which has been reported on in an article
presented at FM99.
The contribution to Mnesia has probably not been that much, but at
least a patent could be written by Hans as a side-effect of the
started verification.

The case study indicated that the tool lacked some features and
the development of a second (totally new) version of the tool
was carried out over the next year. This tool, called EVT, has
been used in the Lab by a master student for performing some
smaller case studies. It turned out that one still needs to learn
very much in order to be able to use the tool. A user interface
has been developed to partly overcome this problem.

The ASTEC partners developing the tool are very open for
suggestions and try hard to make the tool as useful as possible
for our needs. The development went a little slower than expected,
mainly because of the underestimated amount of work that was
involved in building EVT. However, without the ASTEC cooperation, we
would not have had a tool at all.

The main focus now is extending and refining the tool such that a
higher level of automation can be reached. This is done in parallel
with some case study directly taken from the Erlang programs present
within Ericsson.

ASTEC brought, above all, much knowledge into Ericsson. The area
of Software Verification is a rather new one and Ericsson has to stay
upto date w.r.t. the developments in this field. The ASTEC cooperation
is a perfect way for that. The approached followed is state-of-the-art
and leading in its field, as is demonstrated by several scientific
publications.
ASTEC brought a tool to the research lab which has been and will be
used on case studies of small, but realistic examples.

The cooperation also pointed out an application area for software
verification, viz. software patents, which had not yet been in the
picture before. Patents describe relatively small algorithms that need

to be correct, but for which it is not so important how long time
the verification takes.

The HiPE project - letter 1

Date:22 Aug 2000
From: bjarne@erix.ericsson.se
Organization: CSLab
Subject: Evaluation HiPE

Answers from Ericsson regarding the HiPE project.

> - What did you expect from the ASTEC collaboration.

Ericsson has developed the concurrent, functional
programming language Erlang and a basic system OTP
(Open Telecom Platform). These are used in some large
and important projects within Ericsson which finance
a product unit for their maintenance and further
development.

The HiPE project presents an alternative compiler
based on aggressive techniques from current research.
Ericsson does not use the HiPE compiler directly
but benefits greatly from the collaboration with
the HiPE team.

> - How are the results so far in relation to your expectations?

Much greater than expected. The HiPE team has been
much more practical and concrete than we expected.

> - Did ASTEC bring any technology to your company?

The HiPE team has proposed and developed a new tagging
schema for Erlang which means that Erlang programs have
access to the full address space of 4 Gbyte. Their
implementation has been incorporated into the Erlang/OTP
compiler and this means that it can be presented to
the users already in rev 7 instead of rev 8 which
means several months earlier.

In addition the HiPE team has proposed many optimzations
in their reports which the Ericsson development team
has been able to use to improve their system.

> - Has ASTEC served as a forum for trying or assessing new technology?

Rather as discussion partner.

> - Has ASTEC contributed to your products or your development procedures?

Yes, please see above.

The manager of the Ericsson Erlang/OTP product unit
hopes that this collaboration will continue at least
on this level next year.

Best regards

Bjarne Däcker

The HiPE project - letter 2

The concurrent functional programming language Erlang was
developed at Ericsson and a productified compiler and
implementation is maintained by Ericsson. Erlang is
available externally both open source and with support
contract.

HiPE (High Performance Erlang) is a research project
within Astec to develop an alternative compiler exploiting
up-to-date research results.

"HiPE has been highly beneficial to us at Ericsson Utvecklings
AB where we develop the Erlang/OTP product. During the six months
of year 2000 we have achieved very concrete results in a short
time thanks to assistance from HiPE. We have introduced a new
tag schema in the Erlang virtual machine which it would have
taken us many months more without the knowledge and the
prototypes we received from the HiPE team.

The new solution will be included in the next version of Erlang/OTP
which will be released in October. This new solution means that
the Erlang virtual machine will be able to address a full 32
bit address space, i.e. 4 Gbyte (compared to 1 Gbyte with the
present machine) and that it will be easier to port the
implementation to other operating systems.

Furthermore we have had great use of the HiPE team with regard
to compilation techniques and optimizations. In coming versions
of our own Erlang compiler we expect to be able to include
even further optimizations based on results from HiPE (both
measurements and implementations).

We have excellent relations to the HiPE team and I really hope
that their activities can continue at the same rate next year."

Rgrds, Kenneth Lundin (Manager Erlang/OTP product development)

IAR systems AB

Results from coopration within ASTEC

C. Industrial relevance, benefits and effects

Industrial involvement and interaction

From IAR Systems point of view the industrial involvement has increased since the centre started. We decided to take part in the WCET (Worst Case Execution Time) related activities in order to understand the possibilities of providing tools that could be really useful to the real-time system developer. Since then our involvement has also emerged into the related field of compiler optimisation technology, specifically the WPO (Whole Program Optimisation) technology. We have part financed several M.Sc. diploma workers as well as three industrial Ph.D. students (the Ph.D. students are working part time as researchers and part time as developers at IAR Systems AB). Until today no IAR Systems developers have joined the research related academic world (we have, however, a few developers attending higher university education on a part time basis).

Industrial partnersí expectations

The IAR Systems expectations on the centre were very high. When joining the centre we were hoping for simple solutions to the very complex problems in the WCET area. The first try was a very pragmatic approach that was tested using a M.Sc. diploma worker. The results were very promising but did not lead to any commercial products. The reason for this was mainly the lack of interest from the IAR Systems customers (it was very hard to find the customers who really understood the benefits from the newly developed prototype tool).

Later on we have tried a more íscientificí approach and the amount of work put into the projects have been substantial (at least according to our measures). We have these three very skilled Ph.D. thesis workers and we really believe that we will be able to use the results that they will come up with in real commercial products within the next two years. Specifically in the WPO area we see a possibility of implementation work starting during next year. This is somewhat ironical but at the same time probably common in these research co-operations: The best results come from the projects not originally planned for but emerging in the creative environment where researchers meet the industry based developers.

Commercialisation and technology transfer activities

From IAR Systems perspective, no IPR-results have come out of the centre.

Evidence of industrial benefits

- New networks and collaborative linkages

  The academic contacts have increased substantially: We now have good contacts with all the participating academic partners (SICS, KTH, UU and Mlardalens Hgskola). Our international academic contact network has also grown: From no international contacts to more or less close co-operations with German (Paderborn and Dortmund), Korean (Seoul) and American (Houston) universities. This has been one of our main benefits from the centre (so far).

  The industrial partners of the centre have also contributed to our understanding of the end-user problems when using our products. My personal opinion is that we (both IAR Systems as a company and ASTEC as a centre) could improve in this area to really make full use of these valuable industrial contacts.

- Build up of new and increase of existing competence

  We have not yet been able to hire any of the centre graduates (although we hope to hire all of our industrial Ph.D. students once they graduate). On the other hand we have hired quite a few graduates from the university where the first contacts have been made through the centre of the associated reserachers.

  IAR Systems have also been able to offer some of our employees the possibility to attend the parts of the relevant Ph.D courses provided by the university. Thereby we have been able to give these employees both relevant education and a way of keeping in contact with the research area.

- Technical assistance and problem solving

  We have been able to recruit more than five diploma workers and three Ph.D. students. These people have helped us solve a lot of interesting technical problems. We have also been fortunate enough to work together some of the more distinguished senior researchers at UU/SICS in seminars and ìstudy projectsî.

- Access to new ideas and know-how, evaluation of new technology

  For IAR Systems the results implemented so far are only a minor part of what we believe will come:
  - We have implemented (for us) the new technology of instruction scheduling,
  - New and better code analysis in the compiler (to prepare for future optimisations),
  - Created a better execution simulator (cycle accurate) based on a lot of the WCET experiences,
  - Created a research version of our compiler in order to gather statistic information about embedded programs (this has proven to be very useful information) and,
  - Used this research compiler in our internal product optimisation work.

Olle Landström
IAR-systems AB

ABB Automation products AB

Results from coopration within ASTEC

From: ulf.h.hammar@se.abb.com
Date: Fri, 25 Aug 2000
Subject: Erfarenheter av AF100 projektet

Hej

Skickar en liten kommentar till projektet.

METODEN:
- - UPPAAL är ett mycket bra verktyg för att modellera och simulera. Det är
lätt att använda och intuitivt för en programmerare. Kopplingen mellan
modellen och koden är lättförstådd.

- - Redan på ett tidigt stadium hittade vi avvikelser i protokollet trots
att modellen var mycket liten, framtagen på bara några timmar.

- - Vi har ännu inte fått slutrapport från Alex så vi kan inte säga hur
utfallet blir......hoppas kunna slutföra under september - oktober, så vi
befinner oss fortfarande i den tidiga optimismen

- -Det står ju klart att hela modellen inte kan verifieras pga dess storlek
och begränsningar i metoden men försöket att dela upp modellen i mindre
modeller vilka approximerar är inte förkastligt. Att skapa flera modeller
och att verifiera dem mot varandra medför förståss merarbete och risk för
inkonsistens.

PROJEKTET:
- - Projektet har gått bra. Vi har dock från vår sida ägnat för lite tid
till det. Vi satsar på "tekniköverföringen" nu i höst.

FORTSÄTTNINGEN:
- - Eventuella fel måste vara av en viss dignitet, dvs påverka bussens
funktion, för att det ska vara försvarbart att ändra i produkten. Vi har inte funnit
något sådant ännu.

- - Vi hoppas kunna introducera användningen av UPPAAL i vår organisation.
Ett pilotprojekt inom nyutveckling är kanske ett naturligt sätt att börja.
För att användningen ska bli bred så måste metoden ingå i processerna och
projektplanerna.

- - Vi kommer troligen inte att arbeta med gammal kod. Kod som säljs och
fungerar vill man inte gärna ändra.

- - Ytterligare en introduktion till UPPAAL och metoden har efterlysts och
vi hoppas kunna engagera er i detta under hösten.

Mvh,

Ulf Hammar

- Uppsala University
  - Department of Information Technology
    - ASTEC, ASTEC internal pages

Gunnar Stålmarck
Prover Technology AB

August 30, 2000

Our cooperation within ASTEC

Founded in 1989, Prover Technology is a world leader in the industrial application of Formal Methods. Prover Technology develops and applies products for automatic validation and verification to ensure that complex systems are correct, free of faults, and function according to specification. To date our methods have been successfully applied to systems developed in avionics, nuclear power generation, railways, automotive and telecommunications, as well as a number of industrial and academic research projects at national and international level.

The basis for our commercial work is our implementation of Stålmarck's method. We regard *model checking* as an important application area for our future commercial efforts. The work of the project concerns expanding the applicability of Stålmarck's algorithm to perform model checking. The initial work carried out in the project has resulted in a tool (FixIt) which scales up better than classical BDD-based techniques on several classes of systems. These early results provide strong evidence that Stålmarcks method is a most suitable basis for further development of such verification methods.

We intend to further extend our cooperation by employing an industrial PhD student during 2000/2001 to work jointly at Prover and Uppsala University.

In conclusion, the project addresses central problems with a big commercial potential for our company. We shall continue to take part in the proposed project, and expect to use the results in our future commercial activities.

Yours Sincerely

Gunnar Stålmarck

Results of participation in ASTEC projects

This paper describes the state of the art concerning the involvement by Validation AB in ASTEC projects.

1. Industrial Involvement and Interaction.

Validation AB has been involved in ASTEC projects concerning Automated Testing.

During the period work has been carried out and forthgoing in areas such as testing of Web-based services dealing with objectives such as:

- The use of existing automated test tools, how to use script tools for automated test executions.
- Automated penetration of Web applications in order to apply automated test tools, grafical presentations and realisation of new test methods.

In this work Validation AB has participated in the work and supplied with test tools and equipment in our test plant.

2. Industrial Partner´s Expectation

Validation AB is a company working with quality and test assurance.

There is a need to keep ahead with the technical and market evolution to cope with more efficient and advanced methods and tools for validation in the development process. The cooperation with ASTEC is expected to give new and extended knowledge and more effcient ways of quality assurance.

3. Commercialisation and Technology Transfer Activities

At present no commercialised product has been developed. The reults so far are meerely seen as extending the knowledge in the area and to be input for further activities in creating future products (testing and validation products).

4. Industrial Benefits

Benefits so far is a better understanding of needs and possibilities in the penetrated areas. An important benefit of the involvement is the transfer of knowledge between the parties

Benefits and effects of participation in ASTEC

VCT's expectations on the centre are based on the fact that the company's business is heavily relying on access to both the latest results of academic research and heavy industrial application experience. Participation in the centre helps us to further widen our contacts in the academic world, thus ensuring continued access to academic resources.

The experience from our viewpoint has been very positive this far, identifying a number of potential areas for joint activities, and research projects and completing one specific project – a diploma work. The aims of the project – to develop a packaging and scheduling algorithm for LIN (Local Interconnect Network) - has been successfully achieved. (See Appendix)

This algorithm is going to be part of a commercial product, to be launched during Q4 2000 by VCT.

We have the intension of further developing our collaboration with ASTEC in a near future due to the significant benefits we potentially can achieve.

The most important of these would be direct access to the international scientific community, increase of existing competence, and possible employment of research staff and graduates.

V. Frölunda, 2000-08-28

…………………………..
Antal Rajnák
MD

Local Interconnect Network (LIN) – Packaging and Scheduling

Magnus Ahlmark

The usage of computer networks in vehicles is becoming more and more common. The number of computers in vehicles will increase dramatically in the next generation of new vehicle platforms. However, when adding so many computers to the car several different types of communication networks are required to reach cost effective solutions. A modern European car usually contains one or two Controller Area Network (CAN)-networks. However, when the number of computers increases so dramatically, CAN is too expensive to use for connecting simple devices such as simple switches and non-safety critical functions like indoor lights etc. Therefore, a new low cost communication solution called Local Interconnection Network (LIN) has been developed in a consortium including major car vendors, Motorola, and Volcano Communications Technologies AB. The purpose of LIN is not to replace the CAN-bus already running in the vehicles, but to be a low cost complement for connecting simple functions. In this paper, we propose a bandwidth allocation algorithm that can be applicable to the LIN protocol. The bandwidth allocation algorithm not only satisfies the performance requirements of real-time systems but also fully utilises the bandwidth of the LIN. We also present two scheduling algorithms including the process of deriving period times to satisfies the performance requirements of real-time systems

Thesis for master degree in Computer Engineering 20 p / 2000-05-22

Volvo Teknisk Utveckling AB

Results from coopration within ASTEC

Date: Wed, 30 Aug 2000 13:28:44 +0200
To: bengt@csd.uu.se
From: Mats Larsson
Subject: ASTEC feedback

Hej Bengt!

Ska sent omsider försöka sammanfatta vår erfarenhet från ASTEC samarbetet.

Till att börja med måste jag understryka hur litet vårt deltagande är. Vi har gjort ett exjobb hittills och avser att göra ett till. Det ger inte mycket till underlag eller påverkan på organisationen.

Det bästa tycker jag har varit ditt aktiva handledande av Johns exjobb och det stora personliga engagemang du visat. Det tycker jag är det som skiljer det här exjobbet från "vanliga" exjobb där examinatorns roll vanligtvis är ganska liten. Det gör att det känns som ett "riktigt" samarbete mellan Volvo och Uppsala universitet även om det tar sig formen av ett exjobb. En annan (antagligen besläktad) fördel jag ser är det tydliga fokus som du styrt in vårt deltagande mot. I vårt fall är det testning och då framförallt av realtidssystem. Jag tror det är bra att ha en "ram" för samarbetet annars divergerar det lätt till en mängd disparata insatser.

När det gäller nackdelar ser jag egentligen bara en och det är den geografiska tyngdpunkten hos ASTEC på Uppsala-Stockholmsområdet. Flera gånger har det varit intressanta föredrag/presentationer som annonserats av ASTEC men det är omöjligt för oss att åka till Uppsala för ett 1 timmes seminarium. Det gör att vi inte känner så stor samhörighet med ASTEC och de övriga deltagarna. Detta avspeglar sig tex. i vårt aktiva ointresse för att delta i styrelsemöten odyl. Eftersom allas tid är knapp bör man fundera över hur man samarbetar i ett distribuerat nätverk på ett tids och resurs-effektivt sätt. Utan att ha någon patentlösning inbillar jag mig att vägen framåt kan vara internetbaserad. Med detta menar jag dock mer än en hemsida. Det måste finnas en nytta med att koppla upp sig eftersom människan drivs av egenintresse. Ett förslag kunde tex. vara att sända ut alla presentationer som ges live på internet. Det skulle ge oss och andra distansmedlemmar en chans att ta del av dynamiken i ASTEC (som jag hoppas finns).

Det var vad jag kunde komma på just nu. Som sagt, ledsen att det dröjde men jag hoppas det kan vara till någon nytta ändå.

Mvh, Mats

ASTEC

Advanced Software Technology

ASTEC (Advanced Software TEChnology) is a competence center in the area of software technology. Its purpose is to develop and support industrially applicable techniques for software specification, design, and development. It shall bring new technology into industrial applications and perform academic research on industrially relevant problems in software development. High-level specification and programming languages, together with tools for specification, analysis, validation, simulation, and compilation are central topics of the center. Particular emphasis is put on methods supporting the development of software for communication and control applications.

Partners:

ASTEC has been formed as a consortium of the following academic and industrial partners during phase 2.

1. Academy at Uppsala University (UU)
   The Department of Computer Systems
   The Computing Science Department
   Mälardalen University
   Swedish Institute of Computer Science (SICS).

2. Industry
   ABB Automation Products AB,
   Ericsson Utvecklings AB,
   IAR Systems AB,
   Mecel AB,
   Prover Technology AB,
   Telelogic AB,
   Telia Validation AB,
   UPAAL Sweden AB,
   Volcano Communication Technologies AB,
   Volvo Teknisk Utveckling AB,

3. NUTEK, the Swedish National Board for Industrial and Technical Development.