INFORMATION SOCIETY TECHNOLOGIES
(IST)
PROGRAMME

Contract for: Shared-cost RTD

Annex 1 – "Description of Work"

Project acronym: AMETIST
Project full title: Advanced Methods for Timed Systems
Proposal/Project no.: IST-2001-35304
Related to other Contract no.: none

Date of preparation of Annex 1 : March 6, 2002

Operative commencement date of the contract: the first day of the month after the last signature of the contracting parties

Contents

1 Project summary

The AMETIST project will develop a powerful methodology supported by efficient computerised problem-solving tools for the *modelling* and *analysis* of *complex, distributed real-time systems*. In particular, the project will address the problems in connection with *time-dependent behaviour* and *(distributed, dynamic) resource allocation*. Problems of this type are manifested under different names in application domains such as *manufacturing*, *transport*, *communication networks* and *real-time software* and are treated using theories and methods currently scattered around many disciplines. All of these applications involve distributed, reactive systems of considerable complexity. The consortium will develop a unifying *mathematical framework* for modelling and analysing these phenomena by extending and refining the existing body of theory and tools for the so-called timed automata model, which has emerged as a very promising formalism for the modelling and analysis of real-time related phenomena. The consortium will develop algorithms for the analysis of models based on the timed automata paradigm and test their applicability on *complex* industrial case-studies and benchmarks. The outcome of this project will be a significant contribution to the problem-solving tool-box of system designers in numerous application domains. The new methodology and techniques will help them in designing more efficient, safe and flexible systems that can operate in uncertain environments. Thus the project will initiate first steps in the development of an emerging discipline, *computer-aided timing analysis and design*.

2 Project objective

The objective of AMETIST is to explore timed automata as a preferred formalism for describing and solving timing-related problems. To this end the consortium will extend the timed automaton framework (theory, methodology and tools) both in terms of expressivity and in terms of performance. The consortium intends to move this framework from the current stage of an academic proof of concept to that of a methodologically sound prototype that provides a starting point for further industrial development. This should provide an excellent opportunity for tangible practical results in the medium term.

This objective is realised by the development of a unifying *mathematical modelling framework* that has the following attractive features: 1) It is sufficiently expressive to describe the essential aspects of time-dependent real-life problems in a variety of application domains; 2) It provides for models with well-defined and clear dynamic semantics; 3) These models are amenable to computer-aided analysis methods such as *simulation, verification, optimisation* and *controller synthesis*. This leads to the following subgoals:

1. Extension of the timed automata paradigm in terms of *expressiveness*,
2. Development of effective *analysis methods* for these models, and implementing them as prototype *modelling* and *analysis tools*,
3. Application of this framework to several representative (and thus complex) industrial *case studies*.

These subgoals are elaborated below.

Approach

Modelling: Work on modelling real-time software, communication protocols, digital circuits and manufacturing plants using timed automata has been reported extensively in the literature. The ability to model such a diverse class of phenomena adequately using basically the same type of mathematical object is an indication for the genericity of the latter. This fact will guarantee a significant return on the investment in the theory and practice of timed systems, especially on the

algorithmic side. In the project the modelling activity will serve to extend the application scope of the timed automata family of models, both in terms of expressiveness and complexity. As part of this activity the consortium will develop suitable models for its set of case studies and problems. This will not only produce motivated extensions and modifications of the basic model, but also generate methodological knowledge on how to model a great diversity of phenomena in terms of timed automata.

The basic phenomenon that the consortium wants to model is that of time-sensitive planning and scheduling problems in the presence of various types of *uncertainty*. A first task here is to classify fundamental properties of the types of (extended) timed automata which are used to model each of these situations. In order for the approach to scale up, it is vital that the structure in the timed automaton models is exploited. The consortium therefore also will develop a compositional modeling methodology for large-scale distributed systems. Other extensions that the consortium will work on are the association of cost functions to automaton runs in order to make optimisation meaningful, and combining the *qualitative* treatment of temporal uncertainty by timed automata with the *quantitative* approach used in other formalisms for performance evaluation such as continuous time Markov chains. The application of a control synthesis paradigm provides a basis for modelling, and thus designing scheduling algorithms. In fact, a scheduler can be considered as a controller that resolves conflicts between the choices concerning future actions so as to satisfy certain constraints. Although the application of the control synthesis paradigm may not lead to practical results directly, the consortium believes that this fundamental way of looking at scheduling problems deserves proper attention.

Analysis and Tools: Under this title all the methods, algorithms and prototype tools are included for using these timed models in the design and validation of systems. This includes performance improvements and new algorithms for existing TA analysis problems (heuristics and guided search, distributed state-space exploration, partial-order methods, approximation techniques) in order to cope with industrial-size systems, development of algorithms adapted to the new models (adapting controller synthesis algorithms to situations of scheduling under uncertainty). These algorithms will be supported by efficient data-structures and software libraries for manipulating combinations of *logical* and *temporal* constraints.

These developments will be implemented as prototype add-ons to existing tools for the analysis of timed models. Those will include front-ends for efficient translation from high-level input languages, closer to the application domains, into a timed automaton models to which all algorithms can be applied. Prototypes of these tools will be distributed publicly in order to receive feedback from potential users.

Case Studies: The consortium will drive the project activities by four challenging application case studies supplied by the industrial partners. Two of the case-studies involve resource allocation in manufacturing (smart card production and value chain management) and the two others deal with resources in real-time computer control systems (memory management for radar sensor data and an automotive application). These case studies will provide important input for the modelling activities and will serve as benchmarks for the analysis methods and tools developed in the project, serving as feasibility tests for the whole proposed methodology.

3 Participant list

Role	*No*	*Name*	*Short name*	*Country*	*Enter*	*Exit*
C	1	Katholieke Universiteit Nijmegen	KUN	NL	start of project	end of project
A	2	Robert Bosch GmbH	Bosch	D	start of project	end of project
A	3	Cybernetix Recherche	CYR	F	start of project	end of project
A	4	Axxom Software AG	Axxom	D	start of project	end of project
A	5	Terma A/S	Terma	DK	start of project	end of project
P	6	Aalborg University	AAU	DK	start of project	end of project
P	7	Universität Dortmund	Uni DO	D	start of project	end of project
P	8	VERIMAG	VERIMAG	F	start of project	end of project
A	9	Weizmann Institute of Science	WIS	IL	start of project	end of project
P	10	Laboratoire d'Informatique Fondamentale de Marseille	LIF	F	start of project	end of project
P	11	University of Twente	UT	NL	start of project	end of project

VERIMAG is a public research lab, supported by the scientific University of Grenoble (UJF), the National Research Center (CNRS) and Grenoble Polytechnical Institut (INPG). Formally, not VERIMAG but the three supporting institutes are partners in the AMETIST project. Whenever this annex refers to VERIMAG as a contractor, actually the supporting institutes are meant.

Similarly, the Laboratoire d'Informatique Fondamentale (LIF) de Marseille is supported by CNRS, the Université de la Méditerranée (UII), and the Université de Provence (UP). Again, formally, not LIF but the three supporting institutes are partners in AMETIST, and whenever this annex refers to VERIMAG as a contractor, actually the supporting institutes are meant.

4 Contribution to programme/key action objectives

The problems of time-dependent behaviour in general, and dynamic resource allocation in particular, pervade many aspects of modern life. The computer-aided timing technology that the consortium will develop can contribute to domains ranging from the reliability and efficient use of communication resources in a telecommunication network to the allocation of tracks in a continental railway network, from scheduling the usage of computational resources on a chip for durations of nano-seconds to the weekly, monthly or longer-range reactive planning in a factory or a value chain.

The timed automata paradigm provides a key technology for the model-based design and analysis of all sorts of embedded systems. In particular, the state-of-the-art of application of tools for timed automata is very promising, with notable applications to verification (and debugging) of industrial real-time communication protocols and control programs, and applications to sequencing and resource allocation problems. These tool developments and applications have to a large extent been conducted by members of the consortium in previous EU and national projects. Timed automata also seems to provide an interesting middle-ground between purely finite-state systems and general hybrid systems: there are at present no tools or techniques available for the analysis

of systems with general continuous dynamics of more than toy size, whereas there are such tools available if the dynamics are abstracted to timed automata.

The project will develop a *unifying* framework for dealing with real-time problems in the timed automata paradigm. This will not only lead to scientific innovation and the development of new tools, but will also address methodological issues such as best modelling and analysis practices for real-time systems, which will be laid down in pragmatic "how-to" guides and cookbooks. This will have benefits for European industries in terms of a reduced training effort for real-time system designers and more widely applied and standardised tools. The techniques of the project can lead to better design and more reliable operation of transportation, communication, control and manufacturing systems, a better utilisation of their resources over time, and hence to cheaper products and more timely service for their end users.

Most of the project is naturally situated within Key Action IV, *Essential Technologies and Infrastructures*, especially the action line:

- IV.2.1 Real time distributed systems: *"... models, technologies and tools for sharing and interactive use in real time of applications and resources... novel scientific and technological concepts, algorithms, methods and tools for the design implementation, validation/verification, testing and integration of robust and fault tolerant, distributed, real time controls for complex uncertain systems"*

The formulation of this action line fits the description of the AMETIST project very well, and its last part (item (iii) of the text of WP2001) could in fact be seen as an abstract description of the project. The consortium believes that the timed automaton paradigm provides the most fitting theoretical context in which these ambitions can be brought to realisation.

5 Innovation

The potential of timed automata for the modelling and analysis of real-time problems has been documented extensively in the literature, see for instance [9, 5]. Since their introduction by Alur and Dill [2] in 1990, several verification tools for timed automata have been developed. Due to use of clever data structures, compositionality techniques, heuristics, etc., there has been an enormous increase in the performance of these tools over the years, and they are now applied routinely to industrial case studies.

Recently, there has been much interest in the application of timed automata tools and techniques to scheduling and planning problems, see for instance [7, 11, 3, 4, 1, 10, 8]. Even though only rudimentary prototypes were used for the experiments carried out in these papers, the performance in some cases was competitive on some standard benchmarks taken from the literature on combinatorial optimisation (for instance, job shop problems in [1] and airplane landing problems in [10]).

Scientifically it is exciting to aim at integration of timed automata model checking with ideas from the field of combinatorial optimisation (such as branch-and-bound, MILP, etc). In order to achieve this scientific goal, the consortium thinks it will be very helpful to tackle complex practical problems that have not been treated satisfactorily thus far.

From the perspective of timed model checking, this integration will lead to increased efficiency of the tools. Some constraint manipulation takes place in timed model checking (for instance, when a DBM is brought into normal form) but there is much room for improvement there. Also, when state space models are too big to be searched completely (and there is no way to reduce the size automatically or with assistance of the modeller) branch-and-bound techniques allow one to cleverly search for errors by exploring carefully selected parts of the state space. From the perspective of scheduling, major advantages of an integration will be the availability of some very natural and powerful (state based) modelling primitives, as well as a host of verification techniques that have been developed by the model checking community to fight the state space explosion problem.

Below the major ingredients of the innovations that will be achieved by the consortium are worked out in some more detail.

5.1 Time-dependent Behaviours: State-Space Models

A lot of the success in discrete verification and in control theory is due to *state-space* based models of their underlying dynamical systems. Verification is based on transition systems models such as automata while control theory is based on continuous dynamical systems where state-variables evolve according to differential equation. Such system models where the values of state variables determine the possible future evolutions have a tremendous, positive effect on the understanding of system dynamics. The phenomena that the consortium wants to treat cannot benefit from these two classes of models as they are: purely-discrete models are too poor and continuous models are too detailed (for the purpose of solving a scheduling problem there is no use in modelling the process of executing a production step using differential equations). The timed models that the consortium will use are the ideal candidate for *filling this modelling gap*. They enrich discrete models with additional state-variables, the clocks, which encode into a state exactly the information necessary to determine the future: each clock represents the *time* that has elapsed since the occurrence of a certain past event upon which the future depends.

In contrast, many approaches to timing problems, such as those used in operation research, AI or performance modelling, are not always based on such a rich dynamical model, but rather on formulating and solving static optimisation problems whose relation with the underlying dynamics is sometimes obscured. Such an approach is sometimes very successful in solving particular problems efficiently, but their ad-hoc nature can prevent their reusability. The consortium strongly believe that if computer-aided timing analysis and design is to become a mature discipline, its problem solving approach should be based on modelling problems faithfully by a clean semantic model, and *not* in terms of the specific technique used to solve them. Such an approach makes the computational difficulty of the original problem explicit and allows much more freedom later in choosing the solution method that gives the best trade-off between its computational complexity and the quality of the solution it provides.

Another advantage of the automaton-based approach is that it enables the user to formulate, in a very natural fashion, distributed systems comprising of small interacting sub-systems, using parallel and/or hierarchical composition operators. In other approaches one does not have such intuitive notions of communicating sub-systems to solve such problems, but rather a very large number of equations and inequalities in which the dynamical and compositional aspects are not made explicit.

5.2 Verification: From Untimed to Timed and from Safety to Performance

Verification methodology had a lot of success during the last decade due to verification tools that can predict the behaviours of complex discrete systems such as digital circuits and communication protocols. Many models used in this methodology are purely discrete and their treatment of time is purely qualitative, that is, behaviours are just sequences of events appearing one after the other but without any quantitative timing information about the duration of actions and the time between events. Timed models, such as the ones the consortium will employ, provide for a more detailed level of modelling and incur, because of this a considerable computational overhead associated with the treatment of clocks. It is fair to say that, although already quite a number of successful applications of timed automata have been reported, most applications do not go beyond the stage of a proof of concept. The concentrated effort of the project to improve the methodology and algorithmics of timing analysis could lead to a significant progress in this domain, similar, perhaps, to the introduction of symbolic techniques in discrete verification. Another dimension of innovation with respect to standard verification is the evaluation of behaviours in terms of *quantitative* properties of (timed) behaviour, such as e.g. elapsed time, i.e. a judgement in terms

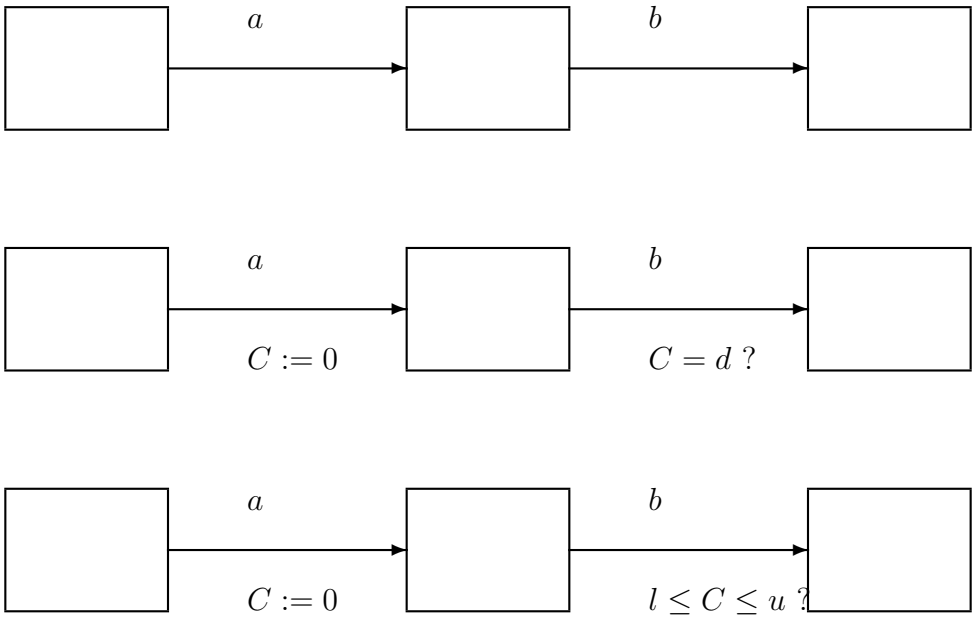

Figure 1: Refining an untimed system description to a timed one. In the untimed automaton a is followed by b, while in the timed automaton the distance between the two events is d. Uncertainty in the duration is modeled using a non-deterministic automaton in which a transition can be taken anywhere in the interval $[l, u]$.

of *performance* rather than the traditional classification into "good" and "bad" behaviours.

5.3 Scheduling: Certainty vs. Uncertainty

Classical models for scheduling in manufacturing such as the job-shop problem, are somewhat detached from industrial practices. They assume that the duration of every step as well as the arrival times are fixed and known with certainty. In practice, it is rarely the case that a schedule is executed as planned. The problem of coping with uncertainty is identified (by providers of scheduling tools and by their clients) as one of the major problems in the domain. There have been various attempts to model and solve such problems, but no unified approach has emerged. Using non-deterministic timed automata with controlled and uncontrolled transitions (for representing the uncertainty coming from the plant) one can model a large class of such problems, and provide efficient off-line algorithms for synthesising reactive schedulers. Such algorithms can plan for the best, worst or average case, but the scheduling strategies they produce are *adaptive* and can take advantage, for example, of the fact that a task has terminated before it was expected, and use the new empty time slot. The models the consortium will build can serve in the future as the reference models for a large class of problems.

It is worth noting that inasmuch as manufacturing scheduling models are too static compared to the reality, in real-time operating systems one observes an opposite phenomenon: problems that could be solved statically (scheduling of periodic tasks) are solved using dynamic priority-based policies that add a lot of unnecessary overhead to the system. The rigorous modelling and analysis effort of the project will clarify these issues and classify systems according to the policies that are useful for them.

5.4 Uncertainty: Quantitative vs. Qualitative

Due to historical reasons, most uncertain phenomena in system behaviour are treated probabilistically. For example in the theory of queuing systems, it is often assumed that the inter-arrival times and service times of clients are random variables. In this setting, an optimal scheduler is one which optimises the *expected value* of the performance over all possible behaviours. Under certain assumptions on the nature of the probabilistic processes analytical solutions can be found for such optimisation problems. Unfortunately, these assumptions are sometimes very restrictive, and unrealistic for many modern applications. Without them numerical solutions can be devised, but their complexity can be very high, making them often also unsuitable for the treatment of large systems. Timed automata suggest an alternative formulation for temporal uncertainty: instead of specifying a probability distribution on durations only upper- and lower-bounds are given, see Figure 1 for a small example. From these models, policies can be derived which are optimal with respect to optimistic or pessimistic or average estimates, but which are nevertheless guaranteed to function for all cases. Because of the less involved model, the consortium hopes that the computational difficulty of deriving such policies can be smaller than in the probabilistic framework. The consortium intends to find out under what conditions such benefits would materialise.

Even so, the potential of the above nondeterministic approach over stochastic methods must be weighed against the advantages of stochastic modelling in other cases. It is well-known that stochastic models can sometimes be based on gross simplifications of the functional architecture of a system without significant loss of accuracy. Both approaches, therefore, offer interesting and potentially powerful abstraction principles. The consortium intends to study the connections between the two approaches and compare their relative merits in typical application domains.

5.5 Distributed Decision Making: Rigorous Models

Building dedicated production units to produce special products for well-defined markets is not always an economically viable approach. Instead, the overall production chain may be fragmented, and distributed over many production sites, where each subprocess is executed where it is done most economically. This leads to tremendous coordination problems which are dealt with under the heading of *supply* or *value chain management*.

In such production networks, it is not feasible to perform resource allocation in a centralised fashion. Besides the unmanageable combinatorial complexity, a central issue is that the transfer of information between subprocesses exchange is typically limited (e.g. their owners may be competitors). Thus, local decision making algorithms are used that reflect partial goals and priorities. The effect of the types and the parameters of the local allocation strategies on the performance of the coupled production chains is hard to assess intuitively. The distributed nature of the allocation algorithms and the processes calls for a modular, compositional model which can serve as a basis for simulation, performance analysis and optimisation.

Automata-based approaches carry a large potential for such applications because of their ability to model the local phenomena in a transparent and modular fashion, and the availability of tools which can be used to analyse even relatively large, interconnected systems built from such blocks. The treatment of uncertainty by intervals for the required time and resources is very attractive, because usually no precise models or extensive data from the past are available to estimate parameters accurately. The overall system must thus be robust against variations of the effectivity of the processes involved. A promising concept for the application of the timed automata paradigm is that of a *contract net*. The contract net models transfer of control in a distributed system using the metaphor of negotiation among autonomous intelligent entities. The net consists of a set of automata that negotiate with one another through a set of messages and a 'blackboard'.

The consortium will develop rigorous models for the description and analysis of such distributed decision making processes based on the timed automaton framework in combination with available application-oriented concepts, like that of contract nets.

5.6 Comparison to Related EU Projects

- Esprit LTR project 26270 VHS (Verification of hybrid system).
  The AMETIST project is a successor of VHS (1998-2001), where the suitability of timed automata for modeling and solving planning problems in manufacturing was first observed and exploited in some case-studies [8]. AMETIST aims to extend the techniques developed in VHS and broaden their scope in order to solve larger and richer problems.

- IST-2001-33520 CC (Computation and Control in Hybrid Systems)
  The CC project, which is another successor of VHS, focuses on the real hybrid aspects that manifest themselves at a level of abstraction closer to the physical world and, hence, requires more interaction with continuous control theory. While both CC and AMETIST are eventually interested in the design of correct and efficient systems, the models and techniques are quite different: CC intends to develop novel exploratory techniques for treating hybrid automata (automata with differential equations). AMETIST works within the more mature and better understood framework of timed automata where the major challenge is to scale-up existing results. This difference is also seen in the structure of the consortia: CC consists mostly of control engineers and AMETIST of computer scientists.

- IST 2001-32460 Hybridge (Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time System Design)
  The objective of Hybridge is to develop a methodology to embed control system designs for safety critical operations within sound safety management systems such that the level of safety stays under control of humans. Like with CC, a difference is that whereas Hybridge studies truly hybrid control systems, AMETIST takes the somewhat more abstract setting of timed automata. Both Hybridge and AMETIST intend to extend existing models with stochastic techniques, but whereas in Hybridge the purpose is mainly to arrive at a stochastic analysis framework for accident risk modelling (with Air Traffic Management as the motivating application area), AMETIST studies stochastic techniques mainly to improve resource allocation heuristics.

- IST-2001-32141 Omega (Correct Development of Real-Time Embedded Systems in UML)

  The objective of this project is to define and study a UML-compatible methodology for the development of embedded and real-time systems which is based on formal techniques, and will be used to extend and improve commercially available tools.

  The consortium will seek contact with the Omega project, aiming to interface its tools with the UML tools that Omega develops.

- IST-1999-10069 AIT-WOODDES (Workshop for object oriented design and development of embedded systems)
  The aim of this project is to "improve the design process to allow an efficient development of high quality real time embedded systems". The main focus is on the definition of an appropriate UML profile and method for the development of real-time embedded systems. This is accompanied by some tool support demonstrating the benefits of formal methods within the design process. The research focus in AIT-WOODDES is in exchange formats and RT profile for UML. Only at a much smaller scale verification is addressed. The work within AMETIST on exploiting hierarchical structure supplements nicely the work in AIT-WOODDES.

6 Community added value and contribution to EU policies

The AMETIST project aims to develop a powerful modeling methodology supported by efficient computerised problem-solving tools for the *modeling* and *analysis* of *complex, distributed real-time systems*, notably for distributed resource allocation. Application domains include a wide spectrum,

from *manufacturing*, *transport*, *communication networks*, *real-time software* and *digital circuits*. All of these are fields with a strong international competition. Moreover, these are domains where the markets are either already international or — as is the case for traditionally conservative national markets in the engineering domain — are about to be transformed to multinational markets. Competitiveness both in research and in industry can no longer be expected to be achieved at a national level.

Indeed, previous experience of AMETIST partners in the context of the Esprit project VHS has shown that certain domains of manufacturing automation (programming) still favour national solutions. This causes friction in the opening European market: Nationally focussed methods (even national programming languages) and legislation oblige "exporting" manufacturers to adapt to national particularities. As this is often too expensive, these markets maintain a protectionism between individual European countries. This constitutes a weakness for the global competitiveness.

For the future development of key disciplines for engineering applications, therefore, it is essential to work at a European level. The tools of tomorrow are being developed by the researchers of today, most of whom contribute, as academic teachers, directly to the training of future generations of engineers and managers. In this way European consensus on the required directions and results of basic research in timing technology can contribute to a better understanding among future IT managers and engineers of the technical issues involved and available methods to address them.

There is a clear added value for multinational cooperation in the area of timing technology: the AMETIST consortium is composed of partners from several European countries with both common and complementary expertise in the area of Timing Technology that *cannot be found at this level in any single European country.*

- The three currently most active European research groups working on timed automata techniques are included in the consortium (F, DK, NL).
- Their competence is complemented by research groups from closely neighbouring research areas with interdisciplinary competence (F,DK,NL,IL,D).

Working research cooperations between all the partners in this consortium – notably on the basis of European projects – already exist out of necessity: They represent the state of the art in research on automatic timing analysis and closely related side disciplines and are highly competitive on a global level. The AMETIST project will provide the infrastructure for a continued and intensified cooperation. The cooperation of core timed automata research groups and interdisciplinary partners will provide the critical mass to extend the possibilities of automatic analysis of timed systems. Such progress is needed to maintain the world leadership of European research in algorithmic timing analysis for the years to come.

The multinational academic consortium is complemented by industrial partners from three European countries. The industrial partners chosen represent a balanced and, from the point of view of application areas, a complementary spectrum of potential users. Their views on the application of AMETIST technology represents some of the European variety in engineering. It will help to focus the research of the academic consortium members on the common needs of European industries rather than national particularities.

Conversely, the industrial partners and the internationally composed industrial end-user panel will be in an excellent position to absorb the unifying approach of the project. This will hopefully influence the course of future developments within these industries, and indirectly help European industry to converge in their use of advanced computer-aided timing analysis and design.

7 Contribution to Community social objectives

7.1 Quality of life and safety

Clearly, the quality of life of the Union's citizens has improved considerably due to the ongoing change from an industrial to an information-based society. In fact, this is what motivates the EU's Information Society Technologies (IST) Program. The main enabler of the Information Society is the use of software and hardware products developed by the computing community; its successful realisation is greatly dependent upon the quality of these products. Successful software development involves not only the application of good software engineering techniques, the use of modern programming practices, software design methodologies, and more reliable high-level languages, but also requires the use of advanced methods and tools to assure the quality of the software being developed.

The AMETIST project aims at providing such advanced methods and tools for the engineering of timed systems. During recent years, methods and tools based on the timed automata paradigm, as developed by members of the AMETIST consortium, have revealed subtle but catastrophic bugs in many real-time systems, and have helped to improve the quality of a large number of challenging industrial applications (a Bang & Olufsen Audio/Video Protocol, the IEEE 1394 Firewire root contention protocol, a prototype gearbox controller for vehicles by Mecel AB, a Philips audio control protocol, etc; we refer to `www.uppaal.com` and `www-verimag.imag.fr/TEMPORISE/kronos` for many other examples).

AMETIST will move the state-of-the-art to a new level of maturity, extending the scope of applicability of this technology to include distributed scheduling and planning problems, and leading it to numerous new application areas. Starting point will be the applications provided by the industrial partners in AMETIST, such as Bosch the radar system (Terma case study), and the *pre-crash detection* and *blind spot supervision* applications (Bosch case study). These applications clearly illustrate the link between the AMETIST research programme and issues that address the quality of life and safety of EU citizens.

7.2 Employment prospects

The EU summit in Lisbon of March 2000 emphasised the importance of the IT industry for the economic future of Europe. Indeed the remarkable growth in the nineties of the number of jobs in the US is largely due to the development of the American computer and software industry. AMETIST computer-aided analysis and design methods and tools will in the medium term contribute to the development of high-quality embedded systems. In this rapidly growing area European industry can obtain a significant advantage over their world-wide competitors by the integration of such advanced technology into their software process.

7.3 Preserving and/or enhancing the environment and minimum use of natural resources

An important application area of AMETIST technology will be real-time planning and scheduling problems, such as distributed resource allocation problems. In practice, the ability to solve these type of problems almost always leads to a reduced use of (natural) resources, and indirectly contributes to the preservation of the environment. As an example we mention one of the AMETIST industrial case studies: the smart card personalisation system. Here, AMETIST technology can be used to maximise the throughput of the manufacturing machines. As a consequence the energy consumption per produced smart card is reduced.

8 Economic development and S&T prospects

AMETIST will contribute to solutions for the growing industrial need to design reliable and efficient time dependent systems. In particular, it will provide theory and tools for error-detection, control and optimisation of real-time distributed systems. Its approach will be based on translating state-of-the-art academic research into methods and tools that can be a basis for an industrial design practice of such systems.

In addition to it technological contributions, AMETIST will work actively on knowledge transfer to the European industry of computer-aided timing analysis and design. Moreover, it is expected that the academic dissemination of the AMETIST research results will influence and advance the field of timed systems research, and (indirectly) contribute to the education of future generations of system engineers.

8.1 Towards industrial use

Whereas timed automata and the tools for their analysis are widely accepted in academia and are being used at hundreds of universities and research laboratories all around the world, they have yet to find their way into industry. The aim of AMETIST is to advance and mature the related models, tools, and methods to allow this situation to change.

The growing industrial interest in the use of finite state model checking can serve as a recent example of successful technology transfer in a closely related field. This technique is increasingly being used for the development of critical software and hardware in telecommunications and the design of electronic circuits. Industry is learning to appreciate the economic benefits of these methods for their business:

> "Model checking techniques help to find bugs in early design phases of integrated circuits and telecommunication devices. On the one hand, they thus help to speed up the development and decrease the time to market of these products. On the other hand, product bugs detected only after introduction into the market can be very costly."

The need for automatic tools that allow reasoning about time is evident. Beyond manufacturing, telecommunication and hardware, it is of essential importance for the growing market of embedded systems (from car electronics to home automation). However, there are several obstacles that seem to hinder the use of timed automata technology in industry at this time:

- Scalability: Currently, tools based on timed automata do not allow to handle big examples. There are industrial scale examples that have been treated with these tools but only after tedious manual simplification involving a lot of work in each case.
- Convenience: Current timed automata tools are stand-alone programs and their input formalisms lack important features for convenient specification in an industrial setting.
- Accessibility: To make optimal use of the currently available tools requires quite some sophistication on the user's part, which makes them practically inaccessible even to well-trained engineers.

The main thrust of AMETIST aims to improve this situation regarding scalability, by introducing better algorithms and data-structures to model and manipulate large systems, in particular in the area of real-time controller synthesis, planning and scheduling. Moreover, the project will work on tool interaction to allow the interfacing of different tools, which can help to improve usability. Finally, the integrated framework that will be a deliverable of AMETIST should be an excellent starting point for further work to improve the accessibility of computer-aided timing tools. If computer-aided timing analysis and design should become a standard technique in the development of timed systems, as intended by the AMETIST project, then this should lead to reduced development costs and improved quality control, in cheaper and more reliable products.

8.2 Industrial exploitation

Although AMETIST is primarily focussed on basic research on computer-aided timing analysis and design, is has a strong potential for industrial exploitation in the medium and long term. The industrial exploitation of AMETIST research will be furthered by three instruments:

1. **Direct interaction with industrial partners.**

   A principal role of the industrial partners in AMETIST is to provide challenges for the methods and tools under development in the form of representative case studies. At the same time they can familiarise themselves with AMETIST methods and tools. This interaction will lead to research results with an improved industrial relevance, as well as increased awareness and understanding of the potential of AMETIST technology for the individual industrial partners.

   Some of the case studies are, in fact, related to strategic products of the industrial partners, e.g., the smart card personalisation machine of Cybernetix and the Terma radar system. An intended result of these case studies will be an improved design for new product generations. In the case of Axxom the collaboration may lead to a direct integration of algorithms/components into their products and tools for the optimisation of value chains.

2. **Integrating framework and tool interaction.**

   AMETIST will integrate the results of its research into a coherent framework. This will make it easier for interested industrial parties to assess and absorb the advances made in computer-aided timing analysis and design. In addition, AMETIST will address the issue of tool interoperability. The time is not yet ripe for full integration of tools, as best practices in functionality and implementation have not yet crystallised due to the rapid changes that the field is experiencing. Moreover, such an implementation effort is well beyond the limitations of the project resources. Nevertheless, considerable attention can and will be paid to support common interfaces across the variety of tools that will play a role in this project. Such interface formats will help to combine functionalities of different tools, and will simplify their embedding in existing industrial design processes.

   The two most well-known timed automata tools are Kronos and Uppaal, maintained by the AMETIST partners Verimag and BRICS, respectively (these are not the only tools developed/maintained in the consortium, but are the most prominent ones for AMETIST). AMETIST research will help to advance these tools to include new features (new algorithms, alternative data structures, exchange formats) and improve their effective ranges of application. Since these tools are publicly available, their world-wide user communities will be able to apply and evaluate the new versions as they result from the AMETIST research effort. Given that these tools are also widely used in academic courses on real-time system design and validation, the educational impact can be considerable.

3. **End user panel.**

   In addition to the AMETIST industrial project partners, an industrial *end user panel* will be created as an important means for interaction with the industry at large. The panel will serve both as a dissemination channel for the project results and as a provider of feed-back on the development of the project. Panel members will participate in discussions on future directions within the project and will be kept informed about the developments as well as the technological perspective of the work.

   The panel will consist of representatives of companies that have expressed an interest in AMETIST (among others: ABB, ASML, LCN, Lucent, NLR, Siemens Mobile Phones, Siemens R&D) and have committed to participate in the yearly project meetings. In principle, this panel is an open forum and it is intended to attract more participants in the course of the project.

Complementary to the above activities standard scientific dissemination procedures will be followed. The concentrated effort of the AMETIST project is expected to effect significant progress in

the area of computer-aided timing analysis, with a substantial improvement of the current state of the art. This will manifest itself in scientific publications, workshops and tutorials. An AMETIST web site with a document and software repository, links to partner sites and related web sites, will also be part of the the project information and promotion activities.

As part of Workpackage 4, the AMETIST consortium will organise yearly workshops. Moreover, consortium members will be steering and programme committees members of leading international conferences related to AMETIST research topics. This will create ample opportunity to expose AMETIST and its results to the international scientific community, and will help to establish computer-aided timing analysis as a recognised discipline in the longer term.

9 Project workplan

9.1 General description

To achieve its aims, AMETIST will develop results in the following interdependent directions:

- **Modelling**
- **Analysis and Tools**
- **Case Studies**

The principal aim of the project is to advance the algorithmics and pragmatics of timing analysis and dynamic resource allocation toward industrial-scale applicability while maintaining a more general and less ad-hoc flavour. To this end the consortium will investigate several representative classes of time-related problems and see how they are modeled within the timed automata paradigm. This activity will constitute the **Modelling** workpackage (WP1).

Once the classes of models are defined, *algorithmic methods* will be developed for the control synthesis and validation problems that they pose. The analysis methods will include abstraction and compositional principles that can help to control the size and complexity of the models as well as improvements in the efficiency of existing algorithms. The development and the implementation of the above constitutes the **Analysis and Tools** workpackage (WP2).

The work in the previous workpackages will be driven by a number of industrial case-studies grouped under the **Case Studies** workpackage (WP3). These case-studies will influence the choice of models and algorithms and will serve as a final benchmark for the viability of the approach.

Apart from these three technical workpackages, there will also be workpackages related to **Project Management** (WP0) and **Dissemination** (WP4).

The AMETIST project will start on the basis of extended previous theoretical and practical experience of the consortium members, notably in the areas of algorithmics, tools and modelling with timed automata, constraint-based methods in scheduling and process control, and general experience in construction and verification of real-time systems. The implementations of the new algorithms will be based on an existing developed code basis for timed automata maintained by consortium members. Hence, it is possible to start working on all three technical workpackages at once. The description of these workpackages is elaborated in more detail below.

WP1 Modelling

This workpackage is intended to produce *classes* of models which are suitable for depicting real-life situations occurring in the application domains. This activity will be driven from above by the rich experience of the partners in modeling of discrete, real-time and hybrid systems for the purpose of verification, and from below by the case-studies provided by the industrial partners. The following tasks represent the main directions of research that will be needed to achieve the project goals.

T1.1: Model Classification

In this task the consortium will develop a methodology that will allow to classify resource allocation problems according to their required modeling features. Among the parameters that will be used in this classification one might find *system size* (number of tasks and resources, time horizon), *types of resources* (for example, in transportation systems where some of the resources are physical locations, the geometry should be taken into account; or in computer systems unlike steel plants, tasks can be preempted) *sources of uncertainty* (variations in arrival and duration times, breaking of machines, external inputs), *optimality criteria* (time, cost), *quantification of behaviours* (worst-case, expected, other), *computational constraints* (both on-line and off-line), etc.

This activity will go hand in hand with the work on the case-studies in WP3 and will culminate in a final report summarising the methodological recommendation for future users of timing technology.

T1.2: Model Composition

To model larger system and control problems effectively one needs various mechanisms for constructing systems from subsystems. In this task the consortium intends to see how important, well-understood compositional methods from various areas including process algebra, Statecharts (UML), I/O automata, etc. extend to control synthesis and validation problems in the timed automata setting. There are two major difficulties: the first is that in timed systems, time is a state variable common to all components and hence one has to be careful not to define composition operators that block the evolution of the system. The second obstacle is in the different "identity" of the components: if one adopts a game-theoretic view (as in Task 1.5 below), the question is which transitions are controllable (performed at the decision of the scheduler) and which reflect uncontrolled choices of the plant. These distinctions between transitions (including the passage of time) should be maintained by the composition operation.

Other compositionality related work, in particular, the ability to infer the behaviour of a composite system from that of its components, will be discussed in the analysis and tools workpackage.

T1.3: Quantitative Modelling

Traditionally, in verification models there have been no quantitative measures associated with system behaviours. However for the purpose of optimisation one needs to compare behaviours (or sets of behaviours) quantitatively in order to prefer one controller over the other. First steps in this direction have been done by consortium members who associated time duration and costs with the runs of a timed automaton. The consortium intends to investigate to what extent these models are suitable for the class of applications under consideration and whether they can be extended while maintaining the analysis tractable.

A more important quantitative aspect is manifested when one moves to stochastic models. In many situations real-time description of systems, their environments and requirements are given in stochastic rather than absolute terms. For example, in some cases the arrival times of new jobs may be best characterised by a certain probability distribution instead of a single, guaranteed maximal arrival time. Likewise, a system might be expected to miss deadlines in very a small probability, rather than not to miss it at all. Studying the functional correctness of such systems is very closely linked to performance analysis. For many modern applications, such as multi-media network protocols and more generally the class of "soft" real-time systems it is in fact impossible to separate functional correctness from performance in the form of guaranteed quality-of-service (QoS).

The purpose of this task is to study and develop stochastic extensions of the basic model of timed automata emphasising their specification and composition. The conceptual problems posed by this task are rather subtle because currently the semantics of timed automata consists of sets of continuous time behaviour, while in a stochastic setting the behaviour is a continuous time evolution of a probability distribution over the state-space as, for example in continuous-

time Markov chains. It is expected that the definition of a stochastic delay operator and its composition with logical elements will lead to models much richer than traditional models; it will be a significant challenge to develop tractable analysis methods for them.

T1.4: Scheduling and Planning

Scheduling and planning are subjects studied from different perspectives by the Operation Research (OR) and the Artificial Intelligence (AI) communities. Typically, OR models tend to reduce these problem to well-defined static optimisation problems to be solved by mathematical programming techniques. AI models emphasise complex logical structure and dynamic interactions between actions and pay less attention to quantitative aspects. The consortium will work toward establishing timed automata as a common denominator of the two approaches.

The AI community has developed a formalism called PDDL (Planner Domain Description Language) as a common language for defining benchamark problems on which different planning and scheduling algorithms can be evaluated. In this language one can define object-types (e.g. plane, city, person) together with a number of associated attributes (speed, capacity, location). The possible plans spanned by the domain are described by a number of parameterised actions, where the execution of an action-instance may depend on and affect the values of the attributes. Such a language allows richer semantic description than standard OR models and it turned out that algorithms based on verification techniques have very good performance on such problems.[1] Recently, in order to reinforce the quantitative aspects, an extension of PDDL, called PDDL+, has been defined, where actions are additionally equipped with constraints on durations. In this task the consortium will investigate translations from PDDL+ into the timed automata modelling framework in order to allow the timing analysis methods of AMETIST to be applied to benchmarks written in this language.[2]

From the OR side, the consortium will develop abstract timed automata models that add different types of uncertainty to classical *job-shop scheduling* models, which assume that all tasks are known in advance as well as their execution times. The consortium intend to build models that relax these assumptions gradually. In the first model the consortium will introduce uncertainty into the task duration, i.e. the duration of a step is only known to be inside an interval $[l, u]$. Such a simple modification in the model raises a lot of methodological questions. One approach is to assume some *nominal* future evolution (optimistic, pessimistic, etc.), find a schedule which is optimal with respect to this prediction, and re-compute a schedule whenever the actual execution deviates from the nominal path. A major disadvantage of this approach is in the need to perform costly computations on-line, that is, during the execution of the jobs. A question the consortium intends to investigate is whether some of the re-scheduling can be performed off-line using synthesis methods (see T1.5). After resolving these issues the consortium will proceed to more complicated models of uncertainty involving arrival and release time of jobs, preemption, breaking of machines, etc. For all of these models the consortium will formulate the corresponding algorithmic problems that need to be solved.

T1.5: Control Synthesis

So far, timed automata have been studied and successfully applied mainly to classical *verification* problems, i.e. to check that a timed automaton satisfies a given logical requirement or to establish behavioural equivalences between timed automata. The class of problems to be treated in this project calls rather for *synthesis* problems: find a (dynamic) scheduler that achieves certain performance. Representing control problems in this framework leads to equation solving problems: the controller (i.e. the dynamic scheduler) appears as the unknown component that composed with the uncontrolled behaviour yields the desired behaviour. Using another terminology, the

[1] E.g.: in 2000, the BDD-based tool MIPS by Stefan Edelkamp and Malte Helmert, Freiburg University, was awarded for "Distinguished Performance" at the yearly AI conference on planning and scheduling (AIPS).

[2] A similar formalism is currently being used at NASA Ames research center for specifying plans for space craft missions.

interaction between the scheduler and the rest of the system can be viewed as a two-player game where a winning strategy determines a scheduler which achieves the best possible results in the presence of uncontrolled uncertainty.

It has already been shown by members of the consortium that the controller synthesis problem can be posed and solved, in principle, for arbitrary timed automata. However there are many aspects which are specific to scheduling and resource allocation problems which need to be explored. In particular, finding a meaningful way to compare schedulers by criteria other than their worst-case performance is needed in order to evaluate solutions for the problem of job-shop under uncertainty. Other problems to be investigated are related to adapting control synthesis to distributed decision making situations where decisions should be based on partial information. Such problems have been treated in the past in the context of (untimed) discrete event systems but the problem they raise in timed systems are more difficult, for example, what information does one "agent", modeled as a timed automaton, know about the clock values of another agent, and whether it can use auxiliary clocks in order to infer the missing information.

WP2 Analysis and Tools

This workpackage is concerned with the algorithmic basis of distributed timed systems: Basic algorithms for analysis and synthesis of timed systems, data structures and heuristics. The choice for timed automata as a basic model motivated by the fact that – while being quite expressive – the reachability, model checking and synthesis problems are known to be decidable (most often PSPACE-complete). The challenge however is to adapt and to improve the algorithms so as to deal with big systems. The traditional approach currently implemented in the major tools suffers from the state explosion problem arising from analysis or synthesis of big composed systems. The tasks in this workpackage represent several working directions which the consortium will explore in parallel to be able to cope with realistic big systems in spite of the generally high complexity. To experimentally evaluate the practical usefulness of techniques that are developed, substantial effort will be made in constructing prototype tools.

T2.1: Abstraction, Compositionality, and Structure Exploitation

In this task the consortium will study the application of abstraction, compositionality and structure exploitation as key techniques in controlling and reducing the complexity involved in analysing real-time system models.

Abstraction and Composition are well established for model checking and theorem proving approaches to discrete state system verification. Abstraction – either based on generic principles (like from timed to untimed systems, infinite data domains to finite one) or on case-specific user suggested simplifications – serves to simplify the models by omitting aspects that are not relevant for analysis. Compositionality provides a divide-and-conquer to manage complexity: properties of complicated systems are inferred from properties of components.

In particular the consortium will work on the following reduction strategy: consider a system consisting of many interacting timed automata such that the size of the global state- and clock-space is prohibitively large. One can take a sub-system consisting of a subset of the components and analyse it in isolation, treating the rest of the components as under-specified inputs. The set of behaviours exhibited by the reduced system, when projected on the variables that interact with the rest of the system, is an over-approximation of the actual behaviour, however is may have a much smaller model which can be plugged to the rest of the system and yield a tractable model. If the verification results hold for this smaller model then it hold for the real system. The consortium will develop techniques to perform automatic decomposition and approximation in this spirit.

For the verification of finite-state systems a number of techniques for *exploiting the composite structure* of the model exists. Partial order reduction and compositional backwards reachability are methods which help to reduce search spaces for loosely coupled concurrent components. Likewise, methods exploiting symmetries and hierarchical structure have shown to be very successful.

The consortium aims at developing similar structure exploiting techniques in the real-time setting. The main difficulty is that the strong synchrony on time between the components of a real-time system is an obstacle in transferring directly the successful techniques from the finite-state setting. The consortium intends to identify practically useful restrictions of the timed automata formalism that will allow the development of similar structure exploiting techniques in the presence of real-time.

T2.2: Controller Synthesis and Scheduling Algorithms

The problems of control synthesis, scheduling and planning may be formalised as games between a system (player) and an environment (adversary): The player may influence the adversary by taking choices based on his knowledge of the current state and vice versa. The goal for the player is to keep the environment within a desired range of states (or dually to steer it towards a desired type of state) by making the right choices following a winning (or optimal) strategy. Depending on the setting, algorithms for synthesising control strategies and schedules for finite state or real time systems and planning problems are known. In practice however, environments with large state spaces make such a synthesis hopelessly difficult.

In this task the consortium will attack the algorithmic aspects of controller synthesis and planning including approaches that prefer a simpler sub-optimal strategy over an optimal one. Modification and extension of heuristic methods from model checking and operations research will be investigated to allow for transfer to (optimal) control synthesis and to the closely related domain of online scheduling problems.

In analysing timed automata models obtained from PDDL+ domain descriptions, the consortium expects to benefit from static analysis of the PDDL+ source in obtaining information about independencies and mutual exclusions between action-instances. A specific structural property of timed automata models of job-shop scheduling problems is that they are acyclic. This reduces their complexity and provides for specialised algorithms for analysis and synthesis including heuristic forward search, especially in the context of optimisation.

T2.3: State Space Representation and Manipulation

Timing related problems involve combinations of *logical* and *temporal* constraints. (e.g. constraints of the form $x - y \geq d$ for real clocks x, y). Such constraints occur in the verification of timed automata as well as in other approaches for solving scheduling problems and their manipulation is a *major computational difficulty* in all time-dependent reasoning and optimisation. Current verification tools for timed automata use particular data structures for representing and manipulating such constraints, such as certain varieties of BDDs and efficient matrix structures. Other approaches to similar problems are used in other disciplines e.g. constraint propagation in constraint programming or relaxed mixed integer linear programming.

The crude distinction between state based and constraint based specification and analysis is that the former uses a dynamic model (change of state) whereas the latter is based on a static via (logic) constraints (and time is just a variable). Mutual translations between state based and constraint based models are possible, depending on the questions asked. The consortium intends to enrich existing timed verification tools by methods inspired by the constraints approach and adapt constraint satisfaction techniques to treat mixed Boolean and temporal constraints. In addition the consortium will continue with the related effort of improving the data structures for storing such constraints and the algorithms for manipulating them.

Traditionally, the verification algorithms for timed automata have been based on pre-determined search orders (e.g. breadth-first or depth-first) on the symbolic state-space graph of the automaton. For finding optimal paths it is useful to employ more sophisticated, heuristic search strategies that favour the exploration of the most promising branches — possibly guided by user provided information — and that can avoid exhaustive exploration. Such techniques can also be useful when applying real-time verification tools as advanced debuggers: here preference should be given

to branches that are most likely to lead to errors.

In addition, the consortium will work on distributing the exploration and analysis algorithms in order to benefit from the consortiums access to tightly-coupled clusters of PCs as well as the loosely coupled GRID computers. Here the challenge will be to reduce the communication overhead (e.g. by identifying compact formats for communicating symbolic representations of sets of states) in order to obtain speed-up as close to linear as possible.

T2.4: Stochastic Techniques

The various extensions of the timed automata paradigm to a stochastic setting lead to a wide range of models that include features from discrete and continuous Markov chains, Markov decision processes, stochastic discrete event systems, etc. The challenge is to combine techniques for timed automata verification with those for performance analysis into effective, integrated methods for analysing such hybrid models. In particular, the traditional techniques for dealing with large stochastic systems (e.g. sparse matrices, Kronecker representation, linear programming, MTBDDs, ADDs, PDGs) must be combined with efficient data structures for symbolic manipulation of timed automata models (e.g. DBMs, CDDs, DDDs, NDDs). Current work on applying compositional and model checking techniques for the analysis of various Markovian models is a good starting for the work in this task.

The consortium aims at combining tools currently developed by members of the consortium for model checking and performance analysis of purely Markovian models with existing real-time verification tools.

T2.5: Tool Interaction

The tasks within the analysis and tools workpackage will lead to the development of a number of individual prototype tools as well as improved and extended versions of existing real-time verification and validation tools. To allow for the functionality of each tool to be accessible by other tools within the project as well as related tools outside the project, the consortium will provide detailed interface descriptions of the individual prototype tools, including required input- and output-formats.

Based on these interface descriptions, the project will develop automatic translations between a number of tools within and outside the project.

As a result of the experiences gained from interaction between the prototype tools, the consortium will propose an architectural design of a fully integrated and extendible tool set, including suggestions for common format(s) for exchange of model descriptions.

WP3 Case Studies

This workpackage comprises several case studies dealing with (distributed, dynamic) resource allocation problems. There are four main case studies, each one sponsored by one of the assistant industrial contractors. In addition, it is anticipated that during the course of the project new relevant case studies will appear. The work on each case-study will progress along the following scheme. First, the case provider will present the application domain and one or more problems will be isolated. Then, a preliminary problem description language will be defined. It will allow to define variants of the problem in end-user terms. After the principles of translating such problems into suitable timed automata models are understood, a translator from the language to these models will be written and the result will be subject to the analysis methods and tools developed in WP2. The results will be evaluated at the end of the project by the provider.

T3.1: Smart Card Personalisation System

Industrial partner CYR is manufacturing machines for smart card personalisation. These machines take piles of blank smart cards as raw material, program them with personalised data, print them and test them. The machines have a throughput of thousands of cards per hour. It is required that the output of cards occurs in a predefined order. Unfortunately, some cards are defective and they have to be discarded, but without changing the output order of personalised cards. Decisions on how to reorganise the flow of cards must be taken within fractions of a second, if no production time is to be lost.

Aim of this case study is to model the desired production requirements, the timing requirements of operations of the machine and on this basis synthesise the coordination of the tracking of defective cards. The goal is to maximise the throughput of the machine under certain error assumptions.

As part of this case study, the consortium will also study the possibilities for the integration of timed automata technology into the control software process of CYR as a representative control system provider.

T3.2 Real-time Memory Management in Radar Sensor Equipment

Industrial partner Terma is producing radar sensors mainly used for traffic control in ports and airports and for coastal surveillance. The real-time processing of radar signals includes integration of several received signals, requiring the signals to be stored temporarily in memory. The interface between the signal processing hardware and the memory consists of an arbiter and a collection of 9 FIFO buffers. During processing the buffers are not allowed to become empty or overflow. The arbiter includes a scheduling algorithm deciding when to access the buffers. The aim of the case study is to verify that the behaviour of the scheduling algorithm is correct. A second step will be to synthesise a scheduler for a set of integrators and buffers. This is particular interesting for Terma as the next generation of radar sensors will include similar memory interfaces, though with increased demands on access to the memory.

T3.3: Real-time Service Allocation in a Car Periphery Supervision System

Industrial partner Bosch is developing a system that integrates a number of services (e.g. parking support, pre-crash detection, etc.) for car periphery supervision. The system concept is based on a limited number of sensors (current work is focused on radar technology) and micro-controllers that have to be shared by the different services. Currently, the car periphery supervision system may consist of up to 12 radar or ultrasonic sensors, up to four 32-bit-microprocessors with 128 K RAM and upto 2M Flash Memory. Thus, being a far from trivial problem, it is necessary to find a suitable allocation scheme for the hardware (sensors and controllers) and software processes like measurement pre-processing, interpretation of measurements, identification of the appropriate reaction, supervision and diagnosis, etc.

The main challenge posed by this integration is that it is not only time-critical, but also depends on the current situation. The aim of this case study is to use the timed automata framework to specify precisely the logical and timing requirements, and to design and verify (or alternatively, automatically synthesise) a dynamical resource allocation scheme on this basis.

T3.4: Value Chain Management

Axxom is a manufacturer of tools to optimise value chains, offering customers suitable models and algorithms that are needed to solve their problems, which are job-shop problems with additional constraints, value chain management, and optimisation in distribution. Future improvements of the tools are concentrated on the development of reactive schedulers that can deal with feedback information to handle operation in 'uncertain' environments.

Axxom will provide several case studies of different complexity for value chain management problems. One of these is the coordination of injection molding in the automotive industry. Injection molding is a process which may be performed either by a car manufacturer himself, or one of many other companies. Based on a real-life scenario in car manufacturing the cooperation of the injection molding department of a car manufacturer with his suppliers will be evaluated and tested by means of a contract net model. In this case study many constraints have to be taken into account. Typical constraints are related to the resources, inventory, products, production times, change-over times, workflows, material flows, etc.

T3.5 Miscellaneous Case Studies

The consortium will start work in parallel on all of the above four case studies provided by the industrial partners. In addition, the consortium anticipates that during the course of the project, new relevant case studies will appear, either as a direct follow-up on the four industrial case studies above, or as case studies obtained internally between the academic partners.

9.2 Workpackage list

No	Title	Leader	PM	Start	End	Deliverables
WP0	Project Management	KUN	33	0	36	0.1.1–0.1.6, 0.2.1–0.2.3, 0.3.1–0.3.3
WP1	Modelling	UT	72.3	0	36	1.1–1.5
WP2	Analysis and Tools	AAU	175.9	0	36	2.1.1, 2.1.2, 2.2.1, 2.2.2, 2.3–2.5
WP3	Case Studies	Uni DO	107.6	0	36	3.1.1–3.1.4, 3.2.1–3.2.4, 3.3.1–3.3.4, 3.4.1–3.4.4, 3.5.1–3.5.3
WP4	Dissemination	VERIMAG	16	0	36	4.1.1, 4.1.2, 4.4, 4

NB The person months (PMs) that are mentioned in the above table correspond to the additional personal as mentioned in the CPFs. The own contribution of PMs by partners that work under the AC model are not included here, nor in the tables in the next subsection.

9.3 Workpackage descriptions

WP0 Project Management

WP leader: KUN WP number: 0 Start date: 0

Partner	KUN	Bosch	CYR	Axxom	Terma	AAU	Uni DO	VERIMAG	WIS	LIF	UT
PM	11	0	0	0	0	2	2	12	2	2	2

Objectives:
This workpackage monitors the technical content and progress of each workpackage, coordinates the cooperation between the workpackages, reports to the CEC, and closely follows external developments which are relevant to the project and arranges appropriate adaptation, if needed. This workpackage finally produces the Framework Reports that contain the unified modelling framework (the ultimate goal of the project).

Description of Work:
Task 0.1 Project coordination (KUN)
The Project Coordinator from KUN will be responsible for the day-to-day coordination of the project. He will also be the main interface between the Consortium and the European Union, and also between the Consortium and the End-User Panel. He will consolidate the project planning, progress reports, milestone reports, cost statements, budgetary overviews, *etc.* using the inputs from the other participants, and he will coordinate the communication between the participants. The Project Coordinator will chair the Project Coordination Committee (PCC) which will decide about the high level management issues. The PCC will consist of the responsible scientists from all participants.
The Workpackage Leaders are responsible for the coordination, planning, monitoring and reporting of the Workpackage and for the coordination of the tasks within and between Workpackages.
Task 0.2 Scientific Coordination (VERIMAG)
It is the responsibility of the Scientific Coordinator to monitor and coordinate the scientific activities within the project, and to produce every year two *Framework Reports*, that reflect the results of respectively Workpackages 1 and 2, incorporating the experiences made in the case studies in Workpackage 3. The final versions of these framework reports will ultimately form the unified modelling framework.
Task 0.3 Project administration (KUN, all)
The PCC manages its own budget for management tasks and it controls the budget for the Project Meetings (lodging costs: hotel and conference room costs), the budget for the visits to conferences and workshops outside the EU, and the budget for dissemination of results including publication costs.

Deliverables:

No.	Description	↓	nature	dissem.	resp.
0.1.1	Project Report - progress & evaluation	6	R	PU	KUN, all
0.1.2	Project Report - progress & evaluation	12	R	PU	KUN, all
0.1.3	Project Report - progress & evaluation	18	R	PU	KUN, all
0.1.4	Mid Term Assessment Report	24	R	PU	KUN, all
0.1.5	Project Report - progress & evaluation	30	R	PU	KUN, all
0.1.6	Final Project Report - progress & evaluation	36	R	PU	KUN, all
0.2.1	Framework Report (v1)	12	R	PU	VERIMAG, all
0.2.2	Framework Report (v2)	24	R	PU	VERIMAG, all
0.2.3	Framework Report (final)	36	R	PU	VERIMAG, all
0.3.1	Financial Review	12	R	PU	KUN, all
0.3.2	Financial Review	24	R	PU	KUN, all
0.3.3	Financial Review	36	R	PU	KUN, all

Milestones and expected results:
Month 12: Framework Report: first version
Month 24: Framework Report: second version
Month 36: Framework Report: final version

Interaction with other WPs:
This WP interacts with all other WPs.

WP1 Modelling

WP leader: UT	WP number: 1	Start date: 0

Partner	KUN	Bosch	CYR	Axxom	Terma	AAU	Uni DO	VERIMAG	WIS	LIF	UT
PM	10	0	0	3.3	0	8	9	14	8	12	8

Objectives:
Evaluate and extend the timed automata paradigm as a formalism for control synthesis and validation for real-time systems.

Description of Work:
Emphasis in this task will be in the first two project years, when model extensions will be studied and defined that are needed for the other workpackages. The third year is intended for wrap-up and identification of other potentially interesting extensions of the timed automata paradigm.

Task 1.1 Model Classification (VERIMAG, Uni DO, LIF, WIS, KUN)
Provide a methodology for classifying resource allocation problems according to the features required by the timed automata framework. Produce a hierarchy of models within the timed automata paradigm, with refinement and abstraction principles that relate them.

Task 1.2 Model Composition (KUN, Uni DO, WIS)
Investigate how important, well-understood compositional methods from various areas including process algebra, Statecharts (UML), I/O automata, etc. extend to control synthesis and validation problems in the timed automata setting.

Task 1.3 Quantitative Modelling (UT, AAU, Uni DO, VERIMAG, KUN)
Study and develop stochastic and quantitative extensions of the basic model of timed automata emphasising their specification and composition.

Task 1.4 Scheduling and Planning (Uni DO, AAU, VERIMAG, LIF)
Study how scheduling and planning problems can be formulated, and how various analysis questions can be reduced to scheduling and planning problems.

Task 1.5 Control Synthesis (VERIMAG, WIS, Axxom, LIF)
Investigate the various ways in which control and optimality can be formulated and studied within the timed automata paradigm.

Deliverables:

No.	Description	↓	nature	dissem.	resp.
1.1	Modelling: Model Classification	36	R	PU	VERIMAG
1.2	Modelling: Model Composition	24	R	PU	KUN
1.3	Modelling: Quantitative Modelling	24	R	PU	UT
1.4	Modelling: Scheduling and Planning	24	R	PU	Uni DO
1.5	Modelling: Control Synthesis	12	R	PU	VERIMAG

Milestones and expected results:
Month 12: Identification of extensions needed for case studies, initial results
Month 24: Complete formalisation of extensions supported by analysis methods & tools
Month 36: Incorporation of the result in the Framework Report: Modelling & identification of open issues.

Interaction with other WPs:
This Workpackage forms a prerequisite for some of the work in Workpackage 2: T1.5 is a prerequisite for T2.2, T1.2 is a prerequisite for T2.1, and T1.4 is needed for T2.2. Furthermore, this workpackage will be used in WP3 Case Studies. The work in WP3 will provide feedback to this workpackage, which will be reflected by the Framework Report: Modelling, as produced in WP0.
Although consolidation of results is in the form of end-of-year deliverables, the technical interaction between WP1, WP2, and WP3 will be carried out on a continuous basis to promote a rapid exchange of information.

WP2 Analysis and Tools

WP leader: AAU WP number: 2 Start date: 0

Partner	KUN	Bosch	CYR	Axxom	Terma	AAU	Uni DO	VERIMAG	WIS	LIF	UT
PM	27	0	20	0	3	20	7	32	15	30	21.9

Objectives:
Develop fundamental algorithms and data structures for verification and synthesis of timed systems with an emphasis on novel techniques for treating dynamic resource allocation problems and fighting the combinatorial complexity of the problems (state-space explosion). Furthermore, work on interaction between the various tools, as a first step towards their (future) integration.

Description of Work:
Task 2.1 Abstraction, Compositionality, and Structure Exploitation (KUN, AAU, VERIMAG, WIS, UT, LIF)
Study the application of abstraction and compositionality as key techniques in controlling and reducing the complexity involved in analysing real-time system models. Identify practically useful restrictions of the timed automata paradigm that allow the development of structure exploiting techniques like partial-order search, McMillan prefixing and CBR in the presence of real-time.
Task 2.2 Controller Synthesis and Scheduling Algorithms (VERIMAG, AAU, Uni DO, LIF, WIS, CYR)
Modify and extend heuristic methods from model checking and operation research to allow for transfer to (optimal) control synthesis and the closely related domains of planning and online scheduling problems.
Task 2.3 State Space Representations (LIF,AAU,VERIMAG)
Study algorithms and data structures for the efficient representation and manipulation of state spaces. Establish algorithmic basis of the integration of timed automata methods and constraint based methods.
Task 2.4 Stochastic Techniques (UT, AAU, Uni DO, KUN)
Combine model checking and stochastic analysis.
Task 2.5 Tool Interaction (AAU, Uni DO, LIF, KUN, UT, WIS, CYR, Terma)
Address the question of the interaction between the various tools developed in this workpackage. Also establish links with relevant tools developed by others. An important objective is the design of a fully integrated tool set, based on an open, extensible format.

Deliverables:

No.	Description	↓	nature	dissem.	resp.
2.1.1	A & T: Abstraction and Compositionality	24	R/P	PU	KUN
2.1.2	A & T: Structure Exploitation	36	R/P	PU	KUN
2.2.1	A & T: Control Synthesis Algorithms	24	R/P	PU	VERIMAG
2.2.2	A & T: Scheduling and Planning Algorithms	36	R/P	PU	VERIMAG
2.3.a	A & T: State Space Representations (v1)	12	R/P	PU	LIF
2.3.b	A & T: State Space Representations (v2)	24	R/P	PU	LIF
2.3.c	A & T: State Space Representations (v3)	36	R/P	PU	LIF
2.4.a	A & T: Stochastic Analysis (v1)	24	R/P	PU	UT
2.4.b	A & T: Stochastic Analysis (v2)	36	R/P	PU	UT
2.5.a	A & T: Tool Interaction (v1)	24	R/P	PU	AAU
2.5.b	A & T: Tool Interaction (v2)	36	R/P/D	PU	AAU

Milestones and expected results:
Month 12: Identification of analysis methods related to WP1 and WP3 work, initial elaboration
Month 24: Identification and elaboration of analysis methods for implementation
Month 36: Final report, including identification of further potentially interesting analysis methods

Interaction with other WPs:
This WP interacts with WP1 Modelling (and indirectly with WP3) on the modelling formalisms for which analysis techniques and tools must be developed. Although consolidation of results is in the form of end-of-year WP reports, the technical interaction with the other WPs will be carried out on a continuous basis to promote a rapid exchange of information.

WP3 Case Studies

WP leader: Uni DO		WP number: 3		Start date: 0							
Partner	KUN	Bosch	CYR	Axxom	Terma	AAU	Uni DO	VERIMAG	WIS	LIF	UT
PM	15	3	8.9	8	3.7	10.4	16	16	3.6	17	6

Objectives:
This workpackage consists of a number of industrial and academic case studies that provide the basis for the application and evaluation of the discipline of computer-aided timing analysis and design under development in the project.

Description of Work:
Task 3.1 Smart Card Personalisation System (LIF, CYR, VERIMAG)
Model the desired production requirements and the timing requirements of operations of machines for smart card personalisation, and on this basis synthesise the coordination of the tracking of defective cards. The goal is to maximise the throughput of the machine under certain error assumptions. Secondly, explore other scalable architectures of the machine with increased potential throughput and decreased penalty for defective cards.
Task 3.2 Real-time Memory Management in Radar Sensor Equipment (AAU, Terma)
Model the memory management system of a radar sensor system and verify that the input buffers are never empty and that the output buffers never overflow. Another, more ambitious goal, is to automatically generate an arbiter, which is basically a scheduling algorithm deciding when to empty/fill which buffers, ensuring correct behaviour with respect to the buffers and with ideally minimal memory requirement.
Task 3.3 Real-time Service Allocation for Car Periphery Supervision (Uni DO, Bosch, KUN, UT)
Use the timed automata framework to specify precisely the logical and timing requirements for the interaction and allocation of the different services of the car supervision system, and design and verify (or alternatively, automatically synthesise) a dynamical resource allocation scheme on this basis.
Task 3.4 Value Chain Optimisation System (Uni DO, Axxom, KUN, VERIMAG, WIS)
Develop a generic model for value chains (or multistage planning and scheduling) based on timed automata. Use this model to investigate the effect of decision strategies on the overall behaviour of the system. Define three examples of value chain problems, ranging from elementary to real-world size.
Task 3.5 Miscellaneous Case Studies (UT, all CRs)
Study the application of the timed automata paradigm to a selection of internal case studies of the CRs.

Deliverables

No.	Description	↓	nature	dissem.	resp.
3.1.1-3.4.1	Case Study 1-4: Preliminary Description	6	R	PU	see above
3.1.2-3.4.2	Case Study 1-4: Model	12	R	PU	see above
3.5.1	Miscellaneous Case Studies: First Year Report	12	R	PU	UT, all CRs
3.1.3-3.4.3	Case Study 1-4: Optimisation	24	R	PU	see above
3.5.2	Miscellaneous Case Studies: Second Year Report	24	R	PU	UT, all CRs
3.1.4-3.4.4	Case Study 1-4: Final Report	36	R	PU	see above
3.5.3	Miscellaneous Case Studies: Final Report	36	R	PU	UT, all CRs

Milestones and expected results:
Month 12: Complete models of case studies.
Month 24: Optimisation studies of case studies available.
Month 36: Final reports, feedback on analysis methods and tools.

Interaction with other WPs:
This WP interacts with WP1 Modelling, which provides the modelling techniques that will be applied, and with WP2 Analysis and Tools, which provides the techniques and tools that will be applied to the case study benchmarks.

WP4 Dissemination

WP leader: VERIMAG WP number: 4 Start date: 0

Partner	KUN	Bosch	CYR	Axxom	Terma	AAU	Uni DO	VERIMAG	WIS	LIF	UT
PM	2	0	0	0	0	2	2	4	2	2	2

Objectives:
This workpackage takes care of the dissemination of results via appropriate channels.

Description of Work:
Task 4.1 Workshops and Conference (VERIMAG)
AMETIST will organise annual workshops (combined with a project meeting) to disseminate results among the partners and the members of the End-User Panel, and invited participants from outside the consortium.
Several members of the AMETIST consortium are active in organising and steering several conferences and workshops on topics closely related to the research within AMETIST. Thus the annual AMETIST workshop could be easily and ideally attached to one of these.
Task 4.2 Contacts with related projects (all)
The consortium will establish an exchange of information and (hopefully) fruitful collaboration with related EU, national and international projects. Related EU projects include CC, Hybridge, Omega and AIT-WOODDES (see also Section 5.6). Apart from planning working visits, AMETIST intends to organise common (or overlapping) project meetings.
Task 4.3 Tutorials (all)
Members of the AMETIST consortium frequently act as (invited) speakers and/or tutorial presenters at major scientific events. Utilising these occasions makes for excellent opportunities for disseminating the results of AMETIST to a wider audience.
Task 4.4 Website (UT)
AMETIST will maintain a website `http://ametist.cs.utwente.nl/` with all publicly available results. In particular all scientific publications on modelling formalisms and analysis methods will be available. Also, it will be possible to download executable versions of the tools developed within the project.
Task 4.5 Scientific Publications (all)
The consortium will aim at realising a significant number of publications at leading international scientific conferences and journals related to the topics of AMETIST, such as RTSS, ETAPS, TACAS, FLOC, CAV, HSCC, FTRTFT, ..., CACM, IEEE Computer, ...

Deliverables

No.	Description	↓	nature	dissem.	resp.
4.4	AMETIST Website	1	O	PU/CO	UT, all
4	Dissemination and Use plan	6	O	PU	VERIMAG, all
4.1.1	AMETIST Workshop	6	O	PU	VERIMAG
4.1.2	AMETIST Conference	36	O	PU	VERIMAG

Milestones and expected results:
AMETIST workshops & conference
Fruitful exchange of information and collaboration with related EU, national and international projects
AMETIST tutorials
AMETIST website
AMETIST publications

Interaction with other WPs:
This WP interacts with all other WPs.

9.4 Deliverables list

No	Description	Date	Nat	Diss	Resp
4.4	AMETIST Website	1	O	PU/CO	UT, all
0.1.1	Project Report - Progress & Evaluation	6	R	PU	KUN, all
3.1.1	Case Study 1: Preliminary Description	6	R	PU	LIF, CYR
3.2.1	Case Study 2: Preliminary Description	6	R	PU	AAU, Terma
3.3.1	Case Study 3: Preliminary Description	6	R	PU	Uni DO, Bosch
3.4.1	Case Study 4: Preliminary Description	6	R	PU	Uni DO, Axxom
4	Dissemination and Use plan	6	O	PU	VERIMAG, all
4.1.1	AMETIST Workshop	6	O	PU	VERIMAG
0.1.2	Project Report - Progress & Evaluation	12	R	PU	KUN, all
0.2.1	Framework Report (v1)	12	R	PU	VERIMAG, all
0.3.1	Financial Review	12	R	PU	KUN, all
1.5	Modelling: Control Synthesis	12	R	PU	VERIMAG
2.3.a	A & T: State Space Representations	12	R/P	PU	LIF
3.1.2	Case Study 1: Model	12	R	PU	LIF, CYR
3.2.2	Case Study 2: Model	12	R	PU	AAU, Terma
3.3.2	Case Study 3: Model	12	R	PU	Uni DO, Bosch
3.4.2	Case Study 4: Model	12	R	PU	Uni DO, Axxom
3.5.1	Miscellaneous Case Studies: First Year Report	12	R	PU	UT, all CRs
0.1.3	Project Report - Progress & Evaluation	18	R	PU	KUN, all
0.1.4	Mid Term Assessment Report	24	R	PU	KUN, all
0.2.2	Framework Report (v2)	24	R	PU	VERIMAG, all
0.3.2	Financial Review	24	R	PU	KUN, all
1.2	Modelling: Model Composition	24	R	PU	KUN
1.3	Modelling: Quantitative Modelling	24	R	PU	UT
1.4	Modelling: Scheduling and Planning	24	R	PU	Uni DO
2.1.1	A & T: Abstraction and Compositionality	24	R/P	PU	KUN
2.2.1	A & T: Control Synthesis Algorithms	24	R/P	PU	VERIMAG
2.3.b	A & T: State Space Representations (v2)	24	R/P	PU	LIF
2.4.a	A & T: Stochastic Analysis (v1)	24	R/P	PU	UT
2.5.a	A & T: Tool Interaction (v1)	24	R/P	PU	AAU
3.1.3	Case Study 1: Optimisation	24	R	PU	LIF, CYR
3.2.3	Case Study 2: Optimisation	24	R	PU	AAU, Terma
3.3.3	Case Study 3: Optimisation	24	R	PU	Uni DO, Bosch
3.4.3	Case Study 4: Optimisation	24	R	PU	Uni DO, Axxom
3.5.2	Miscellaneous Case Studies: Second Year Report	24	R	PU	UT, all CRs
0.1.5	Project Report - Progress & Evaluation	30	R	PU	KUN, all
0.1.6	Final Project Report - Progress & Evaluation	36	R	PU	KUN, all
0.2.3	Framework Report (final)	36	R	PU	VERIMAG, all
0.3.3	Financial Review	36	R	PU	KUN, all
1.1	Modelling: Model Classification	36	R	PU	VERIMAG
2.1.2	A & T: Structure Exploitation	36	R/P	PU	KUN
2.2.2	A & T: Scheduling and Planning Algorithms	36	R/P	PU	VERIMAG
2.3.c	A & T: State Space Representations (v3)	36	R/P	PU	LIF
2.4.b	A & T: Stochastic Analysis (v2)	36	R/P	PU	UT
2.5.b	A & T: Tool Interaction (v2)	36	R/P/D	PU	AAU
3.1.4	Case Study 1: Final Report	36	R	PU	LIF, CYR
3.2.4	Case Study 2: Final Report	36	R	PU	AAU, Terma
3.3.4	Case Study 3: Final Report	36	R	PU	Uni DO, Bosch
3.4.4	Case Study 4: Final Report	36	R	PU	Uni DO, Axxom
3.5.3	Miscellaneous Case Studies: Final Report	36	R	PU	UT, all CRs
4.1.2	AMETIST Conference	36	O	PU	VERIMAG

9.5 Project planning and timetable

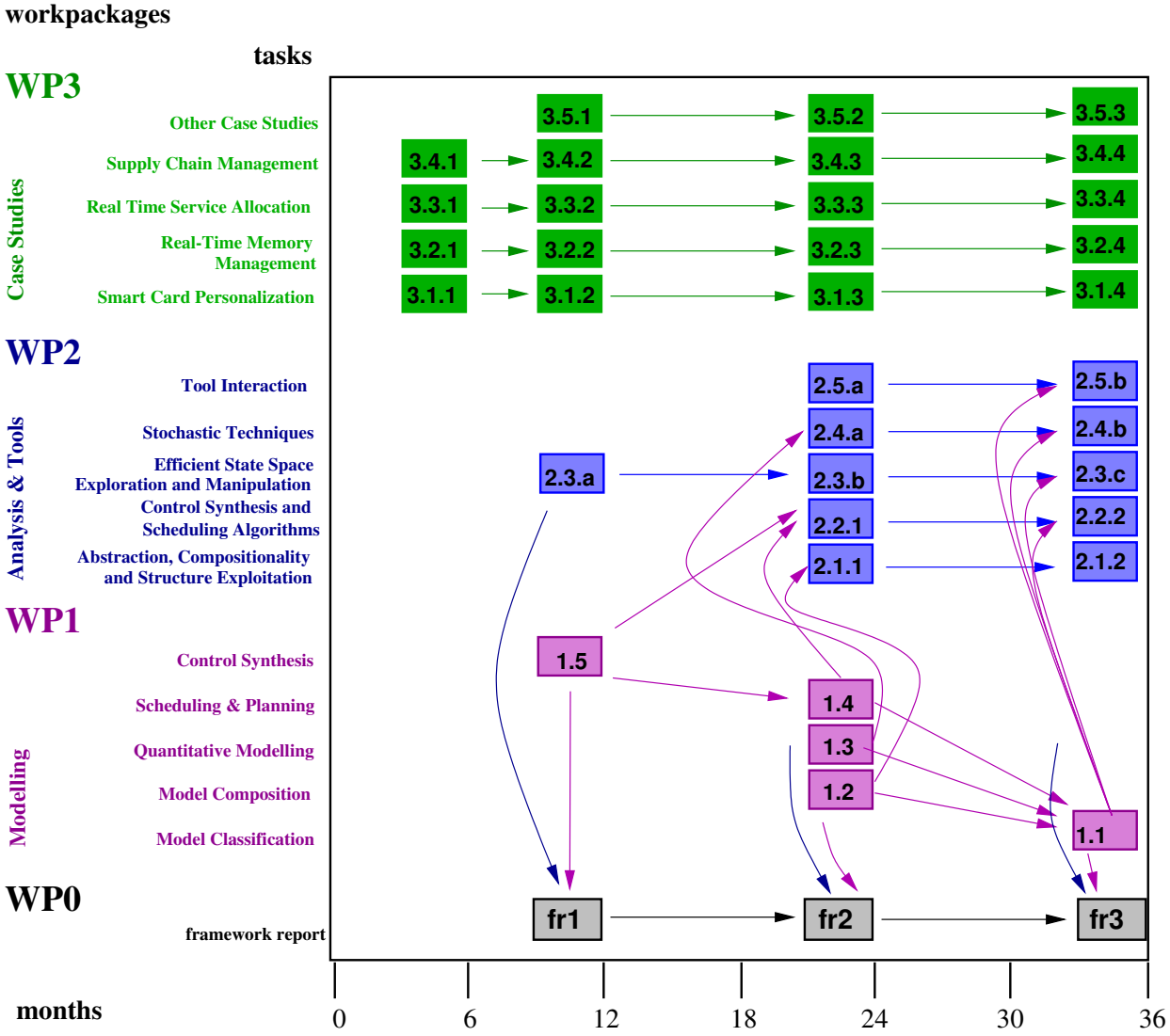

Figure 2: Gantt/Pert diagram of the workpackages of the AMETIST project. Interactions between WP3 and the other WP's are not displayed. For reasons of clarity also dome other links have been omitted.

9.6 Graphical presentation of project components

See Figure 2 above.

9.7 Project management

The University of Nijmegen (KUN) will be responsible for the project management and coordination. The project coordinator, Prof.Dr. F.W. Vaandrager has ample research management experience; he will be assisted by the Unit Financial & Contract Management (FCM) of the Faculty of Science, which has coordinated and assisted the management of over 200 EU projects over the last 13 years.

Project Coordination Committee (PCC) A Project Coordination Committee will be formed to decide about the high level management issues, including scientific, technical dissemination and exploitation, financial, planning and control matters. The PCC will consist of the responsible scientists from all the participants. The PCC will meet at least once per twelve months or more often in case of special issues to be discussed. The project coordinator will be the chairperson.

Management by budget The PCC has its own budget for management tasks and it controls the budget for the project meetings (lodging costs: Hotel and conference room costs), the budget for the visits to conferences and workshops outside the EU, and the budget for dissemination of results including publication costs. In this way the PCC can use its budget efficiently (who is coming or going where and when; how knowledge is incorporated in or spread from the Consortium, and how knowledge is best protected and can lead to economic benefit for the Consortium members and the European Community). The Unit FCM will periodically analyse the expenses of the Consortium members, will give forcasts and advise them on their budgetary and other resource questions. Each year at least five relevant workshops and conferences outside the EU are foreseen. The PCC will provide funding for participation to each such meeting on behalf of the Consortium for two of its members.

Project coordinator The project coordinator will be responsible for the day-to-day coordination of the project. He will also be the main interface between the Consortium and the European Union, and also between the Consortium and the End-User Panel. He will consolidate the project planning, progress reports, milestone reports, cost statements, budgetary overviews, *etc.* using the inputs from the other participants, and he will coordinate the communication between the participants. He will organise and finance all project meetings and the visits of members of the Consortium to workshops and conferences outside Europe.

Scientific coordinator In addition to the general coordination of the project, AMETIST will also have a Scientific Coordinator. It is the responsibility of the Scientific Coordinator to monitor and coordinate the scientific activities within the project, and to work toward the emergence of a unifying framework for timing related issues treated in the various work-packages. The problems addressed in the project have a lot of intersections with topics treated by other scientific and industrial communities, and we believe that creating such a unifying framework will have a long-term effect that will go beyond the achievements of the proposed project. A major responsibility of the Scientific Coordinator is to produce every year the *Framework Report Deliverables* that integrate the yearly work done within the project, as well as provide links to important related developments outside the project.

Workpackage leaders The workpackage leaders are responsible for the detailed coordination, planning, monitoring and reporting of the workpackage and for the detailed coordination of the tasks within the workpackage and with the other workpackages in the project. A workpackage group will meet according to the specific needs of its tasks, under the chairpersonship of the workpackage leader, at least every six months. The participants in the workpackage groups will report to their responsible WP-leader every three months in short progress reports. Events that have or could have influence on the progress of a task will be reported immediately.

Review meetings The project coordinator will prepare the annual review meetings and reports. Together with the EU-project manager and EU-evaluators the Consortium will discuss at these meetings the results so far, and the possibly necessary adaptations of the plans and planning in order to meet the goals set in the EU-contract.

Communication strategy The communication strategy aims to keep all the participants fully informed about the project status, the planning and all other issues which are important to the participants in order to obtain maximum transparency for all involved and to increase the synergy of the cooperation. The project coordinator will inform the participants about the expected deliverables by periodically updated project agendas which describe clearly who, what and when.

A special webpage of the project will be used both for communication within the project and for dissemination of results. Interactive management meetings and scientific meetings take an important rôle in the communication strategy. All information (like minutes of meetings, visit reports, workpackage reports, relevant publications, *etc.*) will be communicated to the project coordinator, who will be responsible for

channeling this information to the other participants, when appropriate. The aim of the communication strategy is also to communicate effectively with parties outside the Consortium. The communication strategy—which includes a planning for some key publications to be written, presentations to be given and conferences to be attended on behalf of the Consortium—will be a topic at each PCC meeting. Information obtained through research within the project will be disseminated to a wider scientific audience via the project's webpage and through participation in international conferences and publication in international journals with a high scientific impact.

Special workpackage for project management The Consortium has designed a separate workpackage (WP0) for the management of the risks and challenges that are inevitable to any project in this particular field. The area of timing technology is still very much in development—like the rest of the IT sector. Therefore, planning in advance should be done with care and flexibility. One of the reasons why this project involves many person-months is to have the resources to quickly incorporate new developments into the project. Also, we note that despite the fact that verification tools (and the underlying hardware) have improved considerable over the last few years, actually doing tool-assisted verifications is still very labour-intensive: completing a case study in the area of formal methods always takes more time than one initially expects. Thus, in order to do the validation work in this project much time and effort has to be invested.

Day-to-day management Strategic and technical management will be distinguished.

Strategic management: Decisions about key personnel; Recommendations about major changes in the work programme, including re-distribution of the budget; Recommendations about changes to the Consortium; Exploitation issues, including patenting, licensing and publications; High level review of resource status and project progress; Decisions about representation at meetings, conferences and workshops outside the EU; Decisions about cooperation with related projects; Training aspects (in case additional training is needed).

Technical management: Detailed planning of technical work and deliverables; Detailed monitoring of technical progress; Decisions about technical methods and equipment (including hard- and software); Preparation of technical progress reports; Preparation and review of technical publications; Representation at conferences and workshops.

The end-user panel Close contacts with interested industries will be maintained via an *End-User Panel*, with as members, apart from the participating industrial partners, ABB, LCN, ASML, Lucent, NLR, Siemens Mobile Phones A/S, and Siemens R&D.

The members of this panel support the AMETIST project and have committed themselves to be present at the annual meetings, and to contribute to the user-oriented focus of the AMETIST project. Foreseen is that the partners and members of the End-User Panel itself will locate still not represented users and invite them to become members of the End-User Panel.

References

[1] Y. Abdeddaïm and O. Maler. Job-shop scheduling using timed automata. In *Proc. CAV'2001*, LNCS. Springer, 2001.

[2] R. Alur and D.L. Dill. Automata for modeling real-time systems. In M. Paterson, editor, *Proceedings* 17^{th} *ICALP,* Warwick, volume 443 of *Lecture Notes in Computer Science*, pages 322–335. Springer-Verlag, July 1990.

[3] R. Alur, S. La Torre, and G. Pappas. Optimal paths in weighted timed automata. In Di Benedetto and Sangiovanni-Vincentelli [6].

[4] G. Behrmann, A. Fehnker, T.S. Hune, K.G. Larsen, P. Pettersson, J.M.T. Romijn, and F.W. Vaandrager. Minimum-cost reachability for priced timed automata. In Di Benedetto and Sangiovanni-Vincentelli [6], pages 147–161.

[5] M. Bozga, C. Daws, O. Maler, A. Olivero, S. Tripakis, and S. Yovine. Kronos: A Model-Checking Tool for Real-Time Systems. In A.J. Hu and M.Y. Vardi, editors, *Proceedings of the 10th International Conference on Computer Aided Verification,* Vancouver, BC, Canada, volume 1427 of *Lecture Notes in Computer Science*, pages 546–550. Springer-Verlag, June/July 1998.

[6] M.D. Di Benedetto and A.L. Sangiovanni-Vincentelli, editors. *Proceedings Fourth International Workshop on Hybrid Systems: Computation and Control (HSCC'01),* Rome, Italy, volume 2034 of *Lecture Notes in Computer Science*. Springer-Verlag, March 2001.

[7] Ansgar Fehnker. Scheduling a Steel Plant with Timed Automata. In *Sixth International Conference on Real-Time Computing Systems and Applications (RTCSA'99)*. IEEE Computer Society Press, 1999.

[8] Ansgar Fehnker. *Citius, Vilius, Melius: Guiding and Cost-Optimality in Model Checking of Timed and Hybrid Systems*. PhD thesis, University of Nijmegen, April 2002.

[9] K. G. Larsen, P. Pettersson, and W. Yi. UPPAAL in a Nutshell. *Int. Journal on Software Tools for Technology Transfer*, 1(1–2):134–152, October 1997.

[10] K.G. Larsen, G. Behrmann, E. Brinksma, A. Fehnker, T.S. Hune, P. Petterson, and J.M.T. Romijn. As cheap as possible: Efficient cost-optimal reachability for priced timed automata. In *Proceedings CAV'01*, 2001.

[11] P. Niebert and S. Yovine. Computing optimal operation schemes for chemical plants in multi-batch mode. *European Journal of Control (EJC)*, 2001. special issue on Hybrid Systems.

A Consortium description

The AMETIST consortium is composed of seven academic partners and four industrial partners as indicated in the table below. The coordinator is listed first, followed by the industrial partners on places 2-5, followed by the remaining academic partners on places 6-11.

No	*Name*	*Contact person*	*URL*	*Role*
CO1	University of Nijmegen	Frits Vaandrager	`www.cs.kun.nl/ita`	Technology Provider
AC2	Bosch	Stefan Kowalewski	`www.bosch.com`	User
AC3	Cybernetix	Patrice Gauthier	`www.cybernetix.fr`	User
AC4	Axxom	Dagmar Ludewig	`www.axxom.de`	User
AC5	Terma	Thomas Hune	`www.terma.com`	User
CR6	University of Aalborg	Kim Larsen	`www.cs.auc.dk/research/FS/`	Technology Provider
CR7	University of Dortmund	Sebastian Engell	`astwww.chemietechnik.uni-dortmund.de`	Technology Provider
CR8	VERIMAG	Oded Maler	`www-verimag.imag.fr`	Technology Provider
AC9	Weizmann Institute	Amir Pnueli	`www.wisdom.weizmann.ac.il`	Technology Provider
CR10	LIF Marseille	Peter Niebert	`www.lif.univ-mrs.fr`	Technology Provider
CR11	University of Twente	Ed Brinksma	`fmt.cs.utwente.nl`	Technology Provider

The academic partners, which all have a proven record of excellence have been cooperating successfully for many years in European projects such as BRA CONCUR, BRA CONCUR2 and LTR VHS. In fact all academic partners except Twente participate in the VHS project. Twente closely collaborates with Nijmegen and Aalborg in several other projects. All academic partners share a common mission, which is to conduct research on the application of formal methods for the development of computer based systems with the long range objective of transforming the application of formal methods from an academic research topic into an engineering practice. Even though the academic partners have a common background knowledge which facilitates collaborative work, they all bring in complementary expertise:

Nijmegen	verification and analysis of distributed real-time algorithms and systems, concurrency theory
Aalborg	tool builder (Uppaal), process algebra
Dortmund	process control, hybrid systems, production planning and scheduling
Verimag	tool builder (Kronos), timed systems
Weizmann	synthesis, abstraction and composition techniques
Marseille	symbolic verification, constraint programming
Twente	validation tools (TorX), stochastic methods, verification of soft real-time systems

The industrial partners, which are all prominent players in the embedded systems area, will bring in complementary case studies, and use and evaluate the project results. Each industrial partner has a privileged relation with one of the academic partners: Bosch and Axxom with Dortmund, Cybernetix with Marseille, and Terma with Aalborg.

Below brief details are given about the participants and their rôle in the project. Also selected references are included.

A.1 University of Nijmegen (KUN)

The Nijmeegs Instituut voor Informatica en Informatiekunde (NIII) encompasses all the research on Computing and Information Science at the Katholieke Universiteit Nijmegen (KUN). Within the NIII currently four research groups are active, including the Informatics for Technical Applications group, headed by Prof. Vaandrager. This group is well-known for its work on models and logics for specification and verification of state based systems. Unique about the group is that it brings together specialists on three different and

important approaches in this area: automata, Hoare's logic, and coalgebras. Some major contributions of the group are:

a. Theoretical results on extensions of the above approaches to settings with real-time, probabilities and hybrid phenomena. See [1, 2, 3, 4].

b. Mechanisation of these extensions using theorem proving and model checking tools such as PVS, Isabelle and Uppaal. See [5, 6].

c. Application of developed theory to a large number of challenging case studies, for instance the formal requirements engineering for command and control systems, and the verification of the vector class from the standard Java API, fragments of the IEEE Firewire and HAVi consumer electronics protocols, a membership protocol for networks with processor crashes and joins, control software for a chemical batch plant, and schedulability for a steel plant. See [7, 8, 9, 10, 11].

Participation The KUN will participate in the project on AC basis for 65 person months, which includes 11 person months for project coordination. In addition, the KUN itself will contribute 51 person months to the project.

Rôle of team in the project Nijmegen will lead WP0 (coordination) and will be responsible for the management of the project. On the scientific side, Nijmegen will contribute to WP1 (Model composition, in particular extension of timed automata with statecharts like structuring mechanisms), WP2 (Guided model checking for timed systems, interaction between timed automata tools and RT-UML tools), and WP3 (case studies, in particular those provided by Axxom and Bosch).

Key personnel

Prof. Frits Vaandrager received his PhD in 1990 (Amsterdam, supervisor Prof. Bergstra) on concurrency theory, and worked since then at MIT (group Prof. Lynch), the Ecole des Mines (group Dr. Berry in Sophia-Antipolis), CWI and the University of Amsterdam. In 1995 he accepted a chair in Nijmegen. Over the last few years his research concentrates on the theories of I/O automata and timed automata and the verification of distributed real-time algorithms and protocols. At CWI, he was scientific manager of the BRA CONCUR2. Also, together with Prof. Klop, he coordinated the HCM network EXPRESS. In addition he has been or is involved in seven other European projects (METEOR, VIP, CONCUR, SPECS, BOOST, VHS, VOSS). He served on PCs of numerous international conferences.

Dr. Jozef Hooman received an MSc degree in computer science from the University of Nijmegen. Next he joined the Eindhoven University of Technology, first as a research assistant in the context of several Esprit projects and later as a lecturer. Since September 1998 he is appointed as a senior lecturer at the University of Nijmegen, with a part-time secondment to the CWI Amsterdam.

The central research theme of Jozef Hooman is the formal specification and compositional verification of distributed real-time and fault-tolerant systems. Compositional proof methods have been devised and applied to a large number of case studies, including hybrid systems and distributed real-time protocols. Since 1993, these verifications are supported by the interactive theorem prover PVS.

Jozef Hooman is involved in IST project Omega (Correct Development of Real-Time Embedded Systems in UML).

References

[1] N.A. Lynch and F.W. Vaandrager. Forward and backward simulations, II: Timing-based systems. *Information and Computation*, 128(1):1–25, July 1996.

[2] N.A. Lynch, R. Segala, and F.W. Vaandrager. Hybrid I/O automata revisited. In Di Benedetto and Sangiovanni-Vincentelli [12], pages 403–417.

[3] M.I.A. Stoelinga and F.W. Vaandrager. Root contention in IEEE 1394. In J.-P. Katoen, editor, *Proceedings 5th International AMAST Workshop on Formal Methods for Real-Time and Probabilistic Systems,* Bamberg, Germany, volume 1601 of *Lecture Notes in Computer Science*, pages 53–74. Springer-Verlag, 1999.

[4] G. Behrmann, A. Fehnker, T.S. Hune, K.G. Larsen, P. Pettersson, J.M.T. Romijn, and F.W. Vaandrager. Minimum-cost reachability for priced timed automata. In Di Benedetto and Sangiovanni-Vincentelli [12], pages 147–161.

[5] G. Behrmann, A. Fehnker, T.S. Hune, K.G. Larsen, P. Pettersson, and J.M.T. Romijn. Efficient guiding towards cost-optimality in UPPAAL. In Margaria and Yi [13], pages 174–188.

[6] T.S. Hune, J.M.T. Romijn, M.I.A. Stoelinga, and F.W. Vaandrager. Linear parametric model checking of timed automata. In Margaria and Yi [13], pages 189–203.

[7] D.J.B. Bosscher, I. Polak, and F.W. Vaandrager. Verification of an audio control protocol. In H. Langmaack, W.-P. de Roever, and J. Vytopil, editors, *Proceedings of the Third International School and Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'94),* Lübeck, Germany, September 1994, volume 863 of *Lecture Notes in Computer Science*, pages 170–192. Springer-Verlag, 1994.

[8] A. Mader, E. Brinksma, H. Wupper, and N. Bauer. Design of a PLC control program for a batch plant — VHS case study 1, 2001. To appear in *European Journal of Control*.

[9] Ansgar Fehnker. Scheduling a Steel Plant with Timed Automata. In *Sixth International Conference on Real-Time Computing Systems and Applications (RTCSA'99)*. IEEE Computer Society Press, 1999.

[10] Ansgar Fehnker. *Citius, Vilius, Melius: Guiding and Cost-Optimality in Model Checking of Timed and Hybrid Systems*. PhD thesis, University of Nijmegen, April 2002.

[11] J.M.T. Romijn. A timed verification of the IEEE 1394 leader election protocol. In S. Gnesi and D. Latella, editors, *Proceedings of the Fourth International ERCIM Workshop on Formal Methods for Industrial Critical Systems (FMICS'99)*, pages pages 3–29, 1999. Full version to appear in *Formal Methods in System Design*.

[12] M.D. Di Benedetto and A.L. Sangiovanni-Vincentelli, editors. *Proceedings Fourth International Workshop on Hybrid Systems: Computation and Control (HSCC'01),* Rome, Italy, volume 2034 of *Lecture Notes in Computer Science*. Springer-Verlag, March 2001.

[13] T. Margaria and W. Yi, editors. *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems,* Genova, Italy, volume 2031 of *Lecture Notes in Computer Science*. Springer-Verlag, April 2001.

A.2 Bosch

The Robert Bosch Group is one of the largest internationally operating industrial enterprises in Germany. In 2000, the company increased its worldwide consolidated sales by 11,9 percent to 31.24 billion Euro, and employs 199,000 people of which around 90,000 work inside Germany. The name Robert Bosch is closely connected with the automobile. The company is the second biggest automotive supplier worldwide. Bosch though, is not only a household name for automotive equipment, but also for a wide spectrum of product areas: For electric power tools just as for thermotechnology, for household appliances just as for automation technology and packaging machinery.

Worldwide, the Bosch Group has around 16,300 scientists, engineers and technicians working on the development of new products and systems, the improvement of the function and reliability of existing products as well as on new production processes. 4,600 of these individuals work outside of Germany. Together, they make an essential contribution to ensuring that Bosch will continue to be renowned for its innovative strength in the future. Total expenditures for research and development in 2000 increased to 2.05 billion Euro.

The department FV/SLD in Frankfurt is part of the corporate research and development. Since several years it is concerned with systematic engineering methods for software-intensive embedded automotive control systems. The main goal of the department is to develop or adapt modern design methods to the specific needs of Bosch, to test and prove the applicability in pilot projects, and, in the long run, to establish them in the product divisions. The department has a long record in European funded research: Members of FV/SLD participated in the ESPRIT project PRAISE and have been members of the ITEA-ESAPS and the ITEA-CAFE consortiums. Further international cooperation is maintained with the Software Engineering Institute (SEI) of the Carnegie Mellon University, Pittsburgh, USA.

Participation Bosch, who is a user member of the consortium, will participate for 3 person months on a FC basis.

Rôle of team in the project As part of task T3.3, Bosch will prepare and provide an example for a case study in real-time resource allocation in automotive control systems, support the principal partners' understanding of the example, and observe and review the principal partners' efforts in modeling and analysing the example.

Key personnel

Dr. Stefan Kowalewski is senior researcher and project leader in the field of safety and reliability of software-intensive, embedded automotive control systems. His work is concerned with systematic methods to assess these qualities in early design phases, as well as to support the design of safe and reliable systems by appropriate aids. In the context of ITEA-CAFE, his interest lies in evaluating the safety of product line architectures for embedded systems with respect to the dynamic behaviour. Dr. Kowalewski got his Dipl.-Ing. degree in Electrical Engineering from the University of Karlsruhe in 1990, and his Ph.D. in Control Engineering from the University Dortmund in 1995. He published extensively in the area of Discrete Event, Real-Time, and Hybrid Systems, and participated in the ESPRIT project *Verification of Hybrid Systems (VHS)*.

References

[1] R. Huuck, Y. Lakhnech, L. Urbina, S. Engell, S. Kowalewski, and J. Preußig. Integrating timed condition/event systems and timed automata for the verification of hybrid systems. *Journal of Parallel and Distributed Computing Practices*, 1(2):45–60, June 1998. Special Issue on "Parallel and Distributed Real-Time Systems".

[2] S. Kowalewski, J. Preußig, O. Stursberg, and H. Treseler. Block-diagram based modeling and analysis of continuous processes under discrete control. *European Journal of Automation (JESA)*, 32(9–10):1097–1118, 1998.

[3] S. Kowalewski, S. Engell, J. Preußig, and O. Stursberg. Verification of logic controllers for continuous plants using timed condition/event system models. *automatica*, 35(3), 1999.

[4] O. Stursberg, S. Kowalewski, and S. Engell. On the generation of timed discrete approximations for continuous systems. *Mathematical and Computer Modelling of Dynamical Systems*, 6(1):51–70, 2000. Special Issue on "Discrete Event Models of Continuous Systems".

[5] S. Engell, S. Kowalewski, C. Schulz, and O. Stursberg. Continuous-discrete interaction in chemical processing plants. *Proceedings of the IEEE*, 88(7):1050–1068, July 2000.

[6] S. Kowalewski, P. Herrmann, S. Engell, H. Krumm, H. Treseler, Y. Lakhnech, R. Huuck, and B. Lukoschus. Approaches to the formal verification of hybrid systems. *at-Automatisierungstechnik*, 49(2):66–74, 2001.

[7] S. Kowalewski, O. Stursberg, and N. Bauer. An experimental batch plant as a case example for the verification of hybrid systems. *European Journal of Control*, 2001. To appear.

[8] S. Kowalewski and J. Preußig. Timed condition/event systems: A framework for modular discrete models of chemical plants and verification of their real-time discrete control. In *Tools and Algorithms for the Construction and Analysis of Systems, Proc. 2nd International Workshop TACAS'96, Passau, 1996*, Lecture Notes in Computer Science 1055, pages 225–240. Springer, 1996.

[9] R. Huuck, Y. Lakhnech, L. Urbina, S. Engell, S. Kowalewski, and J. Preußig. Comparing timed c/e systems with timed automata. In *Int. Workshop on Hybrid and Real-Time Systems (HART'97), Grenoble, Frankreich, 1997*, Lecture Notes in Computer Science 1201, pages 81–86. Springer, 1997.

[10] O. Stursberg, S. Kowalewski, I. Hoffmann, and J. Preußig. Comparing timed and hybrid au-tomata as approximations of continuous systems. In *Hybrid Systems IV: 4th Int. Workshop on Hybrid Systems, Ithaca, USA, October, 12-14, 1996*, Lecture Notes in Computer Science 1273, pages 361–377. Springer, 1997.

[11] J. Preußig, S. Kowalewski, T.H. Henzinger, and H. Wong-Toi. An algorithm for the approximate analysis of simple rectangular automata. In *Proc. 5th Int. School and Symposium on Formal Techniques in Fault Tolerant and Real Time Systems, Lyngby, Denmark, 1998*, Lecture Notes in Computer Science 1486, pages 228–240. Springer, 1998.

[12] J. Preußig, O. Stursberg, and S. Kowalewski. Reachability analysis of a class of switched continuous systems by integrating rectangular approximation and rectangular analysis. In Frits W. Vaandrager and Jan H. van Schuppen, editors, *Hybrid Systems: Computation and Control, Proc. 2nd Int. Workshop, HSCC'99, Berg en Dal, The Netherlands, March 1999*, Lecture Notes in Computer Science 1567, pages 209–222. Springer, 1999.

[13] S. Kowalewski, O. Stursberg, M. Fritz, H. Graf, I. Hoffmann, J. Preußig, S. Simon, M. Remelhe, and H. Tresler. A case study in tool-aided analysis of discretely controlled continuous systems: the two tanks problem. In *Hybrid Systems V: 5th Int. Workshop on Hybrid Systems, Notre Dame, 1997*, Lecture Notes in Computer Science 1569, pages 163–185. Springer, 1999.

A.3 Cybernetix Recherche, Marseille (CYR)

Ever since it was founded in 1985, CYBERNETIX has always had a strategy of growth based on innovation and globalisation. The group is developing its activities in automated systems and robotics in the fields of Micro-electronics, Picking-Sorting-Logistics and service robotics.

CYBERNETIX RECHERCHE was created in 1997 with an aim of concentrating the activities of research and development of the group within a better definite legal framework. In Micro-electronics, CYBERNETIX is one of the world's leading providers of robotised equipment and turnkey plants for smart card manufacture, testing and personalisation (supplies BULL, FNMT, GEMPLUS, OBERTHUR, SAGEM, SCHLUMBERGER, etc.)

In the field of Automated sorting, CYBERNETIX develops robotised equipment for handling, sorting, packaging and identifying large numbers of homogeneous objects (letters, parcels, flats objects) in partnership with MANNESMANN (provides equipment for the French, Swedish, Swiss, Portuguese, American and Chinese post offices).

In service robotics CYBERNETIX offers innovative solutions aiming to extend human actions in hostile or dangerous environments, and to eliminate the need to perform difficult, repetitive or uninteresting tasks. In nuclear robotics, CYBERNETIX is present in the dismantling and cleansing market. Also the group develops automated quality control systems and vision systems for the sectors of food production, pharmaceuticals. And in offshore field CYBERNETIX develops autonomous universal vehicle.

The CYBERNETIX GROUP, a major player in technological innovation, is an official Contract Research Company (SRC) approved by ANVAR, the French national agency for innovation, and indeed its subsidiary CYBERNETIX RECHERCHE gives it tremendous capacity for innovation. More than 20% of its engineers devote their energies to industrial research and technological innovation.

The Industrial and Control software Department is part of the CYBERNETICS RECHERCHE Technical Services.Its functions within the group are :

- Provide a support for software related studies and tasks within the context of multi-disciplinary projects managed by other departments or companies within the Group.
- Assume overall responsibility for projects which are preponderantly software related.
- Manage any software related work packages which may be sub-contracted outside the Group.

In order to succeed, the software team have a wide field of knowledge and experience in all the different disciplines within the CYBERNETIX GROUP - being able to cooperate effectively with the engineers and technicians in the fields of robotics, automation, optics, electrical and electronic engineering ..... The Industrial and Control software Department is involved in both the conceptual and study phases as Systems Architects, and in the phases of system build and integration.

Participation CYBERNETIX, who is a user member of the consortium, will participate for 28.9 person months on a FC basis.

Rôle of team in the project CYBERNETIX RECHERCHE has the rôle of a customer in the AMETIST consortium, supplying industrial benchmarks with real need for advanced timing technology, notably by providing models of the coordination problems in their microelectronics manufacturing sector (Task 3.1). In cooperation with the academic partners, Cybernetix Recherche will then work on generalisations of the control principles for future larger machines of similar type and related scheduling problems (Task 2.2).

Besides these technical challenge for academic partners, CYBERNETIX will provide an extended inside look into their software process in order to analyse the options and needed improvements in order to

render AMETIST technology usable for process industry, results of which will be presented in form of interfaces and mock tools as requirement specification of future tool development (Task 2.5). The main hope behind using timed automata in the manufacturing software process is to replace the currently used (hand written) simulation technique: Timed automata with their non-determinism are ideal for modelling the execution environment of a control programme. It is intended to synthesise critical parameters in the code (time critical constants) and to verify that the program behaves correctly under lax assumptions on the environment.

Manufacturing programming at Cybernetix corresponds to the widely used iec-61131 standard. Hence, our experiences will be made available and will be of use for the whole of manufacturing programming.

Key personnel

Patrice Gauthier is the head of the *Industrial and Control Software* department of CYBERNETIX RECHERCHE, which counts 15 engineers and technicians. Patrice Gauthier holds a (French) engineering degree from the well known "Ecole Centrale Paris". In 1991 he joined CYBERNETIX, where he is mainly occupied in robotics within offshore projects and real time applications.

A.4 Axxom

Axxom is one of the leading software companies in the process industry. Our international industrial customers use Axxom solutions and optimisers in the chemical and automotive industry and distribution and related fields. In all industries the software is used for the strategic and tactical optimisation of value chains, simulations and layout studies. Axxom belongs to the DMC group which employs 300 people. It was founded in 1994. The headquarter is in Munich but it has offices all over Germany, Vienna, Princeton/USA. The main focus is the optimisation tool ORion-PI.

Optimisation methods — Many kinds of algorithms calculate the best solution but there are only very few which actually optimise and decrease costs. The optimisation methods used by ORion-PI deliver exemplary market leading results. The careful integration of the single modules allow a transparent and efficient process of optimisation and planning.

ORion-PI trusts in a combination of mathematical, empirical and heuristic methods. Which single procedure or combination of methods is applied, is determined automatically from the structure of a given problem or can be established by the user.

- Support of the company policy: Multi target optimisation determines the best target compromise for the overall company. The value-adding chain has to be designed according to the strategic and tactical company objectives. The multi target optimisation of ORion-PI finds the most promising compromise for conflicting objectives.
- Layout optimisation: New existing layouts can be examined and optimised within a short period of time. It can be easily displayed what advantages and drawbacks investments and de-investments have on the material flow and the supply chain.
- Integrated solutions for distribution with ORion-PI Shipping: Minimisation of transport units: Calculate the content, volume, weight and quantity of containers/boxes before collecting products and articles in the shipping floor such that the number of containers/boxes shipped are minimised.
- Material flow optimisation: Knowing in advance what will happen on the floor. Avoid any "traffic jams" with optimal routings.

These general modules can also be applied to your entire value chain considering transport costs and balancing the load between the different sites and partners.

Participation Axxom, who is a user member of the consortium, will participate for 11.3 person months on a FF basis.

Rôle of team in the project
WP3, T3.4: Axxom contributes the case studies to the 'value chain optimisations'. This contribution will contain scenarios of industrial partners in the chemical industry, distribution centers and the automotive industry.

WP1, T1.5: Decomposition of models and (master-)data to achieve parallelism, modeling of large networks of processes, transformation of feasible plans.

Key personnel

Dr.-Ing. Dagmar Ludewig studied chemical engineering with a focus on biotechnology and modelling at the Technical University Hamburg-Harburg in Germany. In her PhD-thesis (Prof. Munack, Braunschweig and Prof. Bellgardt, Hannover) she developed a general modelling approach for biotechnical processes. This was then implemented in an expert system shell. In her first industrial job she did material flow - and process simulation for biotechnological and pharmaceutical applications. The simulation was a very important method to guarantee the feasibility of multiproduct plants, to evaluate resource needs for processes with high simultaneity and to optimise the equipment layout. Since 2001 she is *international project manager* at Axxom Software AG.

A.5 Terma A/S, Radar Systems Division

The main part of Terma including the Radar Systems Division is located in Lystrup outside Aarhus. Currently Terma employs 850 people, 340 of these work on development projects. Terma has a long experience in cooperating with universities during development projects, most notable is the Danish Ørsted satellite. During a number of projects the Radar Systems Division has been working closely with researchers from both University of Aalborg and the Technical University of Denmark.

The Radar Systems Division is developing and producing high quality radar sensors mainly used for coastal surveillance, traffic control in ports and airports and environmental surveillance. Development of control software and most of the hardware development takes place at Terma.

Participation Terma, who is a user member of the consortium, will participate for 6.7 person months on a FC basis.

Rôle of team in the project The main contribution of Terma will be the case study for Task 3.2. The involvement of Terma will be both in providing a description of the case study (and additional information as needed) and in evaluating the proposed solutions. Terma will also participate in development of tools (Task 2.5) and in the end-user panel.

Key personnel

Thomas Hune has received his PhD in 2001 from University of Aarhus supervised by M. Nielsen on theory and tools for analysing real-time systems. During his studies, he has published a number of papers on development of tools for analysing real-time systems in journals and proceedings, and participated in the Esprit project Verification of Hybrid Systems (VHS). He has worked at Terma since finishing his PhD.

A.6 University of Aalborg (AAU)

At Aalborg University there is considerable expertise in techniques and tools for design and analysis of reactive systems and real-time systems and hybrid systems. In particular, this work has led to the development of the successful tool UPPAAL for automatic verification and analysis of real-time systems (more than 1000 users in 60 countries). Some major contributions of the group is:

- Development of the realtime verification tool UPPAAL in collaboration with Uppsala University, Sweden. This work is based on a large number research contributions to the data structures and algorithms allowing for efficient (symbolic) state-space exploration. Also, a number of variants of the tool has been created. In particular, versions of UPPAAL allowing for cost-optimal analysis, parameterised analysis, and distributed analysis has been implemented in collaboration with the research group from Nijmegen. Relevant publications for AMETIST include [1, 2, 3, 4, 5].
- Collaboration with the company IAR visualSTATE. In particular, this collaboration lead to finite-state verification techniques exploiting the (hierarchical) structure of the models, allowing for systems with more than 1400 parallel components (and a more than 10^{500} states) to be verified in

minutes on a regular PC. The method is now patented and implemented in the commercial version of the visualSTATE tool. Relevant publications for AMETIST include [6, 7, 8].

- The group has a strong process algebraic background. Thus, much research has been made in compositional verification and semantics. Relevant publications for AMETIST include [9, 10, 11].
- A number of large and industrial real-time case-studies has been dealt with using UPPAAL. These include a real-time communication protocol used b Bang& Olufsen. Using UPPAAL a 10 year old bug was revealed, diagnosed and corrected. Other case-studies include a power-control (Bang& Olufsen), a collision-avoidance protocol, control software for a chemical batch plant, and schedulability for a steel plant. Relevant publications for AMETIST include [12, 13, 14].
- Recently the group has made significant contributions to the area of realtime testing [15, 16].

Participation The University of Aalborg, which participates in the project on AC basis, asks for EU support for 42.4 person months. In addition, the University of Aalborg itself will contribute 75 person months to the project.

Rôle of team in the project Aalborg University, will lead WP2 on analysis and tools. It will participate in all tasks within this work package, with emphasis on symbolic data structures and exploitation of structure, and on bringing UPPAAL to the level of a commercial tool. In addition, Aalborg University will contribute to the development of stochastic extensions of timed automata (Task 1.3), the modelling of scheduling and planning problems (Task 1.4), and to various case studies (WP3).

Key personnel

Prof.dr. Kim Guldstrand Larsen received his PhD in 1985 (Edinburgh, supervised by Prof. Robin Milner). From 1993 Professor at Aalborg University and in the period 2000-02 part-time industrial professor at Twente University. From 1991-97 CS member of the Danish Research Council for Natural Science. Director of BRICS at Aalborg. Awarded and Honorary Doctorate (Honoris causa) from Uppsala University in 1999. Since 2000 member of Royal Danish Academy of Sciences and Letters. Founding coordinator and first year SC manager for the EU BRA CONCUR2. Involved in two European projects VHS and FIREWORKS. Co-founder and SC-member of the conference-series TACAS, SC-member of CONCUR. Host and PC-chair for CAV'91, ICALP'98, CONCUR'01. PC-chair for CAV'02. Member of IFIP WG 2.2. PC member of international conferences such as ADPM, CAV, CONCUR, ICALP, LICS, MOVEP, PROBMIV, TACAS, RTSS.

References

[1] Gerd Behrmann, Thomas Hune, and Frits Vaandrager. Distributed timed model checking - How the search order matters. In *Proc. of 12th International Conference on Computer Aided Verification*, Lecture Notes in Computer Science, Chicago, Juli 2000. Springer-Verlag.

[2] Kim G. Larsen, Paul Pettersson, and Wang Yi. UPPAAL in a Nutshell. *Int. Journal on Software Tools for Technology Transfer*, 1(1–2):134–152, October 1997.

[3] G. Behrmann, K.G. Larsen, J. Pearson, C. Weise, and W. Yi. Efficent timed reachability analysis using clock difference diagrams. In *Proceedings of CAV'99*, volume 1633 of *Lecture Notes in Computer Science*, 1999.

[4] Kim G. Larsen, Gerd Behrmann, Ed Brinksma, Ansgar Fehnker, Thomas Hune, Paul Pettersson, , and Judi Romijn. As cheap as possible: Efficient cost-optimal reachability for priced timed automata. In *Proceedings of CAV2001*, Lecture Notes in Computer Science, 2001.

[5] Fredrik Larsson, Kim G. Larsen, Paul Pettersson, and Wang Yi. Efficient Verification of Real-Time Systems: Compact Data Structures and State-Space Reduction. In *Proc. of the 18*th *IEEE Real-Time Systems Symposium*, pages 14–24. IEEE Computer Society Press, December 1997.

[6] J. Staunstrup, K.G. Larsen, H.R. Andersen, H. Hulgaard, G. Behrmann, K. Kristoffersen, J. Lind-Nielsen, H. Leerberg, A. Skou, and N.B. Theilgaard. Practical verification of embedded software. *IEEE Computer*, 33(5), 2000.

[7] J. Lind-Nielsen, H.R. Andersen, G. Behrman, H. Hulgaard, K. Kristoffersen, and K.G. Larsen. Verification of large state/event systems using compositionality and dependency analysis. *Formal Methods in System Design*, 2001. To appear.

[8] G. Behrman, K.G. Larsen, H.R. Andersen, H. Hulgaard, and J. Lind-Nielsen. Verification of hierarchical state/event systems using reusability and compositionality. *Formal Methods in System Design*, 2001. To appear.

[9] L. Aceto, P. Boyyer, A. Burgueno, and K.G. Larsen. The power of reachability testing for timed automata. In *Proceedings of TACAS'98*, volume 1530 of *Lecture Notes in Computer Science*, 1998.

[10] K. Kristoffersen, F. Laroussinie, K.G. Larsen, P. Pettersson, and W. Yi. A compositional proof of a real-time mutual exclusion protocol. In *Proceedings for FASE97*, number 1214 in Lecture Notes in Computer Science, 1997.

[11] H.E. Ejersbo, K.G. Larsen, and A. Skou. Scaling up uppaal – automatic verification of real-time systems using compositionality and abstraction. In *Proceedings of FTRTFT00*, volume 1926 of *Lecture Notes in Computer Science*, 2000.

[12] K. Havelund, K.G. Larsen, and A. Skou. Formal verification of a power controller using the real-time model checker uppaal. In *Proceedings of 5th International AMAST Workshop*, volume 1601 of *Lecture Notes in Computer Science*, 1999.

[13] K. Havelund, A. Skou, K.G. Larsen, and K. Lund. Formal modelling and analysis of an audio/video protocol: An industrial case study using uppaal. In *Proceedings of the 18th IEEE Real-Time Systems Symposium*, 1997.

[14] Thomas Hune, Kim G. Larsen, and Paul Pettersson. Guided Synthesis of Control Programs Using UPPAAL. In Ten H. Lai, editor, *Proc. of the IEEE ICDCS International Workshop on Distributed Systems Verification and Validation*, pages E15–E22. IEEE Computer Society Press, April 2000. full version to appear in Nordic Journal of Computing.

[15] B. Nielsen and A. Skou. Automated test generation timed automata. In *Proceedings of TACAS01*, Lecture Notes in Computer Science, 2001.

[16] B. Nielsen and A. Skou. Automated test generation timed automata. In *'21st IEEE Real-Time Systems Symposium 2000 WiP-Session'*, IEEE, 2000.

A.7 University of Dortmund (Uni DO)

The Process Control Laboratory is an interdisciplinary group, part of the Department of Chemical Engineering of the University of Dortmund, focused on the control of chemical processes and processing plants, where control is understood in a broad sense. The laboratory was founded in 1990 and quickly grew to its present size of 15-20 researchers, mostly PhD candidates funded from outside sources.

About half of the research effort is devoted to discrete phenomena in the control and operation of processing plants. Of particular interest are the design and verification of logic controllers which are responsible for the sequencing of operations and for plant safety, the modeling and simulation of hybrid systems, e.g. flexible batch plants, scheduling of operations, optimal start-up and shut-down, and event detection from measurements. Most of this research is performed in cooperative projects with groups in computer science, mathematics, and dynamics and control at the same as well as at other universities. International cooperations in this area exist with Carnegie-Mellon University, Pittsburgh (jointly funded by DAAD and NSF), the University of Loughborough (funded by DAAD and ARC) and several European groups in the context of the ESPRIT Project VHS-Verification of Hybrid Systems. The group also was an active member in the European research network CAPE.NET.

The research in the timed- and hybrid systems area was reported recently in articles in leading journals as Automatica and the Proceedings of IEEE. The group provided a case study for the VHS project which became a benchmark problem for several papers by other groups which will be published in the European Journal of Control. Members of the group gave invited presentations on continuous-discrete systems in process control at both recent AIChE perspective conferences on Chemical Process Control, in 1996 and 2001, respectively.

The role of the group in general and also in this project is to interface between theoretical developments and industrial problems and applications, actively contributing to some degree on both aspects and on the integration and solution of real-world problems.

Since 1995, 6 PhD theses in the area of timed and hybrid systems and scheduling were published. About 10 more projects are finished or currently under way. Specific topics include: hybrid simulation of batch plants, scheduling of production systems using heuristics, genetic algorithms, constraint programming, and mathematical programming, abstraction of continuous dynamics into timed automata, and verification of logic controllers based upon timed-automata models of the controlled plant.

Participation The University of Dortmund, which participates in the project on AC basis, asks for EU support for 36 person months. In addition, the University of Dortmund itself will contribute 18 person months to the project.

Rôle of team in the project Dortmund will be involved in the following tasks:
T1.1: Classification of problems and models.
T1.2: Model composition.
T1.3: Quantitative modeling, in particular scenario-based approaches.
T1.4: Scheduling and planning, in particular description of constraints and uncertainty.
T2.2: Scheduling algorithms, in particular real-time algorithms.
T2.4: Stochastic techniques, in particular scenario-based approaches.
T2.5: Tool interaction, in particular coupling of TA models and tools to MILP solvers and description languages (e.g. GAMS).
WP3: Coordination of Workpackage. Modular modelling of supply chains and distributed resource allocation algorithms in supply chains and in transportation systems with autonomous vehicles. Research on the representation of uncertainty in scheduling problems. Testing of solution approaches for value chain test cases of different levels of complexity.

Key personnel

Prof. Sebastian Engell Sebastian Engell was born in 1954 in Düsseldorf, Germany. He received a Dipl.-Ing. degree from the Ruhr-Universität Bochum in Electrical Engineering in1978, and a Dr.-Ing. degree from the Department of Mechanical Engineering of the University of Duisburg in 1981. He was granted the "venia legendi" in control by the same university in 1987. In 1986 he joined the Fraunhofer-Institut IITB in Karlsruhe, Germany, defining and coordinating mostly industry-sponsored R&D projects in industrial automation before he was appointed to his present position as full professor of process control in 1990. He was founding Co-Editor of the IEEE Transactions on Control Systems Technology, Associate Editor of the European Journal of Control and has served on numerous conference program committees. He is the Chairman of the Technical Committee on Control Design of IFAC and an Associate Editor of Journal of Process Control. He was strongly involved in the successful application for the focused research programme KONDISK on hybrid systems in Germany and coordinates the Graduiertenkolleg "Modeling and Model-Based Design of Complex Systems" at the University of Dortmund.

Olaf Stursberg obtained a Dr.-Ing. degree from the Chemical Engineering Department of the University of Dortmund in 2000. His thesis treated the abstraction of continuous dynamic systems into timed and hybrid automata and the verification of control logic for chemical processes. He now works on the optimisation of start-up sequences for processing plants with discrete and continuous inputs. Olaf Stursberg spent several months working on cooperative projects at Carnegie Mellon University, Pittsburgh, PA, and Loughborogh University, GB.

References

[1] S. Engell, S. Kowalewski, and B. Krogh. Discrete events and hybrid systems in process control. In J. E. Kantor, C. E. Garcia, and B. Carnahan, editors, *5th International Conference on Chemical Process Control,* Tahoe City, number 316(93) in AIChE Symposium Series, pages 165–176, 1997.

[2] R. Huuck, Y. Lakhnech, L. Urbina, S. Engell, S. Kowalewski, and J. Preussig. Combining a computer science and control theory approach to the verification of hybrid systems. *Journal of Parallel and Distributing Practices*, pages 45–60, 1998.

[3] S. Kowalewski, S. Engell, J. Preussig, and O. Stursberg. Verification of logic controlles for continuous plants using timed condition/event-system models. *Automatica*, 35:505–518, 1999.

[4] O. Stursberg, S. Kowalewski, and S. Engell. On the generation of timed discrete approximations for continuous systems. *Mathematical and Computer Models of Dynamical Systems (MCMDS)*, 6:51–70, 2000.

[5] M. Otter, M. Remelhe, S. Engell, and P. Mostermann. Hybrid models of physical systems and discrete controllers. *at-Automatisierungstechnik*, 48:426–437, 2000.

[6] G. Sand, S. Engell, C. Schulz, and R. Schultz. Approximation of an ideal online scheduler for a multiproduct batch plant. *Computers & Chemical Engineering*, 24:361–397, 2000.

[7] S. Engell, S. Kowalewski, C. Schulz, and O. Stursberg. Continuous-discrete interactions in chemical processing plants. *Proc. of the IEEE*, 88:1050–1068, 2000.

A.8 Verimag, Grenoble

VERIMAG is a large academic research laboratory, affiliated with the university of Grenoble (UJF), the national center for scientific research (CNRS) and the engineering school of Grenoble (INPG). The research at VERIMAG, conducted by more than 40 researchers and graduate students, addresses all theoretical and practical aspects of formal methods for system development. VERIMAG has a proven record in both fundamental results and in development of tools such as the verification package CADP, the data-flow synchronous language LUSTRE (used for programming embedded control systems), the KRONOS tool for verification of timed automata and the recently-developed **d/dt** prototype tool for analysis of continuous and hybrid systems. VERIMAG is composed of three groups with strong mutual interaction: 1) The *synchronous programming* group concentrating on the Lustre/Scade programming environment for writing safety-critical embedded applications. The main feature of Lustre is the combination of a control-oriented date-flow language based on block diagrams, rigorous semantics and efficient compilation; 2) The *distributed systems* group focusing on verification of asynchronous communication protocols (such as those written in SDL) and of smart card applications; 3) The *timed and hybrid systems* group whose research agenda includes the exportation of verification methodology toward new application domains, including timing analysis, optimisation and control system design.

VERIMAG has a long history of successful participation and coordination of European projects, and among the recent European project in which it participated one can find the projects SYRF, VIRES, CRISYS and VHS, for which it was a coordinator. VERIMAG has strong working relations with leading centers in embedded systems research in the US such as Berkeley, Stanford, CMU and Penn, as well as ongoing interaction with industry including Telelogic, France Telecom, Schneider, Aerospatiale, Gemplus, Silicomp, EDF and others.

The timed and hybrid systems group of VERIMAG has been the one of the principal promoters of timed and hybrid systems research in Europe. In particular it coordinated the recent VHS project, for which the proposed project can be viewed as a successor. Some results of the VHS project concerning timing analysis of batch plants appeared recently in a special issue of the *European Journal of Control*. The timed automata verification tool Kronos developed by the group was among the first timing verification tools and a source of inspiration for many other tools. In addition, VERIMAG researchers were involved in fundamental research on timed automata including timed regular expressions, the relation between discrete and continuous time models, controller synthesis and scheduling with timed automata and the composition of timed modules. Current research effort in the timing domain is focused on specialising KRONOS to treat three important classes of applications:

1. Using timed automata to solve dynamic scheduling problems via synthesis techniques.
2. Verifying schedulability of embedded software on a given architecture.
3. Timing analysis of digital circuits with bi-bounded delays.

These applications drive the development of Kronos and motivate research in new algorithmic techniques for improving the performance of the tool.

Participation VERIMAG participates in the project on an FC basis. It will contribute 78 person months to the project.

Rôle of team in the project VERIMAG will focus on the general principles of modelling time-dependent phenomena and resource allocation problems using timed automata and on the algorithmic problems related to timed automata analysis. The major effort will be directed to the modeling of dynamic

scheduling problems in the presence of different types of uncertainties and partial information. On the algorithmic side VERIMAG will focus on efficient heuristic algorithms for approximate optimisation, on abstraction techniques as a tool for treating large scale systems and on integrating the TA approach with other approach based on constraint resolution. This work is part of packages WP1, WP2 and WP3. In addition VERIMAG will participate in the scientific coordination of the project where its main role will be to synthesise the results at various parts of the project into a unified framework. VERIMAG will also be responsible for the dissemination of project results (WP4).

Key personnel

Oded Maler received his B.A. in Computer Science from Technion, Haifa (1979), an M.Sc. in Management Science – Information Systems from Tel-Aviv Univ. (1984) and a Ph.D. in Computer Science from Weizmann Inst., Rehovot, Israel (1990). Since 1992 he is with VERIMAG (from 1994 as a researcher (CR1) in the CNRS and from 2001 as a research director (DR2)) where he leads the timed and hybrid systems group. He coordinated in the past several networks and project on timed and hybrid systems and is currently the coordinator of the Esprit project 26270 VHS (verification of hybrid systems, 13 partners, 1998-2001). He organised several international workshops on timed and hybrid systems.

Sergio Yovine obtained his Ph.D. thesis from the Grenoble engineering school INPG in 1993. His thesis included the development of Kronos, the first verification tool for timed automata. After spending 2 years at the University of California, Berkeley, working mostly on the automated highway project (PATH) he returned to Verimag as researcher (CR2 and later CR1). His current interests include the application of timed automata to verification and schedulability analysis of embedded software. He was a PC member of several conferences on real-time systems.

References

[1] T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. *Information and Computation*, 111(2):193–244, 1994.

[2] C. Daws, A. Olivero, S. Tripakis, and S. Yovine. The tool kronos. In *Hybrid Systems III*, volume 1066 of *LNCS*. Springer, 1996.

[3] Sergio Yovine. Kronos: A verification tool for real-time systems. *Int. Journal on Software Tools for Technology Transfer*, 1(1–2):123–133, October 1997.

[4] S. Yovine. Model-checking timed automata. In G. Rozenberg and F. Vaandrager, editors, *Embedded Systems*, volume 1494 of *LNCS*. Springer, 1998.

[5] O. Maler and A. Pnueli. Timing analysis of asynchronous circuits using timed automata. In H. Eveking P.E. Camurati, editor, *Proc. CHARME'95*, volume 987 of *LNCS*, pages 189–205. Springer, 1995.

[6] O. Maler and S. Yovine. Hardware timing verification using kronos. In *Proc. 7th Conf. on Computer-based Systems and Software Engineering*. IEEE, IEEE Press, 1996.

[7] E. Asarin, P. Caspi, and O. Maler. A Kleene theorem for timed automata. In *Proc. 12th Annual IEEE Symposium on Logic in Computer Science (LICS'97)*, pages 160–171, Warsaw, June 1997. IEEE, IEEE Computer Society.

[8] M. Bozga, O. Maler, A. Pnueli, and S. Yovine. Some progress in the symbolic verification of timed automata. In O. Grumberg, editor, *Proc. CAV'97*, volume 1254 of *LNCS*, pages 179–190. Springer, 1997.

[9] A. Bouajjani, S. Tripakis, and S. Yovine. On-the-fly symbolic model-checking for real-time systems. In IEEE Computer Society, editor, *RTSS 1997 proceedings*, 1999.

[10] E. Asarin, O. Maler, and A. Pnueli. On discretization of delays in timed automata and digital circuits. In R. de Simone and D. Sangiorgi, editors, *Proc. Concur'98*, volume 1466 of *LNCS*, pages 470–484. Springer, September 1998.

[11] E. Asarin, O. Maler, A. Pnueli, and J. Sifakis. Controller synthesis for timed automata. In *Proc. System Structure and Control*, pages 469–474. IFAC, Elsevier, July 1998.

[12] E. Asarin and O. Maler. As soon as possible: Time optimal control for timed automata. In F. Vaandrager and J. van Schuppen, editors, *Hybrid Systems: Computation and Control*, volume 1569 of *LNCS*, pages 19–30. Springer, Mars 1999.

[13] K. Altisen, G. Goessler, A. Pnueli, J. Sifakis, S. Tripakis, and S. Yovine. A framework for scheduler synthesis. In IEEE Computer Society, editor, *RTSS 1999 proceedings*, pages 154–163, 1999.

[14] M. Bozga and O. Maler. On the representation of probabilities over structured domains. In N. Halbwachs and D. Peled, editors, *Proc. CAV'99*, volume 1633 of *LNCS*, pages 261–273. Springer, June 1999.

[15] M. Bozga, O. Maler, and S. Tripakis. Efficient verification of timed automata using dense and disrete time semantics. In T. Kropf and L. Pierre, editors, *Proc. CHARME'99*, volume 1703 of *LNCS*, pages 125–141. Springer, September 1999.

[16] O. Bournez and O. Maler. On the representation of timed polyhedra. In U. Montanari, J.D.P. Rolim, and E. Welzl, editors, *Proc. ICALP'00*, volume 1853 of *LNCS*, pages 793–807. Springer, July 2000.

[17] Y. Abdeddaïm and O. Maler. Job-shop scheduling using timed automata. In *Proc. CAV'2001*, LNCS. Springer, 2001.

A.9 Weizmann Institute (WIS)

The Weizmann Institute is a research Institute based in Rehovot, Israel. The Institute contains about 500 researchers and auxiliary scientific staff and conducts research in diverse areas, including Chemistry, Life-Sciences, Physics, and Mathematics. The department of Applied Mathematics was formed in 1947 and among other world known achievements, introduced the first computer to Israel – the WEIZAC which was built at the Institute and completed in 1955. Today the department has several groups, which excel in theoretical computer science areas such as Cryptography, Complexity, Distributed Systems, Semantics and Logics of Programs. The last area is headed by Professors Amir Pnueli and David Harel who have been occupied in the last 21 years in research on formal specification and verification of programs and systems, and developed the concepts and theories of Dynamic Logic, Temporal Logic, Reactive Systems, and Statecharts. The John von Neumann Minerva Center for Verification of Reactive systems has been founded at the Weizmann Institute in 1998. Its current director is Amir Pnueli. The mission of the center is to conduct research in the application of formal methods for the development of (software and hardware) systems with the long range objective of transforming the application of formal methods from an academic research topic into an Engineering practice.

Participation WIS participates in the project on an AC basis. It asks for 30.6 person months of support of the EU, and brings in 30.6 person months itself.

Rôle of team in the project WIS intends to contribute mostly to the work on using abstraction and compositional methods to treat large systems (tasks **T1.2/T2.1**). In particular it will focus on extending to the timed case some well-known abstraction and composition techniques such as *network invariants* and *predicate abstraction* as well as time-specific techniques based on changing the granularity of time.

In addition, WIS will contribute to the work on synthesis (tasks **T1.5/T2.2**), focusing on the use of high-level specifications such as UML, Statecharts and Message Sequence Charts as a starting point for synthesising timing preserving executable code.

Key personnel

Prof. Amir Pnueli is the 1996 recipient of the ACM Turing award "For his seminal work introducing temporal logic into computing science and for outstanding contributions to program and system verification. He is mainly known for the introduction of temporal logic into Computer Science; his work on the application of temporal logic and similar formalisms for the specification and verification of reactive systems; the identification of the class of "Reactive Systems" as systems whose formal specification, analysis, and verification require a distinctive approach; and the development of a rich and detailed methodology, based on temporal logic, for the formal treatment of reactive system; extending this methodology into the realm of real-time systems; and more recently, introducing into formal analysis the models of hybrid systems with appropriate extension of the temporal-logic based methodology.

Beside his more theoretical work, concerning a complete axiom system and proof theory for program verification by temporal logic, he also contributed to algorithmic research in this area. He developed a deductive system for linear-time temporal logic and model-checking algorithms for the verification of temporal properties of finite-state systems. Together with David Harel, Pnueli worked on the semantics and implementation of Statecharts, a visual language for the specification, modeling, and prototyping of reactive systems. This language has been applied to avionics, transport, and electronic hardware systems. His current research interests involve synthesis of reactive modules, automatic verification of multi-process systems, and specification methods that combine transition systems with temporal logic.

References

[1] E. Asarin, O. Bournez, T. Dang, O. Maler, and A. Pnueli. Effective controller synthesis of switching controllers for linear systems. *Proceedings of the IEEE*, 88(7):1011–1025, 2000.

[2] A. Pnueli, S. Ruah, and L. Zuck. Automatic deductive verification with invisible invariants. In *Proceedings TACAS'01,* Genova, Italy, pages 82–97, 2001.

[3] Y. Kesten and A. Pnueli. Verification by finitary abstraction. *Information and Computation, a special issue on Compositionality*, 163:203–243, 2000.

[4] Y. Kesten, O. Maler, M. Marcus, A. Pnueli, and E. Shahar. Symbolic model checking with rich assertional languages. *Theoretical Computer Science*, April 2001. A special issue on infinite state systems. To appear.

[5] Y. Kesten, Z. Manna, and A. Pnueli. Verification of clocked and hybrid systems. *Acta Informatica*, 26(11):836–912, 2000.

[6] A. Pnueli and E. Shahar. Liveness and acceleration in parameterized verification. In *Proceedings CAV'00*, pages 328–343, 2000.

[7] Y. Kesten and A. Pnueli. Control and data abstractions: The cornerstones of practical formal verification. *Software Tools for Technology Transfer*, 4(2):328–342, 2000.

[8] E. Asarin, O. Maler, A.Pnueli, and J. Sifakis. Controller synthesis for timed automata. In *IFAC Symposium on System Structure and Control*, pages 469–474. Elsevier, 1998.

A.10 Laboratoire d'Informatique Fondamentale de Marseille (LIF)

The Laboratoire d'Informatique Fondamentale de Marseille (LIF) is cooperatively maintained by the Université de la Mediterranée, the Université de Provence and the Centre National de la Recherche Scientifique (CNRS).

Computer Science research in Marseille has traditionally been strong in artificial intelligence, logic programming and constraint solving. *Prolog* and later *constraint logic programming* were conceived there, accompanied by a series of successful applications in industry. The LIF currently consists of five research groups, notably the "Modelling and Verification" research group. Key competences for AMETIST in the latter domain concern the modeling and efficient automatic verification of parallel systems, also in industrial applications similar to those of AMETIST. The interdisciplinary AMETIST team will include researchers from several research groups (logic and complexity).

Participation LIF participates in the project on a FF basis. It will contribute 63 person months to the project.

Rôle of team in the project LIF's key rôle in the project is to bring in competence in heuristic algorithms as components for timing analysis, resulting from multidisciplinary competence in heuristic verification methods and in constraint based methods. With an interdisciplinary team, LIF will help bridging the gap between the two cultures of verification and constraint solving in the real time application domain, especially in the *Analysis and Tools* work package (WP2) with contributions to T2.1, T2.2 and T2.3. Working next door, LIF is the major academic contact of CYBERNETIX and will participate in their case study T4.1. LIF will also participate in tool-related efforts in T3.1 and T2.5.

Key personnel

Peter Niebert obtained his PhD in computer science in 1998 in Hildesheim, Germany. 1998–2000, he was contractual researcher in VERIMAG (Grenoble, AMETIST partner). Since 2000, he is assistant professor (maître de conférences) at the University Aix-Marseille I.

For his PhD, Peter Niebert worked on partial order logics and methods for distributed system verification. At VERIMAG, he has participated in several industrial research projects and in the Esprit project *Verification of Hybrid Systems*. He thus worked on several levels of real time systems (from system modeling to compilation techniques for real time languages).

Alain Colmerauer obtained his PhD in Computer Science from the University of Grenoble 1967. 1967–1970, he was assistant professor at the University of Montréal. Since 1970, he is professor at the University Aix-Marseille II. He has headed the Artificial Intelligence Group (1973-1985 and 1991–1993) and the LIM (1993–1995).

Out of need for an expressive formalism for describing natural language translators – a domain to which he substantially contributed throughout the seventies – Colmerauer conceived the first version of Prolog in 1972, a mile stone in computer science. Around 1980, he took interest in the improvement of Prolog. His subsequent work ignited *constraint logic programming*, a continuous path to Prolog IV (1996) and beyond: First order constraints.

Alain Colmerauer's substantial contributions to computer science have been honoured by numerous awards and decorations, notably he is senior member of the *Institut Universitaire de France*, a distinction currently shared only by two computer scientists.

References

[1] P. Niebert, M. Huhn, S. Zennou, and D. Lugiez. Local first search – a new paradigm in partial order reductions. In *CONCUR*, number 2154 in LNCS, pages 396–410, 2001.

[2] P. Niebert, S. Tripakis, and S. Yovine. Minimum-time reachability for timed automata. In *IEEE Mediteranian Control Conference*, 2000. Patras, Greece.

[3] P. Niebert and S. Yovine. Computing optimal operation schemes for chemical plants in multi-batch mode. *European Journal of Control (EJC)*, 2001. special issue on Hybrid Systems.

[4] D. Lugiez and Ph. Schnoebelen. The regular viewpoint on pa-processes. In *9th Int. Conf. Concurrency Theory, CONCUR'98*, LNCS, pages 50–66, Nice, France, 1998.

[5] R. M. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In *International Conference on Concurrency Theory (CONCUR)*, pages 380–394, 2000.

[6] F. Giannesini, H. Kanoui, R. Pasero, and M. van Caneghem. *Prolog*. Addison Wesley, 1986.

[7] N. Guerinik and M. Van Caneghem. Solving crew scheduling problem by constraint programming. In *Principles and Practice of Constraint Programming (CP)*, pages 481–498, 1995.

[8] F. Benhamou and A. Colmerauer, editors. *Constraint Logic Programming: Selected Research*. MIT Press, 1993.

[9] A. Colmerauer. Toward an ideal unified constraints domain. In *Practical Application of Constraint Technology, PACT'96*, 1996.

A.11 University of Twente (UT)

The Formal Methods and Tools (FMT) group, headed by Prof. Dr. Ed Brinksma, consists of 16 staff members and is part of the Faculty of Computer Science at the University of Twente, The Netherlands. It has internationally recognised competence in formal specification, verification, conformance testing, formal methods for object-oriented systems, and combining formal methods with performance analysis.

The group is currently involved in the following research projects: *Hard and Softly Timed Systems* (HaaST), together with the University of Nijmegen and Philips, *Côte-de-Resyste*, in collaboration with the University of Eindhoven, Philips, and Lucent, *Atomyste*, with Philips, Lucent, and Ordina, *VOSS* (Validation of Stochastic Systems), with the universities of Aachen, Bonn, Erlangen en Nijmegen, *Specification-based Performability Checking* (SPACE) and *Compositional Analysis and Specification of Hybrid Systems* (CASH), funded by the Netherlands Organisation for Scientific Research (NWO).

In the AMETIST project the FMT group will collaborate with people from the Distributed and Embedded Systems (DIES) group, also at the University of Twente. This group, headed by Prof. Dr. Pieter Hartel, provides one of the case studies and has substantial experience with both the design of real-time systems and their validation based on formal methods.

Participation FMT participates in the project on an FC basis. It will contribute 39.9 person months to the project.

Rôle of team in the project Twente will be involved in the following tasks:
T1.3 Quantitative Modelling: Based on work done on stochastic automata [1] and work on stochastic model checking [2, 3].
T2.1 Abstraction and Compositionality: Based on work on McMillan prefixes [4] and partial orders in a stochastic setting [5].
T2.4 Stochastic Techniques: stochastic model checking [2, 3] and validation [6, 7].
T2.5 Tool Interaction: Based on very recent work in progress on a common format based on transition systems.
Furthermore, Twente will participate in **WP3** (Case Studies) and have a somewhat larger involvement in **WP0** (Project Management) and **WP4** (Dissemination), related to the organisation of project meetings and setting up and maintaining the project web-page.

Key personnel

Prof. Dr. Ed Brinksma After studying mathematics at the University of Groningen Ed Brinksma obtained a PhD in computer science at the University of Twente (1988). He worked at the universities of Groningen and Twente, and at the Swedish Institute for Computer Science (1990). In 1991 he accepted a chair in Twente. Ed was chairman of the ISO standardisation committee for the formal specification technique LOTOS, published as an International Standard (ISO IS 8807). He has been/is involved in many international projects (e.g. SEDOS, LOTOSPHERE, REACT, VOSS). He is a member of IFIP WG6.1 and SCs of leading conferences in the area of formal methods (FORTE/PSTV, ETAPS, TACAS), as well as PCs (e.g. CAV, FASE, FM, FMOODS, SPIN). He on the editorial boards of IEEE Transactions on SE and the International Journal of Software Tools for Technology Transfer.

Dr. J-P. Katoen is an associate professor in the Formal Methods and Tools Group at the University of Twente. He received his M.Sc. degree (with honours) and PhD degree in Computer Science from the same university in 1987 and 1996, respectively. Previously he held positions at the Eindhoven University of Technology (1988-1990), Philips Research Laboratories (1990-1992) and the University of Erlangen-Nürnberg (1997-1999). He authored over 60 papers in scientific conferences and journals and is member of several program committees, such as the steering committee of the int. workshop on Probabilistic Methods in Verification (PROBMIV). He acted as a program chair of the 5th AMAST workshop on real-time and probabilistic systems and is co-chair of the 7th TACAS conference in 2002. His main interests are system validation techniques and combining formal methods and performance analysis.

References

[1] P.R. D'Argenio, J.-P. Katoen, and E. Brinksma. Specification and analysis of soft real-time systems: Quantity and quality. In *Proceedings of the 20th IEEE Real-Time Systems Symposium,* Phoenix, Arizona, USA. IEEE Society Press, 1999.

[2] B. Haverkort, H. Hermanns, and J-P. Katoen. On the use of model checking for quantitative dependability evaluation. In *19th IEEE Symposium on Reliable Distributed Systems (SRDS)*, pages 228–238. IEEE Computer Society Press, 2000.

[3] C. Baier, B. Haverkort, H. Hermanns, and J.-P. Katoen. Model checking continuous-time markov chains by transient analysis. In *Computer-Aided Verification CAV'2000*, volume 1855 of *Lecture Notes in Computer Science*, pages 358–372. Springer-Verlag, 2000.

[4] R. Langerak and E. Brinksma. A complete finite prefix for process algebra. In N. Halbwachs and D. Peled, editors, *11th International Conference on Computer Aided Verification*, number 1633 in Lecture Notes in Computer Science. Springer Verlag, 1999.

[5] Theo C.Ruys, Rom Langerak, Joost-Pieter Katoen, Diego Latella, and Mieke Massink. First passage time analysis of stochastic process algebra using partial orders. In T. Margaria and W. Yi, editors, *TACAS2001*, number 2031 in Lecture Notes in Computer Science. Springer Verlag, 2001.

[6] R. de Vries, J. Tretmans, A. Belinfante, J. Feenstra, L. Feijs, S. Mauw, N. Goga, L. Heerink, and A. de Heer. Côte de Resyste in PROGRESS. In STW Technology Foundation, editor, PROGRESS *2000 – Workshop on Embedded Systems*, pages 141–148, Utrecht, The Netherlands, October 13 2000.

[7] A. Belinfante, J. Feenstra, R.G. de Vries, J. Tretmans, N. Goga, L. Feijs, S. Mauw, and L. Heerink. Formal test automation: A simple experiment. In G. Csopaki, S. Dibuz, and K. Tarnay, editors, 12^{th} *Int. Workshop on Testing of Communicating Systems*, pages 179–196. Kluwer Academic Publishers, 1999.

[8] Ed Brinksma and Angelika Mader. Verification and optimization of a plc control schedule. In *Proceedings of the SPIN'2000 Workshop*, volume 1885 of *Lecture Notes in Computer Science*, pages 73–92. Springer Verlag, 2000.

[9] A. Mader, E. Brinksma, H. Wupper, and N. Bauer. Design of a PLC Control Program for a Batch Plant – VHS Case Study 1. Accepted for publication in the *European Journal of Control*, 2001.

B Contract preparation forms