Information Societies Technology
(IST)
Programme

Future and Emerging Technologies - Open Domain

Contract for: Shared-Cost RTD

Annex 1 - Description of Work

Project acronym: Advance

Project full title:

Advanced Validation Techniques
for Telecommunication Protocols

Contract no:
Related to other Contract no:

Date of preparation of Annex 1: April 2000

Proposal number: IST-1999-29082

Operative commencement date of contract:

Contents

List of Figures

1 Project summary

1.1 Objectives

Telecommunication protocols are critical systems of very high complexity. The goal of the project is to develop a new generation of validation tools based on advanced and novel techniques allowing to tackle problems that arise in the validation of modern protocols, and that are beyond the scope of the state-of-the-art methods and tools. The objectives of this project are (1) to develop a general methodology for the specification and automated validation of telecommunication protocols, taking into account important aspects such as: complex timing constraints, use of unbounded data structures like counters and queues, parametrization, mobility, etc. (2) to provide tool support for this methodology, and (3) to prove it substantially advances the state of the art by applying it to industrially relevant case studies.

1.2 Description of the work

Experience shows that the verification of realistic systems cannot be achieved without applying a tight combination of several approaches and analysis techniques. We are convinced that the next generation validation tools should be built by embedding several specialized tools in a single framework. These tools should apply complementary approaches and be able to communicate and cooperate easily. The goal of our project is to produce such a framework. Our approach consists of a combination of powerful abstraction techniques, and efficient validation procedures based on reachability analysis of finite and infinite-state systems. These techniques are embedded in a common formal framework based on the model of extended automata, i.e., automata with data structures. All usual models like timed automata, counter automata, Petri nets, unbounded FIFO-channel automata, automata with unbounded arrays (relevant for modeling unbounded networks and networks of mobile processes), etc, are particular instances of this general model. Our validation environment will be built from several tools (for abstraction, symbolic analysis, etc) dealing with extended automata. The connections between the different tools will be made through a common format for the description of extended automata. We have already a definition of such a format. In order to make our validation framework effectively usable, we will connect it to a specification environment for SDL. Our framework will be experimented and evaluated on industrial scale case studies: the PGM protocol (Pragmatic General Multicast) and the SIP (Session Initiation Protocol).

1.3 Milestones and expected results

The main outcome of the project will be the production of a novel validation environment including:

- Abstraction tools for automatic construction of abstract models,
- Symbolic reachability analysis procedures for various infinite-state extended automata,
- Efficient state-space explorers based on symbolic and partial-order techniques.

2 Project objectives

The goal of the project is to develop a new generation of tools for automatic validation of telecommunication protocols. Our aim is to develop powerful techniques allowing to tackle problems that arise in the validation of modern protocols, e.g., complex timing constraints, communication through unbounded queues, unbounded number of components, mobility, etc. All these problems are beyond the scope of the existing verification methods and tools. The main outcome of this project will be the production of a specification and validation environment based on these techniques, and its application to industrially relevant protocols.

2.1 Motivation

The evolution of modern society is tightly related to the spectacular progress in information technologies, based on the use of worldwide telecommunication networks. Mastering and developing the technologies involved in these networks is economically and strategically vital.

One of the fundamental activities underlying the development of telecommunication networks is the design of software controllers based on communication protocols. The critical nature of these systems and their high complexity make it essential to have rigorous design methods and automated validation techniques. Indeed, integrating formal specification methods and validation techniques in the design process is necessary for all critical applications, and for communication protocols in particular, since any erroneous behavior may have important (economical and human) consequences. Moreover, the sooner an error is detected during the design process, the easier is its repair, and the smaller are its consequences and its cost. Hence, validation techniques are needed at all the stages of the design and implementation: At the early stages of the design, various models of the system are analyzed at different levels of abstraction using *verification* techniques. Later, the final implementation of the system is validated using *testing* techniques.

During the last two decades, an important effort has been devoted to the development of verification techniques and their application. Significant achievements have been obtained, and efficient tools have been developed for *automatic* verification of *finite-state systems* (i.e., systems with finitely many configurations), based essentially on reachability analysis algorithms. All major constructors of hardware and software controllers have already created verification groups that use these techniques. This is particularly true after the recent occurrence of costly errors like the Pentium bug and the Ariane crash.

However, the existing techniques and tools have several limitations concerning the nature of the systems they can handle and their sizes.

Indeed, the kind of systems we are interested in, i.e., telecommunication protocols, are *distributed systems* that communicate in an *asynchronous* manner (through buffers). The asynchronous style of communication makes the analysis problem far more difficult than the synchronous one (e.g., in hardware verification) since each component of the system can act independently of its partners, according to its own speed. The consequence is a combinatorial explosion in the number of computations and in the state space of the systems (w.r.t. the size of their components). One of the major challenges in computer-aided verification is actually the design and the development of new *effective verification methods* that can scale up for such systems.

Moreover, while the finite-state framework is well suited for reasoning about e.g., logical circuits, it cannot deal with essential aspects in the behaviors of software systems like protocols. Our analysis of industrial protocols, in particular the case studies of the proposal (see Section 5.5), shows the necessity of dealing with the following aspects:

- **Asynchronous communication:** A natural model for asynchronous communicating systems are automata with *unbounded* FIFO queues (FIFO-channel systems). Indeed, we need abstract models allowing to reason about qualitative properties of a system without imposing bounds on the capacities of the buffers. The model of FIFO-channel systems is actually the basis of widely used specification languages like SDL [1].

- **Data manipulation:** Communication protocols manipulate complex data structures and variables ranging over different *infinite* data domains, e.g., integer counters, queues with an arbitrary length, etc.

- **Real-time constraints:** The behaviors of communication protocols involve various mechanisms based on timing constraints (time-outs for instance). This implies that we need models in which real-time constraints can be expressed, e.g., using real-valued clocks to measure delays between events.

- **Parametrization:** Many protocols are designed in a parametric way. For instance, the upper bounds defining the time-outs, the sizes of the transmitted files, the number of allowed retransmissions, etc., can be considered as parameters of the protocol that may range over infinite domains. Networks of processes with an arbitrary number of processes are also an important class of parametrized systems (the parameter in this case is the size of the system).

- **Mobility:** Mobility is an important feature of modern protocols for mobile phones, wireless terminals, etc. It induces dynamic changes in the logical communication structure of the network. Processes can be created, communicate, change partners, and then disappear. Hence, we have to consider systems with an unbounded number of components, and an unbounded number of communication structures.

To take into account aspects such as those mentioned above, we must be able to reason about models which may have *infinitely* many configurations. Actually, an important research topic in the domain of computer-aided verification is to extend the applicability of automatic verification techniques in order to deal with *infinite-state systems*.

2.2 Aim of the project

As shown in the discussion above, to cope with complex systems like modern telecommunication protocols, the development of computer-aided validation tools must perform a breakthrough both from the quantitative and qualitative point of view. Our ambition is to design advanced and novel techniques for the next generation validation tools.

The objectives of this project are (1) to develop a general methodology for the specification and automated validation of telecommunication protocols, taking into account all the important aspects mentioned above (state explosion problem, unboundedness of data structures, parametrization, etc), (2) to provide tool support for this methodology, and (3) to prove that it substantially advances the state of the art by applying it to industrially relevant and challenging case studies.

[1]SDL is the ITU-T (CCITT) international standard language for the specification of telecommunication protocols.

3 List of Participants

List of Contractors

No	Name	Short name	Country	Status	Date enter	Date exit
1	LIAFA, Univ. Paris 7	UP7	France	C	0	36
2	CNET - France Telecom	CNET	France	P	0	36
3	Univ. of Liège	Liège	Belgium	P	0	36
4	Tech. Univ. of Munich	TUM	Germany	P	0	36
5	Univ. of Uppsala	Uppsala	Sweden	P	0	36
6	VERIMAG, Univ. Grenoble 1	UJF	France	P	0	36
7	Weizmann institute	Weizmann	Israel	P	0	36

List of Observers

Name	Short name	Country	Date enter	Date exit
Ericsson Utvecklings AB	Ericsson-UAB	Sweden	0	36
Siemens AG	Siemens	Germany	0	36

4 Contribution to programme objectives

Information society needs the development of advanced communication technologies. The design of *reliable* telecommunication protocols is one of the fundamental activities underlying the development of these technologies.

The services that are required by modern applications, such as audio/video on demand, mobile telephony, Internet telephony, etc, involve many aspects that make the design of protocols extremely complex. Hence, there is a real need on developing techniques and automatic tools that help on the design and on the validation of these complex systems.

The validation of modern protocols (such as those presented in Section 5.5) is beyond the capabilities of the state-of-the-art techniques and tools. The challenging goal of our project is to provide a validation environment integrating different powerful new techniques that can deal with modern complex protocols. Such a validation environment will be a valuable tool for industrial designers and will contribute in decreasing the costs of the design and the validation of their products.

5 Innovation

Experience shows that the verification of realistic systems cannot be achieved without applying a tight *combination* of several approaches and analysis techniques. We are convinced that the next generation validation tools should be built by embedding several specialized tools in a single framework. These tools should apply *complementary approaches* and be able to *communicate and cooperate easily.* The goal of our project is to produce such a framework.

Our approach consists of a combination of powerful *abstraction techniques*, and *efficient* validation procedures based on *reachability analysis* of finite and *infinite-state systems*. These techniques are embedded in a *common formal framework* based on the model of *extended automata*, i.e., automata with data structures. All usual models like timed automata, counter automata, Petri nets, unbounded FIFO-channel automata, automata with unbounded arrays (relevant for modeling parametrized networks), etc, are particular instances of this general model.

Our validation environment will be built from several specialized tools (abstraction tools, symbolic analysis tools, etc) dealing with (classes of) extended automata. The connections between the different tools will be made through a *common format* for the description of extended automata based on the format IF defined by the contractor (**UJF**) [23]. In order to make our validation framework effectively usable, we will connect it to an existing (commercial) specification environment for SDL. Figure 1 gives a schematic representation of the environment we propose to build.

5.1 Abstraction techniques

Abstraction techniques are necessary in order to obtain models that can be handled by automatic validation procedures. Indeed, the set of reachable configurations of a protocol is in general hard to compute and to represent due to the large number of possible interactions between its components and the complex relations that exist between its variables. This set is in general infinite, or finite but of such a huge size that it cannot be handled with the state-of-the-art automatic tools. Then, a natural approach is to divide the verification problem into several tasks by considering *abstractions* of the system corresponding to simplified views of the behavior of the system. Abstractions are obtained by focusing only on certain aspects of the behavior, and depend on the properties under consideration. To achieve that, we need to develop (1) automatic strategies for *generating abstraction functions* derived from a concrete model and a property to check, and (2) automatic techniques for *constructing abstract models* for given abstraction functions. It is worth noting that, in our approach, the abstract model is not necessarily finite-state. Indeed, as far as we know, all existing abstraction techniques aim at producing finite-state models in order to be able to apply finite-state analysis techniques. However, finding faithful finite abstractions is often hard since many aspects in the behavior of the system must be hidden or encoded in a nontrivial and ad-hoc manner, e.g., timing constraints, queue contents, etc. One of the innovative aspects of our approach is to consider abstraction techniques that can produce infinite-state models for which automatic (infinite-state) analysis techniques are available. This allows to use *hierarchies of abstractions* and provides a formal framework for reasoning about systems through different abstraction levels.

5.2 Reachability analysis

Most of the addressed verification problems, e.g., verification of safety properties, can be reduced to reachability analysis problems: The crucial problem is how to explore the set

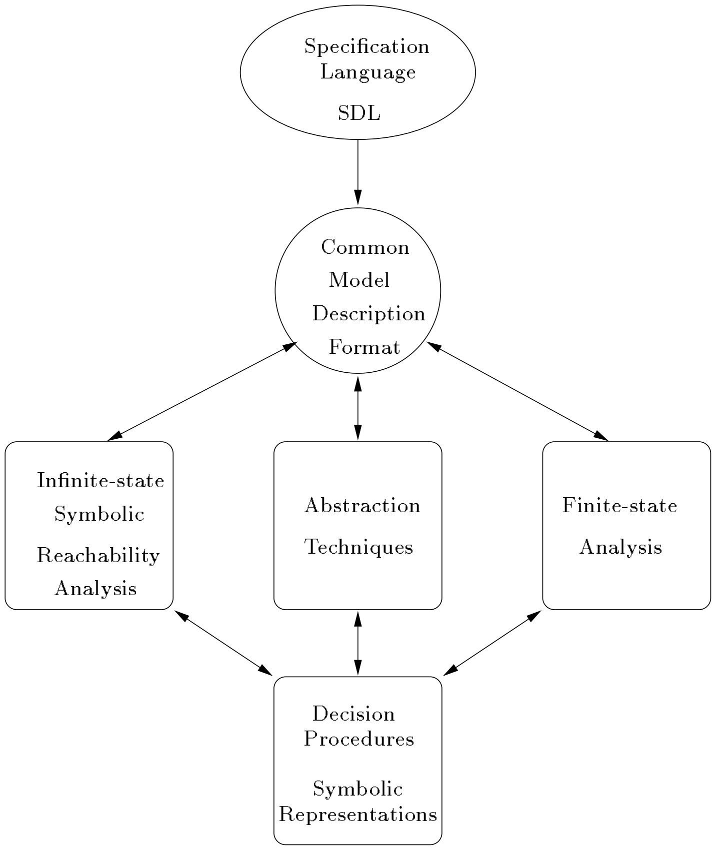


Figure 1: A specification and validation environment

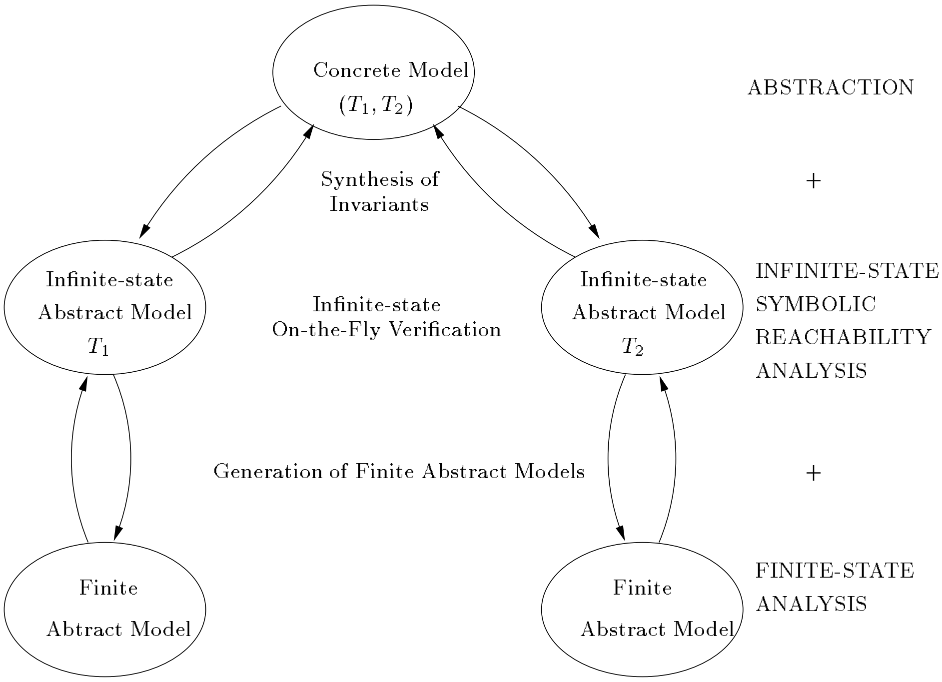


Figure 2: The general methodology

of reachable configurations, and more generally, how to compute and represent this set effectively. One of our main research directions is:

- Developing efficient techniques to cope with the combinatorial explosion in the size of the models, and to reduce the complexity of the state-space exploration, both in time and memory.

  For that, we will consider *symbolic techniques* based on efficient BDD-like representation structures and on efficient SAT decision procedures (e.g., Stålmarck's method), and *partial-order techniques* based on the use of the notions of stubborn sets, ample sets, and unfoldings.

  In particular we intend to explore new ideas on using SAT procedures in model-checking, and to develop partial order techniques based on unfoldings for extended automata, e.g., FIFO-channel automata, timed automata.

- Developing algorithmic or semi-algorithmic techniques based on powerful reachability analysis procedures and efficient symbolic representations for various kinds of *infinite-state* extended automata, e.g., communicating automata through unbounded FIFO queues, automata with counters, timed Petri nets, automata with unbounded arrays modeling parametrized networks of automata or networks of mobile processes, etc. Our aim is to identify fundamental structures for symbolic representation of infinite state-spaces, and to define general methods and techniques for computing the set of reachable configurations for extended automata. This constitutes one of the most challenging parts of our project since we believe that such symbolic analysis techniques will be the kernel of future validation frameworks.

5.3 Combining abstraction with reachability analysis

As we mentioned previously, the strength of our approach is to allow the combination of different powerful techniques in order to analyze complex systems. We aim at developing a general methodology based on combining abstraction steps with reachability analysis, both for finite and infinite-state systems. Figure 2 shows the principle of our methodology: abstraction is used to simplify models and project them on several dimensions corresponding to different aspects in their behaviors. These aspects are directly related to the types of the variables and data structures that are needed. The obtained abstract models may be finite or infinite-state. For instance, a protocol may be modeled by an extended automaton manipulating integer counters and unbounded queues. Abstractions of the concrete model may lead to either a counter automaton or to a FIFO-channel automaton, both of which are infinite-state models. Then, symbolic procedures are applied to analyze these models and compute their set of reachable states. This reachability analysis will be used in three different ways:

- *On-the-fly verification*: Properties can be checked directly on the abstract model during the exploration of its set of configurations,

- *Synthesis of invariants*: The set of reachable configurations of the abstract model represents in fact an invariant of the concrete model. It can be used as an auxiliary invariant in the analysis of the concrete model.

- *Generation of finite abstract models*: Each partition of the set of reachable configurations leads to the definition of a finite symbolic graph which simulates the original concrete model. Hence, finite abstractions can be generated automatically during the computation of the set of reachable configurations. The considered partition can be defined according to several criteria depending on the model and on the property to check, and it can be refined as needed.

The realization of this general methodology requires the definition of a uniform framework in which different representation structures can be manipulated, and that allows different decision procedures and analysis techniques to communicate and cooperate. This represents an important challenge. We will define such a framework (see Figure 1) around the formal model of extended automata and a common description format for this model based on the IF format furnished by the contractor (**UJF**) [23].

5.4 Main outcome of the project

As mentioned before, the main outcome of our project will be a novel specification and validation environment for complex telecommunication protocols. This environment will be built by integrating several specialized tools developed by the different partners and connected to a widely used commercial specification environment for the language SDL.

One of the main vendors of SDL specification environments (VERILOG) has allowed the contractor (**UJF**) to develop through a special API a compiler that translates SDL specifications into extended automata. These automata are described in the format IF defined by (**UJF**). This format (syntactical analyzer, simulator, etc.) is publically available and several research groups use it. Through this format, several validation tools (e.g., SPIN) have been already integrated to the environment. In our project, we will adopt the format IF as a *common description format* and work on extending this format in order to include aspects such as real-time, parametrization, dynamism and mobility. All the developed tools will communicate and cooperate through this common format. This allows the project to benefit from an existing widely used specification and validation environment (Object-Geode of VERILOG), and to build the next generation of this environment.

The architecture of the environment is given in Figure 1. It can be decomposed into three layers: (1) a layer containing symbolic representation and decision procedure packages allowing the manipulation of basic structures (automata, arithmetical constraints, etc.), (2) a second layer containing validation tools including abstraction tools and (finite and infinite-state) reachability analysis tools, (3) and a layer which consists of a common model description format connected to the specification language SDL. Notice that this architecture can be easily extended to other specification languages (e.g., UML) through the common description format.

5.5 Applications

Our project will be guided by real-life case studies furnished by industrial partners. These case studies involve various aspects mentioned above: complex timing constraints, use of unbounded data structures, parametrization, and mobility.

The first case study is the PGM protocol (Pragmatic General Multicast) which is a reliable multicast transport protocol built on top of the IP multicast. The specification of this protocol will be furnished by the contractor (**CNET**). Several other companies like CISCO SYSTEMS are working on this protocol. This case study is a good candidate for validating the approach of the project since such a protocol: (1) is *very complex* when dealing with several levels of routers (need of abstractions), (2) has *very strong timing constraints*: it will be used for example for video on demand (need of new timed models and timed verification techniques), and (3) *employs asynchronous transmission*, which introduces losses of messages, retransmissions, etc (need of reasoning about models such as automata communicating through unbounded queues).

The second case study is the SIP (Session Initiation Protocol) which is a simple signaling protocol for Internet conferencing and telephony. SIP was published in RFC 2543 (March 17, 1999) as a proposed standard. SIP provides the necessary protocol mechanisms so that end systems and proxy servers can provide services like: call forwarding; the ability to reach a called party under a single, location independent address even when the user changes terminal; terminal-type negotiation and selection (e.g. internet telephony, mobile phone, answering service); blind and supervised call transfer and invitations to multicast conferences. Hence, the consideration of this case study will allow to address important issues such as *mobility*, and reasoning about unbounded networks with dynamic structures (*dynamic networks*). The specification of this protocol will be furnished by the observer (**Ericsson-UAB**).

6 Community added value and contribution to EU policies

Developing environments for automatic validation of software, and especially of telecommunication protocols, is one of the major scientific and technological challenges in computer science today. This activity requires an important amount of man power, and a variety of complementary and specialized skills that cannot be found, at the top level, in a same research group or even in a same european country.

The participants of our project are leading academic and industrial research groups having already well established cooperation links. They have the will to strengthen their cooperation in order to carry out a common research project of important scale.

7 Contribution to Community social objectives

The evolution of modern society is tightly related to the development of worldwide telecommunication networks. There is a real need of providing telecommunication services with a *guaranteed quality* (reliability, speed, etc). Indeed, these services are the basis of all the network applications that are developed, and that will be developed in the future (audio/video on demand, Internet telephony, etc). These telecommunication services are ensured by complex telecommunication protocols that must be designed carefuly and validated before their use.

8 Economic developement and S&T prospects

Telecommunication protocols are critical systems in the sense that erroneous behaviours or bad performances may have important economical (and human) consequences: For companies that commercialize telecommunication services, offering noncompetitive products may imply the loss of important market share, and consequently, the loss of huge financial benefits and a lot of jobs.

The complexity of software systems, e.g., telecommunication protocols, and their critical nature make it essential to have rigourous design methods and automated validation techniques. These techniques and automatic tools should be accessible to engineers who design the software products, and should be applicable to systems of industrial scale. Our aim is to offer such validation tools that will contribute in decreasing the costs of the design of complex software systems such as telecommunication protocols.

9 Project Workplan

9.1 General description

9.1.1 Structure of the workplan

Our work will be decomposed into three interdependent working packages, each of them being decomposed into several tasks. The structure of these working packages is as follows:

- WP1: Methods and Tools,
  - T1.1: Abstraction,
  - T1.2: Symbolic analysis,
  - T1.3: Efficient state-space exploration.
- WP2: Integration of tools and Experimentations,
  - T2.1: Common language and interface,
  - T2.2: Integration of tools,
  - T2.3: Experimentations and case studies.
- WP3: Project management /assessment.
  - T3.1: Management and coordination,
  - T3.2: Assessment and quality control,
  - T3.3: Dissemination and transfer activities.

The aim of the work in WP1 is to investigate the conceptual and technical problems encountered in the analysis of complex telecommunication protocols, to furnish new validations methods and techniques, and to provide tools based on these techniques. Hence, WP1 includes two activities: conceptual work and tool development. The 3 tasks of the workpackage correspond to complementary approaches and techniques. Within each of these tasks, we will address the validation problem of different kinds of systems: extended automata with unbounded data structures (queues, counters, clocks), parametrized systems, dynamic networks, mobile processes.

The aim of the work in WP2 is to furnish a common validation environment which allows the user a smooth navigation between several validation approaches and tools. The work in WP2 includes also experimentations and case studies. We will consider two industrial scale case studies: the PGM protocol and the SIP protocol. The aim of this experimental work is to investigate the problems that appear in the analysis of modern protocols, and to show the effectiveness and the robustness of the approaches and tools we propose in project.

Finally, WP3 consists in coordinating the work in the project, and in following its progression in order to ensure the realisation of the expected objectives. Each of the working packages is under the responsability of a coordinator (lead contractor) who will be helped by coordinators assigned to each task. The prime contractor has the responsability of the global coordination. Work in WP3 includes also activities of transfert of knowledge and dissemination of results and tools through, regular publications and communications in international conferences and symposia, permanent interaction with industrial partners and observers, and the organization of workshops where external academic specialists and industrials will be invited.

9.1.2 Progression of the work and Dependencies

The work in the project can also be seen as a set of continuous interdependent streams (streams are feeding each others). We can identify the following streams:

- two streams in WP1: (S1) methodological and conceptual work, and (S2) tool development,
- two streams in WP2: (S3) integration of tools in a common environment, and (S4) experimentations and case studies,
- two streems in WP3: (S5) Assessment and coordination, and (S6) dissemination and transfer.

Note that in the case of WP1, this decomposition into streams is orthogonal to its decomposition into tasks defined in the previous section.

The work in all the WP's will start at the same time and will be carried out as follows: The conceptual work in WP1 (S1) will continousely feed the development activity within the same working package (S2). The development of tools must respect common formats and model description languages that will be designed in the first months of the project in T2.1 of WP2 (S3). Tools developed by different partners will be integrated in T2.2 in a common validation environment, and will be available through a common interface (T2.1). Hence, stream S2 depends on the common language activity in S3 (T2.1). Conversely, S2 will continuously feed the activity of tool integration of S3 (T2.2).

As for the experimental work (T2.3), the first year will be devoted to the study of the specifications of the protocols PGM and SIP, and to the identification of the problems that the analysis of such protocols raises. This work is a source of inspiration of the work in WP1 (S1) and will trigger the development of new validation techniques and tools. Hence, S4 will also feed continuously S1 (which feeds S2). Experimentations using the tools developed in the project (WP1 and T2.2) will start at the beginning of the second year and will continue all the duration of the project following the development of our validation environment. Hence, S2 and S3 will feed S4.

The progress of the work in the project will be followed and controlled in S5 of WP3 (Task T3.2). During the project, the quality of the obtained results will be evaluated and compared with the expected intermediary results (see deliverables). Observations and evaluations will occur every 6 months (an annual report will be produced and integrated to the annual project report). This evaluation activity will help WP's and Tasks coordinators (coordination Task T3.1) to adapt the efforts to the required results in order to meet the final objectives of the project.

The work in S6 (Task T3.3) consists in a parallel task which includes: (1) Academic dissemination through publications, communications, and tool demonstrations in international conferences and symposia, (2) Knowledge and technology transfer through permanent interaction and collaboration with industrial partners. Indeed, our project includes one industrial contractor and two industrial observers who will help in targetting the work in the project toward industrially relevant problems, and on the other hand, will use the techniques and tools developed in the project in order to enhance their design methods and techniques, (3) Organisation of meetings and workshops open to external academic and industrial specialists, where our techniques and tools will be presented, compared with other existing ones, and tested against industrial needs. The proceedings of these workshops will be published in special issues of international scientific journals (e.g., the journal Formal Methods in System Design).

As we have said previously, the aim of our work is to furnish a validation environment allowing to deal with several aspects that are essential for reasoning about modern and complex protocols, and that are not taken into account in existing validation frameworks. These aspects will be addressed during the project by considering different *levels of increasing complexity.* These aspects will be also investigated through all the different WP's and tasks of our project: their investigation starts in WP1 (S1) and goes through the different streams (S2 then S3) giving rise to the development of validation tools and their application (S4) in WP2.

We intend to address the following aspects in the specified ordering:

1. Extended automata with heterogeneous unbounded data structures, e.g., integer counters, Fifo-channels, and clocks.

2. Parametrized systems (systems with parametrized bounds on variables, networks with parametrized size, etc),

3. Dynamic networks and mobiles processes.

Notice that, the investigation of these aspects will follow the ordering above within each stream, but since streams are parallel, these aspects will be considered in parallel at different phases (progress level). Notice also that all these aspects will be considered within each of the 3 tasks of WP1, i.e., they will be addressed using different approaches that will be compared and combined. The resulting techniques and tools will be integrated and experimented in WP2.

Figures 3 and 4 show a graphic overview of the workplan.

9.2 Workpackage list

Work-package No	Workpackage title	Lead contractor No	Person-months	Start month	End month	Deliverable No
1	Methods and tools	5	184.7	0	36	D1, D2 D6, D7, D8 D14, D15
2	Integration of tools and experimentations	6	146.9	0	36	D3, D4 D9, D10, D11, D12 D16, D17, D18
3	Project Management and Assessment	1	17.1	0	36	D5, D13, D19
	TOTAL		348.7			

9.3 Paid/Non paid persons-months effort

Participant	**WP1**	**WP2**	**WP3**	**Total**
1	26 / 12	30 / 12	4 / 3	60 / 27
2	6	6	0	12
3	26 / 4.2	10 / 2	0 / 1	36 / 7.2
4	22 / 11	14 / 6	0 / 1	36 / 18
5	21 / 9	16 / 7	2.6 / 2	39.6 / 18
6	25	26	3	54
7	18 / 4.5	13.9 / 4	0 / 0.5	31.9 / 9
	144 / 40.7	115.9 / 31	9.6 / 7.5	269.5 / 79.2

9.4 Workpackages description

Workpackage number:	1	**Start date or starting event**	0			
Participant number:	1	2	3	4	5	6	7
Person-months per participant:	38	6	30.2	33	30	25	22.5

Objectives

The aim of the work in WP1 is (1) to investigate problems encountered in the analysis of complex telecommunication protocols taking into account several aspects such as timing constraints, use of unbounded counters or queues, parametrization, mobility, etc, (2) to furnish new validations methods and techniques allowing to tackle these problems, and (3) to provide tools (prototypes) based on these techniques.

Description of work

WP1 includes two activities: (1) design of methods and techniques, and (2) tool development. The work in WP1 is decomposed into 3 parallel tasks: T1.1: Abstraction, T1.2: Symbolic analysis, and T1.3: Efficient state-space exploration. Within each of these tasks, which correspond to complementary approaches and techniques, will be addressed the validation problem of different kinds of systems: extended automata with unbounded data structures (queues, counters, clocks), parametrized systems, dynamic networks, mobile processes.

Deliverables		**Delivery month**
D1	Methods and tools for extended automata	12
D2	Methods and algorithms for parametric reasoning	12
D6	Tools for efficient analysis of extended automata	24
D7	Methods and tools for parametric reasoning (part 1)	24
D8	Methods and algorithms for dynamic networks and mobile processes	24
D14	Methods and tools for parametric reasoning (part 2)	36
D15	Methods and tools for the analysis of dynamic networks and mobile processes	36

Milestones and expected results

We will investigate several essential aspects in the analysis of modern protocols by considering them at different levels of increasing complexity, and using different approaches that will be compared and combined. We intend to address the following aspects in the specified order:

1. Extended automata with heterogeneous unbounded data structures, allows to reason about systems with timing constraints, unreliable communication channels, etc.
2. Parametric reasoning (systems with parametrized bounds on variables, networks with parametrized size, etc),
3. Dynamic networks (dynamic creation of processes) and mobiles processes.

We will produce for each of these classes of systems new validation methods and tools.

Workpackage number:	2	**Start date or starting event**	0			
Participant number:	1	2	3	4	5	6	7
Person-months per participant:	42	6	12	20	23	26	17.9

Objectives

The aim of the work in WP2 is (1) to furnish a common validation environment which allows the user a smooth navigation between several validation approaches and tools, and (2) the use of this environment in two cases studies: the PGM protocol and the SIP protocol. The aim of the experimental work is to investigate the problems that appear in the analysis of modern protocols, and to show the effectiveness and the robustness of the approaches and tools we propose in project.

Description of work

The work in WP2 includes the definition of a common model description language and interface, the integration of different techniques and tools, as welll as experimentations with the developed validation environment on two industrially relevant protocols. The work in WP2 is decomposed into 3 parallel tasks: T2.1: Common language and interface, T2.2: Integration of tools, and T2.3: Experimentations.

Deliverables		**Delivery month**
D3	Common model description language	12
D4	Integration of abstraction and symbolic analysis tools for extended automata	12
D9	Common interface for a general validation environment	24
D10	Integration of abstraction tools with efficient finite-state tools	24
D11	Integration of tools for parametric reasoning about heterogenous systems	24
D12	Experiments on the PGM and SIP protocols (first report)	24
D16	Integration of tools for the analysis of paremeterized systems and dynamic networks	36
D17	Finalized common validation framework	36
D18	Experiments on the PGM and SIP protocols (final report)	36

Milestones and expected results

The main results we expect are (1) a common validation framework where different approaches and powerful techniques (e.g., abstraction, symbolic analysis) are integrated, and (2) the application of this framework to the validation of two industrially relevant and challenging case studies.

Workpackage number:	3	**Start date or starting event**	0				
Participant number:	1	3	4	5	6	7	
Person-months per participant:	7	1	1	4.6	3	0.5	

Objectives

Coordination of the work in the project.

Description of work

The work in the project will be under the overall responsability of a management and coordination board constituted by the lead contractors of the working packages and tasks (participants 1,3,4,5 and 6). This board will address management issues as well as technical issues related to the quality control and assessment of the work. The board will also coordinate dissemination and organizational activities such as the organization of workshops and the edition of special issues of journals. The work will be globally coordinated by participant 1 (project coordinator).

Deliverables		**Delivery month**
D5	Dissemination/assessment/progress report (Year 1)	12
D13	Dissemination/assessment/progress report (Year 2)	24
D19	Final dissemination/assessment/progress report	36

Milestones and expected results

Our aim is to coordinate the efforts and exploit the skills and complementarities of the partners in order to achieve the expected objectives of the project. Moreover, with the help of our industrial partners, we will work on improving the popularity of automatic and formal validation techniques in the industrial world by making these techniques more accessible to industrials, and showing their relevance to industrial problems.

9.5 Deliverable list

Deliverable No	Deliverable title	Delivery date	Nature	Dissemination level
D1	Methods and tools for extended automata	12	R, P	PU
D2	Methods and algorithms for parametric reasoning	12	R	PU
D3	Common model description language	12	R	PU
D4	Integration of abstraction and symbolic analysis tools for extended automata	12	R,P	PU
D5	Dissemination/assessment/progress report (year 1)	12	R	PU
D6	Tools for efficient analysis of extended automata	24	P	PU
D7	Methods and tools for parametric reasoning (part 1)	24	R, P	PU
D8	Methods and algorithms for dynamic networks and mobile processes	24	R	PU
D9	Common interface for a general validation environment	24	P	PU
D10	Integration of abstraction tools with efficient finite-state tools	24	P	PU
D11	Integration of tools for parametric reasoning about heterogenous systems	24	R,P	PU
D12	Experiments on the PGM and SIP protocols (first report)	24	R	PU
D13	Dissemination/assessment/progress report (year 2)	24	R	PU
D14	Methods and tools for parametric reasoning (part 2)	36	R,P	PU
D15	Methods and tools for the analysis of dynamic networks and mobile processes	36	R,P	PU
D16	Integration of tools for the analysis of paremeterized systems and dynamic networks	36	R,P	PU
D17	Finalized common validation framework	36	R,P	PU
D18	Experiments on the PGM and SIP protocols (final report)	36	R	PU
D19	Final dissemination/assessment/progress report	36	R	PU

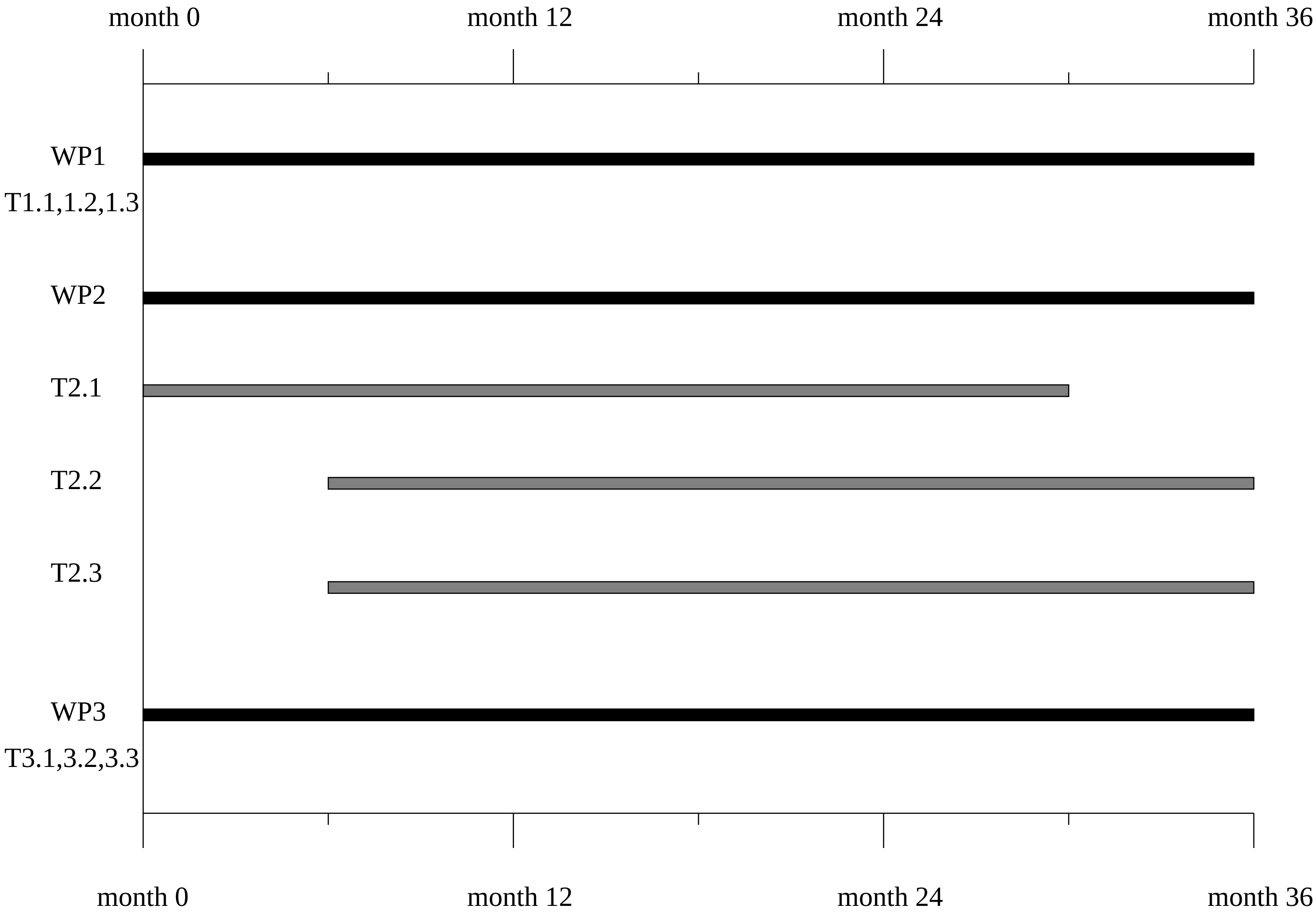
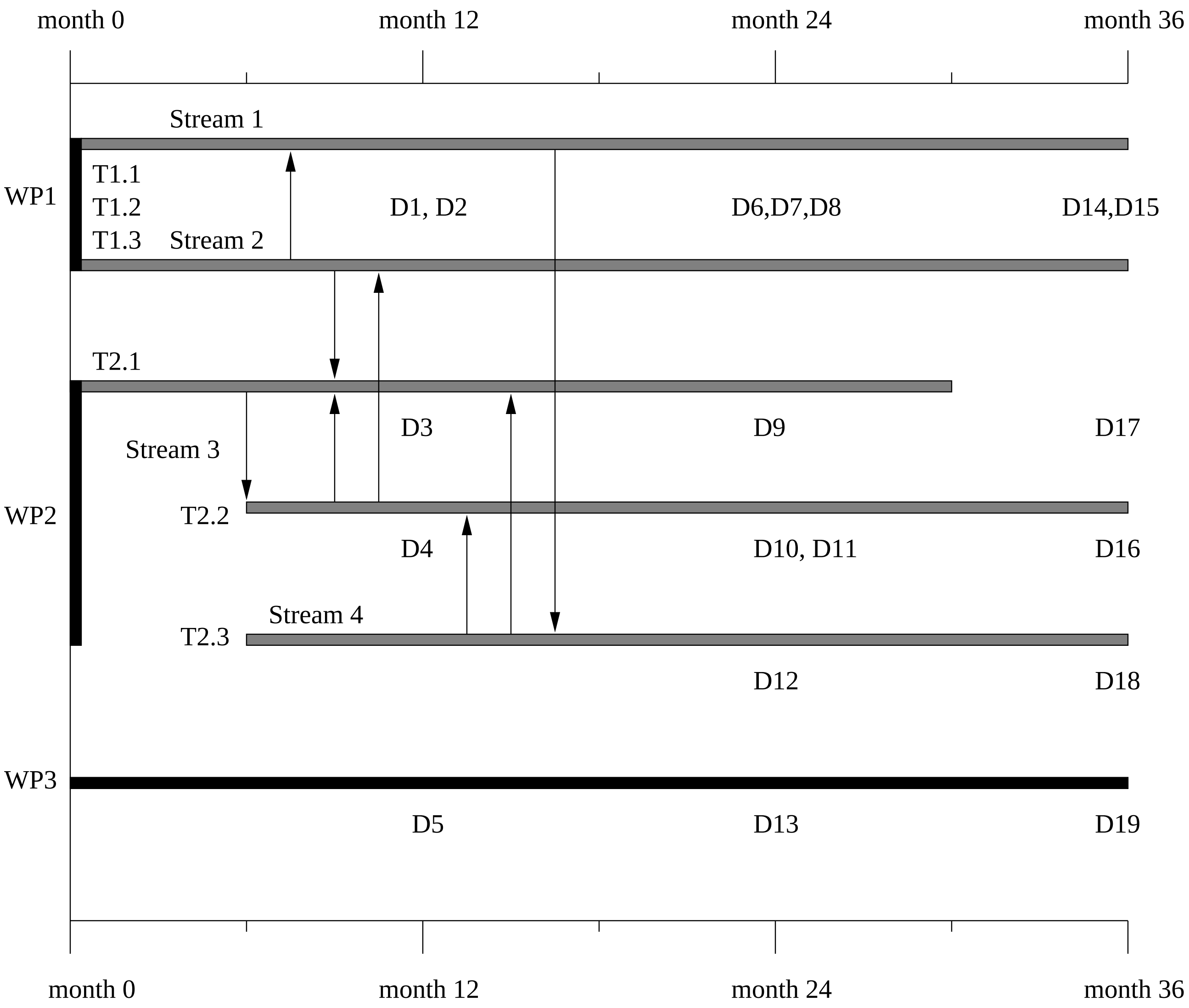


Figure 3: Bar chart



→ indicates the relation "depends on"
The Deliverables D are detailed in the Deliverables List B2.

Figure 4: Pert chart

9.6 Technical realization of the workplan

9.6.1 Background and Skills

The academic partners in the project represent the european and worldwide leadership in the domain of computer-aided verification, and especially in verification of protocols. They have contributed to the emergence and development of this research area since the last two decades and their are among the most active research groups in the area. They have made major contributions to the following topics: Specification and verification methodology for reactive and distributed systems [48, 49, 42, 43], model-checking algorithms [52, 40, 55, 14], efficient state-space exploration algorithms [32, 33, 26, 28], analysis techniques based on abstraction [11, 41, 12, 39], algorithmic approach (based on symbolic reachability analysis) for the verification of infinite-state systems [37, 18, 29, 9, 5, 7, 16, 20, 19, 17, 21, 38, 2, 8, 1, 3, 22, 27], development of widely used specification languages and verification tools [36, 34, 30, 24, 57, 15, 13, 34].

The industrial partners, the principal contractor (**CNET**) as well as the two observers, are among the most advanced groups in the world concerning the development of telecommunication technologies. Their are principal actors in the development of standards in telecommunication protocols, as well as in their worldwide use.

9.6.2 T1.1: Abstraction

The groups (**UJF**) and (**Weizmann**) are worldwide experts in abstraction methods and their applications. Among their major contributions: (1) Study of the classes of properties that are preserved under several kinds of abstractions [11, 41], (2) Study of the power of the verification approach based on abstractions and its comparison with the deductive approach [39], (3) Development of techniques for generating abstraction relations and their corresponding abstract models [12]. They have also developed advanced prototype tools [13] (**UJF**) and [51] (**Weizmann**) corresponding to the state of the art in the domain.

The two groups (**UJF**) and (**Weizmann**) will collaborate in order to develop new abstraction strategies for different classes of systems, and to furnish abstraction tools extending their existing prototypes.

9.6.3 T1.2: Symbolic analysis

The academic partners of our project are among the leading research groups in algorithmic verification of infinite-state systems, in particular based on symbolic reachability analysis. They have produced major contributions concerning the verification of various types of extended automata: timed automata, counter automata, Petri nets, unbounded FIFO-channel automata, parametrized networks, etc. [37, 18, 29, 5, 7, 16, 20, 19, 17, 21, 38, 2, 8, 1, 3, 22, 27]. They have also developed widely used tools for important classes of such systems [24, 57]. Partners (**UP7**), (**UJF**), and (**Uppsala**) have developed an efficient prototype tool for automatic symbolic verification of unbounded FIFO-channel systems [2, 1]. Partner (**Liège**) is also developing a package for symbolic representation, and a tool for symbolic verification of various kinds of extended automata, especially counter automata and FIFO-channel automata.

The partners of the project, especially those mentioned above, will collaborate in order to develop new symbolic representations and efficient analysis procedures for different classes of systems, especially for extended automata with heterogeneous variables and data structures (counters, clocks, fifo queues), networks of parametrized processes, systems with mobile processes, etc. They will furnish tool packages for such systems.

The industrial contractor (**CNET**) will also participate to the work on symbolic reachability analysis, aiming in particular the adaptation of the used techniques to automatic generation of test sequences (for infinite-state systems). Indeed, it has been discovered recently that verification techniques, especially reachability analysis techniques, can be used for the automatic generation of test sequences (this is a work that has been carried out in particular by **UJF**). However, existing works in this domain concern only finite state systems, i.e., the produced test cases are necessarily completely instantiated. In this project, we will investigate the use of symbolic reachability analysis techniques for the automatic generation of *symbolic test sequences* representing sets of instantiated test cases.

9.6.4 T1.3: Efficient state-space exploration

The groups in our projects have produced key contributions to the research on facing the state explosion problem. In particular, the groups (**Liège**) and (**TUM**) are among the major experts in partial-order verification techniques. Indeed, (**Liège**) is one of the main contributors to the research on the widely adopted partial-order reduction techniques used in tools like SPIN [47, 32, 33, 56]. Group (**TUM**) is one of the main contributors to the research on techniques based on unfoldings [26, 28], and to the development of tools involving these techniques [15]. Group (**Uppsala**) has also produced several important contributions on combining partial-order reduction techniques with infinite-state symbolic reachability analysis in the case of timed automata, Petri nets, and lossy channel systems [6, 10]. Members of the group (**UP7**) have a high expertise in trace theory and asynchronous automata which are very relevant for the conception of verification techniques based on partial orders [31, 25]. They have applied their expertise to define new verification algorithms for systems modeled by MSCs [45, 44, 46].

As for symbolic verification techniques, the group (**Uppsala**) has a strong expertise in SAT decision procedures and their use in verification. Recent works show that techniques based on SAT solvers could be in some cases far more efficient than techniques based on the use of BDD-like symbolic representations.

The four groups (**UP7**), (**Liège**), (**TUM**), and (**Uppsala**) will collaborate in order to define general analysis procedures based on partial-order reductions or unfoldings techniques combined with symbolic representations that are applicable for a wide range of finite or infinite-state systems. These techniques will be integrated in finite and infinite-state reachability analysis tools.

9.6.5 T2.1: Common language and interface

We need a common language for the description of models in order to be able to connect different tools and make them cooperate. A first version of a common language is proposed by (**UJF**) who has also developed a connection of this language to a widely used commercial specification environment for the language SDL. The groups of (**UP7**), (**Uppsala**), and (**UJF**) will collaborate on the extension of this language in order to take into account all the aspects that will be addressed in the project (unbounded data structures, timing constraints, parametrization, mobility, etc). The industrial contractor (**CNET**) will also participate actively to this effort.

The groups of (**UP7**) and (**UJF**) will also work on the extension of the connection between our new common model description language and the commercial environment Object-Geode (Verilog) for SDL.

9.6.6 T2.2: Integration of tools

Tools will developed by all partners and will be connected through a common model description language. A special effort will be made in order to unify the symbolic representation structures and the decision procedures packages used by the abstraction and reachability analysis tools in order to optimize the number of components in the environment.

Integration of tools requires also combining different validation techniques and the design of an environment where the user can compose different methods and procedures in order to tackle the validation problem of a complex system.

A first work on combining and integrating abstraction and symbolic reachability analysis tools was carried out recently by (**UP7**), (**Uppsala**), and (**UJF**) and published in [4]. The results we obtained show the effectiveness of our approach and its superiority compared to the state-of-the-art methods.

Partners (**UP7**), (**Uppsala**), and (**Weizmann**) will collaborate in order to develop integrated tools for parametric reasoning using symbolic analysis techniques. These tools will also be combined with abstraction techniques developed by (**UJF**) and (**Weizmann**).

9.6.7 T2.3: Experimentations and case studies

All partners participate in the case studies. They will work on these cases as sources of problems to solve, and as benchmarks to evaluate their methods and tools. The academic partners have a strong experience in case studies due to their permanent interactions with industrial partners, within the frameworks of several national and international projects. The work on case studies in the present project will be followed and advised by the 3 industrial participants to the project who will also furnish the specifications (contractor (**CNET**) will furnish the specification of the PGM protocol, and observer (**Ericsson-UAB**) will furnish the specification of the SIP protocol).

9.7 Project management and assessment

Each of the workpackages has a package coordinator (lead contractor) who is responsible for progress, quality control, and changes in the work package. Packages WP1 and WP2 are the responsibility of the contractors (**Uppsala**) and (**UJF**) respectively. These two workpackage coordinators will be helped in their work by task coordinators. Contractors (**UJF**), (**Liège**), and (**TUM**) will coordinate respectively Task 1.1, Task 1.2, and Task 1.3. Task 2.1 will be the responsibility of the workpackage coordinator (**UJF**), and the prime contractor (**UP7**) will coordinate the work in Task 2.2. The work in Task 2.3 will be under the responsability of (**UP7**). The prime contractor (**UP7**) has the responsability of the global coordination of the project.

The prime contractor (**UP7**) and the two package coordinators (**Uppsala**) and (**UJF**), as well as the two task coordinators (**Liège**) and (**TUM**), form the project's *management and coordination board*. This board will have overall responsibility of the project and will meet at least twice every year (more if necessary) to address management issues as well as coordination and technical issues, especially issues related to the quality control of the work and its evaluation against the expected objectives of the project. Decisions are taken by majority voting and only if more than half of the consortium members are present. Participants that are non present physically can participate to the vote by email or by phone. In case of conflicts, the decision will be taken by a majority vote (with the same conditions as above), restricted to the members of the management and coordination board. Since there is an odd number of the consortium members, and there is also an odd number of members of the management and coordination board, conflicts should be very rare. In case conflicts remain after the two voting phases defined above, these conflicts will be solved by the prime contractor.

Within the management and coordination board, the management task (T3.1) is under the responsability of (**UP7**), and the assessment task (T3.2) is under the responsability of (**Uppsala**). The contractor (**Uppsala**) will follow the work, evaluate its progress (each 6 months), communicate his evaluation to the management/coordination board, and produce an annual assessment report (part of the deliverable of WP3). Contractor (**CNET**) and the observer (**Ericsson-UAB**) will help as consultants in evaluating the work in this task. The success of our project will be measured according to the following lines:

- Production of theoretical and applied results on methodology and validation techniques. The evaluation criteria used for this work are mainly: the technical level and its scientific value, (selectivity of the conferences and journals), the relevance to the project and the proved and/or potential wide range of applications, and the quality of the dissemination (scientific quality and level of diffusion of the conferences and journals, variety of addressed communities). The contribution of each (academic) participant should be at least one high quality publication per year.

- Construction of validation tools and their integration. We will consider as minimal success criterion the production of a validation environment where validation techniques for *infinite-state extended automata* (e.g. automata with counters, clocks, and fifo-channels) are available. This environment must include a combination of abstraction techniques and symbolic reachability analysis techniques, integrated to a specification environment for SDL (based on the industrial environment Object-Geode of VERILOG). Producing such a validation environment will be a significant improvement of the state of the art. Further steps we intend to reach consists in the extension of this general validation environment in order to be able to deal also with

(1) *parametrized systems* (e.g., networks with unbounded number of components, parametric timed automata, etc), and (2) *dynamic networks* and *mobile processes*. Those are important and highly exploratory (and hence risky) steps. We will consider as a success any progress toward the development of new methods, techniques, and prototype tools for dealing with these kinds of systems.

- Applications and experimentations. We consider as minimal success criterion showing the application of our techniques and tools to nontrivial cases. The main success criterion we consider here is the power of our methods, techniques, and tools from the *qualitative* point of view: showing that our approach allows to tackle in a systematic way classes of systems that are, by nature, beyond the scope of the existing approaches. The second criterion we consider is the power of our techniques from the *quantitative* point of view: showing that our techniques allow to deal with cases of important sizes (e.g., the cases studies PGM and SIP). The main objective of our work on the PGM and SIP is indeed to experiment and to evaluate our techniques and tools according to the criteria above: we will use abtraction techniques in order to decompose and extract from these cases different models allowing to capture the essential aspects in their behaviours, and then we will apply a combination of techniques in order to analyze these models.

Finally, the management and coordination board will also supervise dissemination and knowledge transfer activities (see next section). This task will be under the responsability of (**UP7**). A chapter of the annual report of the project (deliverable of WP3) will be devoted to this activity.

9.8 Dissemination activities

One of our tasks (T3.3) consists in dissemination and knowledge transfer activities. These activities includes:

1. Dissemination of results: The scientific and technical results produced in the project will be published in national and international workshops and conferences. Computer-aided verification, especially the verification of infinite-state systems, is a very challenging and very active research domain. This domain attracts more and more researchers from different communities. The results developed in our project will contribute to the worldwide effort, and in particular to the european effort, of developing strong formal and automatic techniques for the design of reliable complex systems. We expect to be regularly present and to publish our results in workshops, conferences, and symposia such as:
   - The International Conference on Computer Aided Verification *CAV* (USA/Europe),
   - The Annual International Conference on Theory of Concurrency *CONCUR* (Europe/USA),
   - The International Conference on Tools and Algorithms for the Construction and Analysis of Systems *TACAS* (Europe),
   - The International SPIN Workshop on Model Checking of Software (USA),
   - The IEEE International Conference on Logic in Computer Science *LICS* (USA/Europe),
   - The IEEE Real-Time Systems Symposium *RTSS* (USA),
   - The International Static Analysis Symposium *SAS* (Europe/USA),
   - The ACM Symposium on Principles of Programing Languages *POPL* (USA),
   - The EATCS International Colloquium on Automata, Languages, and Programming, *ICALP* (Europe),
   - The International Symposium on Theoretical Aspects in Computer Science *STACS* (Europe),
   - The International Conference on Foundations of Software Technology and Theoretical Computer Science *FST&TCS* (India).
2. Knowledge and technology transfer: Our project involves an industrial contrator (**CNET**) and two industrial observers (**Ericsson-UAB** and **Siemens AG**) who represent important actors in the domain of developing telecommunication protocols. The participation of these industrial partners to our project has two implications: (1) they will help in targetting the project toward industrially relevant problems (e.g., they will furnish case studies, and they will follow and evaluate the work on these studies), and (2) they will participate to the development of new validation techniques and tools, and they will be able to use these tools in their industrial context in order to enhance their design and development methods.
3. Diffusion of tools: We have chosen to develop our environment of validation around the common model description format IF. This format is used by several academic and industrial groups to connect their tools to the industrial spécification and validation environment Object-Géode (VERILOG) for SDL. Our connection to this environment through the format IF guarantees the wide diffusion and use of the tools we will develop.

4. Organization of an international workshop: we intend to organize in the last year of the project an international workshop where the results and the achievements of our project will be presented. Researchers and developers from the academia and from the industry will be invited in order to exchange their opinions, compare their results, and confront these results to industrial needs. The proceedings of this workshop will be published in a special issue of an international scientific journal.

10 Other contractual conditions

10.1 Travels outside EU countries and Conference fees

All members of our consortium are highly productive researchers. They are very present in all major international conferences, workshops, and symposia that are related to the domain of formal methods and automatic validation of systems. Many of these conferences hold outside EU countries, mostly in North America or in Asia (e.g., India, Japan). For instance, in the year 2000, almost all major conferences and workshops in our domain such as CAV (Computer Aided Verification), CONCUR (Concurrency), LICS (Logic in Computer Science), and SAS (Symp. on Static Analysis), hold in the USA. Participating to these conferences and presenting our work in such meetings contributes to the effort of dissemination, and is necessary to maintain our leadership in the domain. For this, we need travel support in order to be able to attend conferences outise EU member states and associated states. We will request prior permission to the Commission for all travels outside the EU states, and for the fees of conferences (inside or outside EU).

10.2 Travel support for industrial observers

Our consortium includes two industrial observers (**Ericsson-UAB** and **Siemens AG**). Their role is to help in targetting the work in the project toward industrial problems and needs, and to evaluate the results obtained during the project. Observer (**Ericsson-UAB**) will furnish a case study (SIP) and will help the contractors in understanding it and in studying the problems related to its modelisation and its analysis. He will also participate to the assessment task by evaluating the applicability to this case study of the techniques and tools developed in the the project. Hence, we need financial support in order to be able to invite the two industrial observers (**Ericsson-UAB**) and (**Siemens AG**) to our working meetings.

10.3 Workshop organization

Also in the framework of dissemination activities, we intend to organize an international workshop (at least one) at the end of the project where academic and industrial specialists will be invited. The aim is to present our achievements and confront our approach with other existing ones and with industrial needs. For that, we need financial support for invited speakers and other additional associated costs.

A Appendix A: Consortium description

A.1 Composition

The consortium is composed of seven principal contractors: six academic research groups, and one industrial research group. In addition, the consortium includes two industrial observers.
The *principal contractors* in the project are :

1. LIAFA laboratory - University of Paris 7 (**UP7**),
   key persons: Ahmed Bouajjani and Peter Habermehl,
2. CNET-France Telecom (**CNET**),
   key person: Yves-Marie Quemener,
3. University of Liège (**Liège**),
   key persons: Pierre Wolper and Bernard Boigelot,
4. Technical University of Munich (**TUM**),
   key person: Javier Esparza,
5. University of Uppsala (**Uppsala**),
   key persons: Bengt Jonsson and Parosh A. Abdulla,
6. VERIMAG laboratory - University Joseph Fourier - Grenoble 1 (**UJF**),
   key persons: Joseph Sifakis and Yassine Lakhnech,
7. Weizmann institute (**Weizmann**),
   key person: Amir Pnueli.

The two *industrial observers* are

1. Ericsson Utvecklings AB (Observer 1), key person: Thomas Arts,
2. Siemens (Observer 2), key person: Klaus Winkelmann.

A.2 Role of the partners

The aim of the academic partners is to develop the new generation of validation tools allowing to tackle aspects that appear in modern protocols (such as complex timing constraints, asynchronous communication through unbounded queues, parametrization, and mobility) that are beyond the scope of the state-of-the-art techniques and tools. Hence, the role of academic partners is to provide innovative validation techniques, to provide tool support for them, and to experiment them on significant case studies. The role of the industrial partners is to (1) help to target the project towards industrial applications by providing nontrivial case studies and showing the relevant problems to tackle, (2) to evaluate the techniques and tools developed in the project, especially with respect to the proposed case studies, and (3) to follow closely the design and the improvement of the new validation techniques and tools in order to use them in their industrial context.

A.3 Experience and Expertise

The academic partners in the project represent the european and worldwide leadership in the domain of computer-aided verification, and especially in verification of protocols. They have contributed to the emergence and development of this research area since the last two decades. Among their major contributions: the concept of reactive systems [35, 50], the introduction of temporal logics as specification formalisms for them [48, 49], and the development of general methods for proving such systems [42, 43], the introduction of model-checking techniques, in particular the automata-theoretic approach [52, 40, 55, 14], the development of efficient exploration algorithms based on partial-order techniques [32, 33, 26, 28], the development of analysis techniques based on abstraction [11, 41, 12, 39], the development of the algorithmic approach (based on symbolic reachability analysis) for the verification of infinite-state systems, including timed systems, hybrid systems, systems with unbounded data structures like counters and queues, Petri nets, and parametrized systems [37, 18, 29, 9, 5, 7, 16, 20, 19, 17, 21, 38, 2, 8, 1, 3, 22, 27], the development of widely used specification languages like Statecharts [36] and specification and verification tools like CADP [30], KRONOS [24, 57], PEP [15], INVEST [13], STATEMATE [34], etc.

The industrial partners, the principal contractor (CNET-France Telecom) as well as the two observers (Ericsson Utvecklings AB and Siemens), are among the most advanced groups in the world concerning the development of telecommunication technologies. Their are principal actors in the development of standards in telecommunication protocols, as well as in their worldwide use.

A.4 Complementarities

All partners in the project share a common solid background in specification and validation of reactive and distributed systems. In addition, each group has specific domains of expertise that will be combined in order to carry out the project.

- The groups of LIAFA, VERIMAG, and Weizmann includes experts in specification languages for telecommunication protocols, and the development of specification environments for reactive systems in general. In particular, VERIMAG has developed a language for the description of extended automata called IF which will be the common language for our tools. A connection between the SDL environment Object-Geode of VERILOG [2] and IF has been developed by VERIMAG. This allows to build our validation framework around a widely used specification environment.

- The groups of VERIMAG and Weizmann are experts in validation techniques based on abstraction. They have also developed advanced prototype tools INVEST (VERIMAG) [13] and TLV (Weizmann) [51] corresponding to the state of the art in the domain.

- The groups of VERIMAG and Uppsala are expert in the verification of real-time systems based on the model of timed automata. They have developed the two best existing tools for such systems: KRONOS and UPPAAL.

- The groups of LIAFA, Liège, TUM, Uppsala, and Weizmann are experts in algorithmic verification techniques, especially verification procedures based on symbolic reachability analysis for infinite-state systems. They are developing novel prototype tools for such systems, e.g., LCS [1], and LASH (Liège Automata-based Symbolic Handler).

[2] VERILOG is one of the two main vendors of SDL specification tools.

- The groups of Liège, TUM, and Uppsala are experts in efficient state-exploration techniques, especially in partial-order techniques. Liège is one of the inventors of the widely adopted partial-order reduction techniques used in tools like SPIN [47, 32, 33, 56], and TUM is involved in the development of the tool PEP based on unfoldings techniques [26, 28, 15]. The group of LIAFA includes experts in the theory of traces and asynchronous automata that are relevant for the design of partial-order reduction techniques. The group of Uppsala is an expert in symbolic validation techniques based on efficient SAT decision procedures (Uppsala is a consultant of *Prover Technology AB*).

- Specialized validation tools will be developed by different partners and integrated to the global environment: VERIMAG and Weizmann will develop tools for automatic generation of abstract models. LIAFA, Liège, TUM, Uppsala, and Weizmann will develop symbolic analysis tools for different classes of (infinite-state) models. LIAFA, TUM, and Uppsala will develop tools for efficient state-space exploration for finite and infinite-state models. CNET will collaborate with the other academic partners in order to adapt the symbolic analysis techniques developed in the project to the automatic generation of symbolic test sequences.

- The industrial groups of CNET-France Telecom, Ericsson Utvecklings AB, and Siemens have strong expertise in the development of telecommunication protocols. CNET will provide an implementation of PGM (Pragmatic General Multicast), and Ericsson Utvecklings AB will furnish the specification of the SIP (Session Initiation Protocol). The three industrial groups will provide their advice on application issues and follow the work on the case studies.

A.5 Existing links and collaborations

The partners of this project maintain very tight collaborations and have several common works carried out within several national and european projects.

- The CNET has a collaboration with VERIMAG in the framework of national research programs on Telecommunications (e.g., the RNRT project PROUST).

- Three persons of the team of LIAFA involved in the project (Ahmed Bouajjani, Peter Habermehl, and Mihaela Sighireanu) are former members of VERIMAG who moved to Paris in 1998 and 1999.

- The teams of Liège, VERIMAG (including the actual members of LIAFA), Uppsala, and Weizmann were partners in several successive ESPRIT projects (SPEC, REACT, VIRES, VHS).

- Javier Esparza from TUM was invited Professor at VERIMAG (Ahmed Bouajjani) for two months in 1996. He will visit LIAFA for one month in March 2000. From 1997 to 1998, TUM had a PROCOPE european collaboration project with VERIMAG.

- Parosh Abdulla from Uppsala was invited Professor at VERIMAG (Ahmed Bouajjani) for three months in 1999. Ahmed Bouajjani will visit Uppsala for two months in 2000.

- Amir Pnueli from Weizmann visits regularly VERIMAG (one or two months per year). In particular, from 1993 to 1996, he held the Grenoble municipal chair at the University of Grenoble.

A.6 LIAFA, University of Paris 7 (participant 1)

The group: LIAFA, headed by Daniel Krob, is one of the descendants of the LITP laboratory, one of the major centers in theoretical computer science in Europe. LIAFA is a young laboratory which has the ambition to become one of the major international centers in algorithmics, their foundations and their applications. The goal of the laboratory is to develop strong theoretical research as well as to study real applications in collaboration with industrial partners, mainly in the domain of Telecommunication. The laboratory collaborates currently with industrial partners like Bouygues Telecom and Nortel Matra Cellular.

LIAFA has among its members worldwide experts in all the fields of theoretical computer science, especially in algorithmics, combinatorics, automata and language theory.

The team which is directly involved in the present project is a part of the group *Modelisation and Verification* of LIAFA, headed by Paul Gastin. Among the members of this team, there are three former members of VERIMAG who moved recently to LIAFA: Ahmed Bouajjani, Peter Habermehl, and Mihaela Sighireanu (who was at INRIA before moving to LIAFA). Their domains of expertise are: algorithmic verification for infinite-state systems, real-time systems, specification languages, and protocol validation. They have published numerous papers in journals and international conferences like CAV, CONCUR, ICALP, POPL, LICS, STACS, RTSS, and FORTE/PSTV. They have also produced or participated in the development of several tools, e.g.: (1) Ahmed Bouajjani and his student Aurore Annichini have developed the tool LCS at VERIMAG, in collaboration with Parosh Abdulla from Uppsala [1]. This tool allows the automatic analysis of systems communicating through unbounded lossy channels, (2) Bouajjani and Habermehl, in collaboration with Uppsala and VERIMAG, participated in the conception and the implementation of the extension of INVEST[3] with automata-based decision procedures, and to the interconnection of INVEST with LCS [4], (3) Mihaela Sighireanu has participated in the development of the verification tool CADP at VERIMAG and INRIA [30]. Mihaela Sighireanu has a strong experience with case studies in protocol specification and validation [54, 53].

The team of LIAFA includes also Paul Gastin and Anca Muscholl who are among the best experts in the theory of traces and the theory of asynchronous automata, which are particularly relevant to the design of partial-order verification techniques [45, 31, 25, 44, 46].

The team of LIAFA participates currently to european cooperation research projects (two Franco-German projects in the PROCOPE programme), and to a national project of the CNRS in the framework of the *Telecommunication Program*, in collaboration with VERIMAG.

A.6.1 CVs of key persons

Ahmed Bouajjani: Ahmed Bouajjani received his Ph.D. in Computer Science from the University of Grenoble in 1989. He also received his Habilitation from the same institution in 1999 for work on the verification of infinite-state systems (the dissertation was entitled "Verification beyond the finite-state framework").

From October 1990 to August 1999, he was "Maître de Conférences" (assistant professor) for Computer Science at the University of Grenoble, and member of the laboratory VERIMAG. Since September 1999, he is Professor at the University of Paris 7, and member of the laboratory LIAFA.

[3] INVEST is a tool developed at VERIMAG for automatic generation of abstractions and for invariant analysis.

His research interests are focused on the specification and the verification of infinite-state systems, real-time systems, automata and logics. He has over 30 publications in international journals and conferences.

He participated in the ESPRIT projects SPEC, REACT, CONCUR2, VIRES, and VHS. He was the co-responsable of a PROCOPE project for research cooperation with TUM (team of Javier Esparza).

Peter Habermehl: Peter Habermehl received his Ph.D. from the University of Grenoble in January 1998. His dissertation was entitled "On the verification of infinite-state systems". He prepared his thesis at VERIMAG where he participated in several projects, in particular he was envolved in the Franco-German PROCOPE cooperation project between VERIMAG and TUM. In 1998, he was a post-doc researcher at SRI (Menlo Park, California, USA). He was also a visiting researcher at NASA (Langley, Virginia, USA) for one month in August 1999. Since September 1998, he is "Maître de conférences" (assistant professor) at the University of Paris 7, and member of the laboratory LIAFA. His research interests are focused on algorithmic verification techniques for infinite-state systems and their combination with abstraction methods.

A.7 CNET-France Telecom (participant 2)

A.7.1 The group

CNET is the Research and Development Centre of FRANCE TELECOM. It employs currently 4200 people including 3400 engineers, scientists, and technicians, as well as 150 scientists or doctoral candidates from other organizations. The annual budget of CNET amounts to 3 billion francs. The activities of CNET are distributed among 10 R&D Departments focused on FRANCE TELECOM's major strategic targets and critical technical areas. The tremendous impact of telecommunications on economic development has intensified the efforts of the European Community to promote R&D in this sector. CNET is thus working with numerous partners including universities and manufacturers from all over Europe on more than 100 cooperation research projects which are partly supported by ACTS, ESPRIT and TELEMATICS programs.

In the present project, CNET will be represented by the *Department of Software Techniques*. More precisely, the team involved in the project is dealing with (1) the improvement of formal languages for protocol specification, e.g., SDL, and (2) the development of techniques and tools for protocol validation, including techniques for automatic generation of test sequences.

A.7.2 CVs of key persons

Yves-Marie Quemener: Yves-Marie Quemener is an engineer of the *Ecole Nationale Supérieure des Télécommunications de Bretagne* since 1992. He has got a Ph.D. of the University of Rennes in 1996. He prepared his thesis in the research team of Claude Jard, which is one of the strongest teams in the validation of protocols and protocol engineering. The subject of his thesis was the validation of protocols with infinite reachability sets, modeled by automata communicating through unbounded FIFO queues. He introduced a novel approach for the analysis of such systems based on the representation of the reachability graph of a protocol by means of a graph grammar. Since 1997, he works at CNET. His current research is focused on the automatic generation of test sequences.

A.8 University of Liège (participant 3)

A.8.1 The group

The team of the University of Liège has a substantial experience in the area of the proposal and has produced several key developments, for instance the automata-theoretic approach to model-checking, the concept of data-independence, reduction methods based on the use of partial-order methods, state-space compaction schemes, the use of meta-transitions for symbolically exploring infinite state spaces, and the use of finite-state representations for sets of queue contents or sets of integer values. Many of the results mentioned above were obtained in the context of the ESPRIT-BRA projects SPEC (3096), REACT-P (6021) and VIRES (23498) and have been adopted in verification tools that are in widespread use, for instance SPIN.

A.8.2 CVs of key persons

Pierre Wolper: Pierre Wolper obtained an electrical engineering degree from the University of Liège in 1978. In 1982, he obtained a Ph.D. in computer science from Stanford University (California, USA).

From 1982 to 1986, he was a member of the technical staff of Bell Laboratories (Murray Hill, New Jersey, USA) where he was pursuing research on program specification and verification, distributed computing, modal logic and foremost the applications of temporal logic to computer science.

In 1986 he was appointed to the faculty of the University of Liège and promoted to full professor in 1989. He has participated in the ESPRIT projects TEMPORA (2469) and SPEC (3096), was the coordinator of REACT-P (6021) and is sharing the coordination of VIRES (23498).

Bernard Boigelot: Bernard Boigelot obtained an electrical engineering degree from the University of Liège in 1993, and a Ph.D. in computer science from the same institution in 1998.

Since 1993, he has been working at the University of Liège as a research assistant ("aspirant") and then as a post-doctoral researcher ("chargé de recherches") for the National Fund for Scientific Research (Belgium).

His research interests are mainly focused on the verification of infinite-state systems. He has participated in the ESPRIT projects REACT-P (6021) and VIRES (23498).

A.9 Technische Universität of München (participant 4)

A.9.1 The group

The Faculty of Computer Science of the Technical University of Munich was founded in 1975, and is one of the largest in Germany. It is divided into 15 "'Lehrstühle", which cover nearly all areas of Computer Science. Lehrstuhl VII for Theoretical Computer Science and Foundations of AI, directed by Wilfried Brauer, conducts research in concurrency theory and artificial intelligence. The concurrency group is composed of 8 members (2 Professors, Wilfried Brauer and Javier Esparza, 1 post-doc and 5 Ph.D. students), working on the development of automatic and semi-automatic techniques for the verification of distributed systems. The group has published numerous papers in journals and conferences like CAV, CONCUR, ICALP, LICS, and STACS on automatic verification of finite and infinite state systems. It participated in the ESPRIT project DEMON, the ESPRIT Working Group Caliban, and is involved in German research projects (Sonderforschungsbereich "Tools and methods for parallel computer architectures") and bilateral research projects (PROCOPE-projects with VERIMAG and INRIA). The group has produced the verification component of the PEP tool, one of the leader tools for program development using partial-order techniques, and Model Checking Kit, a platform allowing to combine different model-checking techniques.

A.9.2 CVs of key persons

Javier Esparza: Javier Esparza graduated in Physics at the University of Zaragoza, from which he also received his Ph.D. in Computer Science in 1990 for work on structure theory of Petri nets. He received his Habilitation from the University of Hildesheim in 1994 for work on fast verification techniques for concurrent systems. He has been a Research Assistant at the University of Hildesheim and a Research Fellow at the Laboratory for Foundations of Computer Science of the University of Edinburgh. Since 1994 he is an Associate Professor for Theoretical Computer Science at the Technical University of Munich. He has co-authored a book on Petri net theory and has over 60 publications in international journals and conferences. He has served on the programme committee of conferences like CAV, CONCUR, LICS, and STACS.

A.10 University of Uppsala (participant 5)

A.10.1 The group

The Department of Computer Systems (DoCS) of the university of Uppsala was founded in 1982, and has currently more than 60 employees, including 5 full and associate professors, and more than 20 Ph.D. students. The theoretical computer science group has during these years been active in research on formal methods, especially program specification and verification. In recent years, the main emphasis has been on extending the applicability of model checking into the context of infinite-state systems. The group has developed verification algorithms for several classes of infinite-state systems, such as communicating finite-state automata, parametrized systems, Petri nets, real-time systems, etc. Furthermore, they have designed a general theory of infinite-state systems which has been used both to provide uniform explanations of seemingly unrelated results, and more importantly to discover algorithms for new classes of systems. Recently, the group has been implementing a tool for efficient verification of finite-state systems, using SAT based decision procedures as an alternative to Binary Decision Diagrams. Several of the above mentioned results have been obtained in collaboration with the other partners in the project, especially within the frameworks of ESPRIT-BRA projects SPEC and REACT. They are currently participating in several research projects involving cooperation with Swedish companies such as Ericsson, Telia, VOLVO, Prover Technology, etc.

A.10.2 CVs of key persons

Bengt Jonsson: Bengt Jonsson obtained a BA in Mathematics from Stockholm University in 1979, and an MSc in Computer Science from Stanford University in 1985. In 1987 he obtained a PhD in Computer Science from Uppsala University. Since 1992, he is a full professor at the Department of Computer Systems in Uppsala. His research interests include synthesis and development of distributed systems by refinement, semantics of distributed systems, algorithmic verification methods, probabilistic systems, performance of computer systems, real-time systems, and hybrid systems, and the introduction of systematic formal methods into software development in industrial environments. He has over 40 publications in international journals and high-quality refereed symposia, and has served as chairman or program committees member of several conferences such as CAV, CONCUR, FTRTFT, PoDC, and PSTV.

He has participated in the ESPRIT-BRA projects SPEC and REACT.

Parosh Aziz Abdulla: Parosh Abdulla obtained a BSc in electrical engineering from the university of Sulaimaniyah, Iraq, in 1982. He obtained a Ph.D. in Computer Science from Uppsala University in 1990. In 1992 he was appointed as an associate professor at the department of computer systems in Uppsala. In 1997 he received the degree of *"Docent"* in computer science. Since 1997, he has been working on a part-time basis at *Prover Technology AB* in Stockholm. His main research interests include algorithmic verification of infinite-state systems, parametrized systems, and real-time systems. Recently, he has been working in cooperation with Prover Technology, on developing new techniques for efficient verification of finite-state systems.

He has participated in the ESPRIT-BRA projects SPEC and REACT.

A.11 VERIMAG, University of Grenoble 1 (participant 6)

A.11.1 The group

VERIMAG, headed by J. Sifakis, is an academic laboratory focusing on the theoretical and practical aspects of formal methods for software engineering. VERIMAG has a proven record in both basic theoretical research and in development of tools such as the model-checking tool box CADP, the data-flow synchronous language LUSTRE, the KRONOS tool for verification of timed automata and the INVEST tool for the verification of infinite state systems. VERIMAG has an ongoing interaction with industry including VERILOG, CNET, Schneider, and Aerospatiale and with academic partners such as Weizmann, Berkeley, SRI, Uppsala, and Kiel.

A.11.2 CVs of key persons

Joseph Sifakis: Joseph Sifakis is Directeur de Recherche CNRS and director of the VERIMAG laboratory.

He received his "Thèse d'Etat" in Computer Science in 1979 from the University of Grenoble. Since 1976 he works in the area of specification and verification of concurrent systems. He studied and designed specification languages, such as temporal logics, process algebras and the associated verification methods, especially by model checking. His current research interests include the semantics and the analysis of timed systems as well as the semantics and validation of SDL specifications.

Yassine Lakhnech: Yassine Lakhnech received his Ph.D. in Computer Science in 1996 from the University of Kiel on a dissertation titled "Specification and Verification of Hybrid and Real-Time Systems". He received his Habilitation in Computer Science and Applied Mathematics in 1998 from the University Joseph Fourier, Grenoble. From 1990-1995 he was employed at the University of Kiel. In 1995 he was a visiting researcher at the VERIMAG laboratory in Grenoble. From 1996 -1999 he was a researcher "Wissenschaftlicher Assistent", at the university of Kiel, Germany. From October 1999 he is Professor at the University Joseph Fourier in Grenoble and member of the laboratory VERIMAG. He served as the substitute of Prof. de Roever in coordinating Task 3 of the BRA EU project REACT and is coordinating together with Pierre Wolper the Workpackage Methodology and Tools of the LTR project no 23498 "VIRES". His main interests concern the semantics, specification and verification of reactive and, in particular, infinite-state reactive systems.

A.12 Weizmann Institute (participant 7)

A.12.1 The group

The Weizmann Institute is a research Institute based in Rehovot, Israel. It was founded in 1935, and includes today about 500 researchers and auxiliary scientific staff. The department of Applied Mathematics was formed in 1947 and among other 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 main researchers in this last area are Professors Amir Pnueli and David Harel who have been engaged in the last 19 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 group headed by A. Pnueli has been active over the years in development of methodologies and, more recently, tools for the combination of abstraction-based, deductive, and algorithmic approaches to the verification of reactive systems. The tools developed by the group include the TLV system which allowed the detection of bugs in the Futurebus+ system which were overlooked by a previous analysis that used model-checking methods alone.

A.12.2 CVs of key persons

Amir Pnueli: Amir Pnueli graduated in Applied Mathematics at Technion, Haifa, in 1962. He received his Ph.D. in Applied Mathematics from the Weizmann Institute in 1967.

Amir Pnueli is a professor of Computer Science at the Weizmann Institute of Science in Israel. From 1973-1980 he was a professor of Computer Science in Tel-Aviv University, where he founded and headed the department of Computer Science. Before and after this period he was a professor at the Weizmann Institute, frequently visiting Stanford University. In the period 1993-1996 he held the Grenoble municipal chair at the University of Grenoble 1.

Pnueli is mainly known for the introduction of temporal logic into Computer Science; 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 infinite-state systems in general. Together with Zohar Manna, he is the author of a 3-volumes textbook on Temporal Logic and its application to Reactive Systems of which the first two volumes appeared in 1991 and 1995. Pnueli is a recipient of the 1996 Turing Award, the highest distinction in computer science.

He has participated in several ESPRIT projects: DESCARTES, SPEC, REACT, VIRES, VHS, and SACRES.

References

[1] P. Abdulla, A. Annichini, and A. Bouajjani. Symbolic Verification of Lossy Channel Systems: Application to the Bounded Retransmission Protocol. In *TACAS'99*. LNCS 1579, 1999.

[2] P. Abdulla, A. Bouajjani, and B. Jonsson. On-the-fly Analysis of Systems with Unbounded, Lossy Fifo Channels. In *CAV'98*. LNCS 1427, 1998.

[3] P. Abdulla, A. Bouajjani, B. Jonsson, and M. Nilsson. Handling Global Conditions in Parametrized System Verification. In *CAV'99*. LNCS 1633, 1999.

[4] P.A. Abdulla, A. Annichini, S. Bensalem, A. Bouajjani, and Y. Lakhnech P. Habermehl. Verification of Infinite-State Systems by Combining Abstraction and Reachability Analysis. In *11th Intern. Conf. on Computer Aided Verification (CAV'99)*. LNCS 1633, 1999.

[5] P.A. Abdulla and B. Jonsson. Verifying Programs with Unreliable Channels. *Inform. and Comput.*, 127(2):91–101, 1996.

[6] P.A. Abdulla, B. Jonsson, M. Kindahl, and D. Peled. A General Approach to Partial Order Reductions in Symbolic Verification. In *CAV'98*. LNCS 1427, 1998.

[7] Parosh Aziz Abdulla, Karlis Čerāns, Bengt Jonsson, and Tsay Yih-Kuen. General Decidability Theorems for Infinite-State Systems. In *LICS'96*, pages 313–321, 1996.

[8] Parosh Aziz Abdulla and Bengt Jonsson. Verifying Networks of Timed Processes. In *TACAS'98*. LNCS 1384, 1998.

[9] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The Algorithmic Analysis of Hybrid Systems. *TCS*, 138, 1995.

[10] J. Bengtsson, B. Jonsson, J. Lilius, and W. Yi. Partial Order Reductions for Timed Systems. In *CONCUR'98*. LNCS 1466, 1998.

[11] S. Bensalem, A. Bouajjani, C. Loiseaux, and J. Sifakis. Property-preserving simulations. In *CAV'98*. LNCS 663, 1992.

[12] S. Bensalem, Y. Lakhnech, and S. Owre. Computing Abstractions of Infinite State Systems Compositionally and Automatically. In *CAV'98*. LNCS 1427, 1998.

[13] S. Bensalem, Y. Lakhnech, and S. Owre. InVeSt : A Tool for the Verification of Invariants. In *CAV'98*. LNCS 1427, 1998.

[14] O. Bernholtz, M. Vardi, and P. Wolper. An Automata-theoretic Approach to Branching-time Model-checking. In *CAV'94*. LNCS 818, 1994.

[15] E. Best, J. Esparza, B. Grahlmann, S. Melzer, S. Römer, and F. Wallner. The PEP verification system. In *FEmSys'97*. Tool presentation, 1997.

[16] B. Boigelot and P. Godefroid. Symbolic Verification of Communication Protocols with Infinite State Spaces using QDDs. In *CAV'96*. LNCS 1102, 1996.

[17] B. Boigelot, P. Godefroid, B. Willems, and P. Wolper. The power of QDDs. In *SAS'97*. LNCS 1302, 1997.

[18] B. Boigelot and P. Wolper. Symbolic Verification with Periodic Sets. In *CAV'94*. LNCS 818, 1994.

[19] A. Bouajjani, J. Esparza, and O. Maler. Reachability Analysis of Pushdown Automata: Application to Model Checking. In *CONCUR'97*. LNCS 1243, 1997.

[20] A Bouajjani and P. Habermehl. Constrained Properties, Semilinear Systems, and Petri Nets. In *Proc. Intern. Conf. on Concurrency Theory (CONCUR'96)*. LNCS 1119, 1996.

[21] A. Bouajjani and P. Habermehl. Symbolic Reachability Analysis of FIFO-Channel Systems with Nonregular Sets of Configurations. In *ICALP'97*. LNCS 1256, 1997.

[22] A. Bouajjani and R. Mayr. Model Checking Lossy Vector Addition Systems. In *Proc. 16th Intern. Symp. on Theoretical Aspects in Computer Science (STACS'99)*. LNCS 1563, 1999.

[23] M. Bozga, J.Cl. Fernandez, L. Ghirvu, S. Graf, J.P. Krimm, L. Mounier, and J. Sifakis. IF: An intermediate representation for SDL and its applications. In *Proceedings of SDL Forum 99, Montreal*. Elsevier, June 1999.

[24] C.Daws, A.Olivero, S.Tripakis, and S.Yovine. The Tool KRONOS. In *Hybrid Systems III, Verification and Control*. LNCS 1066, 1996.

[25] V. Diekert and P. Gastin. An expressively complete temporal logic without past tense operators for mazurkiewicz traces. In to appear in LNCS, editor, *Proceedings of the Annual Conference of the European Association for Computer Science Logic (CSL'99)*, 1999.

[26] J. Esparza. Model Checking Using Net Unfoldings. *Science of Computer Programming*, 23(2):151–195, 1994.

[27] J. Esparza, A. Finkel, and R. Mayr. On the Verification of Broadcast Protocols. In *LICS'99*. IEEE, 1999.

[28] J. Esparza, S. Römer, and W. Vogler. An Improvement of McMillan's Unfolding Algorithm. In *TACAS'96*. LNCS 1055, 1996.

[29] Javier Esparza. Decidability of Model-checking for Infinite-State Concurrent Systems. *Acta Informatica*, 34:85–107, 1997.

[30] J-C. Fernandez, H. Garavel, A. Kerbrat, R. Mateescu, L. Mounier, and M. Sighireanu. CADP: A Protocol Validation and Verification Toolbox. In *CAV'96*, pages 437–440. LNCS 1102, 1996.

[31] P. Gastin, R. Meyer, and A. Petit. A (non-elementary) modular decision procedure for ltrl. In *Proceedings of the 23rd International Symposium on Mathematical Foundations of Computer Science (MFCS'98)*. LNCS 1450, 1998.

[32] Patrice Godefroid and Pierre Wolper. Using partial orders for the efficient verification of deadlock freedom and safety properties. *Formal Methods in System Design*, 2(2):149–164, April 1993.

[33] Patrice Godefroid and Pierre Wolper. A partial approach to model checking. *Information and Computation*, 110(2):305–326, May 1994.

[34] D. Harel, H. Lachover, A. Naamad, A. Pnueli, M. Politi, R. Sherman, A. Shtull-Trauring, and M. Trakhtenbrot. STATEMATE: A Working Environment for the Development of Complex Reactive Systems. *IEEE Transactions Software Engineering*, 16:403–414, 1990.

[35] D. Harel and A. Pnueli. On the Development of Reactive Systems. *Logics and Models of Concurrent Systems*, volume F-13, 1985.

[36] D. Harel, A. Pnueli, J.P. Schmidt, and R. Sherman. On the Formal Semantics of Statecharts. In *2nd IEEE Symposium Logic in Computer Science (LICS'87)*, 1987.

[37] T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic Model-Checking for Real-Time Systems. In *LICS'92*. IEEE, 1992.

[38] Y. Kesten, O. Maler, M. Marcus, A. Pnueli, and E. Shahar. Symbolic model checking with rich assertional languages. In O. Grumberg, editor, *Proc. CAV'97*, volume 1254 of *LNCS*, pages 424–435. Springer, June 1997.

[39] Y. Kesten and A. Pnueli. Modularization and Abstraction: The Keys to Formal Verification. In *MFCS'98*. LNCS 1450, 1998.

[40] O. Lichtenstein, A. Pnueli, and L. Zuck. The Glory of the Past. In *Proc. Conf. on Logics of Programs*. LNCS 193, 1985.

[41] C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property Preserving Abstractions for the Verification of Concurrent Systems. *Formal Methods in System Design*, 6(1), 1995.

[42] Z. Manna and A. Pnueli. *The Temporal Logic of Reactibe and Concurrent Systems.* Springer-Verlag, 1991.

[43] Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety.* Springer-Verlag, 1995.

[44] A. Muscholl. Matching Specifications for Message Sequence Charts. In *FoSSaCs'99.* LNCS 1578, 1999.

[45] A. Muscholl, D. Peled, and Z. Su. Deciding properties for message sequence charts. In *FoSSaCs'98.* LNCS 1378, 1998.

[46] Anca Muscholl and Doron Peled. Message sequence charts and decision problems on Mazurkiewicz traces. In *MFCS'99.* LNCS 1672, 1999.

[47] Shlomit Pinter and Pierre Wolper. A temporal logic for reasoning about partially ordered computations. In *Proc. 3rd ACM Symposium on Principles of Distributed Computing*, pages 28–37, Vancouver, August 1984.

[48] A. Pnueli. The Temporal Logic of Programs. In *FOCS'77.* IEEE, 1977.

[49] A. Pnueli. Applications of Temporal Logic to the Specification and Verification of Reactive Systems: A Survey of Current Trends. In *Current Trends in Concurrency.* LNCS 224, Springer-Verlag, 1986.

[50] A. Pnueli. Specification and Development of Reactive Systems. In *Information Processing 86.* IFIP, North-Holland, 1986.

[51] A. Pnueli and E. Shahar. A Platform for Combining Deductive with Algorithmic Verification. In *CAV'96*. LNCS 1102, 1996.

[52] J-P. Queille and J. Sifakis. Specification and Verification of Concurrent Systems in Cesar. In *Proc. Intern. Symposium on Programming*. LNCS 137, 1982.

[53] M. Sighireanu. Model-Checking Validation of the LOTOS Descriptions of the Invoicing Case Study. In *1st International Workshop on Comparing System Specification Techn iques, Nantes, France*, 1998.

[54] M. Sighireanu and R. Mateescu. Verification of the Link Layer Protocol of the IEEE-1394 Serial Bus ("FireWire"): an Experiment with E-LOTOS. *Springer International Journal on Software Tools for Technology Transfer (STTT)*, to appear, 1998.

[55] M.Y. Vardi and P. Wolper. An Automata-Theoretic Approach to Automatic Program Verification. In *Proc. 2nd Symp. on Logic in Computer Science (LICS'86)*. IEEE, 1986.

[56] Bernard Willems and Pierre Wolper. Partial-order methods for model checking: From linear time to branching time. In *Proc. 11th Symp. on Logic in Computer Science*, pages 294–303, New Brunswick, July 1996.

[57] Sergio Yovine. Kronos: A verification tool for real-time systems. *Springer International Journal of Software Tools for Technology Transfer*, 1(1/2), October 1997.