ASTEC
Advanced Software Technology

Final Report for Phase 1.

April 8, 1998

The enclosed document is the report from the competence center **Advanced Software Technology (ASTEC)**, for the period 1995-09-01 – 1997-12-31. The structure of the document follows closely the guidelines given by NUTEK. The document summarizes the activities in ASTEC during the first 28 months. Other up-to-date information about current activities can be found on the WWW page `http://www.docs.uu.se/astec/`

Uppsala, April 8 1998

prof. Bengt Jonsson, director

Contents

Summary

ASTEC (Advanced Software Technology) is a competence center 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 major products, such as communication and process control systems, of Swedish industry. An important means to produce better software at lower cost is to employ software technology in the form of 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 research on pre-competitive industrially applicable techniques for software specification, design, and implementation at a high level of abstraction, and to be a forum for contacts and exchange of ideas between academia and industry.

From its start ASTEC has emphasized project work with close collaboration between academia and industry as the most important aspect. Four projects have been conducted in the period 95-09 - 97-08. As of Sept. 1997 four new projects have been initiated.

Since September 1997, several measures have been taken to support long term strategic planning, some of which are listed here.

- A strategic plan has been produced, as a guide for project planning, where 3 technical programs areas and 2 application areas are described. ASTEC is striving to build strong research competence in these areas.
- An advisory board has been appointed,
- Regular mini-workshops are conducted within several program areas.
- Heavier emphasis is put on PhD work. ASTEC presently funds 9 Ph.D. students, whose dissertations are expected to be ASTEC-theses. We expect 4 Ph.D. degrees during 1998/99.

The major results of Phase 1 can be summarized as

- A strong network of collaboration established between academia and industry in the area of ASTECs competence.
- The build up and consolidation of research competence in the program areas of ASTEC.
- Transfer of techniques from academia into commercial tools is in progress.

Sammanfattning

ASTEC (Advanced Software Technology) är ett kompetenscentrum som sysslar med avancerade verktyg och tekniker för programvaruutveckling. Programvaruutveckling står för en betydande del av konstnaderna vid konstruktion av många viktiga produkter inom svensk industri ex.vis kommunikationsssytem och processtyrsystem. Ett viktigt led i att kunna producera programvara av högre kvalite till lägre kostnad är att använda språk för att specifiera och programmera på en hög abstraktionsnivå, som stöds av verktyg för specifiering, analys, validering, simulering och kompilering. ASTECs syfte är att bedriva forskning kring industriellt användbara tekniker för programvaruspecifiering, -konstruktion och -implementering på en hög abstraktionsnivå, och att utgöra ett forum för kontakter och idéutbyte mellan akademi och industri.

Vid starten har ASTEC sett som sin viktigaste uppgift att bedriva projekt med tätt samarbete mellan akademi och industri. Fyra projekt har bedrivits under perioden 95-09 - 97-08. Efter september 1997 har fyra nya projekt satts igång.

Efter september 1997 har flera åtgärder vidtagits i syfte att stärka den långsiktiga strategiska planering, bl.a.

- utarbetande av en strategisk forskningsplan som vägledning för projektplanering,
- tillsättande av ett internationellt vetenskapligt råd
- regelbundna workshops i programområden
- starkare tonvikt på doktorandprojekt. ASTEC stödjer f.n. 9 doktorander, och 4 doktorsexamina förväntas under 1998/99.

De viktigaste resultaten av fas 1 kan sammanfattas som

- Bildandet av ett nätverk av akademiska forskargrupper och industriföretag inom ASTECs kompetensområden.
- Uppbyggnad och konsildering av forskningskompetens inom ASTECs programområden.
- Överföring av forskningsresultat i kommersiella programvaruutvecklingsverktyg pågår.

1 Realization of Goals

The original goals of ASTEC have been:

1. to support the use of advanced techniques for software development in Swedish industry. This meant both to advance the start of the art in research, and to support the industrial use of new techniques.

2. to support the transfer of knowledge between research and industry. This includes being a forum for contacts between research and industrial practice in the area of software development, bringing new technology into industrial applications, and focusing research and graduate education onto industrial problems.

The work in ASTEC has fulfilled these goals in the following ways:

1. To support the use of advanced techniques for software development:

   - ASTEC has conducted and is conducting research projects in collaboration between academia and industry. This type of close collaboration would not have taken place without the establishment of ASTEC. Results from these projects include
     - more than 6 case studies on the application of advanced software techniques to industrial problems.
     - more than 5 software packages implementing advanced software techniques for use on industrial problems.

     Through participation in these collaboration projects, the industrial partners of ASTEC have gained important insights into the potential of techniques within the scope of ASTEC. These insights may well have an impact on future use of techniques within these industrial partners.
   - An alternative way of increasing the use of advanced software technology in industry is to enhance the power and functionality of existing software development tools, such as compilers, and tools for specification and analysis. A large part of ASTEC work is conducted in collaboration between academia and commercial tool manufacturers. Several examples of transfer of techniques from academia into commercial tools is under way: enhanced functionality in compilers for embedded systems (timing analysis), and more efficient techniques for compilation of high-level languages.

2. To support the transfer of knowledge between academia and industry:

   - A significant transfer of knowledge has been achieved through collaboration projects. As mentioned above, the industrial partners have gained important insights into the potential of techniques within the scope of ASTEC.
   - The center has succeeded in guiding and refocusing research directions in academia, as witnessed by the adoption of industrial languages such as Erlang, C and UML, as topics for research.

- The center has generated new research problems for academia. An example is Execution Time Analysis within the project WCET. Other examples are: how to adapt the theorem proving techniques of Prover Technology to new applications (model checking), how to generation code from high-level specifications, and how to present target-code debugging information on the object-code level.
- Having created a network of research and industry groups in its area of competence, ASTEC now serves as a forum for exchanges of ideas between its partners, as witnessed by the number of discussions on problems of participating companies that are taking place.

The evaluation by NUTEK in June 1997 resulted in several points of criticism against the functioning of ASTEC. In response to this criticism, the long-term goals and strategy has been revised.

- It is made clear that ASTEC does not intend to create a nation-wide impact on software development practice, but strives to achieve impact indirectly through its research program.
- The strategy has changed: from the start, ASTECs strategy has been to conduct successful collaboration projects within its area of competence. This ambition has later (97-09) been complemented by a strategic research plan, whose purpose is to guide project planning by defining research directions with long-term research goals.

2 The Added Value of Being a Competence Center

The following effects should be put forward as a result of ASTEC being a Competence Center.

- From its start, ASTEC has put strong emphasis on close and active collaboration between academia and industry in project work. The emphasis on close collaboration has resulted in
  - collaborative case studies, with a genuine exchange of insights and ideas between academia and industry.
  - new research problems for academia
  - understanding of the applicability of techniques to industrial problems
- The collaboration and planning work in ASTEC has created a network of contacts between academia and industry. This network is an important capital, which has been created through a rather substantial investment of time in discussions, meetings, and joint research. Furthermore, the contacts are "global to ASTEC" in that they are not a set of project-specific links, but rather a global forum for discussions and generation of new ideas.

- As a response to the evaluation, ASTEC is now devoting energy to the build-up and consolidation of strong research in the three technical program areas *Validation and Verification*, *Programming Languages and Implementation*, and *Real-Time Distributed Systems*. ASTEC has been the strongest driving force in furthering collaboration in these areas in Stockholm-Uppsala, exemplified by the regular seminar series on these topics.
- Within the ASTEC framework, it is possible to eploit the existing overlap and potential synergies between the technical program areas. Examples are
  - our plans to work on code generation from specification (a combination of specification and compilation),
  - the use of advanced analysis techniques for optimizing compilation.

3 Financial Report for the Period

The following table summarizes the total contributions by each partner (Academic partners, Industrial Partners, NUTEK), per project during the period. The contributions by NUTEK are in the form of Cash. The contributions by the industrial and academic partners are in the form of contributed work and infrastructure. During the period, totally 10 research projects have been conducted (see Section 4.2). In the table below, the contributions to the projects ART-WCET and ART-AUTO are added to those of the project RT, since these two projects are a natural continuation of RT. As a result, the table shows the contributions to 8 projects and the contributions to center scientific and administrative management.

A more detailed elaboration of these figures can be found in the appendix.

Partner	Vocal	RT	Arena	Boom	Erl Ver	Vassco	Hipe	WPO	Man.	Sum
UU/DoCS		1,308	740						1,130	3,178
UU/CSD	144		132			91	130	63		560
KTH				746						746
SICS	624		526		191					1,341
Sum Acad.	768	1,308	1,398	746	191	91	130	63	1,130	5,825
NUTEK	816	2,185	1,024	964	191	142	200	100	68	5,690
ERA	634									634
ETX					150					150
IAR		382						44		426
Prover	790					115				905
Mecel		1,230								1,230
Rational				1,011						1,011
Telia			1,990							1,990
Sum Ind.	1,424	1,612	1,990	1,011	150	115		44		6,346
Total	3,008	5,105	4,428	2,723	532	348	330	209	1,198	17,851

The following table summarizes the contributions by Academia, NUTEK, and Industry.

Academia (work)	5,825	32.6 %
NUTEK (cash)	5,690	31.8 %
Industry (work)	6,346	35.6 %
Total	17,851	100 %

4 Program Areas and Projects

4.1 Program Areas

For the period 95-09 - 97-08, ASTEC has defined its *area of competence* as the union of four main program areas, as shown in the table below.

	Main Area	**Typical Topics**	**Competence**
1	Requirements Engineering	Requirements Capture Formal Specification Methods Informal Specification Methods Validation Methods	Specification Techniques
2	Programming Paradigms	Very High Level Progr. Lang. Program Synthesis Customized Languages	HL Symbolic Programming Languages and Techniques
3	Implementation Techniques	Compiling Technology Debugging Garbage Collection	Advanced Implementation Techniques
4	Analysis Techniques	Reliability Verification Methods	Automated Analysis Techniques

The strategy of ASTEC has been to conduct collaboration projects within its area of competence. A project should demonstrate the application of new software development technology to an industrial problem.

After 97-09 the work in ASTEC has been structured into three technical program areas and two application areas. The program areas are:

- Validation and verification.
- Programming languages and implementation.
- Real Time Distributed Systems.

The application areas are software for:

- Automotive applications.
- Data- and telecommunications.

During the period 95-09 - 97-08, ASTEC has conducted 4 projects. After 97-09, one project (VOCAL) has been completed. In addition, 4 new projects have been initiated in accordance with the strategic plan, and one of the initial projects (RT) has been divided into two projects (WCET and AUTO).

4.2 Projects

Here we give a brief synopsis of the projects that have been conducted, together with a short selection of project results. More elaborate descriptions can be found in the appendix.

Projects During 95-09 - 97-08

During 95-09 - 97-08, research has been carried out within four projects:

- **VOCAL** Verification and Optimization using Constraints And Logic
  Participants *Ericsson Radio AB, IAR Systems AB, Prover Technology AB, UU, SICS*
  Coordinator *Mats Carlsson, SICS/UU*
  This project has explored the combination of constraint programming and theorem proving techniques for solving verification and optimization problems. Examples of such problems are scheduling of industrial processes, and verification of control software in railway switches. The project has developed a package for constraint programming over finite domains for such applications, as well as for general use. The technology has been evaluated in case studies. The project has been completed as of 97-08.
  Examples of Results
  - VOCAL has implemented and evaluated a constraint programming package for constraints over finite domains, combining a general consistency algorithm with a framework for adding special-purpose algorithms, and a library of built-in constraints.
  - VOCAL has implemented and evaluated a theorem prover for propositional formulas over linear constraints, combining the finite domain constraint solver with the Stålmarck method.

- **RT** Real-Time System Software Development
  Participants *IAR Systems AB, Mecel AB, UU*
  Coordinator *Hans Hansson, UU*
  This project intends to develop a design method for Automotive real-time software. This covers high level modeling and analysis, as well as support for mapping specifications to implementations. A particular problem which is given special attention is how to automatically predict execution times of compiled code fragments.
  Examples of Results

- The project has implemented several software packages which address different aspects in calculating execution times for fragments of C-code. The project has also implemented a tool for fixed priority scheduling analysis for a general task model, including overheads, communication, transactions and distributed executions.
- The project has carried out several case studies on formal modeling and analysis applied to some systems in automotive software.

- **ARENA** Astec Requirement Engineering Approach
  Participants *Telia AB, UU*
  Coordinator *Roland Bol, UU*
  The project has developed a methodology for producing and handling requirements for information services in e.g. telecommunication systems. The aim is to improve the usefulness of the resulting requirements specification to design, formal verification and testing. Reuse of requirements and traceability between requirements are important aspects of the methodology that require tool support.
  Examples of Results
  - The project has produced a method (the ARENA method) for structuring and relating collections of requirements during the development of a service, which addresses reuse from a general repository of general requirements.
  - Several commercial tools have been evaluated with regard to their suitability in the context of this method.

- **BOOM** Formal Specification of Object-Oriented Modeling Concepts
  Participants *Rational Software Scandinavia AB, KTH/UU*
  Coordinator *Joachim Parrow, KTH/UU*
  This project aims at developing the semantic basis for object-oriented system development methods. Such a semantics can serve as the basis for adapting support tools to different modeling languages, and for consistency checks of models. A part of the effort has been to participate in the development of UML, the Unified Modeling Language.
  Examples of Results
  - a formal object-oriented specification language, named ODAL, has been developed and given a semantics in the pi-calculus.
  - A meta-model for object-oriented languages, named BOOM. has been developed in order to defined concepts in notations for object-oriented system development, such as UML.

Projects Initiated After 97-09

This section contains a short description of the projects that have been initiated after 97-09, grouped according to technical program area.

In the area *Validation and Verification* the following projects have been initiated.

- **ErlVer** Verification of Erlang Programs
  Participants *Ericsson Telecom, SICS*
  Coordinator *Mads Dam, SICS/KTH*
  This project aims to develop a general verification tool for the Erlang programming language based on a combination of model checking, compositional and symbolic techniques. Apart from the prototype tool itself, project results are expected, and indeed required, in the fields of operational semantics, specification logics, compositional proof systems and their effective implementation.
  Examples of Results

  - Development of a language for formally specifying properties of distributed programs, and a proof system for verifying these properties on programs written in a non-trivial fragment of Erlang.
  - An implemented demonstrator tool, which implements the proof system for Erlang programs with some support for automation.
  - The language and proof system have been demonstrated on a case study, a dynamic resource manager.

- **VassCo** Verification of Asynchronous Systems of Synchronous Components
  Participants *NP Technology AB, UU*
  Coordinator *Roland Bol, UU*
  The general aim of this project is to bridge the gap between the worlds of synchronous specifications and asynchronous implementations. Design and verification are preferable done in the synchronous world, because it is simpler, whereas the reality of distributed and fault-tolerant systems is asynchronous. The aim of the project is to develop methods for translating between synchronous specifications and asynchronous implementations. The method development will be based on applications from automotive software. The project is still in its initial stage.

In the area *Programming Languages and Implementation*, the following projects have been initiated.

- **HIPE** High Performance Erlang
  Participants *Ericsson Telecom, UU*
  Coordinator *Thomas Lindgren, UU*
  The project aims at developing techniques for efficient compilation of concurrent functional programming languages. These languages do not yet reach the performance levels of established languages such as C. New research is needed that addresses the new compilation and optimization problems raised by new languages. In particular, it is important to address efficient compilation of large and realistic programs written in high-level functional languages.

  The project is based on a compiler for Erlang, which is being developed at Uppsala University. This compiler is a platform for experimenting with optimizations, and for application to industrial-size programs, which exist today.
  Examples of Results

- An experimental Erlang compiler is being completed, with facilities for measurements to guide and evaluate optimizations.
- Methods for optimizing parts of programs that cut across module boundaries, even for the case that the system can replace modules by new versions while it is running.

- **WPO** Whole Program Optimization for Embedded Systems
  Participants *IAR Systems, UU*
  Coordinator *Thomas Lindgren, UU*
  In order to move embedded systems out of assembly-language programming, highly optimizing compiler technology is needed. However, embedded applications have to satisfy severe constraints imposed by irregular hardware architectures and limited power and memory, which makes optimizing compilation a challenge.

  The aim of this project is to build a whole-program optimizer for a compiler. Such an optimizer analyzes the entire application and performs optimizations based on the information obtained. For PC applications, this may not be a viable approach, since applications may be many millions of lines of code. Normal applications in the embedded market are, however, orders of magnitude smaller. The purpose of this project during the first year is to make an initial study of whole-program compilation, particularly with respect to embedded systems.
  Examples of Results

  - A design of a whole-program analyzer which fills a small, fast memory with data objects.

Within the area *Real Time Distributed Systems*, the project RT has been restructured, in order to make clear its two components, into:

- **ART-WCET** Calculation of Worst-Case Execution Times
  Participants *IAR Systems AB, UU*
  Coordinator *Hans Hansson, UU*
  Execution time analysis is used to predict timing bounds (typically *worst-case* execution times (WCET)) of programs. Such bounds are required by any real-time related modelling and analysis, as well as for configuration and allocation in Real-Time Systems. Accurate WCET analysis is very important, since optimistic estimates invalidates the analysis, and pessimistic estimates give poor resource utilisation. Current practice in execution time analysis is either inaccurate (e.g. measurements which does not guarantee the worst case to be covered) or pessimistic (e.g. always assumes maximum number of iterations in a loop).

  The project continues the efforts on WCET-prediction, initiated by project RT. As a first effort in combining high and low-level analysis we now study methods to keep track of how compiler optimizations influence execution times
  Examples of Results (in addition to results of RT)

  - A method for relating source-level C-code to optimized compiled code, which can be used to relate execution times of optimized code to execution times of fragments of the source-level program.

- **ART-Auto** A design methodology for embedded real-time systems.
  Participants *Mecel AB, UU*
  Coordinator *Hans Hansson, UU*
  The development and design of automotive electronics is switching paradigm: from single application dedicated hardware and software to highly integrated distributed systems in which virtually all vehicle applications share hardware and system software. This calls for more advanced software design methods, providing support both for provably correct design and convenient handling of modifications and reconfigurations.

  The focus in ART/Auto is on development of a design method for Automotive Real-Time Applications. As starting points for this work we use the software development method proposed in the VIA project (which includes an outline of a signal-flow based design language) together with recent advances in the area of scheduling; and formal real-time modelling and verification.

5 Participating Research Groups and Industry Partners

ASTEC is supported by the following research groups.

- *The Department of Computer Systems, Uppsala University* The main directions of research are methods and tools for design and analysis of distributed and real-time systems, implementation strategies for communications software and distributed real-time systems, and implementation of neural networks for telecommunication applications.
- *The Computing Science Department, Uppsala University* The research includes meta-programming, automated program analysis, compilation and implementation, parallel processing, program development, and intelligent real-time systems, all in the context of computational logic.
- *The Department of Teleinformatics, KTH, and the Formal Design Techniques Group at SICS* The research is directed towards mathematically rigorous techniques for ensuring correctness of distributed system designs. These techniques include design formalisms, analysis methods, and synthesis procedures and spans over theoretical foundations as well as automated tools. The focus is on methods using paradigms from process algebra and modal and temporal logics; key application areas include design of telephony systems (switches, networks and services) and high-speed protocols.
- *The Intelligent Systems Laboratory at SICS* The goal of the groups is to develop methods and tools for complex, symbolic computational tasks in domains such as design, planning, and resource allocation. This includes the necessary implementation techniques and program analysis methods, as well as applications demonstrating the practical advantages of the technologies. Algorithms for constraint solving and for solving combinatorial and optimization problems are a central topic.

5.1 Industrial Partners

The industrial partners of ASTEC are listed below, together with some areas of interest which are important for the involvement in ASTEC

- *Ericsson Radio Systems AB, Kista*, (ERA): Equipment for Cellular phone systems – optimization of design and installation (ERA have completed their involvement in ASTEC as of 97-08).
- *Ericsson Telecom Systems AB, Älvsjö*, (ETX): Public networks and datacom networks, in principle the fixed network whilst ERA handles mobile networks. (have joined as of September 1997)
- *IAR Systems AB*: The company is an international software tools development company with its main office in Uppsala, Sweden.
- *Prover Technology AB* (prior to 98-01, the company was named as NP technology AB and in the report, we use its current name): Tools and support for formal verification of safety-critical software.
- *Mecel AB*: Design of and software development for control and information systems in cars.
- *Rational Software Scandinavia AB* (a subsidiary to Rational Software Corporation): automation of and support for component-based development of software throughout the software life-cycle. Rational Software takes active part in the international standardization of object-oriented techniques e.g., within OMG.
- *Telia AB*: Development of services for the public telephone system.

6 Personnel

Personnel that are active within the center at the end of Phase 1 are shown in the below two tables.

Academic Staff

Name	Affiliation	Category	Amount	Projects
Dirk Auchter	UU	Ph.D. student	80%	VassCo
Johan Bengtsson	UU	Ph.D. student	12%	RT
Roland Bol	UU	Senior	50%	ARENA/VassCo
Mats Carlsson	SICS	Senior	50% until 9708	VOCAL
Mads Dam	SICS	Senior	50%	ErlVer
Jakob Engblom	UU/IAR	Ph.D. student	50%	WCET/WPO
Andreas Ermedahl	UU	Ph.D. student	80%	WCET
Lars-åke Fredlund	SICS	Ph.D. student	75%	ErlVer
Dilian Gurov	SICS	Post Doc	75%	ErlVer
Jan Gustafsson	UU/MDH	Ph.D. student	50%	WCET
Hans Hansson	UU	Senior	32%	WCET/AUTO
Erik Johansson	UU	Ph.D. student.	80%	HIPE
Bengt Jonsson	UU	Prof.	50%	Management
Helena Petterson	UU	Economic Adm.	10%	Management
Christer Jonsson	UU	Res. Eng.	100%	HIPE
Thomas Lindgren	UU	Senior	60%	HIPE/WPO
Olof Lindroth	UU	M.Sc. Stud.	100%	HIPE
Joachim Parrow	KTH/UU	Prof.	25%	BOOM
Paul Pettersson	UU	Ph.D.student	50%	AUTO
Jan Sjödin	UU	Ph.D. student.	80%	WPO
Wang Yi	UU	Senior	12%	AUTO
Gunnar Övergaard	KTH	Ph.D. student	80%	BOOM

Here MDH refers to Mälardalen University in Västerås.

Industrial Staff

Name	Company	Amount	Projects
Thomas Aarts	ETX	50%	ErlVer
Parosh Abdulla	Prover Technology	45%	Validation & Verification
Anders Berg	IAR	10%	WPO
Arne Borälv	Prover Technology	20%	VassCo
Jan-Erik Dahlin	IAR	5%	WPO
Jakob Engblom	UU/IAR	50%	WCET/WPO
Tomas Grelsson	Telia	20%	ARENA
Sten Hellström	Mecel	5%	RT
Olle Landström	IAR	5%	RT
Sven Larsson	Mecel	1%	RT
Anders Lindgren	IAR	1%	WPO
Magnus Lindahl	Mecel	22%	Auto
Anders Lundqvist	Mecel	1%	Auto
Lars Magnusson	Mecel	1%	RT
Karin Olsson	Mecel	1%	BOOM
Karin Palmqvist	Rational	1%	BOOM
Anders Pikas	IAR	4%	WCET
Carl von Platen	IAR	5%	WPO
Mikael Strömberg	Mecel	16%	AUTO

6.1 Mobility of Personnel

- Several Ph.D. level students have during phase 1 been employed by both academia and industry:
  - Dirk Auchter
  - Arne Borälv
  - Greger Ottosson
  - Gunnar Övergaard
- Currently, the center employs one industrial Ph.D. student (industridoktorand), Jakob Engblom, who is employed by both IAR systems and the Department of Computer Systems, Uppsala University.
- Some senior researchers are employed by both academia and industry:
  - Håkan Millroth is employed by ETX, but has a position as Adjunct professor at the Computing Science Department at Uppsala University
  - Parosh Abdulla is employed both as lecturer at the Department of Computer Systems, and part time at Prover Technology AB.

7 Management, Organization and Internal Working

Management

The management is structured as follows:

- ASTEC activities are controlled by a board. The board has consisted of 5 ordinary members, of which 3 are from industry and 2 are from academia. The board has conducted 13 meetings during the first 28 months. Birger Wörkvist from Telia AB has been chairman until 97-03, succeeded by the current chairman Bjarne Däcker, Ericsson Telecom.
- The director is responsible for daily coordination. Professor Bengt Jonsson has been director during the period.
- Project management is conducted by the project coordinators.
- Within each program area, a *program area coordinator* is responsible for synchronizing research efforts e.g. by conducting mini-workshops and seminars.
- An international advisory board with 3 members will review planning and progress of ASTEC work.

Organization

ASTEC is hosted by UU. Research activities are spread over Uppsala, Stockholm, and Göteborg (Mecel AB). All project coordinators (also those at KTH and SICS) have some connection with Uppsala University.

Within UU, ASTEC is a separate financial unit, hosted by the Department of Computer Systems (DoCS). All personnel involved in ASTEC are employed by the participating departments.

Meetings

- 4 one-day seminars on topics central to ASTEC have been conducted.
- ASTEC has co-organized FTRTFT96: 4th international school and symposium on formal techniques in real-time and fault tolerant systems in Uppsala, Sept. 1996.
- Program area workshop series are conducted within the areas *Validation and Verification* and *Programming Languages and Implementation*, twice per year.
- Since 97-10, several meetings have been conducted to discuss how ASTEC can contribute to the industrial partners, e.g. by initiating new projects or by forming new links with other partners.

- More than 100 project meetings have been conducted with participants from academia and industry.
- In collaboration with ARTES, a network for Real-Time research and graduate education in Sweden funded by SSF, a national graduate course "Modelling and Analysis of Real-Time Systems" has been developed and given. We expect more course development in other program areas of ASTEC.

Contracts

The following contracts have been established for ASTEC.

1. The original contract between the 6 industrial partners, NUTEK, and UU.
2. Contracts regulating the relationship between UU, KTH and SICS
3. Contracts between UU and individual researchers
4. Contracts between KTH and individual researchers
5. Agreements have been set up between ASTEC and some of the industrial partners regarding immaterial rights to "background" material.

8 International Collaborations

ASTEC has not itself set up formalized collaboration with other centers. The participating research groups have very good international contacts. The advisory board provides an international exposure of ASTEC work. Two examples of ASTEC-related contacts with other centers are:

- Exchange of ideas with ORKEST, Research on Requirements for the Construction of Embedded Systems. The project is coordinated by Hollandse Signaal B.V., which is known mainly for its advanced defense systems.
- Several ASTEC projects have strong contacts with VERIMAG, Grenoble, France, e.g., the VassCo project which is closely tied to to the Esprit project CRISYS (critical instrumentation and control system) coordinated by VERIMAG. A more systematic collaboration is under discussion.

The following post-docs have been working withing ASTEC:

- Peter Altenbernd (from Univ. Paderborn), 6 months, 1997.
- Dilian Gurov (now at SICS), since autumn 1997.
- Philippas Tsigas (also at Chalmers), autumn 1997.

9 Effects for Companies

We will here give an overview of the general effects within companies as a result of the ASTEC collaboration. Effects can be categorized into the following types:

- The ASTEC center has made it possible for companies to perform explorative research on how their current technology can be enhanced, in a cost-effective way. A few concrete examples of such explorative research are
  - Prover Technology's exploration of finite domain constraint solving (NP(FD)) as a technique in their tools
  - IAR Systems' ongoing efforts (with UU) on adding execution time analysis as a functionality to their products.
- Within ASTEC, it has been possible to evaluate new technology for industrial problems by carrying out case studies. A few examples are:
  - ERA has been able to explore the use of constraint solving techniques for their application problems (frequency allocation in mobile telephone networks).
  - Mecel AB has been able to evaluate the use of formal modeling and verification on their system development.
- The ASTEC work has not yet resulted in products or part of products. However, several examples of integration of techniques from academia into commercial tools is under way: examples are enhanced functionality in compilers for embedded systems (timing analysis), and more efficient techniques for compilation of high-level languages.
- Several companies have, as a result of the ASTEC collaboration, been able to recruit competent M.Sc. and in some cases Ph.D. students from the academic partners.
- The research co-operation within ASTEC can be used to point out, in business relations, that a company is seriously participating on pre-competitive research and development. An example is a newly established co-operation between IAR Systems and a major customer concerning development of customer-specific development tools. One of the main reasons being the close research co-operation. business area where we see a lot of future possibilities.
- An effect of participating in ASTEC collaboration, e.g., in case studies, is that companies gain insight about the potential of formal and semi-formal development methods, which in several cases influences their general software development practice. As an example, one partner states that *The active work within ASTEC has influenced our present working methodology in an important project. We have been able to increase the knowledge of the "real" difficulties in developing cost-efficient real-time systems.*

10 Effects within Academia

We regard the following aspects as the most important effects of ASTEC work, as seen from academia.

- We have built up new research directions, motivated by the industrial problems brought by the ASTEC collaboration. These are:
  - *Optimizing compilation*, geared towards industrial problems. We aim to consolidate this research direction within ASTEC.
  - *Development of Software for Real-Time Systems*, in particular for automotive applications. ASTEC has been a main driving force behind developing a research group on this topic. A present development is that work is in progress on building a national mini-network for research on execution time analysis.
- A large portion of the research carried out in academia has adapted and focussed on languages and techniques that are currently used in industry. In other words, ASTEC has fulfilled its role of giving directions for academic research. The main examples of this are
  - the adaptation towards the language Erlang of research on compilation and on verification,
  - work on semantic foundations is focussed onto UML,

  Part of this trend is that researchers have obtained access to commercial software for research purposes. The main example of this is that academic researchers can obtain access to the C-compiler of IAR systems for research purposes.
- ASTEC has substantially improved collaboration between the participating research groups.
- New development of upper-level undergraduate/beginning graduate courses has started, within each of the three present technical program areas.

11 Scientific Production

This section contains a list of publications generated by ASTEC-work. Publications that are coauthored by researchers from both academia and industry (totally 8) are preceded by a star $*$.

Journal Publications

P. Altenbernd, H. Hansson
The Slack Method: A new method for static allocation of hard real-time tasks. *Real-Time Systems Journal*, to appear.

A. Ermedahl, H. Hansson and M. Sjödin. Response-Time Guarantees in ATM Networks. In *Proc. 18:th IEEE Real-Time Systems Symposium,* San Fransisco CA, December 1997, IEEE Society Press.

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

* H. Hansson, H. Lawson, M. Strömberg and S. Larsson. BASEMENT a distributed real-time architecture for vehicle applications *Real-Time Systems* 11:223-244

* H. Hansson, H. Lawson, O. Bridal, C. Eriksson, S. Larsson, H. Lönn and M. Strömberg. BASEMENT: An Architecture and Methodology for Distributed Automotive *IEEE Trans. on Computers* 46(9):1016-1027, Sept. 1997.

Conference Contributions

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

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

Mats Carlsson, Greger Ottosson, and Björn Carlson.
Towards an Open Finite Domain Solver.
In *Principles and Practice of Constraint Programming—CP96*, pages 531–532. Springer-Verlag LNCS 1118, 1996. Poster.

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

Jakob Engblom, Peter Altenbernd, Andreas Ermedahl,
Facilitating Worst-Case Execution Time Analysis For Optimized Code. *10th Euromicro Workshop on Real-Time Systems*; June 1998. Berlin.

M. Dam, L. Fredlund, and D. Gurov.
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, 1998

Lise Getoor, Greger Ottosson, Markus Fromherz, and Björn Carlson.
Effective redundant constraints for online scheduling.
In *Proceedings of the Fourteenth National Conference on Artificial Intelligence (AAAI '97* American Association for Artificial Intelligence, July 1997.

J. Gustafsson, A. Ermedahl.
Automatic derivation of path and loop annotations in object-oriented real-time programs.

In *Proc. 11th IEEE Int. Parallel Processing Symp.* April 1997, Geneva, Switzerland.

H. Hansson and M. Sjödin.
An Off-line Scheduler and System simulator for the BASEMENT Distributed Real-Time System. In *Proc. 20th IFAC/IFIP Workshop on Real-Time Programming* (WRTP'95), ed. P. Laplante and W. Halang, November, 1995.

Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi.
Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction. In *Proc. of the 18th IEEE Real-Time Systems Symposium*, pages 14-24. San Francisco, California, USA, 3-5 December 1997.

∗ Magnus Lindahl, Paul Pettersson, Wang Yi,
Formal Design and Analysis of a Gear Controller: an Industrial Case Study using UPPAAL. in B. Steffen ed. *Proc. TACAS '98, Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems*, April 1998, Lisbon Portugal,

Henrik Lönn and Paul Pettersson.
Formal Verification of a TDMA Protocol Start-Up Mechanism. In *Proceedings of 1997 IEEE Pacific Rim International Symposium on Fault-Tolerant Systems*, pages 235-242. Taipei, Taiwan, 15-16 December, 1997.

Greger Ottosson and Mikael Sjödin.
Worst-case execution time analysis for modern hardware architectures.
In *ACM SIGPLAN 1997 Workshop on Languages, Compilers, and Tools for Real-Time Systems (LCT-RTS'97* ACM, June 1997.

Gunnar Övergaard.
A Formal Approach to Relationships in the Unified Modeling Language.
To be published at the *Workshop on Precise Semantics for Software Modeling Techniques*, ISCE'98 in Kyoto, Japan, April 1998.

M.Sc. Theses

Dirk Auchter, 1997
From Requirements Engineering to Design: Combining the ARENA and SOMT Method.

Hans Börjesson, 1995.
Incorporating Worst Case Execution Time in a Commercial C-compiler.

Jakob Engblom 1997
Worst-Case Execution Time Analysis for Optimized Code.

Jens Larsson 1996
ScheduLite. A Fixed Priority Scheduling Analysis Tool.

ASTEC Technical Reports by number

1995.

1. Hans Börjesson,
   Incorporating Worst Case Execution Time in a Commercial C-compiler.

1996.

1. Jens Larsson,
   ScheduLite, A Fixed Priority Scheduling Analysis Tool.

2. * ARENA,
   Requirements Engineering and Formalisation in a Telecommunication Environment.

3. * ARENA,
   Applying and Evaluating the ARENA Methodology for Requirements Engineering.

4. Andreas Ermedahl, Jan Gustafsson,
   Redovisning av Studiecirkel/Kurs i Exekveringstidsanalys.

1997.

1. Greger Ottosson, Mikael Sjödin,
   Worst-Case Execution Time Analysis for Modern Hardware Architectures.

2. Jens Larsson,
   Information interface to the scheduling level of a hard real-time systems design model.

3. Jens Larsson,
   Fixed priority scheduling analysis of the powertrain management application example using the schedulite tool.

4. Andreas Ermedahl, Jan Gustafsson,
   Deriving Annotations for Tight Calculation of Execution Time.

5. Dirk Auchter,
   Tool Support for Requirements Engineering: Applying the ARENA Methodology.

6. Andreas Ermedahl, Jan Gustafsson,
   Realtidsindustrins syn på verktyg för exekveringstidsanalys.

7. Greger Ottosson, Mats Carlsson,
   Using Global Constraints for Frequency Allocation.

8. Lise Getoor, Greger Ottosson, Markus Fromherz, Björn Carlson,
   Effective Redundant Constraints for Online Scheduling.

9. * Magnus Lindahl, Paul Pettersson, Wang Yi,
   Formal Design and Analysis of a Gear Controller: an Industrial Case Study using UPPAAL.

10. * Dirk Auchter, Johan Blom, Roland Bol, Lars-åke Fredlund, Tomas Grelsson,
    Requirements Engineering in a Telecommunication Environment. (Replaces report 96/02)

11. Peter Altenbernd,
    Cross-Compiling Software Circuits to CHaRy.

12. Peter Altenbernd, Hans Hansson,
    The Slack Method: A new method for static allocation of hard real-time tasks.

13. Dirk Auchter,
    From Requirements Engineering to Design: Combining the ARENA and SOMT Method.

14. Andreas Ermedahl, Jan Gustafsson,
    Automatic derivation of path and loop annotations in object-oriented real-time programs. WPDRTS'97, WOORTS'97 and IPPS'97.

15. * Björn Carlson, Mats Carlsson, Gunnar Stålmark,
    NP(FD) A Proof System for Finite Domain Formulas.

16. Henrik Lönn, Paul Pettersson,
    Formal Verification of a TDMA Protocol Start-Up Mechanism

1998.

1. Jakob Engblom,
   Worst-Case Execution Time Analysis for Optimized Code. MSc thesis.

2. Jakob Engblom, Peter Altenbernd, Andreas Ermedahl,
   Facilitating Worst-Case Execution Time Analysis For Optimized Code

Other Internal Reports

Arndt Jonason,
A Result on the U_n Formulas.
Prover Technology AB, May 1996.

Gunnar Stålmarck,
The REDUCTIO Hardness of the U_n-formulas.
Prover Technology AB, 1996.

Arne Borälv,
Formal Representation of AMPL Programs Using an Automatic Translator.
Prover Technology AB, June 1996.

Mats Carlsson and Greger Ottosson,
Finite Domain Constraints in SICStus Prolog.