INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team MOSEL

Proof-oriented development of computer-based systems

Lorraine

THEME SYM

Activity Report

2004

Table of contents

1. Team **1**
2. Overall Objectives **1**
3. Scientific Foundations **2**
3.1. Foundations and Methodology 2
3.2. Notation and tools 3
3.3. Applications 3
4. Application Domains **4**
5. Software **4**
5.1. Click'n'Prove 4
5.2. DIXIT 4
6. New Results **5**
6.1. Proof-oriented fault-tolerant systems engineering 5
6.2. Specification of mobile systems 5
6.3. Model checking using alternating automata 5
6.4. Formally Verifying Information Flow Type Systems for Concurrent and Thread Systems 5
6.5. Formalisation of omega-automata 6
6.6. Patterns of translation from B to UML 6
6.7. Development of greedy algorithms 6
6.8. METAPOST: graphical representation tools and 3D-prototyping 6
6.9. History of computer science 7
7. Contracts and Grants with Industry **7**
7.1. RNRT Equast 7
7.2. PUSSEE project 8
7.3. Microsoft Research 8
8. Other Grants and Activities **8**
8.1. Regional cooperation: operation DIXIT' 8
8.2. National cooperation 9
8.2.1. Project CORSS 9
8.2.2. Project DESIRS 9
8.3. European cooperation 9
8.4. International cooperations 9
8.4.1. Projects NSF CNRS 9
8.4.2. Mediterannean, North Africa, and Middle East 10
9. Dissemination **10**
9.1. Program committees and conference organisation 10
9.2. Tutorials, invited talks, panels 10
9.3. Theses, habilitations, academic duties 11
9.4. Teaching 11
10. Bibliography **12**

1. Team

MOSEL is a project of INRIA Lorraine (since February 2004) and LORIA (UMR 7503). It is affiliated with the Université Henri Poincaré Nancy 1, the Université Nancy 2, the Institut national polytechnique de Lorraine, the CNRS, and INRIA Lorraine. One member of MOSEL belongs to the faculty of the University of Metz.

Team Leader

Dominique Méry [Professor, University Henri Poincaré Nancy 1]

Administrative Assistant

Josiane Reffort [Administrative Assistant, University Henri Poincaré Nancy 1]

INRIA Staff

Stephan Merz [Research Director, INRIA]

University Staff

Dominique Cansell [Assistant Professor, University of Metz]
Jacques Jaray [Professor, Institut National Polytechnique de Lorraine et École des Mines de Nancy]
Leonor Prensa Nieto [Assistant Professor, Institut National Polytechnique de Lorraine et École Nationale Supérieure d'Electricité et de Mécanique]
Denis Roegel [Assistant Professor, University Nancy 2]

Post-doctoral Fellow

Pascal Fontaine [INRIA, since October 1st, 2004]

Junior technical staff

Loïc Fejoz [Ministry of Education and Research, ACI Sécurité Informatique]

Ph.D. Students

Marie-Armelle Mesrine [project ST Microelectronics, since February 2004]
Houda Fekih [joint supervision, University of Tunis]
Eun Young Kang [UHP Nancy 1, since October 1st, 2004]
Olfa Mosbahi [joint supervision, University of Tunis]
Cyril Proch [UHP Nancy 1]
Yann Zimmermann [UHP Nancy 1]
Júlia Zappe [region/industry co-funding, until Sep. 30, 2004]

Master Students

Guillaume N'Doli Assielou [DEA Informatique]

Student Interns

Emilie Balland [IUP GMI – UHP Nancy 1, April 1–August 31]
Rishi Bhardwaj [I.I.T. Guwahati, India, May 1–July 31]
Abhinav Bhatele [I.I.T. Kanpur, India, May 1–July 31]
Sébastien Chazallet [ESIAL, until March 2004]
Jean-François Culat [UHP Nancy 1]
Cédric Picard [ESIAL, until March 2004]
Nicolas Richeton [ESIAL, until March 2004]
Fabrice Vergnaud [ESIAL, until March 2004]

2. Overall Objectives

Proof-oriented system development complements standard methods for the design of computerized systems by formal descriptions and analysis techniques that help to ensure higher levels of reliability and correctness. The MOSEL research team develops such concepts, and applies them, focussing on reactive, real-time, distributed, and mobile systems and that may contain both hardware and software components. Key concepts in the approach advocated by our group are *refinement* and *(de-)composition* that support the development of complex systems across several layers of abstraction. Our work is structured along the following lines of research:

Foundations and methodology. The theoretical underpinnings of formal methods have been firmly established since several decades, and we refrain from developing completely new approaches. However, novel concepts of system design or novel application domains, including the security of computerized systems, mobile systems or hardware/software codesign require extensions and adaptations of existing formalisms (B and TLA$^+$ are the two main frameworks used by our group). Moreover, formal methods need to be integrated in standard industrial development cycles, requiring serious attention to the methodology of their application. For example, specifications and proofs represent proper artefacts of system design, and we are engaged in work on their representation, management, and reuse, based on composition and genericity.

Notation and tools. We are developing specific notation to aid system engineers represent their concepts and to integrate different methods and tools of system design. Where necessary, we also engage in developing support tools or—preferably—in interfacing existing tools to facilitate their use or support their application in novel contexts.

Applications. Industrial and academic case studies serve to validate our concepts and theories and lay the foundation for their transfer to use by practitioners in industry. They also force us to recognize deficiencies of our concepts, stimulating further theoretical advances and tool development. We are therefore maintaining active cooperations with partners in industry and academia, including neighboring disciplines such as circuit design. We also use our methods in the courses we teach to evaluate their applicability.

The cooperation with research groups within France and elsewhere helps us to clarify and promote our ideas. Within LORIA, we are actively participating in the QSL (*Qualité et Sûreté des Logiciels*) theme of research.

3. Scientific Foundations

3.1. Foundations and Methodology

Keywords: *abstraction*, *composition*, *concurrency*, *distributed systems*, *formal methods*, *reactive systems*, *refinement*.

Participants: Dominique Cansell, Jacques Jaray, Dominique Méry, Stephan Merz, Leonor Prensa Nieto, Cyril Proch, Júlia Zappe.

The MOSEL team investigates methods to develop provably correct computer-based systems. The class of systems we are interested in includes reactive, distributed, embedded, and mobile systems. In contrast to classical sequential algorithms that can be characterized in terms of their input-output relation, the correctness of such systems is described in terms of their executions (traces). The choice of an adequate formal language depends on which properties are of interest for a given system. For example, methods based on pre- and postconditions suffice for expressing and proving safety properties, while temporal logics can also express liveness.

We are particularly interested in processes and methodologies that underly system *development*, as opposed to the verification of an existing system a posteriori. This view is formally reflected by the notion of *refinement*, which ensures that descriptions produced in later stages of system design preserve earlier, more abstract descriptions; in particular, all properties proven earlier remain valid for the refined model. In this way, the effort of verification is spread over the entire development process, often allowing for a higher degree of automatisation. Crucially, errors can be detected very early, when they are relatively cheap to correct. The formalisms that we are most familiar with are the B method due to Abrial [24][23] and the Temporal Logic of Actions and the TLA$^+$ language introduced by Lamport [29].

The second cornerstone of system development is composition and decomposition [22]. In effect, monolithic system development methods do not scale to realistic systems. Composition refers to the assembly of complex systems from independently developed, possibly pre-existing components. Dually, an entire system (or its specification) can be decomposed into separate subsystems that are then refined individually. Decomposition is a fundamental structuring principle of the event-based B method.

The contributions of the MOSEL team to the foundations of this area concern extensions of the semantic models for particular types of systems such as real-time, mobile or security-sensitive systems (see sections 6.2 and 8.2). We also study ways to make developments more easily reusable by focusing on generic theories and proofs that can later be instantiated for reuse. Work on the RNRT EQUAST project (see section 7.1) opened a new, interesting avenue by showing that formal models can be applied to improve the conceptual understanding of a technical standard by grouping a set of parameters into hierarchies, explaining results that have traditionally relied on the intuition of experienced engineers.

3.2. Notation and tools

Keywords: *B*, *TLA*, *interface*, *model checking*, *proof obligations*, *theorem proving*, *tool integration*.

Participants: Abhinav Bhatele, Rishi Bhardwaj, Dominique Cansell, Loïc Féjoz, Pascal Fontaine, Dominique Méry, Stephan Merz, Leonor Prensa Nieto.

The development of provably correct systems relies on languages with a precise, mathematically defined semantics, in which system specifications are written and proof obligations are stated. For all but toy systems, formal development methods generate a huge number of proof obligations, and highly automated tools become essential to successfully apply the methods. Whereas automated deduction has made substantial progress, each tool typically covers a restricted domain, and the combination of different tools is an active area of research.

Our team has introduced the format of *predicate diagrams* [26][27] to represent Boolean abstractions of reactive systems in the form of finite-state diagrams, with annotations that express fairness and liveness properties. Predicate diagrams give rise to two different kinds of proof obligations: the correctness of an abstraction with respect to a system specification is reduced to proving non-temporal formulas with the help of automatic or interactive theorem provers. On the other hand, correctness properties are established by finite-state model checking. We are constructing a platform for mechanizing the use of predicate diagrams (see the DIXIT project in section 8.1), and related work concerns the integration of deductive components in a single tool platform.

We believe that beyond the sheer capacity of provers for carrying out deductions, adequate interfaces are an important element in order to promote their actual use in system development. Dominique Cansell has developed a new interface for the interactive prover of Atelier B, the primary support tool for the B method (see section 5.1). Its development relies not only on ergonomic concepts, but also on a thorough understanding of how people use an interactive prover. In cooperation with Microsoft Research, we have also worked on a graphical user interface for TLC, the model checker for TLA$^+$.

3.3. Applications

Keywords: *access control*, *digital TV*, *embedded systems*, *hardware-software codesign*, *security*, *service interaction*, *services*, *telecommunications*.

Participants: Dominique Cansell, Houda Fekih, Jacques Jaray, Dominique Méry, Stephan Merz, Olfa Mosbahi, Leonor Prensa Nieto, Cyril Proch, Yann Zimmermann.

A substantial part of our research is driven by work on concrete applications and case studies, as well as by courses that we teach. Several applications currently studied by MOSEL concern hardware-software codesign for embedded systems (see sections 7.1 and 7.2). Within these industrial projects, we are applying the B method. Starting from standard requirement documents, we have been able to generate synthesizable hardware descriptions from the lowest level of our refinement hierarchies.

In the context of two national projects on computer security (see section 8.2), we apply our methods to the development of services and to access-control applications. Our objective is to adjust notations such as B and TLA$^+$ to new application areas, extending or specializing them where necessary in order to facilitate their use.

4. Application Domains

Keywords: *critical systems*, *embedded systems*, *networks*, *protocols*, *telecommunications*.

Our work mainly targets critical systems whose malfunctioning may endanger the health or life of persons, their privacy and security, or that may lead to serious financial consequences. We highly value working on concrete examples that are developed in the context of industrial or cooperative projects, focusing on telecommunications, embedded systems, networks and their protocols, and mobile systems. Some concrete applications have been mentioned in section 3.3.

5. Software

5.1. Click'n'Prove

Participant: Dominique Cansell.

In cooperation with Jean-Raymond Abrial, a new interface, named Click'n'Prove (or “Balbulette” in french) was developed as the result of the QSL operation AdHoc (2001–2003) for the interactive prover of Atelier B, the principal support tool for the B method. This interface, based on (X)Emacs, has been designed to be ergonomic and to guide the user in carrying out a verification task. Until January 2004, Click'n'Prove worked with Atelier B (a commercial tool set). Since February 2004, ClearSy (ClearSy) provides a new tool set called B4free, which is available free of charge for educational and research purposes. Click'n'Prove is available separately from http://www.loria.fr/~cansell/cnp.html. More than 280 subscribers have downloaded Click'n'Prove with B4free:

- 150 students, 60 researchers, 55 professors, 20 engineers,
- many universities, 24 research centers, 8 industrial companies,
- located in France, England, Germany, Australia, Belgium, United States, Tunisia, Switzerland, Finland, and elsewhere.

The interface and the ideas guiding its development have been presented in several seminars and tutorials in France and abroad (see section 9.2).

5.2. DIXIT

Participants: Loïc Féjoz, Dominique Méry, Stephan Merz.

The DIXIT toolkit provides support for the verification of systems using Boolean abstractions in the form of predicate diagrams. It is organized around a visual editor (based on the GEF platform) that allows a user to draw a predicate diagram and enter node and edge annotations. Properties expressed in linear-time temporal logic can be verified from the interface by calling the Spin or LWAASpin model checkers (see also section 6.3), counter-examples are visualized in the editor, and proof obligations that ensure the correctness of the abstraction can be generated. Finally, the toolkit can verify that a predicate diagram refines a more abstract one, ensuring the preservation of temporal logic properties.

DIXIT has been completely rewritten in 2004 and is available for download from our Web site. A paper describing the tool has been submitted.

6. New Results

6.1. Proof-oriented fault-tolerant systems engineering

Keywords: *B method*, *fault tolerance*, *infotronics*, *refinement*.

Participant: Dominique Méry.

Proving system properties such as fail-safety is a challenge for systems engineering since industrial automation is nowadays embedding intensive on-site and remote infotronics components, focusing on intuitive, easy to use techniques. Since a formal proof of the complete safe-behaviour of the resulting ad-hoc system is not possible, we argue [10] that Proof Oriented Systems Engineering formal techniques should bridge the gap with Fault Tolerant Systems Engineering practical techniques in order to mathematically check the proof of fail-safety. Rationales, experiments and open issues are addressed on combining the formal B event-based method using the B proof assistant with a framework used to model technical safety.

6.2. Specification of mobile systems

Participants: Stephan Merz, Júlia Zappe.

We have proposed MTLA, an extension of Lamport's Temporal Logic of Actions [30] by spatial modalities for the specification and verification of systems based on mobile code, focusing on appropriate notions of refinement and their representation in the logic.

In 2004, we have further investigated the theory of MTLA and have proved the decidability of the satisfiability and model checking problems for the propositional fragment. We have also established a complete axiomatization. On the other hand, MTLA has been applied to describing Mobile UML class diagrams and state machines, leading to verification conditions for refinement expressed at the UML level. This work has been published at AMAST 2004 [8] and has been accepted for publication in Theoretical Computer Science.

6.3. Model checking using alternating automata

Keywords: *Spin*, *alternating automata*, *model checking*, *temporal logic*.

Participant: Stephan Merz.

The automata-theoretic approach to LTL model checking has traditionally been based on a translation of LTL formulae to Büchi automata. Unfortunately, this translation is of exponential complexity, limiting the size of formulae that can effectively be verified in this way, and several heuristics have been developed to avoid the exponential blow-up as far as possible. Alternating automata have recently become popular because they offer a more uniform framework. However, no algorithm was known for checking the emptiness problem of alternating automata. We have designed such an algorithm for linear weak alternating automata whose expressiveness corresponds precisely to LTL, based on an analysis of their configuration graphs using a variant of Tarjan's algorithm. This algorithm has been implemented in joint work with Moritz Hammer at the University of Munich as an alternative back-end for the Spin model checker. Experimental results show that this approach can significantly outperform the state-of-the-art combination of Spin and Ltl2ba for large formulas. In particular, in the common case where the formula does not hold of the model, our implementation often reports the error before Ltl2ba has even constructed the Büchi automaton. Our implementation is available from the University of Munich. It was mentioned in the October issue of Spin NewsLetters and a paper has been accepted for publication at TACAS 2005.

6.4. Formally Verifying Information Flow Type Systems for Concurrent and Thread Systems

Keywords: *Isabelle/HOL*, *confidentiality*, *non-interference*, *theorem proving*, *type systems*.

Participant: Leonor Prensa Nieto.

Type systems representing information flow provide an elegant means to enforce that programs guarantee confidentiality properties. Using the proof assistant Isabelle/HOL, Gilles Barthe and Leonor Prensa Nieto have machine-checked a recent work of Boudol and Castellani [25], which defines an information flow type system for a concurrent language with scheduling, and shows that typable programs are non-interferent. As a benefit of using a proof assistant, we are able to handle a more general language than the one studied by Boudol and Castellani. To our best knowledge, the development constitutes the first machine-checked account of non-interference for a concurrent language.

6.5. Formalisation of omega-automata

Keywords: *Isabelle/HOL*, *omega-automata*, *theorem proving*.

Participants: Guillaume N'Doli Assielou, Stephan Merz, Leonor Prensa Nieto.

The theory of finite automata operating on ω-words is one of the standard pillars of model checking for linear-time temporal logic. In cooperation with Tobias Nipkow from the Technical University of Munich and Javier Esparza from the University of Stuttgart we have started a formalization of the basic concepts and results in the interactive theorem prover Isabelle/HOL. As part of his DEA (master's) thesis, G. Assielou defined simple and generalized Büchi automata and proved various closure and translation results, including the closure of ω-regular languages under Boolean operators.

6.6. Patterns of translation from B to UML

Keywords: *B method*, *UML*, *refinement*.

Participants: Houda Fekih, Stephan Merz.

Formal and semi-formal methods of system development emphasize different aspects of system models: whereas semi-formal methods such as UML emphasize system structure, formal methods offer a precise semantics and enable correctness and performance analysis. Previous work on reconciling the two views of system modeling has concentrated on associating formal semantics with models written in semi-formal languages. Unfortunately, the resulting translations tend to produce unnatural models that are difficult to understand and to verify. We propose to consider formal and semi-formal models as two complementary views of a single underlying system that evolve in parallel. Relationships that exist between formal and semi-formal representations should be maintained across refinements, and revisions in one model should be reflected in the other. As a first step, we have considered the representation of B event systems by UML class diagrams and state machines, identifying typical idioms for the representation of classes, attributes and associations, as well as methods and machine states. Part of the work has been presented at AFADL 2004 [6], and it has been validated on several examples with the help of a prototype written in Prolog.

6.7. Development of greedy algorithms

Keywords: *B method*, *greedy algorithms*, *refinement*.

Participants: Emilie Balland, Dominique Méry.

The greedy method provides a way to construct algorithms solving optimisation problems. It is based on the computation of a global optimum from a set of minimal ones and the main question is to prove that the resulting solution is effectively a global optimal solution. The event-based B method has been used to model the mathematical landscape, to construct a generic framework for such algorithms in a step-by-step proof-based way, and to instantiate this framework for several examples.

6.8. METAPOST: graphical representation tools and 3D-prototyping

Keywords: *METAPOST*, *graphics*, *layout*.

Participant: Denis Roegel.

Denis Roegel continues to develop extensions to METAPOST addressing various abstract representations of objects. Currently, he is interested in means to simplify the prototyping of 3-dimensional objects by using the METAPOST interface, while making use of state of the art rendering environments such as OpenGL.

6.9. History of computer science

Keywords: *algorithms*, *mechanical calculators*.

Participant: Denis Roegel.

Denis Roegel has done historical research on the origins of the modern keyboard and found that a *key-driven* calculating machine was invented in 1844, whereas standard texts claimed this invention to have been made in 1850 or 1851. The machine found may therefore be the first such machine, and an ancestor to all our modern keyboards. This research fills a gap and helped identify the model of a later machine now at the Smithsonian Institution in Washington. This study has been described in a technical report [20] and submitted to the *IEEE Annals of the History of Computing*.

He also studied a particular aspect of a calendar algorithm devised in the 16th century, and was able to find a gap, with unsuspected consequences. Extensive research in the literature seems to show that this error was never noticed before, and we claim therefore to have found a (slight) error in an algorithm that is more than 400 years old. This study also appears as a technical report [21] and has been submitted to the *Archive for History of Exact Sciences*.

7. Contracts and Grants with Industry

7.1. RNRT Equast

Keywords: *digital video broadcast*, *fault hierarchy*, *modelling*, *quality of service*.

Participants: Dominique Cansell, Jean-François Culat, Dominique Méry, Cyril Proch.

The RNRT Equast project was initiated in november 2002 for a duration of 30 months. Within this project, we cooperate with the following partners: Thalès B&M, TDF and LIEN (Laboratoire d'Instrumentation d'Electronique de Nancy). Its objective is to develop a circuit to analyze the image quality of terrestrial digital TV as specified by a set of 30 parameters defined in the TR 101 290 standard of the ETSI (European Telecommunications Standard Institute). The contribution of MOSEL is to provide an incremental and proved model of the system.

We have modelled the entire set of parameters in an incremental way using the B refinement (seven refinement levels). This work allowed us

- to exhibit a hierarchy among the parameters defined in the standard and thus to justify the parameters determining the quality of service that had been introduced by TDF (initiated during the European projects QUOVADIS and MOSQUITO),
- to validate all parameters with respect to the requirements in discussions with our partners,
- to derive from our model suggestions for global and reconfigurable architectures of the FPGA to be developed by our colleagues from the LIEN, and
- to derive from our model SystemC code, making use of the “sensitivity” mechanism of SystemC modules.

Our results on the EQUAST project have been published at FDL 2004 [4] (all details can be found in the technical reports [15][12][13][14][16]), they have also been presented at the Nancy-Saarbrücken Workshop on Logic, Deduction and Applications (Saarbrücken, November 25-26, 2004).

7.2. PUSSEE project

Participants: Dominique Cansell, Yann Zimmermann.

In the context of the European project PUSSEE we have worked, with the KeesDa company as our partner from industry, on a case study posed by Volvo (SAE J1708). The case study concerns a communication protocol that allows different components of a car to send and receive messages over a shared bus. The study is carried out in Event-B, an extension of the B method. The system is implemented and decomposed using step-wise refinement. We present how to derive with this method a cycle-accurate hardware model. The model of the communication link system is composed of an arbitrary (but finite) number of identical components that run concurrently. The model contains synchronization of these components required to control access to the communication link. At the end of the refinement we obtain an implementable model of the components which is mechanically translated into VHDL. The generated VHDL design is synthesizable, opening a way for synthesizing hardware from a B development.

In order to give this transition a better foundation, we have defined BHDL, a subset of B for circuit modelling at the register transfer level. BHDL is equipped with a formal semantics, as well as an intermediate language used for the translation, and the translation itself has been formally verified.

We have also addressed the problem of designing a synchronous hardware component from a purely functional description of its behaviour. In a case study of a convolution sum, a pipeline implementation was derived from a high-level specification by a recurrence equation by refinement. The resulting circuit turned out to be smaller than one obtained using a state-of-the-art process. This work was presented at FDL 2004 [7].

Finally, we have identified a fragment of the B language that corresponds to the transactional level of SystemC models. This level of abstraction is interesting because systems can be modeled as a whole without representing the details of communications (and protocols), thus allowing for fast simulation before reaching an implementation level. The ultimate goal of this work is to propose a translation from B to SystemC (without use of sensitivity) at this level.

Formal refinement as offered by the B method has been shown to be applicable in practice and to scale up. However, it has been recognised that it is difficult communicate a formal B model with customers. Recently, we (with KeesDa and Nokia) have investigated the use of UML as an interface to rigorous formal B models.

Our results on the PUSSEE project have been published in [1][2][3].

Dominique Cansell has been a consultant with the company KeesDa for this project.

7.3. Microsoft Research

Keywords: *TLA+*, *TLC*, *interface*, *model checking*.

Participants: Rishi Bhardwaj, Abhinav Bhatele, Sébastien Chazallet, Dominique Méry, Stephan Merz, Cédric Picard, Nicolas Richeton, Fabrice Vergnaud.

In the context of an industrial project in cooperation with Leslie Lamport and Yuan Yu from Microsoft Research Silicon Valley, Mountain View, a group of third-year students at ESIAL developed a graphical user interface for TLC, the TLA$^+$ model checker. It was further extended by two Indian student interns. The interface organizes a verification project into several sessions, with possibly different versions of TLA$^+$ models and model checker options, and maintains the results obtained from TLC. The interface is operational and has been tested internally and with some students, but it will require further extensions to be truly useful, in particular concerning the interpretation of counter examples produced by TLC.

8. Other Grants and Activities

8.1. Regional cooperation: operation DIXIT'

Keywords: *abstract interpretation*, *abstraction*, *predicate diagrams*, *refinement*.

Participants: Loïc Fejoz, Dominique Méry, Stephan Merz.

We are involved in the QSL (*Qualité et Sûreté des Logiciels*) theme of the research hub "Intelligence Logicielle" at the LORIA laboratory.

The operation DIXIT' was approved by the QSL council in the spring of 2003. Its objective is research into the representation of Boolean abstractions of distributed and reactive systems as predicate diagrams and the implementation of an integrated tool set for their manipulation. This tool set has been completely reimplemented in 2004 (see also section 5.2) and consists of a graphical editor, a generator of proof obligations, and interfaces to the Spin and LWAASpin model checkers. It is possible to verify properties with respect to a given system abstraction as well as to prove refinement of a higher-level diagram by a lower-level one. Future work will consist in providing a proof engine for the generated proof obligations.

8.2. National cooperation

Our team is participating in two national research projects concerning the security of computer-based systems (ACI Sécurité Informatique) named CORSS and DESIRS.

8.2.1. Project CORSS

Keywords: *composition*, *interaction of services*, *refinement*, *resource allocation*, *system kernels*, *system services*, *verification*.

Participants: Dominique Cansell, Dominique Méry, Stephan Merz, Leonor Prensa Nieto.

The CORSS project (Composition et raffinement de systèmes sûrs) includes participants with a background in system development and those with a focus on formal methods. Its objective is to study and apply methods and techniques for the development of provably correct systems (or system services) whose specification includes security properties. Our partners for this project are the EMN Nantes (Gilles Muller), the IRIT Toulouse (Jean-Paul Bodeveix and Mamoun Filali), the COMPOSE project of INRIA at Bordeaux (Charles Consel) and the ARLES project at INRIA Rocquencourt (Valérie Issarny). We have worked on case studies provided by ARLES and COMPOSE concerning group establishment protocols for mobile ad-hoc networks and a dedicated language for telephony services.

8.2.2. Project DESIRS

Keywords: *B method*, *deontic logic*, *refinement*, *security*.

Participants: Dominique Cansell, Dominique Méry, Stephan Merz, Leonor Prensa Nieto.

The DESIRS project (Développement de systèmes informatiques par raffinement des contraintes sécuritaires) studies logics and mechanisms that permit the description and development of systems that must conform to security policies, standards or regulations. Our partners in this project are the LISI/ENSMA of the University of Poitiers (Yamine Aït-Ameur), the ENST Bretagne (Frédéric Cuppens), the IRIT Toulouse (Philippe Balbiani) and the CRIL Lens (Salem Benferhat). This year we studied how the refinement concepts of the B method can be extended to preserve certain possibility properties, in view of accomodating access control policies described using the OrBAC model [28].

8.3. European cooperation

Keywords: *UML model checking*, *code mobility*, *temporal logic*.

Participants: Stephan Merz, Dominique Méry, Leonor Prensa Nieto, Júlia Zappe.

A joint project with the University of Munich (Fred Kröger) within the framework of CCUFB (Centre de coopération universitaire franco-bavarois) has helped us pursue our work on UML model checking Hugo, on model checking using linear weak alternating automata (see section 6.3), and on spatio-temporal logics for mobile systems (see section 6.2).

8.4. International cooperations

8.4.1. Projects NSF CNRS

Participants: Dominique Cansell, Dominique Méry.

Since 1998, MOSEL is actively cooperating with the team led by Prof. Ganesh Gopalakrishnan at the University of Utah.

A second cooperation that is funded by an agreement between the U.S. National Science Foundation (NSF) and CNRS concerns the team led by Prof. Beverly Sanders at the University of Florida at Gainesville.

8.4.2. Mediterannean, North Africa, and Middle East

Participants: Houda Fekih, Jacques Jaray, Dominique Méry, Stephan Merz, Olfa Mosbahi.

We have had a very fruitful cooperation with the team led by Professor Samir Ben Ahmed at the Institut Supérieur d'Informatique (ISI) in Tunis for several years. Jacques Jaray was invited several times to teach courses at the Master's level. The cooperation has been reinforced by support from CMCU (*Comité Mixte de Coopération Universitaire*). Currently, Houda Fekih and Olfa Mosbahi are enrolled in a joint Ph.D. program between the University of Tunis and the INPL at Nancy.

9. Dissemination

9.1. Program committees and conference organisation

- Dominique Cansell was a member of the program committees of AFADL 2004 and ZB 2005. He organised a theme day on Proving Pointer Programs within the QSL project on February 26, 2004.
- Dominique Méry was a member of the program committees of IFM 2004 and IFM 2005.
- Stephan Merz served on the program committees of IASSE 2004, WOLFASI 2004, and FASE 2005.

9.2. Tutorials, invited talks, panels

- Dominique Cansell gave a talk at the 11th INRIA-Industry meeting. He gave invited talks at the Universities of Besançon and Bordeaux, and several tutorials on the B event method and the Click'n'Prove tool developed with Jean-Raymond Abrial.
- Dominique Cansell and Dominique Méry gave a course on the B method at the summer school Logics of Formal Software Specification Languages in Stara Lesna, Slovakia [5].
- Dominique Méry gave an invited talk at the IT workshop of the Indo-French meeting in December 2004 in Pune, India.
- Stephan Merz gave courses on TLA$^+$ at the summer schools Logics of Formal Software Specification Languages in Stara Lesna, Slovakia, and Formal Methods and Information Technology in Almaty, Kazakhstan [17].
- Stephan Merz gave invited talks at the EU-NSF workshop on Engineering Software-Intensive Systems, at the Universities of Augsburg, Toulouse and ETH Zürich, and at a Dagstuhl workshop on Atomicity.
- Dominique Cansell, Pascal Fontaine, Stephan Merz, and Cyril Proch gave talks at the Nancy-Saarbrücken workshop on Logics, Proofs, and Programs on November 25/26 in Saarbrücken.

9.3. Theses, habilitations, academic duties

- Dominique Cansell is representing the B group of the GDR ALP at Nancy. He is the scientific leader within MOSEL of the EQUAST project (see section 7.1).
- Dominique Cansell is a member of the hiring committee 27 at the University of Metz.
- Jacques Jaray is director of studies at the Ecole des Mines of Nancy.
- Dominique Méry wrote reports on the Ph.D. theses of Stéphane Delmas (Toulouse) and Ammar Aljer (Lille).
- Until December 2004, Dominique Méry was a member of the teaching commission (CEVU), and since December he is a member of the scientific council of the University Henri Poincaré Nancy 1.
- Dominique Méry is the director of the Master's (DEA) program of computer science in Lorraine and is responsible for the new Master program of computer science of the Universities of Nancy.
- Dominique Méry is a member of the scientific council of the LORIA laboratory.
- Until November 2004, Dominique Méry was a member of the hiring committees 27 (computer science) and 63 (electrical engineering) of University Henri Poincaré Nancy 1.
- Dominique Méry is an expert for the French Ministery of Education (DS9).
- Dominique Méry is the scientific leader of the DIXIT' operation (see section 8.1).
- Stephan Merz wrote reports for Ph.D. theses in Lyon, Munich, and Toulouse.
- Stephan Merz is the deputy director of the QSL research theme at LORIA.
- Stephan Merz is a member of the editorial board of the Journal for Applied Non-Classical Logic.
- Since fall 2004, Stephan Merz is a member of the sub-group on initiative actions of the new Conseil d'orientation scientifique et technologique of INRIA.
- Stephan Merz is a member of the IFIP Working Group 2.2 *Formal Description of Programming Concepts*.
- Stephan Merz is an expert for the European project Protocure.

9.4. Teaching

The majority of the members of the MOSEL team are employed on university positions and have significant teaching obligations. We only indicate the graduate courses they have been teaching in 2004.

- Dominique Cansell gave a course on the B method at the master's program at the University of Poitiers.
- Dominique Cansell and Dominique Méry gave a course in the Master's (DEA) program at Nancy on the specification and modelling of computer-based systems.
- Dominique Méry gives courses on the specification of computer-based systems at the Ecole Supérieure d'Electricité of Metz. He also teaches on the quality and safety of programs in DESS courses. With Edufrance, he has instituted the exchange of foreign students at various levels of university education. He is director of international relations at ESIAL Nancy.
- Together with Loïc Colson from the University of Metz, Stephan Merz gave a course on the semantics of programming languages for the Master's (DEA) program at Nancy.

10. Bibliography

Articles in referred journals and book chapters

[1] D. CANSELL, S. HALLERSTEDE, I. OLIVER. *UML-B specification and hardware implementation of a Hamming coder/decoder*, in "UML-B - Specification for Proven Embedded Systems Design", J. MERMET (editor)., chap. 16, Kluwer Academic Publishers, November 2004.

[2] D. CANSELL, S. HALLERSTEDE, Y. ZIMMERMANN. *Construction sûre de systèmes électroniques*, in "Génie Logiciel", n^{o} 69, June 2004, p. 38–44.

[3] Y. ZIMMERMANN, S. HALLERSTEDE, D. CANSELL. *Formal modelling of electronic circuits using Event-B, Case Study: SAE J1708 Serial Communication Link*, in "UML-B - Specification for Proven Embedded Systems Design", J. MERMET (editor)., chap. 13, Kluwer Academic Publishers, November 2004.

Publications in Conferences and Workshops

[4] D. CANSELL, J.-F. CULAT, D. MÉRY, C. PROCH. *Derivation of SystemC code from abstract system models*, in "Forum on Specification and Design Languages (FDL'04), Lille, France", September 2004.

[5] D. CANSELL, D. MÉRY. *Tutorial on the event-based B method: Concepts and Case Studies*, in "Logics of Formal Software Specification Languages (LFSL'2004), The High Tatras, Slovakia", D. BJØRNER, M. HENSON (editors)., June 2004.

[6] H. FEKIH, L. JEMNI, S. MERZ. *Transformation des spécifications B en des diagrammes UML*, in "Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'2004), Besançon, France", J. JULLIAND (editor)., Impression Burs, Université de Franche-Comté, June 2004, p. 131–145.

[7] S. HALLERSTEDE, Y. ZIMMERMANN. *Circuit Design by Refinement in EventB*, in "Forum on Specification and Design Languages (FDL'04), Lille, France", P. BOULET (editor)., September 2004.

[8] A. KNAPP, S. MERZ, M. WIRSING. *Refining Mobile UML State Machines*, in "10th Intl. Conf. Algebraic Methodology and Software Technology (AMAST'2004), Stirling, Scotland, UK", C. RATTRAY, S. MAHARAJ, C. SHANKLAND (editors)., Lecture Notes in Computer Science, vol. 3116, Springer-Verlag, July 2004, p. 274–288.

[9] G. MOREL, D. MÉRY, J.-B. LÉGER, T. LECOMTE. *Proof-Oriented Fault-Tolerant Systems Engineering: Rationales, Experiments and Open Issues*, in "7th IFAC Symposium on Cost Oriented Automation (COA'2004), Gatineau, Que'bec, Canada", June 2004.

[10] D. MÉRY. *Synthèse formelle par raffinement de modèles et de logiciels pour l'automaisation*, in "Journées d'Etude "Automatique et Informatique", Cachan, France", Club des Enseignants et des Chercheurs en Electronique, Electrotechnique et Automatique, Section Automatique, March 2004.

[11] L. PRENSA-NIETO, G. BARTHE. *Formally Verifying Information Flow Type Systems for Concurrent and Thread Systems*, in "2nd ACM Workshop on Formal Methods in Security Engineering: From Specifications to Code (FMSE'04), Washington D.C., U.S.A.", M. BACKES, D. BASIN, M. WAIDNER (editors)., ACM

SIGSAC, ACM, October 2004, p. 13–22.

Internal Reports

[12] LIEN, LORIA, SODIELEC, TDF, THALES B&M. *Conception fonctionnelle et architecturale: Evaluation des ressources et performances (Délivrable SP3)*, Rapport de recherche, LORIA, June 2004.

[13] LIEN, LORIA, SODIELEC, TDF, THALES B&M. *Documentation technique relative au démonstrateur: Performances des fonctions synthétisées (Délivrable SP41)*, Rapport de recherche, LORIA, September 2004.

[14] LIEN, LORIA, SODIELEC, TDF, THALES B&M. *Démonstrateur THALES: AMETHYST II (Délivrable SP41_1)*, Rapport de recherche, LORIA, October 2004.

[15] LIEN, LORIA, SODIELEC, TDF, THALES B&M. *Projet RNRT EQUAST: SP2 Spécification incrémentale du système*, Rapport de recherche, LORIA, October 2004.

[16] LIEN, LORIA, SODIELEC, TDF, THALES B&M. *Spécification technique Démonstrateur SODIELEC (Délivrable SP41_2)*, Rapport de recherche, LORIA, October 2004.

[17] S. MERZ. *TLA+ Case Study: A Resource Allocator*, Rapport de recherche, LORIA, August 2004.

[18] O. MOSBAHI, J. JARAY. *Représentation du temps en B événementiel pour la modélisation des systèmes temps réel*, Rapport de recherche, LORIA, June 2004.

[19] O. MOSBAHI, J. JARAY. *Une démarche formelle de développement de systèmes de contrôle-commande*, Rapport de recherche, LORIA, June 2004.

[20] D. ROEGEL. *The First Key-driven Calculating Machine (1844)*, Rapport de recherche, LORIA, November 2004.

[21] D. ROEGEL. *The missing new moon of A.D. 16399 and other anomalies of the Gregorian calendar*, Rapport de recherche, LORIA, November 2004.

Bibliography in notes

[22] W.-P. DE ROEVER, H. LANGMAACK, A. PNUELI (editors). *Compositionality: The Significant Difference*, Lecture Notes in Computer Science, vol. 1536, Springer-Verlag, 1998.

[23] J.-R. ABRIAL. *Extending B without changing it (for developing distributed systems)*, in "1st Conference on the B method", H. HABRIAS (editor)., IRIN Institut de recherche en informatique de Nantes, 1996, p. 169–190.

[24] J.-R. ABRIAL. *The B-Book: Assigning Programs to Meanings*, Cambridge University Press, 1996.

[25] G. BOUDOL, I. CASTELLANI. *Noninterference for concurrent programs and thread systems*, in "Theoretical Computer Science", Special issue “Merci, Maurice. A mosaic in honour of Maurice Nivat”, vol. 281, n^o 1, 2002, p. 109–130.

[26] D. CANSELL, D. MÉRY, S. MERZ. *Predicate Diagrams for the Verification of Reactive Systems*, in "2nd Intl. Conf. on Integrated Formal Methods (IFM 2000), Dagstuhl, Germany", Lecture Notes in Computer Science, vol. 1945, Springer-Verlag, November 2000, p. 380–397.

[27] D. CANSELL, D. MÉRY, S. MERZ. *Diagram Refinements for the Design of Reactive Systems*, in "Journal of Universal Computer Science", vol. 7, n^o 2, 2001, p. 159–174.

[28] A. A. E. KALAM, R. E. BAIDA, P. BALBIANI, S. BENFERHAT, F. CUPPENS, Y. DESWARTE, A. MIÈGE, C. SAUREL, G. TROUESSIN. *Organization-Based Access Control*, in "4th Intl. Workshop Policies for Dist. Systems and Networks (Policy 2003), Lake Como, Italy", J. MOFFETT, F. GARCIA (editors)., IEEE Press, June 2003.

[29] L. LAMPORT. *Specifying Systems*, Addison-Wesley, Boston, Mass., 2002.

[30] L. LAMPORT. *The Temporal Logic of Actions*, in "ACM Transactions on Programming Languages and Systems", vol. 16, n^o 3, May 1994, p. 872–923.